aws

Guide de l’utilisateur

Amazon Virtual Private Cloud

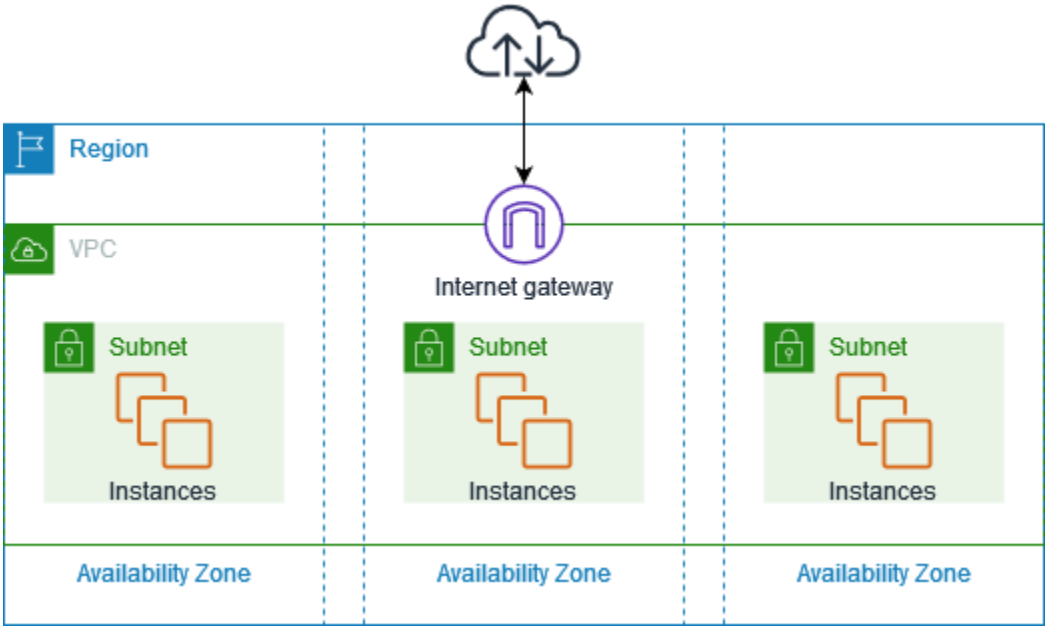
Amazon Virtual Private Cloud: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon VPC ?

Avec Amazon Virtual Private Cloud (Amazon VPC), vous pouvez lancer AWS des ressources dans un réseau virtuel isolé de manière logique que vous avez défini. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre data center, et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Le diagramme suivant illustre un exemple de VPC. Le VPC possède un sous-réseau dans une zone de disponibilité dans la Région, des instances EC2 dans chaque sous-réseau et une passerelle Internet pour autoriser la communication entre les ressources dans votre VPC et sur Internet.



Pour en savoir plus, consultez Amazon Virtual Private Cloud (Amazon VPC).

Fonctionnalités

Les fonctionnalités suivantes vous aident à configurer un VPC afin de fournir la connectivité dont vos applications ont besoin :

Clouds privés virtuels (VPC)

> Un VPC est un réseau virtuel qui ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données. Après avoir créé un VPC, vous pouvez ajouter des sous-réseaux.

Sous-réseaux

Un sous-réseau est une plage d'adresses IP dans votre VPC. Un sous-réseau doit se trouver dans une seule zone de disponibilité. Après avoir ajouté des sous-réseaux, vous pouvez déployer AWS des ressources dans votre VPC.

Adressage IP

Vous pouvez attribuer des adresses IP, tant IPv4 qu'IPv6, à vos VPC et sous-réseaux. Vous pouvez également transférer vos adresses IPv4 publiques et adresses GUA IPv6 vers et les allouer aux ressources de votre VPC, telles que les instances EC2, les passerelles NAT AWS et les équilibreurs de charge réseau.

Routage

Utilisez des tables de routage pour déterminer où le trafic réseau de votre sous-réseau ou de votre passerelle est dirigé.

Passerelles et points de terminaison

Une passerelle connecte votre VPC à un autre réseau. Par exemple, utilisez une passerelle Internet pour connecter votre VPC à internet. Utilisez un point de terminaison VPC pour vous connecter Services AWS en privé, sans passer par une passerelle Internet ou un périphérique NAT.

Connexions d'appairage

Utilisez une connexion d'appairage de VPC pour acheminer le trafic entre les ressources de deux VPC.

Mise en miroir du trafic

Copiez le trafic réseau à partir des interfaces réseau et les envoyer aux appareils de sécurité et de surveillance pour une inspection approfondie des paquets.

Passerelles de transit

Utilisez une passerelle de transit, qui agit comme un hub central, pour acheminer le trafic entre vos VPC, vos connexions VPN et vos AWS Direct Connect connexions.

Journaux de flux VPC

Un journal de flux capture des informations sur le trafic IP circulant vers et depuis les interfaces réseau dans votre VPC.

Connexions VPN

Connectez vos VPC à vos réseaux sur site à l'aide de AWS Virtual Private Network (AWS VPN).

Mise en route avec Amazon VPC

Vous Compte AWS incluez un VPC par défaut dans chacun d'entre eux. Région AWS Vos VPC par défaut sont configurés de telle sorte que vous pouvez directement commencer à lancer des instances EC2 et à vous y connecter. Pour plus d'informations, consultez Mise en route.

Vous pouvez choisir de créer des VPC supplémentaires avec les sous-réseaux, les adresses IP, les passerelles et le routage dont vous avez besoin. Pour plus d'informations, consultez the section called "Création d'un VPC".

Utilisation d'Amazon VPC

Vous pouvez créer et gérer vos VPC à l'aide des interfaces suivantes :

- AWS Management Console — Offre une interface web que vous pouvez utiliser pour accéder à vos VPC.
- AWS Command Line Interface (AWS CLI) — Fournit des commandes pour un large éventail de AWS services, y compris Amazon VPC, et est compatible avec Windows, Mac et Linux. Pour plus d'informations, consultez AWS Command Line Interface.
- AWS SDK — Fournit des API spécifiques au langage et prend en charge de nombreux détails de connexion, tels que le calcul des signatures, la gestion des nouvelles tentatives de demande et la gestion des erreurs. Pour plus d'informations, consultez AWS Kits SDK .
- API de requête : Fournit des actions d'API de bas niveau appelées à l'aide de demandes HTTPS. L'utilisation de l'API de requête est le moyen le plus direct d'accéder à Amazon VPC;, mais elle nécessite que votre application gère les détails de bas niveau, tels que la génération d'un hachage pour signer la demande et le traitement des erreurs. Pour plus d'informations, consultez les actions Amazon VPC dans la Référence API d'Amazon EC2.

Tarification pour Amazon VPC

Il n'y a pas de frais supplémentaires pour l'utilisation d'un VPC. Certains composants VPC, tels que les passerelles NAT, le gestionnaire d'adresses IP, la mise en miroir du trafic, l'analyseur de

reachabilité et l'analyseur d'accès réseau, sont toutefois payants. Pour de plus amples informations, veuillez consulter la Tarification Amazon VPC.

Presque toutes les ressources que vous lancez dans votre cloud privé virtuel (VPC) vous fournissent une adresse IP pour la connectivité. La grande majorité des ressources de votre VPC utilisent des adresses IPv4 privées. Les ressources qui nécessitent un accès direct à Internet via IPv4 utilisent toutefois des adresses IPv4 publiques.

Tarification des adresses IPv4 publiques

Une adresse IPv4 publique est une adresse IPv4 routable depuis Internet. Une adresse IPv4 publique est nécessaire pour qu'une ressource soit directement accessible depuis Internet via IPv4.

Si vous êtes un client existant ou un nouveau client du niveau AWS gratuit, vous bénéficiez de 750 heures d'utilisation gratuite d'adresses IPv4 publiques. Si vous n'utilisez pas le niveau AWS gratuit, les adresses IPv4 publiques sont facturées. Pour obtenir des informations tarifaires spécifiques, veuillez consulter l'onglet Adresse IPv4 publique dans Tarification d'Amazon VPC.

Les adresses IPv4 privées (RFC 1918) ne sont pas facturées. Pour plus d'informations sur le mode de facturation des adresses IPv4 publiques pour les VPC partagés, consultez Facturation et facturation pour le propriétaire et les participants.

Les types d'adresses IPv4 publiques sont les suivants :

- Adresses IP élastiques (EIP) : adresses IPv4 publiques statiques fournies par Amazon que vous pouvez associer à une instance EC2, à une interface réseau élastique ou à une ressource. AWS
- Adresses IPv4 publiques EC2 : adresses IPv4 publiques attribuées à une instance EC2 par Amazon (si l'instance EC2 est lancée dans un sous-réseau par défaut ou si l'instance est lancée dans un sous-réseau configuré pour attribuer automatiquement une adresse IPv4 publique).
- Adresses BYOIPv4 : adresses IPv4 publiques de la plage d'adresses IPv4 que vous avez introduites à l' AWS aide de Bring your own IP addresses (BYOIP).
- Adresses IPv4 gérées par le service : adresses IPv4 publiques automatiquement provisionnées sur les AWS ressources et gérées par un service. AWS Par exemple, les adresses IPv4 publiques sur Amazon ECS, Amazon RDS ou Amazon. WorkSpaces

La liste suivante répertorie les AWS services les plus courants qui peuvent utiliser des adresses IPv4 publiques.

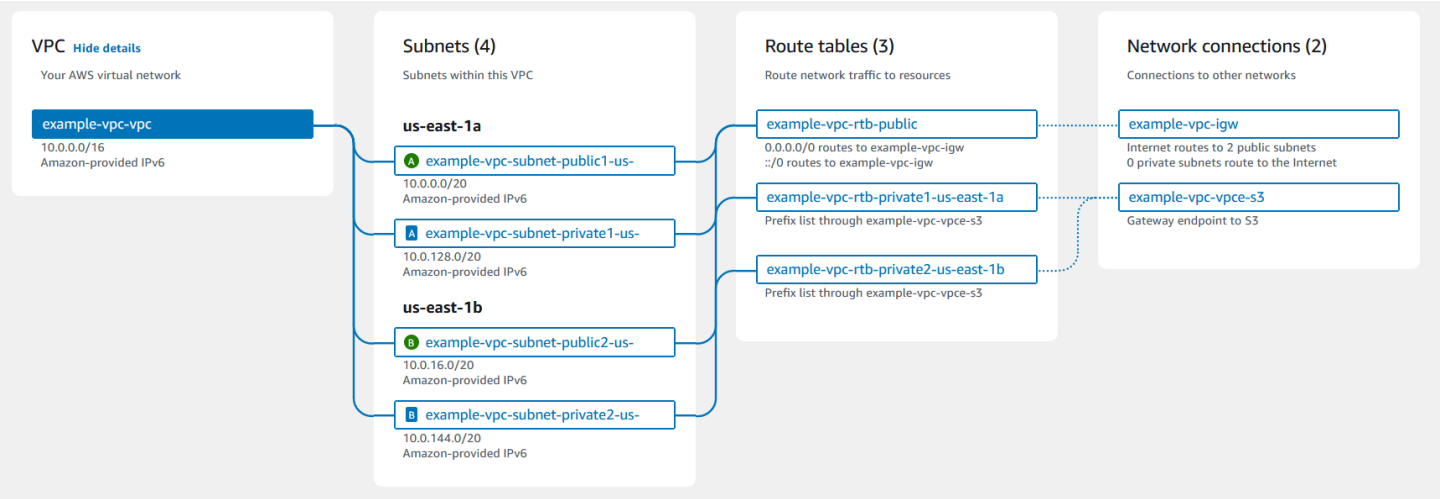
- Amazon AppStream 2.0

- AWS Client VPN
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR
- Amazon GameLift
- AWS Global Accelerator
- AWS Mainframe Modernization
- Amazon Managed Streaming for Apache Kafka
- Amazon MQ
- Amazon RDS
- Amazon Redshift
- AWS Site-to-Site VPN
- Passerelle NAT Amazon VPC
- Amazon WorkSpaces
- Elastic Load Balancing

Fonctionnement d'Amazon VPC

Avec Amazon Virtual Private Cloud (Amazon VPC), vous pouvez lancer AWS des ressources dans un réseau virtuel isolé de manière logique que vous avez défini. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre data center, et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Vous trouverez ci-dessous une représentation visuelle d'un VPC et de ses ressources à partir du volet Aperçu affiché lorsque vous créez un VPC à l'aide de la AWS Management Console. Pour un VPC existant, vous pouvez accéder à cette visualisation dans l'onglet Mappage des ressources. Cet exemple montre les ressources initialement sélectionnées sur la page Créer un VPC lorsque vous choisissez de créer le VPC et d'autres ressources de mise en réseau. Ce VPC est configuré avec un CIDR IPv4 et un CIDR IPv6 fourni par Amazon, des sous-réseaux dans deux zones de disponibilité, trois tables de routage, une passerelle Internet et un point de terminaison de passerelle. Comme nous avons sélectionné la passerelle Internet, la visualisation indique que le trafic provenant des sous-réseaux publics est acheminé vers Internet, car la table de routage correspondante envoie le trafic vers la passerelle Internet.



Concepts

- VPC et sous-réseaux
- VPC par défaut et personnalisés
- Tables de routage
- Accéder à Internet
- Accéder à un réseau d'entreprise ou domestique

- Connecter des VPC et des réseaux
- AWS réseau mondial privé

VPC et sous-réseaux

Un cloud privé virtuel (VPC) est un réseau virtuel dédié à votre compte AWS . Il est logiquement isolé des autres réseaux virtuels du AWS Cloud. Vous pouvez spécifier une plage d'adresses IP pour le VPC, ajouter des sous-réseaux, ajouter des passerelles et associer des groupes de sécurité.

Un sous-réseau est une plage d'adresses IP dans votre VPC. Vous lancez des ressources AWS , telles que des instances Amazon EC2, dans vos sous-réseaux. Vous pouvez connecter un sous-réseau à l'Internet, à d'autres VPC et à vos propres centres de données, et acheminer le trafic vers et depuis vos sous-réseaux à l'aide de tables de routage.

En savoir plus

- Adressage IP
- Clouds privés virtuels
- Sous-réseaux

VPC par défaut et personnalisés

Si votre compte a été créé après le 4 décembre 2013, il dispose d'un VPC par défaut dans chaque région. Un VPC par défaut est configuré et prêt à être utilisé. Par exemple, il possède un sous-réseau par défaut dans chaque zone de disponibilité de la région, une passerelle Internet attachée, un routage dans la table de routage principale qui envoie tout le trafic à la passerelle Internet et des paramètres DNS qui attribuent automatiquement des noms d'hôte DNS publics aux instances avec Adresses IP et activent la résolution DNS via le serveur DNS fourni par Amazon (consultez Attributs DNS dans votre VPC). Par conséquent, une instance EC2 lancée dans un sous-réseau par défaut a automatiquement accès à Internet. Si vous disposez d'un VPC par défaut dans une région, mais que vous n'indiquez pas de sous-réseau lors du lancement d'une instance EC2 dans cette région, nous choisissons l'un des sous-réseaux par défaut et lançons l'instance dans ce celui-ci.

Vous pouvez également créer votre propre VPC et le configurer selon vos besoins. Ce système est appelé VPC personnalisé. Les sous-réseaux que vous créez dans votre VPC personnalisé et les sous-réseaux supplémentaires que vous créez dans votre VPC par défaut sont appelés sous-réseaux personnalisés.

En savoir plus

- the section called "VPC par défaut"
- the section called "Création d'un VPC"

Tables de routage

Une table de routage contient un ensemble de règles, appelées routes, qui permettent de déterminer où diriger le trafic réseau à partir de votre VPC. Vous pouvez associer explicitement un sous-réseau à une table de routage particulière. Sinon, le sous-réseau est implicitement associé à la table de routage principale.

Chaque itinéraire d'une table de routage spécifie la plage d'adresses IP dans laquelle vous souhaitez acheminer le trafic (la destination) et la passerelle, l'interface réseau ou la connexion via laquelle envoyer le trafic (la cible).

En savoir plus

- Configuration des tables de routage

Accéder à Internet

Vous contrôlez comment les instances que vous lancez dans un VPC accèdent à vos ressources à l'extérieur du VPC.

Un VPC par défaut inclut une passerelle Internet et chaque sous-réseau par défaut est un sous-réseau public. Chaque instance que vous lancez dans un sous-réseau par défaut possède une adresse IPv4 privée et une adresse IPv4 publique. Ces instances peuvent communiquer avec Internet via la passerelle Internet. Une passerelle Internet permet à vos instances de se connecter à Internet via la périphérie de réseau Amazon EC2.

Par défaut, chaque instance que vous lancez dans un sous-réseau personnalisé possède une adresse IPv4 privée mais pas d'adresse IPv4 publique, sauf si vous en assignez une de manière spécifique lors du lancement ou si vous modifiez l'attribut de l'adresse IP publique du sous-réseau. Ces instances peuvent communiquer ensemble, mais ne peuvent pas accéder à Internet.

Vous pouvez activer l'accès à Internet pour une instance lancée dans un sous-réseau personnalisé en attachant une passerelle Internet à son VPC (si son VPC n'est pas un VPC par défaut) et en associant une adresse IP Elastic à l'instance.

Pour permettre à une instance dans votre VPC d'initier des connexions sortantes sur Internet mais arrêter des connexions entrantes non sollicitées provenant d'Internet, vous pouvez également utiliser un périphérique NAT (Network Address Translation, traduction d'adresses réseau). NAT mappe plusieurs adresses IPv4 privées en une seule adresse IPv4 publique. Vous pouvez configurer un périphérique NAT avec une adresse IP Elastic et le connecter à Internet via une passerelle Internet. Cela permet à une instance dans un sous-réseau privé de se connecter à Internet via le périphérique NAT qui achemine le trafic de l'instance vers la passerelle Internet, et achemine les réponses vers l'instance.

Si vous associez un bloc CIDR IPv6 à votre VPC et que vous affectez des adresses IPv6 à vos instances, les instances peuvent se connecter à Internet via IPv6 via une passerelle Internet. Sinon, les instances peuvent initier des connexions sortantes à Internet via IPv6 à l'aide d'une passerelle Internet de sortie uniquement. Le trafic IPv6 est séparé du trafic IPv4 ; vos tables de routage doivent inclure les routes distinctes pour le trafic IPv6.

En savoir plus

- Connecter à l'Internet à l'aide d'une passerelle Internet
- Activer le trafic sortant IPv6 à l'aide de passerelles Internet de sortie uniquement
- Connectez-vous à Internet ou à d'autres réseaux à l'aide de périphériques NAT

Accéder à un réseau d'entreprise ou domestique

Vous pouvez éventuellement connecter votre VPC à votre propre centre de données d'entreprise à l'aide d'une AWS Site-to-Site VPN connexion IPSec, faisant du AWS cloud une extension de votre centre de données.

Une connexion VPN de site à site consiste en deux tunnels VPN entre une passerelle privée virtuelle ou une passerelle de transit sur le AWS côté et un dispositif de passerelle client situé dans votre centre de données. Un appareil de passerelle client est un appareil physique ou une appliance logicielle que vous configurez de votre propre côté de la connexion Site-to-Site VPN.

En savoir plus

- AWS Site-to-Site VPN Guide de l'utilisateur
- Passerelles de transit Amazon VPC

Connecter des VPC et des réseaux

Vous pouvez créer une connexion d'appairage de VPC entre deux VPC qui permet de router le trafic entre ces derniers de manière privée. Les instances des deux VPC peuvent communiquer entre elles comme si elles se trouvaient dans le même réseau.

Vous pouvez également créer une passerelle de transit et l'utiliser pour interconnecter vos VPC et réseaux locaux. La passerelle de transit agit comme un routeur virtuel régional pour le trafic circulant entre ses pièces jointes, qui peuvent inclure des VPC, des connexions VPN, des AWS Direct Connect passerelles et des connexions d'appairage de passerelle de transit.

En savoir plus

- Amazon VPC Peering Guide
- Passerelles de transit Amazon VPC

AWS réseau mondial privé

AWS fournit un réseau mondial privé à hautes performances et à faible latence qui fournit un environnement de cloud computing sécurisé pour répondre à vos besoins en matière de réseau. AWS Les régions sont connectées à plusieurs fournisseurs d'accès Internet (FAI), ainsi qu'à un backbone de réseau privé mondial, ce qui améliore les performances réseau pour le trafic inter-régions envoyé par les clients.

Les considérations suivantes s'appliquent :

- Le trafic se trouvant dans une zone de disponibilité, ou entre les zones de disponibilité de toutes les régions, est acheminé via le réseau mondial AWS privé.
- Le trafic entre les régions est toujours acheminé via le réseau mondial AWS privé, à l'exception des régions chinoises.

Une perte de paquets réseau peut être causée par un certain nombre de facteurs, y compris les collisions de flux réseau, les erreurs de niveau inférieur (couche 2) et les autres défaillances du réseau. Nous développons et faisons fonctionner nos réseaux en vue de minimiser les pertes de paquets. Nous mesurons le taux de perte de paquets (PLR) sur l'ensemble du réseau mondial qui relie les régions. AWS Nous faisons fonctionner notre réseau backbone en vue d'obtenir un p99 pour le PLR horaire de moins de 0,0001 %.

Commencer avec Amazon VPC

Effectuez les tâches suivantes pour vous préparer à créer et à connecter vos VPC. Lorsque vous avez terminé, vous serez prêt pour le déploiement de votre application sur AWS.

Tâches

- Inscrivez-vous pour un Compte AWS
- Vérifier les autorisations
- Déterminer vos plages d'adresses IP
- Sélectionner vos zones de disponibilité
- Planifier votre connectivité Internet
- Créer votre VPC
- Déploiement de votre application

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Vérifier les autorisations

Avant de pouvoir utiliser Amazon VPC, vous devez disposer des autorisations requises. Pour plus d'informations, consultez Identity and Access Management pour Amazon VPC et Exemples de stratégie Amazon VPC.

Déterminer vos plages d'adresses IP

Les ressources de votre VPC communiquent entre elles et avec des ressources sur Internet à l'aide d'adresses IP. Lorsque vous créez des VPC et des sous-réseaux, vous pouvez sélectionner leurs plages d'adresses IP. Lorsque vous déployez des ressources dans un sous-réseau, comme des instances EC2, vous recevez des adresses IP de la plage d'adresses IP du sous-réseau. Pour plus d'informations, consultez Adressage IP.

Lorsque vous choisissez la taille de votre VPC, prenez en compte le nombre d'adresses IP dont vous aurez besoin entre vos Comptes AWS et vos VPC. Assurez-vous que les plages d'adresses IP de vos VPC ne se chevauchent pas avec les plages d'adresses IP de votre propre réseau. Si vous avez besoin d'une connectivité entre plusieurs VPC, vous devez vous assurer qu'aucune adresse IP ne se chevauche.

IP Address Manager (IPAM) facilite la planification, le suivi et la surveillance des adresses IP pour votre application. Pour plus d'informations, consultez le Guide IP Address Manager.

Sélectionner vos zones de disponibilité

Une AWS région est un emplacement physique où nous regroupons des centres de données, appelés zones de disponibilité. Chaque zone de disponibilité dispose d'une alimentation, d'un refroidissement et d'une sécurité physique indépendants, ainsi que d'une alimentation, d'un réseau et d'une connectivité redondants. Les zones de disponibilité d'une région sont physiquement séparées par une distance importante et sont interconnectées par un réseau à bande passante élevée et à faible latence. Vous pouvez concevoir votre application pour qu'elle s'exécute dans plusieurs zones de disponibilité afin d'atteindre une tolérance aux pannes encore plus élevée.

Environnement de production

Pour un environnement de production, nous vous recommandons de sélectionner au moins deux zones de disponibilité et de déployer vos AWS ressources de manière uniforme dans chaque zone de disponibilité active.

Environnement de développement ou de test

Pour un environnement de développement ou de test, vous pouvez choisir d'économiser de l'argent en déployant vos ressources dans une seule zone de disponibilité.

Planifier votre connectivité Internet

Prévoyez de diviser chaque VPC en sous-réseaux en fonction de vos besoins en matière de connectivité. Par exemple :

- Si vos serveurs Web reçoivent du trafic en provenance de clients sur Internet, créez un sous-réseau pour ces serveurs dans chaque zone de disponibilité.
- Si vous avez également des serveurs qui ne recevront du trafic qu'en provenance d'autres serveurs dans le VPC, créez un sous-réseau distinct pour ces serveurs dans chaque zone de disponibilité.
- Si certains de vos serveurs reçoivent du trafic uniquement via une connexion VPN à votre réseau, créez pour eux un sous-réseau distinct dans chaque zone de disponibilité.

Si votre application doit recevoir du trafic en provenance d'Internet, le VPC doit disposer d'une passerelle Internet. L'association d'une passerelle Internet à un VPC ne rend pas automatiquement vos instances accessibles depuis Internet. En plus d'attacher la passerelle Internet, vous devez mettre à jour la table de routage du sous-réseau avec un routage vers la passerelle Internet. Vous devez également vous assurer que les instances disposent d'adresses IP publiques et d'un groupe de sécurité associé autorisant le trafic en provenance d'Internet sur les ports et protocoles spécifiques requis par votre application.

Vous pouvez également enregistrer vos instances à partir d'un équilibreur de charge accessible sur Internet. L'équilibreur de charge reçoit le trafic des clients et le distribue entre les instances enregistrées dans une ou plusieurs zones de disponibilité. Pour plus d'informations, consultez Elastic Load Balancing. Pour permettre aux instances d'un sous-réseau privé d'accéder à Internet (par exemple, pour télécharger des mises à jour) sans autoriser les connexions entrantes non sollicitées depuis Internet, ajoutez une passerelle NAT publique dans chaque zone de disponibilité active et mettez à jour la table de routage pour envoyer le trafic Internet vers la passerelle NAT. Pour plus d'informations, consultez the section called “Accéder à Internet à partir d'un sous-réseau privé”.

Créer votre VPC

Une fois que vous avez déterminé le nombre de VPC et de sous-réseaux dont vous avez besoin, les blocs d'adresse CIDR à attribuer à vos VPC et sous-réseaux, ainsi que la manière de connecter votre VPC à Internet, vous êtes prêt à créer votre VPC. Si vous créez votre VPC à l'aide des sous-réseaux publics AWS Management Console et que vous incluez des sous-réseaux publics dans votre configuration, nous créons une table de routage pour le sous-réseau et ajoutons les routes requises pour un accès direct à Internet. Pour plus d'informations, consultez the section called "Création d'un VPC".

Déploiement de votre application

Une fois que vous avez créé votre VPC, vous pouvez déployer votre application.

Environnement de production

Pour un environnement de production, vous pouvez utiliser l'un des services suivants pour déployer des serveurs dans plusieurs zones de disponibilité, configurer la mise à l'échelle de manière à maintenir le nombre minimum de serveurs requis par votre application et enregistrer vos serveurs auprès d'un équilibreur de charge afin de répartir le trafic de manière uniforme entre vos serveurs.

- Amazon EC2 Auto Scaling
- EC2 Fleet
- Amazon Elastic Container Service (Amazon ECS)

Environnement de développement ou de test

Pour un environnement de développement ou de test, vous pouvez choisir de lancer une seule instance EC2. Pour plus d'informations, consultez Démarrer avec Amazon EC2 dans le Guide de l'utilisateur Amazon EC2.

Adressage IP pour vos VPC et sous-réseaux

Les adresses IP permettent aux ressources de votre VPC de communiquer entre elles et avec les ressources sur Internet.

La notation CIDR (Classless Inter-Domain Routing - Routage inter-domaines sans classe) permet de représenter une adresse IP et son masque réseau. Le format de ces adresses est le suivant :

- Une adresse IPv4 individuelle comporte 32 bits, avec 4 groupes de 3 chiffres décimaux maximum. Par exemple : 10.0.1.0.
- Un bloc d'adresse CIDR IPv4 comporte quatre groupes de trois chiffres décimaux maximum, de 0 à 255, séparés par des points, suivis d'une barre oblique et d'un nombre de 0 à 32. Exemple : 10.0.0.0/16.
- Une adresse IPv6 individuelle est de 128 bits, avec 8 groupes de 4 chiffres hexadécimaux. Par exemple, 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
- Un bloc d'adresse CIDR IPv6 comporte quatre groupes de quatre chiffres hexadécimaux maximum, séparés par des deux points, suivis d'un double deux points, suivis d'une barre oblique et d'un nombre de 1 à 128. Par exemple, 2001:db8:1234:1a00::/56.

Pour plus d'informations, consultez En quoi consiste le CIDR ?

Table des matières

- AWS services prenant en charge le protocole IPv6

Comparez l'IPv4 et l'IPv6

Le tableau suivant récapitule les différences entre IPv4 et IPv6 dans Amazon EC2 et Amazon VPC. Pour obtenir la liste des AWS services qui prennent en charge la configuration à double pile (IPv4 et IPv6) et les configurations IPv6 uniquement, consultez. Services qui prennent en charge IPv6

Caractéristiques	IPv4	IPv6
Taille du VPC	Jusqu'à 5 CIDR de /16 à /28. Ce quota est réglable.	Jusqu'à 5 CIDR de /44 à /60 par incréments de /4. Ce quota est réglable.
Taille du sous-réseau	De /16 à /28.	De /44 à /64 par incréments de /4.
Sélection d'adresse	Vous pouvez choisir le bloc CIDR IPv4 pour votre VPC ou allouer un bloc CIDR à partir de « Amazon VPC IP Address Manager » (IPAM) (Gestionnaire d'adresses IP de VPC d'Amazon). Pour plus d'informations, veuillez consulter Qu'est-ce qu'IPAM ? dans le Guide de l'utilisateur IPAM Amazon VPC.	Vous pouvez ajouter votre propre bloc d'adresse CIDR IPv6 à AWS votre VPC, choisir un bloc d'adresse CIDR IPv6 fourni par Amazon ou allouer un bloc d'adresse CIDR depuis Amazon VPC IP Address Manager (IPAM). Pour plus d'informations, veuillez consulter Qu'est-ce qu'IPAM ? dans le Guide de l'utilisateur IPAM Amazon VPC.
Accès Internet	Nécessite une passerelle Internet.	Nécessite une passerelle Internet. Prend en charge les communications sortantes uniquement à l'aide d'une passerelle Internet de sortie uniquement.
Adresses IP Elastic	Pris en charge. Attribue à une instance EC2 une adresse IPv4 publique statique et permanente.	Non pris en charge. Les EIP conservent l'adresse IPv4 publique d'une instance statique lors du

Caractéristiques	IPv4	IPv6
		redémarrage de l'instance. Les adresses IPv6 sont statiques par défaut.
Passerelles NAT	Pris en charge. Les instances dans des sous-réseaux privés peuvent se connecter à Internet à l'aide d'une passerelle NAT publique ou aux ressources situées dans d'autres VPC à l'aide d'une passerelle NAT privée.	Pris en charge. Vous pouvez utiliser une passerelle NAT avec NAT64 pour permettre aux instances des sous-réseaux IPv6 uniquement de communiquer avec des ressources IPv4 uniquement au sein des VPC, entre les VPC, dans vos réseaux sur site ou sur Internet.
Noms DNS	Les instances reçoivent des noms DNS basé sur IPBN ou RBN fournis par Amazon. Le nom DNS est résolu en enregistrements DNS sélectionnés pour l'instance.	L'instance reçoit des noms DNS basé sur IPBN ou RBN fournis par Amazon. Le nom DNS est résolu en enregistrements DNS sélectionnés pour l'instance.

Adresses IPv4 privées

Les adresses IPv4 privées (également appelées adresses IP privées dans cette rubrique) ne sont pas accessibles via Internet et peuvent être utilisées pour la communication entre les instances de votre VPC. Lorsque vous lancez une instance dans un VPC, une adresse IP privée principale de la plage d'adresses IPv4 du sous-réseau est attribuée à l'interface réseau par défaut (eth0) de l'instance. Chaque instance se voit également attribuer un nom d'hôte DNS privé (interne) qui est résolu en adresse IP privée de l'instance. Le nom d'hôte peut être de deux types : basé sur les ressources ou sur l'adresse IP. Pour plus d'informations, consultez Dénomination d'instances EC2. Si vous ne spécifiez pas d'adresse IP privée principale, nous sélectionnons pour vous une adresse IP disponible dans la plage de sous-réseaux. Pour plus d'informations sur les interfaces réseau, consultez Elastic Network Interfaces dans le guide de l'utilisateur Amazon EC2.

Vous pouvez assigner des adresses IP privées supplémentaires, appelées adresses IP privées secondaires, aux instances qui s'exécutent dans un VPC. Contrairement à une adresse IP privée principale, une adresse IP privée secondaire peut être réaffectée depuis une interface réseau à

une autre. Une adresse IP privée reste associée à l'interface réseau quand l'instance est arrêtée et redémarrée, et elle est libérée quand l'instance prend fin. Pour plus d'informations sur les adresses IP principales et secondaires, consultez la section Adresses IP multiples dans le guide de l'utilisateur Amazon EC2.

Nous appelons les adresses IP privées les adresses IP qui se trouvent dans la plage d'adresse CIDR IPv4 du VPC. La plupart des plages d'adresses IP du VPC se trouvent dans les plages d'adresses IP privées (qui ne sont pas publiquement routables) spécifiées dans le RFC 1918 ; cependant, vous pouvez utiliser des blocs d'adresses CIDR publiquement routables pour votre VPC. Quelle que soit la plage d'adresses IP de votre VPC, nous ne prenons pas en charge l'accès direct à Internet à partir du bloc d'adresse CIDR de votre VPC, y compris un bloc d'adresse CIDR routable publiquement. Vous devez configurer l'accès à Internet via une passerelle, par exemple une passerelle Internet, une passerelle privée virtuelle, une AWS Site-to-Site VPN connexion ou AWS Direct Connect.

Nous ne publions jamais la plage d'adresses IPv4 d'un sous-réseau sur Internet.

Adresses IPv4 publiques

Tous les sous-réseaux disposent d'un attribut qui détermine si une interface réseau créée dans le sous-réseau reçoit automatiquement une adresse IPv4 publique (également appelée adresse IP publique dans cette rubrique). Par conséquent, lorsque vous lancez une instance dans un sous-réseau dont cet attribut est activé, une adresse IP publique est attribuée à l'interface réseau principale (eth0) qui est créée pour l'instance. Une adresse IP publique est mappée à l'adresse IP privée principale par le biais d'une traduction d'adresses réseau (NAT).

> **Note**
>
> AWS frais pour toutes les adresses IPv4 publiques, y compris les adresses IPv4 publiques associées aux instances en cours d'exécution et les adresses IP Elastic. Pour plus d'informations, consultez l'onglet Adresse IPv4 publique de la page de tarification d'Amazon VPC.

Vous pouvez contrôler si votre instance reçoit une adresse IP publique en effectuant ce qui suit :

- Modifier l'attribut d'adressage IP public de votre sous-réseau. Pour plus d'informations, consultez Modifier l'attribut d'adressage IPv4 public de votre sous-réseau.

- Activer ou désactiver la fonction d'adressage IP public pendant le lancement de l'instance, qui remplace l'attribut d'adressage IP public du sous-réseau.
- Vous pouvez annuler l'attribution d'une adresse IP publique à votre instance après le lancement en gérant les adresses IP associées à une interface réseau. Pour plus d'informations, consultez la section Gérer les adresses IP dans le guide de l'utilisateur Amazon EC2.

Une adresse IP publique est attribuée à partir du groupe d'adresses IP publiques d'Amazon ; elle n'est pas associée à votre compte. Quand une adresse IP publique est dissociée de votre instance, elle est réintégrée dans le groupe et vous ne pouvez plus l'utiliser. Dans certains cas, nous publions l'adresse IP publique de votre instance ou nous lui en attribuons une nouvelle. Pour plus d'informations, consultez la section Adresses IP publiques dans le guide de l'utilisateur Amazon EC2.

Si vous avez besoin d'une adresse IP publique persistante allouée à votre compte qui peut être attribuée aux instances et en être dissociée comme vous le souhaitez, utilisez plutôt une adresse IP Elastic. Pour plus d'informations, consultez Associer des adresses IP Elastic à des ressources dans votre VPC.

Si votre VPC est activé pour prendre en charge les noms d'hôte DNS, chaque instance qui reçoit une adresse IP publique ou une adresse IP Elastic reçoit également un nom d'hôte DNS public. Nous résolvons un nom d'hôte DNS public en adresse IP publique de l'instance en dehors du réseau de cette dernière, et en adresse IP privée de l'instance depuis le réseau de cette dernière. Pour plus d'informations, consultez Attributs DNS pour votre VPC.

Adresses IPv6

Le cas échéant, vous pouvez associer un bloc d'adresses CIDR IPv6 à votre VPC, et associer les blocs d'adresse CIDR IPv6 à vos sous-réseaux. Pour plus d'informations, consultez les rubriques suivantes :

- Ajouter un bloc d'adresse CIDR IPv6 à votre VPC
- Ajouter un bloc d'adresse CIDR IPv6 à votre sous-réseau

Les adresses IPv6 sont globalement uniques et peuvent être configurées pour rester privées ou être accessibles via Internet. Votre instance reçoit une adresse IPv6 si un bloc d'adresses CIDR IPv6 est associé à votre VPC et votre sous-réseau, et si l'une des conditions suivantes est vraie :

- Votre sous-réseau est configuré pour attribuer automatiquement une adresse IPv6 à une instance lors du lancement. Pour plus d'informations, consultez Modifier l'attribut d'adressage IPv6 de votre sous-réseau.
- Vous attribuez une adresse IPv6 à votre instance lors du lancement.
- Vous attribuez une adresse IPv6 à l'interface réseau principale de votre instance après son lancement.
- Vous attribuez une adresse IPv6 à une interface réseau dans le même sous-réseau et vous liez l'interface réseau à votre instance après son lancement.

Lorsque votre instance reçoit une adresse IPv6 lors du lancement, l'adresse est associée à l'interface réseau principale (eth0) de l'instance. Vous pouvez gérer les adresses IPv6 pour l'interface réseau principale de vos instances (eth0) comme suit :

- Attribution et annulation de l'attribution d'adresses IPv6 de l'interface réseau. Le nombre d'adresses IPv6 que vous pouvez assigner à une interface réseau et le nombre d'interfaces réseau que vous pouvez lier à une instance varient en fonction du type d'instance. Pour plus d'informations, consultez la section Adresses IP par interface réseau et par type d'instance dans le guide de l'utilisateur Amazon EC2.
- Activez une adresse IPv6 principale. Une adresse IPv6 principale vous permet d'éviter de perturber le trafic vers les instances ou les ENI. Pour plus d'informations, consultez les sections Création d'une interface réseau et Gestion des adresses IP dans le guide de l'utilisateur Amazon EC2.

Une adresse IPv6 persiste lorsque vous arrêtez (ou mettez en veille) et démarrez votre instance, et est libérée lorsque vous désactivez votre instance. Vous ne pouvez pas réattribuer une adresse IPv6 si elle est déjà attribuée à une autre interface réseau — vous devez d'abord annuler l'attribution.

Vous pouvez contrôler si les instances sont accessibles par le biais de leurs adresses IPv6 en contrôlant le routage de votre sous-réseau ou en utilisant des règles ACL de groupe de sécurité et de réseau. Pour plus d'informations, consultez Confidentialité du trafic inter-réseau dans Amazon VPC.

Pour plus d'informations sur les plages d'adresses IPv6 réservées, consultez Registre d'adresses IPv6 IANA à des fins spéciales et RFC4291.

Utiliser vos propres adresses IP

Vous pouvez ajouter une partie ou la totalité de votre plage d'adresses IPv4 ou IPv6 publiques à votre AWS compte. La plage d'adresses vous appartient toujours, mais AWS la publie sur Internet par défaut. Une fois que vous avez transféré la plage d'adresses AWS, elle apparaît dans votre compte sous forme de pool d'adresses. Vous pouvez créer une adresse IP élastique à partir de votre groupe d'adresses IPv4 et associer un bloc CIDR IPv6 de votre groupe d'adresses IPv6 à un VPC.

Pour plus d'informations, consultez la section Bring your own IP addresses (BYOIP) dans le guide de l'utilisateur Amazon EC2.

Utiliser Amazon VPC IP Address Manager

Amazon VPC IP Address Manager (IPAM) est une fonctionnalité VPC qui vous permet de planifier, suivre et surveiller plus facilement les adresses IP pour vos charges de travail. AWS Vous pouvez utiliser IPAM pour allouer des CIDR d'adresses IP aux VPC à l'aide de règles métier spécifiques.

Pour plus d'informations, veuillez consulter Qu'est-ce qu'IPAM ? dans le Guide de l'utilisateur IPAM Amazon VPC.

Blocs CIDR VPC

Les adresses IP de votre cloud privé virtuel (VPC) sont représentées en notation CIDR (Routage inter-domaines sans classe). Un VPC doit être associé à un bloc d'adresse CIDR IPv4. Vous pouvez éventuellement associer des blocs d'adresse CIDR IPv4 supplémentaires et un ou plusieurs blocs d'adresse CIDR IPv6. Pour plus d'informations, consultez Adressage IP pour vos VPC et sous-réseaux.

Table des matières

Blocs d'adresse CIDR VPC IPv4

Lorsque vous créez un VPC, vous devez spécifier un bloc d'adresse CIDR IPv4 pour le VPC. La taille de bloc autorisée est comprise entre un masque réseau en `/16` (65 536 adresses IP) et un masque réseau en `/28` (16 adresses IP). Après avoir créé votre VPC, vous pouvez lui associer des blocs d'adresse CIDR IPv4 supplémentaires. Pour plus d'informations, consultez Ajouter un bloc d'adresse CIDR IPv4 à votre VPC.

Nous vous conseillons de créer un VPC avec un bloc d'adresse CIDR tiré des plages d'adresses IPv4 privées, comme spécifié dans la norme RFC 1918.

Plage RFC 1918	Exemple de bloc d'adresse CIDR
10.0.0.0 - 10.255.255.255 (préfixe 10/8)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (préfixe 172.16/12)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (préfixe 192.168/16)	192,168.0.0/20

> **Important**
>
> Certains AWS services utilisent la gamme `172.17.0.0/16` CIDR. Afin d'éviter de futurs conflits, n'utilisez pas cette plage lors de la création de votre VPC. Par exemple, des services tels AWS Cloud9 qu'Amazon SageMaker peuvent rencontrer des conflits d'adresses `172.17.0.0/16` IP si la plage d'adresses IP est déjà utilisée n'importe où sur votre réseau. Pour plus d'informations, veuillez consulter la section Impossible de se connecter à l'environnement EC2 car les adresses IP du VPC sont utilisées par Docker du Guide de l'utilisateur AWS Cloud9 .

Vous pouvez créer un VPC avec un bloc d'adresses CIDR publiquement routable ne faisant pas partie des plages d'adresses IPv4 privées spécifiées dans la norme RFC 1918. Toutefois, dans le cadre de cette documentation, nous faisons référence à des adresses IP privées en tant qu'adresses IPv4 se trouvant dans la plage CIDR de votre VPC.

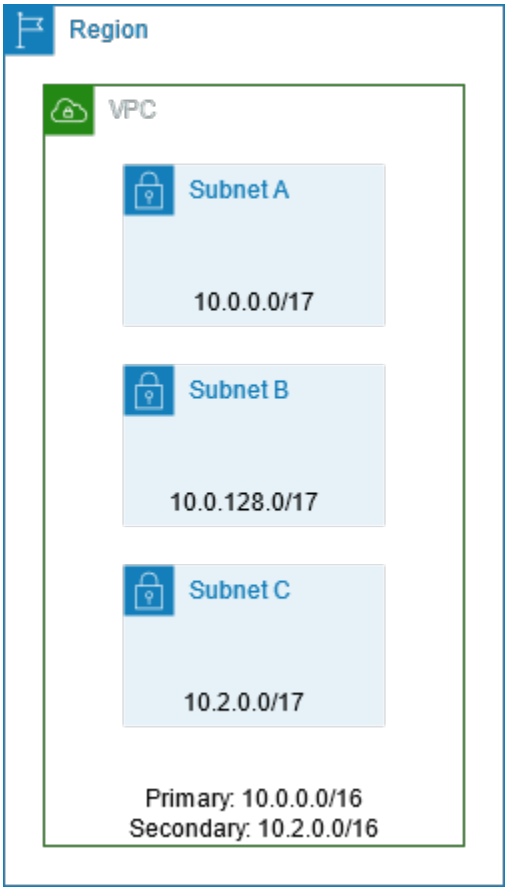
Lorsque vous créez un VPC destiné à être utilisé avec un AWS service, consultez la documentation du service pour vérifier si sa configuration est soumise à des exigences spécifiques.

Si vous créez un VPC à l'aide d'un outil de ligne de commande ou de l'API Amazon EC2, le bloc d'adresse CIDR est automatiquement ramené à sa forme canonique. Par exemple, si vous spécifiez 100.68.0.18/18 pour le bloc d'adresse CIDR, nous créons un bloc d'adresse CIDR de 100.68.0.0/18.

Gestion des blocs d'adresse CIDR IPv4 pour un VPC

Vous pouvez associer des blocs d'adresse CIDR IPv4 à votre VPC. Lorsque vous associez un bloc d'adresse CIDR à votre VPC, une route est ajoutée automatiquement à vos tables de routage VPC afin de permettre le routage au sein du VPC (la destination est le bloc d'adresse CIDR et la cible est `local`).

Dans l'exemple suivant, le VPC comporte un bloc d'adresse CIDR principal et un bloc d'adresse CIDR secondaire. Les blocs CIDR pour le sous-réseau A et le sous-réseau B proviennent du bloc CIDR VPC principal. Le bloc CIDR du sous-réseau C provient du bloc CIDR VPC secondaire.



La table de routage suivante présente les acheminements locaux du VPC.

Destination	Cible
10.0.0.0/16	Locale
10.2.0.0/16	Local

Pour ajouter un bloc d'adresse CIDR à votre VPC, les règles suivantes s'appliquent :

- La taille de bloc autorisée est comprise entre un masque réseau en `/28` et un masque réseau en `/16`.
- Le bloc d'adresse CIDR ne doit chevaucher aucun bloc d'adresse CIDR existant associé au VPC.
- Il existe des restrictions pour les plages d'adresses IPv4 que vous pouvez utiliser. Pour plus d'informations, consultez Restrictions des associations de blocs d'adresse CIDR IPv4.
- Vous ne pouvez pas augmenter ou diminuer la taille d'un bloc CIDR existant.
- Vous avez un quota sur le nombre de blocs d'adresse CIDR que vous pouvez associer à un VPC et le nombre d'acheminements que vous pouvez ajouter à une table de routage. Vous ne pouvez pas associer un bloc d'adresse CIDR si cela entraîne un dépassement de vos quotas. Pour plus d'informations, consultez Quotas Amazon VPC.
- Le bloc d'adresse CIDR ne doit pas être le même, ni être plus important, qu'une plage CIDR de destination d'une route dans une table de routage de VPC. Par exemple, dans un VPC où le bloc CIDR principal est `10.2.0.0/16`, vous avez une route existante dans une table de routage avec une destination de `10.0.0.0/24` vers une passerelle privée virtuelle. Vous souhaitez associer un bloc CIDR secondaire dans la plage `10.0.0.0/16`. En raison de l'itinéraire existant, vous ne pouvez pas associer un bloc CIDR de `10.0.0.0/24` ou plus grand. Toutefois, vous pouvez associer un bloc d'adresse CIDR de `10.0.0.0/25` ou plus petit.
- Les règles suivantes s'appliquent lorsque vous ajoutez des blocs d'adresse CIDR IPv4 à un VPC faisant partie d'une connexion d'appairage de VPC :
  - Si la connexion d'appairage de VPC est `active`, vous pouvez ajouter des blocs d'adresse CIDR à un VPC, à condition qu'ils ne chevauchent pas un bloc d'adresse CIDR du VPC pair.
  - Si la connexion d'appairage de VPC est `pending-acceptance`, le propriétaire du VPC demandeur ne peut pas ajouter de bloc d'adresse CIDR au VPC, qu'il chevauche ou non le bloc d'adresse CIDR du VPC demandeur. Soit le propriétaire du VPC demandeur doit accepter la connexion d'appairage, soit il doit supprimer la demande de connexion d'appairage du VPC, ajouter le bloc d'adresse CIDR, puis demander une nouvelle connexion d'appairage du VPC.

  - Si la connexion d'appairage du VPC est `pending-acceptance`, le propriétaire du VPC demandeur peut ajouter des blocs d'adresse CIDR au VPC. Si un bloc d'adresse CIDR secondaire chevauche un bloc CIDR du VPC demandeur, la demande de connexion d'appairage du VPC échoue et ne peut pas être acceptée.
- Si vous vous connectez AWS Direct Connect à plusieurs VPC via une passerelle Direct Connect, les VPC associés à la passerelle Direct Connect ne doivent pas comporter de blocs CIDR qui se chevauchent. Si vous ajoutez un bloc d'adresse CIDR à l'un des VPC qui est associé à la passerelle Direct Connect, assurez-vous que le nouveau bloc d'adresse CIDR ne chevauche pas un bloc d'adresse CIDR existant d'un autre VPC associé. Pour plus d'informations, consultez la section Passerelles Direct Connect du Guide de l'utilisateur AWS Direct Connect .
- Lorsque vous ajoutez ou supprimez un bloc d'adresse CIDR, il peut passer par différents états: `associating` | `associated` | `disassociating` | `disassociated` | `failing` | `failed`. Le bloc d'adresse CIDR est prêt pour que vous l'utilisiez utilisé lorsqu'il a l'état `associated`.

Vous pouvez dissocier un bloc d'adresse CIDR que vous avez associé à votre VPC, mais vous ne pouvez pas dissocier le bloc d'adresse CIDR avec lequel vous avez initialement créé le VPC (bloc d'adresse CIDR principal). Pour afficher le CIDR principal de votre VPC sur la console Amazon VPC, choisissez Your VPCs (Vos VPC), cochez la case de votre VPC et choisissez l'onglet CIDRs (CIDR). Pour afficher le CIDR principal à l'aide de AWS CLI, utilisez la commande describe-vpcs comme suit. Le CIDR principal est retourné dans le `CidrBlock element` de niveau supérieur.

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d --query Vpcs[*].CidrBlock --output text
```

Voici un exemple de sortie.

```
10.0.0.0/16
```

Restrictions des associations de blocs d'adresse CIDR IPv4

Le tableau suivant donne un aperçu des associations de blocs d'adresse CIDR autorisées et restreintes au VPC. Les restrictions s'expliquent par le fait que certains AWS services utilisent des fonctionnalités inter-VPC et multi-comptes qui nécessitent des blocs CIDR non conflictuels côté service. AWS

Plage d'adresses IP	Associations limitées	Associations autorisées
10.0.0.0/8	Les blocs d'adresse CIDR d'autres plages RFC 1918* (172.16.0.0/12 and 192.168.0.0/16). Si l'un des blocs d'adresse CIDR associés au VPC se trouve dans la plage 10.0.0.0/15 (10.0.0.0 à 10.1.255.255), vous ne pouvez pas ajouter un bloc d'adresse CIDR provenant de la plage 10.0.0.0/16 (10.0.0.0 à 10.0.255.255). Blocs d'adresse CIDR provenant de la plage 198.19.0.0/16.	Tout autre bloc CIDR compris dans la plage 10.0.0.0/8 comprise entre un masque réseau /16 et un masque réseau /28 qui n'est pas restreint. Tout bloc d'adresse CIDR IPv4 routable publiquement (non RFC 1918) entre un masque réseau /16 et un masque réseau /28 ou un bloc CIDR entre un masque réseau /16 et un masque réseau /28 compris entre un masque réseau /16 et un masque réseau /28 de la plage 100.64.0.0/10.
169,254,0,0/16	Les blocs CIDR du bloc « link local » sont réservés comme décrit dans le RFC 5735 et ne peuvent pas être attribués à des VPC.	
172.16.0.0/12	Les blocs d'adresse CIDR d'autres plages RFC 1918* (10.0.0.0/8 and 192.168.0.0/16). Blocs d'adresse CIDR provenant de la plage 172.31.0.0/16. Blocs d'adresse CIDR provenant de la plage 198.19.0.0/16.	Tout autre bloc CIDR compris dans la plage 172.16.0.0/12 comprise entre un masque réseau /16 et un masque réseau /28 qui n'est pas restreint. Tout bloc d'adresse CIDR IPv4 routable publiquement (non RFC 1918) entre un masque réseau /16 et un masque réseau /28 ou un bloc CIDR entre un masque réseau /16 et un masque réseau /28 compris entre un masque réseau /16 et un masque réseau /28 de la plage 100.64.0.0/10.

Plage d'adresses IP	Associations limitées	Associations autorisées
192.168.0.0/16	Les blocs d'adresse CIDR d'autres plages RFC 1918* (10.0.0.0/8 et 172.16.0.0/12). Blocs d'adresse CIDR provenant de la plage 198.19.0.0/16.	Tout autre bloc CIDR compris dans la plage 192.168.0.0/16 comprise entre un masque réseau /16 et un masque réseau /28. Tout bloc d'adresse CIDR IPv4 routable publiquement (non RFC 1918) entre un masque réseau /16 et un masque réseau /28 ou un bloc CIDR compris dans la plage 100.64.0.0/10 comprise entre un masque réseau /16 et un masque réseau /28.
198.19.0.0/16	Blocs d'adresse CIDR provenant des places RFC 1918*.	Tout bloc d'adresse CIDR IPv4 routable publiquement (non RFC 1918) entre un masque réseau /16 et un masque réseau /28 ou un bloc CIDR compris dans la plage 100.64.0.0/10 comprise entre un masque réseau /16 et un masque réseau /28.
Un bloc d'adresse CIDR (non RFC 1918) publiquement routable ou un bloc d'adresse CIDR dans la plage 100.64.0.0/10	Blocs d'adresse CIDR provenant des places RFC 1918*. Blocs d'adresse CIDR provenant de la plage 198.19.0.0/16.	Tout autre bloc d'adresse CIDR IPv4 routable publiquement (non RFC 1918) entre un masque réseau /16 et un masque réseau /28 ou un bloc CIDR entre un masque réseau /16 et un masque réseau /28 compris entre un masque réseau /16 et un masque réseau /28 compris entre 100.64.0.0/10.

*Les plages RFC 1918 sont les plages d'adresses IPv4 privées spécifiées dans RFC 1918.

Blocs d'adresse CIDR VPC IPv6

Vous pouvez associer un seul bloc d'adresse CIDR IPv6 lorsque vous créez un nouveau VPC ou vous pouvez en associer jusqu'à cinq blocs d'adresse CIDR IPv6 de `/44` à `/60` par incréments de `/4`. Vous pouvez demander un bloc d'adresse CIDR IPv6 à partir du groupe d'adresses IPv6 d'Amazon. Pour plus d'informations, consultez Ajouter un bloc d'adresse CIDR IPv6 à votre VPC.

Si vous avez associé un bloc d'adresse CIDR IPv6 à votre VPC, vous pouvez associer un bloc d'adresse CIDR IPv6 à un sous-réseau existant de votre VPC ou lorsque vous créez un sous-réseau. Pour plus d'informations, consultez the section called "Dimensionnement de sous-réseau pour IPv6".

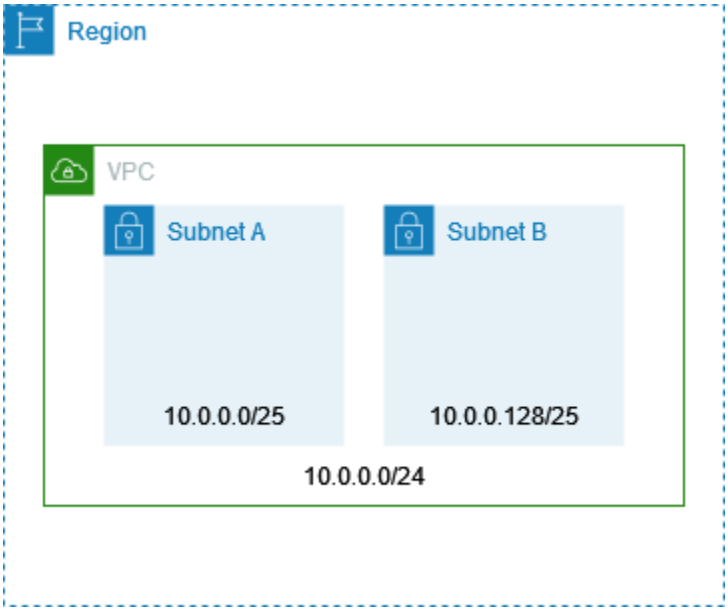
Par exemple, vous créez un VPC et vous spécifiez que vous voulez associer un bloc d'adresse CIDR IPv6 fourni par Amazon au VPC. Amazon attribue le bloc d'adresse CIDR IPv6 suivant à votre VPC : `2001:db8:1234:1a00::/56`. Vous ne pouvez pas choisir vous-même la plage d'adresses IP. Vous pouvez créer un sous-réseau et associer un bloc d'adresse CIDR IPv6 à partir de cette plage ; par exemple, `2001:db8:1234:1a00::/64`.

Vous pouvez dissocier un bloc d'adresse CIDR IPv6 d'un VPC Une fois que vous avez dissocié un bloc d'adresse CIDR IPv6 d'un VPC, vous ne pouvez pas vous attendre à recevoir le même CIDR si vous associez une nouvelle fois un bloc d'adresse CIDR IPv6 à votre VPC ultérieurement.

Blocs d'adresse CIDR de sous-réseau

Les adresses IP de votre sous-réseaux sont représentées en notation CIDR (Routage inter-domaines sans classe). Le bloc d'adresse CIDR d'un sous-réseau peut être identique à celui du VPC (pour créer un sous-réseau unique dans le VPC) ou à un sous-ensemble du bloc CIDR du VPC (pour créer plusieurs sous-réseaux dans le VPC). Si vous créez plusieurs sous-réseaux dans un VPC, les blocs d'adresse CIDR de ces sous-réseaux ne peuvent pas se chevaucher.

Par exemple, si vous créez un VPC avec le bloc d'adresse CIDR `10.0.0.0/24`, il prend en charge 256 adresses IP. Vous pouvez scinder ce bloc d'adresse CIDR en deux sous-réseaux, chacun prenant en charge 128 adresses IP. Un sous-réseau utilise le bloc d'adresse CIDR `10.0.0.0/25` (pour les adresses `10.0.0.0` - `10.0.0.127`) et l'autre utilise le bloc d'adresse CIDR `10.0.0.128/25` (pour les adresses `10.0.0.128` - `10.0.0.255`).



Des outils sont disponibles sur Internet pour vous aider à calculer et à créer des blocs d'adresses CIDR de sous-réseau IPv4 et IPv6. Vous pouvez trouver des outils qui répondent à vos besoins en recherchant des termes tels que « calculateur de sous-réseau » ou « calculateur CIDR ». Votre équipe d'ingénierie réseau peut aussi vous aider à déterminer les blocs d'adresse CIDR IPv4 et IPv6 à indiquer pour vos sous-réseaux.

Dimensionnement de sous-réseau pour IPv4

La taille autorisée d'un bloc d'adresse CIDR IPv4 pour un sous-réseau est comprise entre un masque réseau en `/28` et un masque réseau en `/16`. Les quatre premières adresses IP et la dernière adresse IP de chaque bloc CIDR de sous-réseau ne sont pas disponibles pour votre utilisation, et elles ne peuvent pas être attribuées à une ressource, telle qu'une instance EC2. Par exemple, dans un sous-réseau avec le bloc d'adresse CIDR `10.0.0.0/24`, les cinq adresses IP suivantes sont réservées :

- 10.0.0.0 : adresse réseau.
- 10.0.0.1 : Réservé par AWS pour le routeur VPC.
- 10.0.0.2 : Réservé par. AWS Notez que l'adresse IP du serveur DNS a pour valeur la base de la plage réseau VPC plus deux. Pour les VPC ayant plusieurs blocs CIDR, l'adresse IP du serveur DNS se trouve dans le CIDR principal. Nous réservons également la base de chaque plage de sous-réseau plus deux à tous les blocs d'adresse CIDR du VPC. Pour plus d'informations, consultez Serveur Amazon DNS.
- 10.0.0.3 : Réservé par pour une AWS utilisation future.

- 10.0.0.255 : adresse de diffusion réseau. Nous ne prenons pas en charge la diffusion dans un VPC, par conséquent nous réservons cette adresse.

Si vous créez un sous-réseau à l'aide d'un outil de ligne de commande ou de l'API Amazon EC2, le bloc d'adresse CIDR est automatiquement ramené à sa forme canonique. Par exemple, si vous spécifiez 100.68.0.18/18 pour le bloc d'adresse CIDR, nous créons un bloc d'adresse CIDR de 100.68.0.0/18.

Si vous AWS utilisez BYOIP pour une plage d'adresses IPv4, vous pouvez utiliser toutes les adresses IP de la plage, y compris la première adresse (adresse réseau) et la dernière adresse (adresse de diffusion).

Dimensionnement de sous-réseau pour IPv6

Si vous avez associé un bloc d'adresse CIDR IPv6 à votre VPC, vous pouvez associer un bloc d'adresse CIDR IPv6 à un sous-réseau existant de votre VPC, ou lorsque vous créez un sous-réseau. Les longueurs possibles des masques réseau IPv6 sont comprises entre `/44` et `/64` par incréments de `/4`.

Des outils sont disponibles sur Internet pour vous aider à calculer et à créer des blocs d'adresses CIDR de sous-réseau IPv6. Vous pouvez trouver des outils qui répondent à vos besoins en recherchant des termes tels que « calculateur de sous-réseau IPv6 » ou « calculateur CIDR IPv6 ». Votre équipe d'ingénierie réseau peut aussi vous aider à déterminer les blocs d'adresse CIDR IPv6 à indiquer pour vos sous-réseaux.

Les quatre premières adresses IPv6 et la dernière adresse IPv6 de chaque bloc d'adresse CIDR de sous-réseau ne sont pas disponibles pour utilisation, et ne peuvent donc pas être affectées à une instance EC2. Par exemple, dans un sous-réseau avec le bloc d'adresse CIDR `2001:db8:1234:1a00/64`, les cinq adresses IP suivantes sont réservées :

- `2001:db8:1234:1a00::`
- `2001:db8:1234:1a00::1`: Réservé par AWS pour le routeur VPC.
- `2001:db8:1234:1a00::2`
- `2001:db8:1234:1a00::3`
- `2001:db8:1234:1a00:ffff:ffff:ffff:ffff`

Outre l'adresse IP AWS réservée par au routeur VPC dans l'exemple ci-dessus, les adresses IPv6 suivantes sont réservées au routeur VPC par défaut :

- une adresse IPv6 de lien local dans la plage FE80::/10 générée en utilisant EUI-64. Pour plus d'informations sur les adresses de lien local, voir Adresse de lien local.
- Adresse IPv6 de lien local `FE80:ec2::1`.

Si vous devez communiquer avec le routeur VPC via IPv6, vous pouvez configurer vos applications pour communiquer avec l'adresse qui correspond le mieux à vos besoins.

Grouper des blocs d'adresse CIDR à l'aide de listes de préfixes gérées

Une liste de préfixes gérée est un jeu d'un ou de plusieurs blocs d'adresse CIDR. Vous pouvez utiliser des listes de préfixes pour faciliter la configuration et la maintenance de vos groupes de sécurité et de vos tables de routage. Vous pouvez créer une liste de préfixes à partir des adresses IP que vous utilisez fréquemment et y faire référence en tant qu'ensemble dans les règles et routes de groupe de sécurité plutôt que d'y faire référencer de manière individuelle. Par exemple, vous pouvez consolider les règles de groupe de sécurité avec différents blocs CIDR, mais le même port et le même protocole en une seule règle qui utilise une liste de préfixes. Si vous mettez à l'échelle votre réseau et devez autoriser le trafic provenant d'un autre bloc CIDR, vous pouvez mettre à jour la liste des préfixes correspondante et tous les groupes de sécurité qui utilisent la liste de préfixes sont mis à jour. Vous pouvez également utiliser des listes de préfixes gérées avec d'autres AWS comptes à l'aide de Resource Access Manager (RAM).

Il existe deux types de listes de préfixes :

- Listes de préfixes gérées par le client : ensembles de plages d'adresses IP que vous définissez et gérez. Vous pouvez partager votre liste de préfixes avec d'autres AWS comptes, ce qui permet à ces comptes de référencer la liste de préfixes dans leurs propres ressources.
- AWS-listes de préfixes gérées — Ensembles de plages d'adresses IP pour les AWS services. Vous ne pouvez pas créer, modifier, partager ou supprimer une liste de préfixes gérée par AWS.

Table des matières

- Utiliser des listes de préfixes gérées par le client
- Utiliser des listes AWS de préfixes gérées
- Utiliser des listes de préfixes partagées
- Listes de préfixes de référence dans vos ressources AWS

Le préfixe répertorie les concepts et les règles

Une liste de préfixes se compose d'entrées. Chaque entrée se compose d'un bloc CIDR et, éventuellement, d'une description pour le bloc CIDR.

Listes de préfixes gérées par le client

Les règles suivantes s'appliquent aux listes de préfixes gérées par le client :

- Une liste de préfixes ne prend en charge qu'un seul type d'adressage IP (IPv4 ou IPv6). Vous ne pouvez pas combiner les blocs CIDR IPv4 et IPv6 dans une seule liste de préfixes.
- Une liste de préfixes ne s'applique qu'à la région dans laquelle vous l'avez créée.
- Lorsque vous créez une liste de préfixes, vous devez spécifier le nombre maximal d'entrées que la liste de préfixes peut prendre en charge.
- Lorsque vous faites référence à une liste de préfixes dans une ressource, le nombre maximal d'entrées pour les listes de préfixes est imputé au quota du nombre d'entrées pour la ressource. Par exemple, si vous créez une liste de préfixes avec maximum 20 entrées et que vous référencez cette liste de préfixes dans une règle de groupe de sécurité, cela compte comme 20 règles de sécurité pour le groupe.
- Lorsque vous référencez une liste de préfixes dans une table de routage, des règles de priorité de routage s'appliquent. Pour plus d'informations, consultez Listes des priorités et des préfixes d'acheminement.
- Vous pouvez modifier une liste de préfixes. Lorsque vous ajoutez ou supprimez des entrées, nous créons une nouvelle version de la liste de préfixes. Les ressources qui font référence au préfixe utilisent toujours la version actuelle (la plus récente). Vous pouvez restaurer les entrées d'une version précédente de la liste de préfixes, ce qui a également pour effet de créer une nouvelle version.
- Il existe des quotas liés aux listes de préfixes. Pour plus d'informations, consultez Listes de préfixes gérées par le client.
- Les listes de préfixes gérées par le client sont disponibles dans toutes les AWS régions commerciales (y compris les régions GovCloud (États-Unis) et Chine).

Listes de préfixes gérées par AWS

Les règles suivantes s'appliquent aux listes de AWS préfixes gérées par -managed :

- Vous ne pouvez pas créer, modifier, partager ou supprimer une liste de AWS préfixes gérée.
- Les différentes listes de préfixes AWS gérées ont un poids différent lorsque vous les utilisez. Pour plus d'informations, consultez Pondération de la liste de préfixes gérée par AWS.
- Vous ne pouvez pas afficher le numéro de version d'une liste de préfixes AWS gérée.

Gestion des identités et des accès pour les listes de préfixes

Par défaut, les utilisateurs ne sont pas autorisés à créer, afficher, modifier ou supprimer des listes de préfixes. Vous pouvez créer une politique IAM qui permet aux utilisateurs de se servir de listes de préfixes.

Pour afficher la liste des actions Amazon VPC ainsi que les ressources et clés de condition que vous pouvez utiliser dans une stratégie IAM, veuillez consulter Actions, ressources et clés de condition Amazon EC2 dans le Guide de l'utilisateur IAM.

L'exemple de stratégie suivant permet aux utilisateurs d'afficher et de travailler avec la liste de préfixes `pl-123456abcde123456` uniquement. Les utilisateurs ne peuvent pas créer ou supprimer des listes de préfixes.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:ModifyManagedPrefixList",
        "ec2:RestoreManagedPrefixListVersion"
      ],
      "Resource": "arn:aws:ec2:region:account:prefix-list/pl-123456abcde123456"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeManagedPrefixLists",
      "Resource": "*"
    }
```

```
    ]
}
```

Pour de plus amples informations sur l'utilisation d'IAM dans Amazon VPC, veuillez consulter Identity and Access Management pour Amazon VPC.

Utiliser des listes de préfixes gérées par le client

Vous pouvez créer et gérer des listes de préfixes gérées par le client. Vous pouvez consulter les listes de AWS préfixes gérées par -managed.

Tâches

- Créer une liste de préfixes
- Afficher les listes de préfixes
- Afficher les entrées d'une liste de préfixes
- Afficher des associations (références) pour votre liste de préfixes
- Modification d'une liste de préfixes
- Redimensionner une liste de préfixes
- Restaurer une version précédente d'une liste de préfixes
- Supprimer une liste de préfixes

Créer une liste de préfixes

Lorsque vous créez une liste de préfixes, vous devez spécifier le nombre maximal d'entrées que la liste de préfixes peut prendre en charge.

Limitation

Vous ne pouvez pas ajouter de liste de préfixes à une règle de groupe de sécurité si le nombre de règles plus le maximum d'entrées de la liste de préfixes dépasse le quota de règles par groupe de sécurité pour votre compte.

Pour créer une liste de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Instances gérées.
3. Choisissez Créer une liste de préfixes.

4. Pour Nom de la liste de préfixes, entrez un nom pour la liste de préfixes.
5. Pour Entrées max, entrez le nombre maximal d'entrées pour la liste de préfixes.
6. Pour Famille d'adresses, indiquez si la liste de préfixes prend en charge les entrées IPv4 ou IPv6.
7. Pour Entrées de liste de préfixes, choisissez Ajouter une nouvelle entrée, puis entrez le bloc CIDR et une description de l'entrée. Répétez cette étape pour chaque entrée.
8. (Facultatif) Pour Balises, ajoutez des balises à la liste des préfixes pour vous aider à l'identifier ultérieurement.
9. Choisissez Créer une liste de préfixes.

Pour créer une liste de préfixes à l'aide du AWS CLI

Utilisez la commande create-managed-prefix-list.

Afficher les listes de préfixes

Vous pouvez afficher vos listes de préfixes, celles qui sont partagées avec vous et celles qui sont gérées par AWS.

Pour afficher les listes de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Managed Prefix Lists (Listes de préfixes gérées).
3. La colonne ID du propriétaire indique l'identifiant de AWS compte du propriétaire de la liste de préfixes. Pour les listes de préfixes AWS gérées par -managed, l'ID du propriétaire est. AWS

Pour afficher les listes de préfixes à l'aide du AWS CLI

Utilisez la commande describe-managed-prefix-lists.

Afficher les entrées d'une liste de préfixes

Vous pouvez consulter les entrées de vos listes de préfixes, des listes de préfixes partagées avec vous et des listes de préfixes AWS gérées.

Pour afficher les entrées d'une liste de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le panneau de navigation, choisissez Managed Prefix Lists (Listes de préfixes gérées).
3. Cochez la case correspondant à la liste de préfixes.
4. Dans le volet inférieur, choisissez Entrées pour afficher les entrées de la liste des préfixes.

Pour afficher les entrées d'une liste de préfixes à l'aide du AWS CLI

Utilisez la commande get-managed-prefix-list-entries.

Afficher des associations (références) pour votre liste de préfixes

Vous pouvez afficher les ID et les propriétaires des ressources associées à votre liste de préfixes. Les ressources associées sont des ressources qui font référence à votre liste de préfixes dans leurs entrées ou règles.

Limitation

Vous ne pouvez pas afficher les ressources associées à une AWS liste de préfixes gérée.

Pour afficher les associations de listes de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Managed Prefix Lists (Listes de préfixes gérées).
3. Cochez la case correspondant à la liste de préfixes.
4. Dans le volet inférieur, choisissez Associations pour afficher les ressources qui font référence à la liste des préfixes.

Pour afficher les associations de listes de préfixes à l'aide du AWS CLI

Utilisez la commande get-managed-prefix-list-associations.

Modification d'une liste de préfixes

Vous pouvez modifier le nom de votre liste de préfixes et ajouter ou supprimer des entrées. Pour modifier le nombre maximal d'entrées, reportez-vous àRedimensionner une liste de préfixes.

La mise à jour des entrées d'une liste de préfixes a pour effet de créer une nouvelle version de la liste de préfixes, ce qui n'est pas le cas lorsque vous mettez à jour le nom ou le nombre maximal d'entrées d'une liste de préfixes.

Considérations

- Vous ne pouvez pas modifier une AWS liste de préfixes gérée.
- Lorsque vous augmentez le nombre maximal d'entrées dans une liste de préfixes, la taille maximale augmentée s'applique au quota d'entrées pour les ressources qui font référence à la liste de préfixes. Si l'une de ces ressources ne peut pas prendre en charge la taille maximale augmentée, l'opération de modification échoue et la taille maximale précédente est restaurée.

Pour modifier une liste de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Managed Prefix Lists (Listes de préfixes gérées).
3. Cochez la case correspondant à la liste de préfixes, puis choisissez Actions et Modify prefix list (Modifier la liste des préfixes).
4. Pour Nom de la liste de préfixes, entrez un nouveau nom pour la liste de préfixes.
5. Pour Entrées de liste de préfixes, choisissez Supprimer pour supprimer une entrée existante. Pour ajouter une nouvelle entrée, choisissez Ajouter une nouvelle entrée et entrez le bloc CIDR ainsi qu'une description de l'entrée.
6. Choisissez Enregistrer la liste des préfixes.

Pour modifier une liste de préfixes à l'aide du AWS CLI

Utilisez la commande modify-managed-prefix-list.

Redimensionner une liste de préfixes

Vous pouvez redimensionner une liste de préfixes et modifier le nombre maximal d'entrées (jusqu'à 1 000). Pour plus d'informations sur les quotas de listes de préfixe gérées par le client, consultez Listes de préfixes gérées par le client.

Pour redimensionner une liste de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Managed Prefix Lists (Listes de préfixes gérées).
3. Cochez la case correspondant à la liste de préfixes, puis choisissez Actions et Redimensionner la liste des préfixes).
4. Pour Nex max entries (Nouvelles entrées max), entrez une valeur.

5. Choisissez Redimensionner.

Pour redimensionner une liste de préfixes à l'aide du AWS CLI

Utilisez la commande modify-managed-prefix-list.

Restaurer une version précédente d'une liste de préfixes

Vous pouvez restaurer les entrées d'une version précédente de votre liste de préfixes. Cela a pour effet de créer une nouvelle version de la liste de préfixes.

Si vous avez réduit la taille de la liste de préfixes, vous devez vérifier que la liste de préfixes est suffisamment grande pour contenir les entrées de la version précédente.

Pour restaurer une version précédente d'une liste de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Managed Prefix Lists (Listes de préfixes gérées).
3. Cochez la case correspondant à la liste de préfixes, puis choisissez Actions et Restore prefix list (Restaurer la liste des préfixes).
4. Pour Select prefix list version (Sélectionner la version de liste de préfixes), choisissez une version précédente. Les entrées de la version sélectionnée s'affichent dans Prefix list entries (Entrées de liste de préfixes.
5. Choisissez Restaurer la liste des préfixes.

Pour restaurer une version précédente d'une liste de préfixes à l'aide du AWS CLI

Utilisez la commande restore-managed-prefix-list-version.

Supprimer une liste de préfixes

Pour supprimer une liste de préfixes, vous devez d'abord supprimer toute référence à celle-ci dans vos ressources (par exemple dans vos tables de routage). Si vous avez partagé la liste de préfixes à l'aide d' AWS RAM, toutes les références dans les ressources appartenant au consommateur doivent d'abord être supprimées.

Limitation

Vous ne pouvez pas supprimer une liste de AWS préfixes gérée par -managed.

Pour supprimer une liste de préfixes à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Instances gérées.
3. Sélectionnez la liste des préfixes, puis choisissez Actions, Supprimer la liste des préfixes.
4. Dans le champ de confirmation, entrez `delete`, puis choisissez Supprimer.

Pour supprimer une liste de préfixes à l'aide du AWS CLI

Utilisez la commande delete-managed-prefix-list.

Utiliser des listes AWS de préfixes gérées

AWS-les listes de préfixes gérées sont des ensembles de plages d'adresses IP pour les AWS services.

Table des matières

Utiliser une liste AWS de préfixes gérée

AWS-les listes de préfixes gérées sont créées et maintenues par AWS et peuvent être utilisées par toute personne possédant un AWS compte. Vous ne pouvez pas créer, modifier, partager ou supprimer une liste de AWS préfixes gérée.

Comme pour les listes de préfixes gérées par le client, vous pouvez utiliser des listes de préfixes AWS gérées avec des AWS ressources telles que des groupes de sécurité et des tables de routage. Pour plus d'informations, consultez Listes de préfixes de référence dans vos ressources AWS.

Pondération de la liste de préfixes gérée par AWS

Le poids d'une liste de préfixes AWS gérée fait référence au nombre d'entrées qu'elle occupe dans une ressource.

Par exemple, le poids d'une liste de CloudFront préfixes gérée par Amazon est de 55. Voici comment cela affecte vos quotas Amazon VPC :

- Groupes de sécurité : le quota par défaut est de 60 règles, ce qui laisse de la place pour seulement 5 règles supplémentaires dans un groupe de sécurité. Vous pouvez demander une augmentation de ce quota.
- Tables de routage : le quota par défaut est de 50 routes, vous devez donc demander une augmentation de quota avant de pouvoir ajouter la liste de préfixes à une table de routage.

Listes AWS de préfixes gérées disponibles

Les services suivants fournissent des listes AWS de préfixes gérées.

Service AWS	Nom de la liste des préfixes	Weight
Amazon CloudFront	com.amazonaws.global.cloudfront.origin-facing	55
Amazon DynamoDB	com.amazonaws.*region*.dynamodb	1
AWS Ground Station	com.amazonaws.global.groundstation	5
Amazon Route 53	com.amazonaws.*region*.ipv6.route53-healthchecks	25
	com.amazonaws.*region*.route53-healthchecks	25
Amazon S3	com.amazonaws.*region*.s3	1
Amazon S3 Express One Zone	com.amazonaws.*region*.s3express	6
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice	10
	com.amazonaws.*region*.ipv6.vpc-lattice	10

Pour afficher les listes de AWS préfixes gérées à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Listes de préfixes gérées.
3. Dans le champ de recherche, ajoutez le filtre Owner ID: AWS (ID propriétaire :).

Pour afficher les listes de AWS préfixes gérées à l'aide du AWS CLI

Utilisez la commande describe-managed-prefix-lists comme suit.

```
aws ec2 describe-managed-prefix-lists --filters Name=owner-id,Values=AWS
```

Utiliser des listes de préfixes partagées

Avec AWS Resource Access Manager (AWS RAM), le propriétaire d'une liste de préfixes peut partager une liste de préfixes avec les éléments suivants :

- AWS Comptes spécifiques à l'intérieur ou à l'extérieur de son organisation dans AWS Organizations
- Une unité organisationnelle au sein de son organisation dans AWS Organizations
- Toute une organisation dans AWS Organizations

Les consommateurs avec lesquels une liste de préfixes a été partagée peuvent consulter la liste de préfixes et ses entrées, et ils peuvent y faire référence dans leurs ressources. AWS

Pour plus d'informations AWS RAM, consultez le guide de AWS RAM l'utilisateur.

Table des matières

Conditions préalables au partage de listes de préfixes

- Pour partager une liste de préfixes, vous devez en être propriétaire. Vous ne pouvez pas partager un projet qui a été partagé avec vous. Vous ne pouvez pas partager une AWS liste de préfixes gérée.

- Pour partager une liste de préfixes avec votre organisation ou une unité d'organisation dans AWS Organizations, vous devez activer le partage avec AWS Organizations. Pour de plus amples informations, veuillez consulter Activer le partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM .

Partager une liste de préfixes

Pour partager une liste de préfixes, vous devez l'ajouter à un partage de ressources. Si vous n'avez pas de partage de ressources, vous devez d'abord en créer un à l'aide de la console AWS RAM.

Si vous faites partie d'une organisation et que le partage au sein de votre organisation est activé, les consommateurs de votre organisation ont automatiquement accès à la liste de préfixes partagée. AWS Organizations Dans le cas contraire, les consommateurs reçoivent une invitation pour rejoindre le partage de ressources et ont accès à la liste de préfixes partagés après avoir accepté l'invitation.

Vous pouvez créer un partage de ressources et partager une liste de préfixes que vous possédez à l'aide de la console AWS RAM ou de l' AWS CLI.

Pour créer un partage de ressources et partager une liste de préfixes à l'aide de la console AWS RAM

Suivez les étapes décrites dans la section Créer un partage de ressources du Guide de l'utilisateur AWS RAM . Pour Sélectionner le type de ressource, choisissez Listes de préfixes, puis activez la case à cocher de votre liste de préfixes.

Pour ajouter une liste de préfixes à un partage de ressources existant à l'aide de la console AWS RAM

Pour ajouter un préfixe géré que vous possédez à un partage de ressources existant, suivez les étapes décrites dans la section Mise à jour d'un partage de ressources du Guide de l'utilisateur AWS RAM . Pour Sélectionner le type de ressource, choisissez Listes de préfixes, puis activez la case à cocher de votre liste de préfixes.

Pour partager une liste de préfixes dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez les commandes suivantes pour créer et mettre à jour un partage de ressources :

- create-resource-share
- associate-resource-share
- update-resource-share

Identifier une liste de préfixes partagée

Les propriétaires et les utilisateurs peuvent identifier les listes de préfixes partagées à l'aide de la console Amazon VPC et la AWS CLI.

Pour identifier une liste de préfixes partagée à l'aide de la console Amazon VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Instances gérées.
3. La page affiche les listes de préfixes que vous possédez et les listes de préfixes qui sont partagées avec vous. La colonne ID propriétaire affiche l'ID de compte AWS du propriétaire de la liste de préfixes.
4. Pour afficher les informations sur le partage de ressources d'une liste de préfixes, sélectionnez la liste de préfixes et choisissez Partage dans le volet inférieur.

Pour identifier une liste de préfixes partagée à l'aide du AWS CLI

Utilisez la commande describe-managed-prefix-lists. La commande renvoie les listes de préfixes que vous possédez et les listes de préfixes partagées avec vous. `OwnerId`indique l'ID de AWS compte du propriétaire de la liste de préfixes.

Identifier des références à une liste de préfixes partagée

Les propriétaires peuvent identifier les ressources appartenant au consommateur qui font référence à une liste de préfixes partagée.

Pour identifier les références à une liste de préfixes partagée à l'aide de la console Amazon VPC.

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Instances gérées.
3. Sélectionnez la liste des préfixes et choisissez Associations dans le volet inférieur.
4. Les ID des ressources qui font référence à la liste des préfixes sont répertoriés dans la colonne ID de ressource. Les propriétaires des ressources sont répertoriés dans la colonne Propriétaire de la ressource.

Pour identifier les références à une liste de préfixes partagée à l'aide du AWS CLI

Utilisez la commande get-managed-prefix-list-associations.

Annuler le partage d'une liste de préfixes partagée

Lorsque vous départagez une liste de préfixes, les utilisateurs ne peuvent plus afficher la liste de préfixes ou ses entrées dans leur compte, et ils ne peuvent pas référencer la liste de préfixes dans leurs ressources. Si la liste des préfixes est déjà référencée dans les ressources du consommateur, ces références continuent de fonctionner normalement et vous pouvez continuer à afficher ces références. Si vous mettez à jour la liste de préfixes vers une nouvelle version, les références utilisent la dernière version.

Pour annuler le partage d'une liste de préfixes partagée dont vous êtes le propriétaire, vous devez la supprimer du partage de ressources à l'aide de. AWS RAM

Pour annuler le partage d'une liste de préfixes partagée dont vous êtes propriétaire à l'aide de la console AWS RAM

Consultez la section Mise à jour d'un partage de ressources du Guide de l'utilisateur AWS RAM .

Pour annuler le partage d'une liste de préfixes partagée dont vous êtes le propriétaire à l'aide du AWS CLI

Utilisez la commande disassociate-resource-share.

Autorisations de liste de préfixes partagées

Autorisations accordées aux propriétaires

Les propriétaires sont responsables de la gestion d'une liste de préfixes partagée et de ses entrées. Les propriétaires peuvent consulter les identifiants des AWS ressources qui font référence à la liste de préfixes. Cependant, ils ne peuvent pas ajouter ou supprimer des références à une liste de préfixes dans les AWS ressources détenues par des consommateurs.

Les propriétaires ne peuvent pas supprimer une liste de préfixes si la liste de préfixes est référencée dans une ressource appartenant à un consommateur.

Autorisations accordées aux consommateurs

Les consommateurs peuvent consulter les entrées d'une liste de préfixes partagée, et ils peuvent faire référence à une liste de préfixes partagée dans leurs AWS ressources. Toutefois, les consommateurs ne peuvent pas modifier, restaurer ou supprimer une liste de préfixes partagés.

Facturation et mesures

Il n'y a pas de frais supplémentaires pour le partage des listes de préfixes.

Quotas pour AWS RAM

Pour de plus amples informations, veuillez consulter Service Quotas.

Listes de préfixes de référence dans vos ressources AWS

Vous pouvez faire référence à une liste de préfixes dans les AWS ressources suivantes.

Ressources

- Groupes de sécurité VPC
- Tables de routage des sous-réseaux
- Tables de routage de passerelle de transit
- AWS Network Firewall groupes de règles
- Contrôle d'accès réseau Amazon Managed Grafana
- AWS Outposts suivre les passerelles locales

Groupes de sécurité VPC

Vous pouvez spécifier une liste de préfixes comme source d'une règle entrante ou comme destination d'une règle sortante. Pour plus d'informations, consultez Groupes de sécurité.

Pour référencer une liste de préfixes dans une règle de groupe de sécurité à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité à mettre à jour.
4. Choisissez Actions, Edit inbound rules (Modifier les règles entrantes) or Actions, Edit outbound rules (Modifier les règles sortantes).
5. Choisissez Add rule. Pour Type, sélectionnez le type de trafic. Pour Source (règles entrantes) ou Destination (règles sortantes), choisissez l'ID de la liste des préfixes.
6. Sélectionnez Enregistrer les règles.

Pour référencer une liste de préfixes dans une règle de groupe de sécurité à l'aide du AWS CLI

Utilisez les authorize-security-group-egresscommandes authorize-security-group-ingresset. Pour le paramètre `--ip-permissions`, spécifiez l'ID de la liste de préfixes à l'aide d'`PrefixListIds`.

Tables de routage des sous-réseaux

Vous pouvez spécifier une liste de préfixes comme destination de l'entrée de table de routage. Vous ne pouvez pas référencer une liste de préfixes dans une table de routage de passerelle. Pour plus d'informations sur les tables de routage, consultez Configuration des tables de routage.

Pour référencer une liste de préfixes dans une table de routage à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage et sélectionnez la table de routage.
3. Choisissez Actions, Modifier les routes.
4. Pour ajouter une route, choisissez Add route (Ajouter une route).
5. Pour Destination, entrez l'ID d'une liste de préfixes.
6. Pour Cible, choisissez une cible.
7. Sélectionnez Enregistrer les modifications.

Pour référencer une liste de préfixes dans une table de routage à l'aide du AWS CLI

Utilisez la commande create-route (AWS CLI). Utilisez le paramètre `--destination-prefix-list-id` pour spécifier l'ID d'une liste de préfixes.

Tables de routage de passerelle de transit

Vous pouvez spécifier une liste de préfixes comme destination d'un itinéraire. Pour de plus amples informations, veuillez consulter Références de liste de préfixes dans Passerelles de transit Amazon VPC.

AWS Network Firewall groupes de règles

Un groupe de AWS Network Firewall règles est un ensemble de critères réutilisables pour inspecter et gérer le trafic réseau. Si vous créez des groupes de règles dynamiques compatibles avec Suricata dans AWS Network Firewall, vous pouvez référencer une liste de préfixes à partir du groupe de règles. Pour de plus amples informations, veuillez consulter Référencement des listes de préfixes Amazon VPC et Créer un groupe de règles avec état dans le AWS Network Firewall Manuel du développeur.

Contrôle d'accès réseau Amazon Managed Grafana

Vous pouvez spécifier une ou plusieurs listes de préfixes en tant que règle entrante pour les demandes destinées aux espaces de travail Amazon Managed Grafana. Pour plus d'informations sur le contrôle d'accès réseau d'espace de travail Grafana, notamment sur la manière de référencer des listes de préfixes, veuillez consulter la section Gestion de l'accès réseau (français non garanti) du Guide de l'utilisateur Amazon Managed Grafana (français non garanti).

AWS Outposts suivre les passerelles locales

Chaque AWS Outposts rack fournit une passerelle locale qui vous permet de connecter les ressources de votre Outpost à vos réseaux locaux. Vous pouvez regrouper les CIDR que vous utilisez fréquemment dans une liste de préfixes et référencer cette liste en tant que cible de route dans la table de routage de votre passerelle locale. Pour plus d'informations, voir Gérer les itinéraires des tables de routage des passerelles locales dans le Guide de AWS Outposts l'utilisateur pour les racks.

AWS Plages d'adresses IP

AWS publie ses plages d'adresses IP actuelles au format JSON. Grâce à ces informations, vous pouvez identifier le trafic provenant de AWS. Vous pouvez également utiliser ces informations pour autoriser ou refuser le trafic à destination ou en provenance de certains AWS services.

> **Note**
>
> - Seules certaines plages d'adresses IP de AWS service sont publiées dans ip-ranges.json ; nous publions les plages d'adresses IP des services sur lesquels les clients souhaitent généralement effectuer un filtrage de sortie.
> - Les services peuvent utiliser les plages d'adresses IP pour communiquer avec d'autres services ou les services peuvent utiliser les plages d'adresses IP pour communiquer avec le réseau d'un client.

Pour afficher les plages actuelles, téléchargez le fichier `.json`. Pour conserver l'historique, enregistrez les versions successives du fichier `.json` sur votre système. Pour déterminer si des modifications ont été apportées depuis la dernière fois que vous avez enregistré le fichier, vérifiez l'heure de publication du fichier actuel et comparez-la à l'heure de publication du dernier fichier que vous avez enregistré.

Les plages d'adresses IP que vous transférez AWS via Bring Your Own IP addresses (BYOIP) ne sont pas incluses dans le `.json` fichier.

Certains services publient également leurs plages d'adresses à l'aide de listes de AWS préfixes gérées par -managed. Pour plus d'informations, consultez the section called "Listes AWS de préfixes gérées disponibles".

Table des matières

Téléchargement

Téléchargez ip-ranges.json .

Si vous accédez à ce fichier par programmation, vous êtes tenu de vous s'assurer que l'application télécharge le fichier seulement après avoir correctement vérifié le certificat TLS présenté par le serveur.

Syntaxe

La syntaxe d'`ip-ranges.json` est la suivante.

```
{
  "syncToken": "0123456789",
  "createDate": "yyyy-mm-dd-hh-mm-ss",
  "prefixes": [
    {
      "ip_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
```

```
    }
  ],
  "ipv6_prefixes": [
    {
      "ipv6_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ]
}
```

syncToken

L'heure de publication, au format d'heure Unix epoch.

Type : chaîne

Exemple : `"syncToken": "1416435608"`

createDate

Date et heure de publication, au format UTC YY-MM-DD-. hh-mm-ss

Type : chaîne

Exemple : `"createDate": "2014-11-19-23-29-02"`

prefixes

Les préfixes IP pour les plages d'adresses IPv4.

Type : Array

ipv6_prefixes

Les préfixes IP pour les plages d'adresses IPv6.

Type : Array

ip_prefix

La plage d'adresses IPv4 publiques, en notation CIDR. Notez que cela AWS peut annoncer un préfixe dans des plages plus spécifiques. Par exemple, le préfixe 96.127.0.0/17 du fichier peut être annoncé comme 96.127.0.0/21, 96.127.8.0/21, 96.127.32.0/19 et 96.127.64.0/18.

Type : chaîne

Exemple : `"ip_prefix": "198.51.100.2/24"`

ipv6_prefix

La plage d'adresses IPv6 publiques, en notation CIDR. Notez que cela AWS peut annoncer un préfixe dans des plages plus spécifiques.

Type : chaîne

Exemple : `"ipv6_prefix": "2001:db8:1234::/64"`

network_border_group

Le nom du groupe frontalier du réseau, qui est un ensemble unique de zones de disponibilité ou de zones locales à partir duquel les AWS adresses IP sont publiées, ou`GLOBAL`. Le trafic pour les `GLOBAL` services peut être attiré ou provenir de plusieurs (jusqu'à toutes) zones de disponibilité ou zones locales à partir desquelles les adresses IP AWS sont publiées.

Type : chaîne

Exemple : `"network_border_group": "us-west-2-lax-1"`

region

La AWS région ou`GLOBAL`. Le trafic `GLOBAL` lié aux services peut être attiré ou provenir de plusieurs AWS régions (jusqu'à toutes).

Type : chaîne

Valeurs valides : `af-south-1` | `ap-east-1` | `ap-northeast-1` | `ap-northeast-2` | `ap-northeast-3` | `ap-south-1` | `ap-south-2` | `ap-southeast-1` | `ap-southeast-2` | `ap-southeast-3` | `ap-southeast-4` | `ca-central-1` | `cn-north-1` | `cn-northwest-1` | `eu-central-1` | `eu-central-2` | `eu-north-1` | `eu-south-1` | `eu-south-2` | `eu-west-1` | `eu-west-2` | `eu-west-3` | `me-central-1` | `me-south-1` | `sa-east-1` | `us-east-1` | `us-east-2` | `us-gov-east-1` | `us-gov-west-1` | `us-west-1` | `us-west-2` | `GLOBAL`

Exemple : `"region": "us-east-1"`

web

Le sous-ensemble des plages d'adresses IP. Les adresses répertoriées pour `API_GATEWAY` sont des adresses de sortie uniquement. Spécifiez `AMAZON` pour obtenir toutes les plages d'adresses IP (ce qui signifie que chaque sous-ensemble se trouve également dans le sous-ensemble

AMAZON). Cependant, certaines plages d'adresses IP se trouvent uniquement dans le sous-ensemble AMAZON (ce qui signifie qu'elles ne sont pas disponibles dans un autre sous-ensemble).

Type : chaîne

Valeurs valides : AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | IVS_REALTIME | KINESIS_VIDEO_STREAMS | MEDIA_PACKAGE_V2 | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS

Exemple : `"service": "AMAZON"`

Chevauchements de plages

Les plages d'adresses IP renvoyées par n'importe quel code de service sont également renvoyées par le code de service AMAZON. Par exemple, toutes les plages d'adresses IP renvoyées par le code de service S3 sont également renvoyées par le code de service AMAZON.

Lorsque le service A utilise des ressources du service B, certaines plages d'adresses IP sont renvoyées par les codes de service du service A et du service B. Toutefois, ces plages d'adresses IP sont utilisées exclusivement par le service A et ne peuvent pas être utilisées par le service B. Par exemple, Amazon S3 utilise des ressources d'Amazon EC2. Certaines plages d'adresses IP sont donc renvoyées à la fois par les codes de service S3 et EC2. Toutefois, ces plages d'adresses IP sont utilisées exclusivement par Amazon S3. Par conséquent, le code de service S3 renvoie toutes les plages d'adresses IP utilisées exclusivement par Amazon S3. Pour identifier les plages d'adresses IP utilisées exclusivement par Amazon EC2, recherchez les plages d'adresses IP renvoyées par le code de service EC2 mais pas le code de service S3.

Filtrage du fichier JSON

Vous pouvez télécharger un outil de ligne de commande pour vous aider à ne filtrer que les informations que vous recherchez.

Windows

Les AWS Tools for Windows PowerShell incluent une applet de commande, `Get-AWSPublicIpAddressRange` pour analyser ce fichier JSON. Les exemples suivants illustrent son

utilisation. Pour plus d'informations, voir Interroger les plages d'adresses IP publiques pour AWS et Get- AWSPublicIpAddressRange.

Example 1. Obtenir la date de création

```
PS C:\> Get-AWSPublicIpAddressRange -OutputPublicationDate

Wednesday, August 22, 2018 9:22:35 PM
```

Example 2. Obtenir l'information pour une région spécifique

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1

IpPrefix        Region      NetworkBorderGroup         Service
--------        ------       -------                   -------
23.20.0.0/14    us-east-1    us-east-1                 AMAZON
50.16.0.0/15    us-east-1    us-east-1                 AMAZON
50.19.0.0/16    us-east-1    us-east-1                 AMAZON
...
```

Example 3. Obtenir toutes les adresses IP

```
PS C:\> (Get-AWSPublicIpAddressRange).IpPrefix
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
2406:da00:ff00::/64
2600:1fff:6000::/40
2a01:578:3::/64
2600:9000::/28
```

Example 4. Obtenir toutes les adresses IPv4

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv4"} | select
 IpPrefix

IpPrefix
--------
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
```

```
...
```

Example 5. Obtenir toutes les adresses IPv6

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv6"} | select
 IpPrefix

IpPrefix
--------
2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

Example 6. Obtenir toutes les adresses IP pour un service spécifique

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey CODEBUILD | select IpPrefix

IpPrefix
--------
52.47.73.72/29
13.55.255.216/29
52.15.247.208/29
...
```

Linux

Les exemples de commandes suivantes utilisent l'outil jq pour analyser une copie locale du fichier JSON.

Example 1. Obtenir la date de création

```
$ jq .createDate < ip-ranges.json

"2016-02-18-17-22-15"
```

Example 2. Obtenir l'information pour une région spécifique

```
$ jq '.prefixes[] | select(.region=="us-east-1")' < ip-ranges.json

{
  "ip_prefix": "23.20.0.0/14",
```

```
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.16.0.0/15",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.19.0.0/16",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
...
```

Example 3. Obtenir toutes les adresses IPv4

```
$ jq -r '.prefixes | .[].ip_prefix' < ip-ranges.json

23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

Example 4. Obtenir toutes les adresses IPv6

```
$ jq -r '.ipv6_prefixes | .[].ipv6_prefix' < ip-ranges.json

2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

Example 5. Obtenir toutes les adresses IPv4 pour un service spécifique

```
$ jq -r '.prefixes[] | select(.service=="CODEBUILD") | .ip_prefix' < ip-ranges.json

52.47.73.72/29
13.55.255.216/29
```

```
52.15.247.208/29
...
```

Example 6. Obtenir toutes les adresses IPv4 pour un service spécifique dans une région spécifique

```
$ jq -r '.prefixes[] | select(.region=="us-east-1") | select(.service=="CODEBUILD")
 | .ip_prefix' < ip-ranges.json

34.228.4.208/28
```

Example 7. Obtention d'informations sur un groupe de bordure réseau spécifique

```
$ jq -r '.prefixes[] | select(.region=="us-west-2") |
 select(.network_border_group=="us-west-2-lax-1") | .ip_prefix' < ip-ranges.json
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

Implémentation du contrôle de sortie

Pour autoriser les ressources que vous avez créées avec un AWS service à accéder uniquement aux autres AWS services, vous pouvez utiliser les informations de plage d'adresses IP du fichier ip-ranges.json pour effectuer un filtrage de sortie. Assurez-vous que les règles du groupe de sécurité autorisent le trafic sortant vers les blocs CIDR de la liste AMAZON. Il existe des quotas pour les groupes de sécurité. En fonction du nombre de plages d'adresses IP dans chaque Région, vous pouvez avoir besoin de plusieurs groupes de sécurité par Région.

> **Note**
>
> Certains AWS services sont basés sur EC2 et utilisent l'espace d'adressage IP EC2. Si vous bloquez le trafic vers l'espace d'adresses IP EC2, vous bloquez également le trafic vers ces services qui ne sont pas basés sur EC2.

AWS Notifications relatives aux plages d'adresses IP

Chaque fois que les plages d'adresses AWS IP sont modifiées, nous envoyons des notifications aux abonnés du `AmazonIpSpaceChanged` sujet. La charge utile contient des informations au format suivant :

```
{
  "create-time":"yyyy-mm-ddThh:mm:ss+00:00",
  "synctoken":"0123456789",
  "md5":"6a45316e8bc9463c9e926d5d37836d33",
  "url":"https://ip-ranges.amazonaws.com/ip-ranges.json"
}
```

create-time

La date et l'heure de création.

Les notifications peuvent être diffusées dans le désordre. Par conséquent, nous vous recommandons de vérifier les horodatages pour vous assurer que l'ordre est correct.

synctoken

L'heure de publication, au format d'heure Unix epoch.

md5

La valeur de hachage de chiffrement du fichier `ip-ranges.json`. Vous pouvez utiliser cette valeur pour vérifier si le fichier téléchargé est corrompu.

url

L'emplacement du fichier `ip-ranges.json`.

Si vous souhaitez être averti chaque fois qu'une modification est apportée aux plages d'adresses AWS IP, vous pouvez vous abonner comme suit pour recevoir des notifications via Amazon SNS.

Pour vous abonner aux notifications relatives aux plages d'adresses AWS IP

1. Ouvrez la console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez sélectionner cette région, car les notifications SNS auxquelles vous vous abonnez ont été créées dans cette région.
3. Dans le panneau de navigation, choisissez Abonnements.
4. Choisissez Créer un abonnement.
5. Dans la boîte de dialogue Créer un abonnement, exécutez l'une des actions suivantes :

a. Pour ARN de la rubrique, copiez l'Amazon Resource Name (ARN) suivant :

```
arn:aws:sns:us-east-1:806199016981:AmazonIpSpaceChanged
```

b. Pour Protocole, choisissez le protocole à utiliser (par exemple, `Email`).

c. Pour Point de terminaison, tapez le point de terminaison qui recevra la notification (par exemple, votre adresse e-mail).

d. Choisissez Créer un abonnement.

6. Vous allez être contacté sur le point de terminaison que vous avez spécifié et sur lequel vous avez été invité à confirmer votre abonnement. Par exemple, si vous avez spécifié une adresse e-mail, vous recevrez un message électronique avec l'objet `AWS Notification - Subscription Confirmation`. Suivez les instructions pour confirmer votre abonnement.

Les notifications sont soumises à la disponibilité du point de terminaison. Par conséquent, vous voudrez peut-être consulter le fichier JSON régulièrement pour vérifier que vous disposez bien des dernières plages d'adresses. Pour plus d'informations sur la fiabilité d'Amazon SNS, consultez https://aws.amazon.com/sns/faqs/#Reliability.

Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

Pour vous désabonner des notifications relatives aux plages d'adresses AWS IP

1. Ouvrez la console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Dans le panneau de navigation, choisissez Abonnements.
3. Cochez la case correspondant à l'abonnement.
4. Dans le menu Actions, choisissez Supprimer des abonnements.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour plus d'informations sur Amazon SNS, consultez le Guide du développeur d'Amazon Simple Notification Service.

Notes de mise à jour

Le tableau suivant décrit les mises à jour de la syntaxe de `ip-ranges.json`. Nous ajoutons également de nouveaux codes de région à chaque lancement de région.

Description	Date de publication
Ajout du code de service `IVS_REALTIME` .	11 juin 2024
Ajout du code de service `MEDIA_PACKAGE_V2` .	9 mai 2023
Ajout du code de service `CLOUDFRONT_ORIGIN_FACING` .	12 octobre 2021
Ajout du code de service `ROUTE53_RESOLVER` .	24 juin 2021
Ajout du code de service `EBS`.	12 mai 2021
Ajout du code de service `KINESIS_VIDEO_STREAMS` .	19 novembre 2020
Ajout des codes de service `CHIME_MEETINGS` et `CHIME_VOICECONNECTOR` .	19 juin 2020
Ajout du code de service `AMAZON_APPFLOW` .	9 juin 2020
Ajout de la prise en charge du groupe de bordure réseau.	7 avril 2020
Ajout du code de service `WORKSPACES_GATEWAYS` .	30 mars 2020
Ajout du code de service `ROUTE53_HEALTHCHECK_PUBLISHING` .	30 janvier 2020
Ajout du code de service `API_GATEWAY` .	26 septembre 2019

Description	Date de publication
Ajout du code de service `EC2_INSTANCE_CONNECT` .	26 juin 2019
Ajout du code de service `DYNAMODB`.	25 avril 2019
Ajout du code de service `GLOBALACCELERATOR` .	20 décembre 2018
Ajout du code de service `AMAZON_CONNECT` .	le 20 juin 2018
Ajout du code de service `CLOUD9`.	le 20 juin 2018
Ajout du code de service `CODEBUILD` .	19 avril 2018
Ajout du code de service `S3`.	28 février 2017
Ajout de la prise en charge des plages d'adresses IPv6.	22 août 2016
Première version	19 novembre 2014

En savoir plus

- `AMAZON_APPFLOW` – Plages d'adresses IP
- `AMAZON_CONNECT` – Configurer votre réseau
- `CHIME_MEETINGS` – Configuration pour les médias et la signalisation
- `CLOUDFRONT`— Emplacements et plages d'adresses IP des serveurs CloudFront périphériques
- `DYNAMODB` – Plages d'adresses IP
- `EC2` – Adresses IPv4 publiques
- `EC2_INSTANCE_CONNECT` – Prérequis pour EC2 Instance Connect
- `GLOBALACCELERATOR` – Emplacement et plages d'adresses IP de serveurs périphériques Global Accelerator
- `ROUTE53` – Plages d'adresses IP de serveurs Amazon Route 53
- `ROUTE53_HEALTHCHECKS` – Plages d'adresses IP de serveurs Amazon Route 53

- `ROUTE53_HEALTHCHECKS_PUBLISHING` – Plages d'adresses IP de serveurs Amazon Route 53
- `WORKSPACES_GATEWAYS`— Serveurs de passerelle PCoIP

Ajoutez le support IPv6 à votre VPC

Si vous avez un VPC existant qui prend uniquement en charge IPv4 et que les ressources de votre sous-réseau sont configurées pour utiliser uniquement IPv4, vous pouvez ajouter le support IPv6 à votre VPC et à vos ressources. Votre VPC peut fonctionner en mode double pile : vos ressources peuvent communiquer via IPv4, IPv6 ou les deux. Les communications IPv4 et IPv6 sont indépendantes l'une de l'autre.

Vous ne pouvez pas désactiver la prise en charge d'IPv4 de votre VPC et de vos sous-réseaux ; il s'agit du système d'adressage IP par défaut pour Amazon VPC et Amazon EC2.

Considérations

- Il n'existe aucun chemin de migration des sous-réseaux IPv4 uniquement vers des sous-réseaux IPv6 uniquement.
- Cet exemple part du principe que vous disposez d'un VPC existant avec des sous-réseaux publics et privés. Pour plus d'informations sur la création d'un VPC à utiliser avec IPv6, veuillez consulter the section called “Création d'un VPC”.
- Avant de commencer à utiliser IPv6, assurez-vous d'avoir lu les fonctionnalités de l'adressage IPv6 pour Amazon VPC :. Comparez l'IPv4 et l'IPv6

Processus

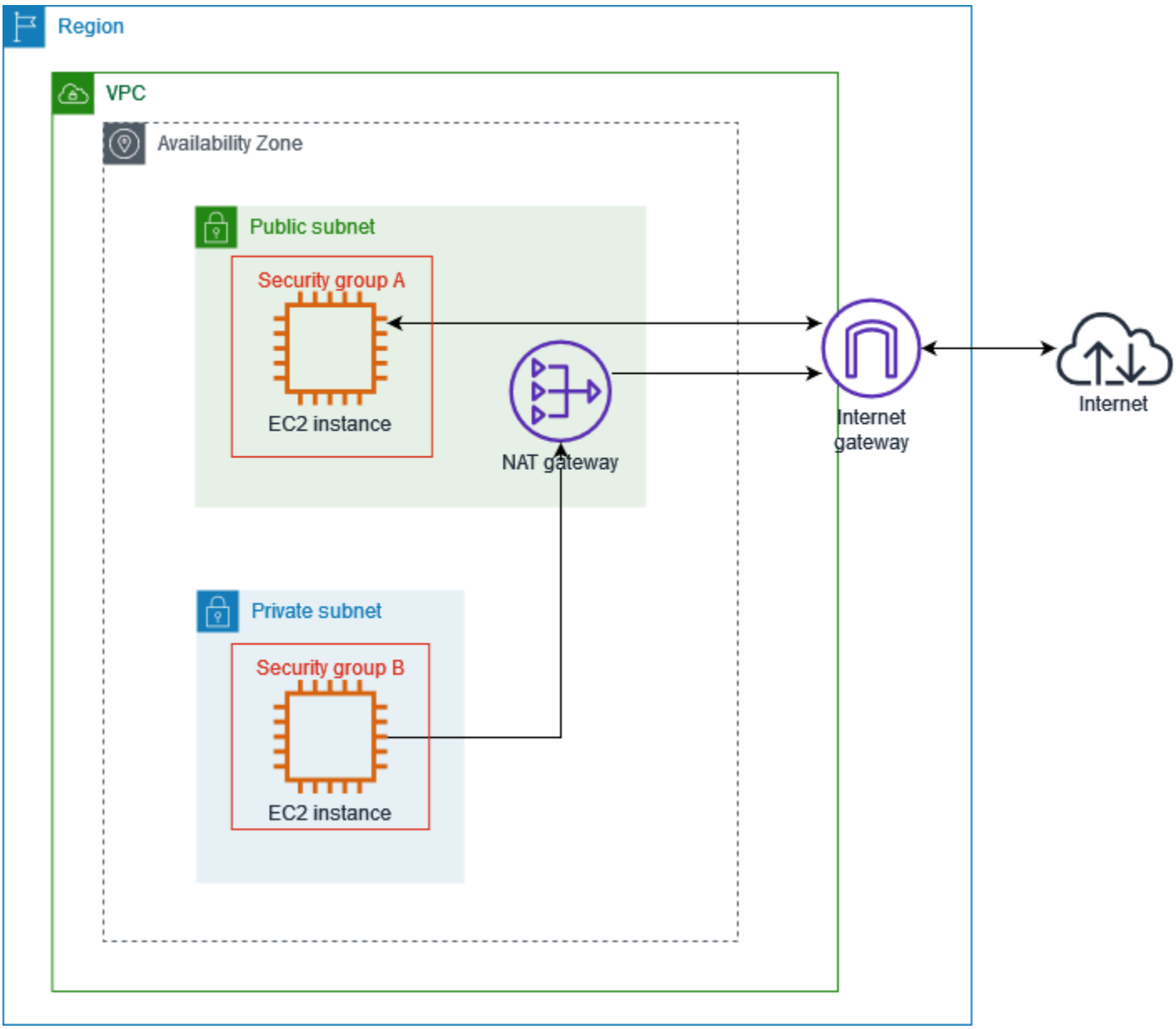
Le tableau suivant fournit une présentation du processus d'activation d'IPv6 pour votre VPC.

Étape	Remarques
Étape 1 : Associer un bloc d'adresse CIDR IPv6 à votre VPC et vos sous-réseaux	Associez un bloc d'adresse CIDR d'IPv6 ou BYOIP fourni par Amazon avec votre VPC et vos sous-réseaux.
Étape 2 : Mettre à jour vos tables de routage	Mettez à jour vos tables de routage pour acheminer le trafic IPv6. Pour un sous-rése au public, créez un routage qui achemine

Étape	Remarques
	l'ensemble du trafic IPv6 du sous-réseau vers la passerelle Internet. Pour un sous-réseau privé, créez un routage qui achemine l'ensembl e du trafic IPv6 Internet entrant du sous-rése au vers une passerelle Internet de sortie uniquement.
Étape 3 : Mettre à jour les règles de votre groupe de sécurité	Mettez à jour vos règles de groupe de sécurité pour inclure les règles des adresses IPv6. Cela active le trafic d'IPv6 en provenance ou à destination de vos instances. Si vous avez créé des règles ACL réseau personnalisées pour contrôler le flux du trafic à destination et en provenance de votre sous-réseau, vous devez inclure les règles de trafic IPv6.
Étape 4 : Attribuer des adresses IPv6 à vos instances	Attribuez des adresses IPv6 à vos instances à partir de la plage d'adresses IPv6 de votre sous-réseau.

Exemple : activer IPv6 dans un VPC avec un sous-réseau public et privé

Dans cet exemple, votre VPC dispose d'un sous-réseau public et un privé. Vous disposez d'une instance de base de données de votre sous-réseau privé ayant des communications sortantes avec Internet via une passerelle NAT de votre VPC. Vous disposez d'un serveur web public dans votre sous-réseau public ayant accès à Internet via la passerelle Internet. Le schéma suivant présente l'architecture de votre VPC.



Le groupe de sécurité de votre serveur web (par exemple avec l'ID de groupe de sécurité `sg-11aa22bb11aa22bb1`) comporte les règles de trafic entrant suivantes :

Type	Protocole	Plage de ports	Source	Commentaire
Tout le trafic	Tous	Tous	sg-33cc44 dd33cc44dd3	Autorisez l'accès entrant pour tout le trafic à partir des instances associées à

Type	Protocole	Plage de ports	Source	Commentaire
				sg-33cc44 dd33cc44d d3 (l'instance de base de données).
HTTP	TCP	80	0.0.0.0/0	Autorise le trafic entrant à partir d'Internet sur HTTP.
HTTPS	TCP	443	0.0.0.0/0	Autorise le trafic entrant à partir d'Internet sur HTTPS.
SSH	TCP	22	203.0.113 .123/32	Autorise l'accès SSH entrant à partir de votre ordinateur local ; par exemple, lorsque vous devez vous connecter à votre instance pour effectuer des tâches d'administration.

Le groupe de sécurité de votre instance de base de données (par exemple avec l'ID de groupe de sécurité `sg-33cc44dd33cc44dd3`) comporte la règle entrante suivante :

Type	Protocole	Plage de ports	Source	Commentaire
MySQL	TCP	3306	sg-11aa22 bb11aa22bb1	Autorise l'accès entrant pour le trafic MySQL à partir d'instanc es associées à sg-11aa22 bb11aa22bb1 (l'instance de serveur web).

Les deux groupes de sécurité comportent la règle de trafic sortant par défaut qui autorise tout le trafic IPv4 sortant, et aucune autre règle sortante.

Le type d'instance de votre serveur web est `t2.medium`. Votre serveur de base de données est une `m3.large`.

Vous voulez que votre VPC et vos ressources soient activés pour IPv6, et vous voulez qu'ils fonctionnent en mode double pile ; en d'autres termes, vous voulez utiliser l'adressage IPv6 et IPv4 entre les ressources de votre VPC et vos ressources via Internet.

Étape 1 : Associer un bloc d'adresse CIDR IPv6 à votre VPC et vos sous-réseaux

Vous pouvez associer un bloc d'adresse CIDR IPv6 à votre VPC, puis associer un bloc d'adresse CIDR `/64` à partir de cette plage à chaque sous-réseau.

Pour associer un bloc d'adresse CIDR IPv6 à un VPC

1. Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Vos VPC.
3. Sélectionnez votre VPC.
4. Choisissez Actions, Modifier les CIDR, puis Ajouter un nouveau CIDR IPv6.
5. Sélectionnez l'une des options suivantes, puis sélectionnez Sélectionner CIDR) :

- Bloc d'adresse CIDR IPv6 fourni par Amazon : utiliser un bloc d'adresse CIDR IPv6 à partir du groupe d'adresses IPv6 d'Amazon. Pour Network Border Group, choisissez le groupe à partir duquel les AWS adresses IP sont publiées.
- Bloc d'adresse CIDR IPv6 alloué par IPAM : utiliser un bloc d'adresse CIDR IPv6 à partir d'un groupe IPAM. Choisissez le groupe IPAM et le bloc d'adresse CIDR IPv6.
- Bloc d'adresse CIDR IPv6 m'appartenant : utiliser un bloc d'adresse CIDR IPv6 à partir de votre groupe d'adresses IPv6 (BYOIP). Choisissez le groupe d'adresses IPv6 et le bloc d'adresse CIDR IPv6.

6. Choisissez Fermer.

Pour associer un bloc d'adresse CIDR IPv6 à un sous-réseau

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
3. Sélectionnez un sous-réseau.
4. Choisissez Actions, Modifier les CIDR IPv6, puis Ajouter CIDR IPv6.
5. Modifiez le bloc CIDR selon vos besoins (par exemple, remplacez `00`).
6. Choisissez Enregistrer.
7. Répétez cette procédure pour tous les autres sous-réseaux dans votre VPC.

Pour plus d'informations, consultez Blocs d'adresse CIDR VPC IPv6.

Étape 2 : Mettre à jour vos tables de routage

Lorsque vous associez un bloc d'adresse CIDR IPv6 à votre VPC, nous ajoutons automatiquement une route locale à chaque table de routage pour le VPC afin d'autoriser le trafic IPv6 au sein du VPC.

Vous devez mettre à jour les tables de routage afin de permettre aux instances (comme les serveurs web) d'utiliser la passerelle Internet pour le trafic IPv6. Vous devez également mettre à jour le tables de routage de vos sous-réseaux privés afin de permettre aux instances (comme les instances de base de données) d'utiliser une passerelle Internet de sortie uniquement pour le trafic IPv6, car les passerelles NAT ne prennent pas en charge IPv6.

Pour mettre à jour la table de routage pour un sous-réseau public

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux). Sélectionnez le sous-réseau public. Dans l'onglet Table de routage, choisissez l'ID de table de routage pour ouvrir la page de détails de la table de routage.
3. Sélectionnez la table de routage. Dans l'onglet Routes, choisissez Edit routes (Modifier les routes).
4. Choisissez Ajouter une route. Choisissez `::/0` pour Destination. Choisissez l'ID de la passerelle Internet pour Cible.
5. Sélectionnez Enregistrer les modifications.

Pour mettre à jour le table de routage pour un sous-réseau privé

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Passerelles Internet de sortie uniquement. Choisissez Créer une passerelle Internet de sortie uniquement. Choisissez votre VPC parmi VPC, puis choisissez Créer une passerelle Internet de sortie uniquement.

   Pour plus d'informations, consultez Activer le trafic sortant IPv6 à l'aide de passerelles Internet de sortie uniquement.
3. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux). Sélectionnez le sous-réseau privé. Dans l'onglet Table de routage, choisissez l'ID de table de routage pour ouvrir la page de détails de la table de routage.
4. Sélectionnez la table de routage. Dans l'onglet Routes, choisissez Edit routes (Modifier les routes).
5. Choisissez Ajouter une route. Choisissez `::/0` pour Destination. Choisissez l'ID de la passerelle Internet de sortie uniquement pour Cible.
6. Sélectionnez Enregistrer les modifications.

Pour plus d'informations, consultez Exemples d'options de routage.

Étape 3 : Mettre à jour les règles de votre groupe de sécurité

Pour activer vos instances de sorte qu'elles envoient et qu'elles reçoivent du trafic sur IPv6, vous devez mettre à jour vos règles de groupe de sécurité, de sorte qu'elles comprennent des règles pour

les adresses IPv6. Par exemple, dans l'exemple ci-dessus, vous pouvez mettre à jour le groupe de sécurité du serveur Web (`sg-11aa22bb11aa22bb1`) pour ajouter des règles autorisant un accès entrant sur HTTP, HTTPS, et SSH depuis à partir des adresses IPv6. Vous n'avez pas besoin d'apporter de modifications aux règles de trafic entrant pour votre groupe de sécurité de base de données ; la règle qui autorise toutes les communications à partir de `sg-11aa22bb11aa22bb1` inclut la communication IPv6.

Pour mettre à jour les règles entrantes de votre groupe de sécurité

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Groupes de sécurité et sélectionnez le groupe de sécurité de votre serveur web.
3. Sous l'onglet Règles entrantes, choisissez Modifier les règles entrantes.
4. Pour chaque règle autorisant le trafic IPv4, choisissez Ajouter une règle et configurez la règle pour autoriser le trafic IPv6 correspondant. Par exemple, pour ajouter une règle autorisant tout le trafic HTTP sur IPv6, choisissez HTTP pour Type et `::/0` pour Source.
5. Lorsque vous avez terminé d'ajouter les règles, choisissez Enregistrer les règles.

Mettre à jour les règles sortantes de votre groupe de sécurité

Lorsque vous associez un bloc d'adresse CIDR IPv6 à votre VPC, nous ajoutons automatiquement une règle sortante aux groupes de sécurité du VPC qui autorise tout le trafic IPv6. Toutefois, si vous avez modifié les règles sortantes d'origine de votre groupe de sécurité, cette règle n'est pas ajoutée automatiquement, et vous devez ajouter des règles sortantes équivalentes pour le trafic IPv6.

Mettre à jour vos règles de liste ACL réseau

Lorsque vous associez un bloc d'adresse CIDR IPv6 à un VPC, nous ajoutons automatiquement des règles à la liste ACL réseau par défaut pour autoriser le trafic IPv6. Toutefois, si vous avez modifié votre liste ACL réseau par défaut ou si vous avez créé une liste ACL réseau personnalisée, vous devez ajouter manuellement des règles pour le trafic IPv6. Pour plus d'informations, consultez Utiliser les ACL réseau.

Étape 4 : Attribuer des adresses IPv6 à vos instances

Tous les types d'instance de la génération actuelle prennent en charge IPv6. Si votre type d'instance ne prend pas en charge IPv6, vous devez redimensionner l'instance vers un type d'instance pris en charge avant de pouvoir attribuer une adresse IPv6. Le processus que vous allez utiliser dépend de

la compatibilité du nouveau type d'instance que vous choisissez avec le type d'instance actuel. Pour plus d'informations, consultez Modifier le type d'instance dans le guide de l'utilisateur Amazon EC2. Si vous devez lancer une instance à partir d'une nouvelle AMI pour prendre en charge IPv6, vous pouvez attribuer une adresse IPv6 à votre instance pendant le lancement.

Après avoir vérifié que votre type d'instance est compatible avec IPv6, vous pouvez attribuer une adresse IPv6 à votre instance à l'aide de la console Amazon EC2. L'adresse IPv6 est attribuée à l'interface réseau principale (eth0) pour l'instance. Pour plus d'informations, consultez la section Attribuer une adresse IPv6 à une instance dans le guide de l'utilisateur Amazon EC2.

Vous pouvez vous connecter à une instance à l'aide de son adresse IPv6. Pour plus d'informations, consultez Se connecter à votre instance Linux à l'aide d'un client SSH dans le guide de l'utilisateur Amazon EC2 ou Se connecter à une instance Windows à l'aide de son adresse IPv6 dans le guide de l'utilisateur Amazon EC2.

Si vous avez lancé votre instance à l'aide d'une AMI pour une version actuelle de votre système d'exploitation, votre instance est configurée pour IPv6. Si vous ne parvenez pas à envoyer une commande ping à une adresse IPv6 depuis votre instance, consultez la documentation de votre système d'exploitation pour configurer IPv6.

AWS services prenant en charge le protocole IPv6

Les ordinateurs et les appareils intelligents utilisent des adresses IP pour communiquer entre eux via Internet et d'autres réseaux. Le développement d'Internet s'accompagne d'un besoin accru d'adresses IP. Le format le plus courant pour les adresses IP est IPv4. Le nouveau format des adresses IP est IPv6. Il fournit un espace d'adressage plus important qu'IPv4.

Services AWS la prise en charge d'IPv6 inclut la prise en charge de la configuration à double pile (IPv4 et IPv6) ou des configurations IPv6 uniquement. Par exemple, un cloud privé virtuel (VPC) est une section isolée de manière logique dans AWS Cloud laquelle vous pouvez lancer des ressources. AWS Au sein d'un VPC, vous pouvez créer des sous-réseaux IPv4 uniquement, à double pile ou IPv6 uniquement.

Services AWS prendre en charge l'accès via des points de terminaison publics. Certains prennent Services AWS également en charge l'accès à l'aide de points de terminaison privés alimentés par AWS PrivateLink. Services AWS peuvent prendre en charge l'IPv6 via leurs points de terminaison privés même s'ils ne prennent pas en charge l'IPv6 via leurs points de terminaison publics. Les points de terminaison qui prennent en charge IPv6 peuvent répondre aux requêtes DNS avec des enregistrements AAAA.

Services qui prennent en charge IPv6

Le tableau suivant répertorie ceux Services AWS qui prennent en charge le double stack, le support IPv6 uniquement et les points de terminaison compatibles IPv6. Nous mettrons à jour ce tableau au fur et à mesure de la sortie d'une prise en charge supplémentaire pour IPv6. Pour plus de détails sur la façon dont un service prend en charge IPv6, reportez-vous à la documentation du service.

Nom du service	Prise en charge de la double pile	Prise en charge d'IPv6 uniquement.	Points de terminaison publics prenant en charge IPv6	Les points de terminaison privés prennent en charge IPv6 1
AWS App Mesh	Oui	Oui	Oui	Non
Amazon AppStream 2.0	Oui	Non	Non	Non
Amazon Athena	Oui	Non	Oui	Oui
Amazon Aurora	Oui	Non	Oui	Non
AWS Cloud9	Oui	Non	Oui	

Nom du service	Prise en charge de la double pile	Prise en charge d'IPv6 uniquement.	Points de terminaison publics prenant en charge IPv6	Les points de terminaison privés prennent en charge IPv6 1
Amazon CloudFront	 Oui	 Non	 Non	
Amazon CloudWatch Logs	 O	 Non	 Oui	 Non
AWS Cloud Map	 Oui	 Oui	 Oui	 Oui
AWS Réseau WAN dans le cloud	 Oui	 Non	 Oui	 Non
Amazon Cognito	 Oui	 Non	 Oui	
AWS Database Migration Service	 Oui	 Non	 Non	 Non

Nom du service	Prise en charge de la double pile	Prise en charge d'IPv6 uniquement.	Points de terminaison publics prenant en charge IPv6	Les points de terminaison privés prennent en charge IPv6 1
AWS Direct Connect	 Oui	 Oui	 Non	
Amazon EC2	 Oui	 Oui	 Oui	 Non
Amazon ECS	 Oui	 Non	 Non	 Non
Amazon EKS	Nœuds : Oui/ Pods : Non	Capsules : Oui/ Nœuds : Non	 Non	 Non
Elastic Load Balancing	Équilibreurs de charge : oui Groupes cibles : non	Équilibreurs de charge : non Groupes cibles : oui	 Non	 Non
Amazon ElastiCache	 Oui	 Oui	 Non	 Non

Nom du service	Prise en charge de la double pile	Prise en charge d'IPv6 uniquement.	Points de terminaison publics prenant en charge IPv6	Les points de terminaison privés prennent en charge IPv6 1
AWS Fargate	 Oui	 Non	 Non	 Non
AWS Global Accelerator	 Oui	 Non	 Non	
AWS Glue	 Non	 Non	 Non	 Oui
AWS IoT	 Oui	 Non	 Oui	 Non
AWS Lake Formation	 Non	 Non	 Non	 Oui
AWS Lambda	 Oui	 Non	 Oui	 Non

Nom du service	Prise en charge de la double pile	Prise en charge d'IPv6 uniquement.	Points de terminaison publics prenant en charge IPv6	Les points de terminaison privés prennent en charge IPv6 1
Amazon Lightsail	 Oui	 Oui	 Non	
AWS Network Firewall	 Oui	 Oui	 Non	
Amazon OpenSearch Service	 Oui	 Non	 Oui	 Non
AWS PrivateLink	 Oui	 Oui	 Oui	
Amazon RDS	 Oui	 Non	 Oui	 Non
Amazon Route 53	 Oui	 Oui	 Non	

Nom du service	Prise en charge de la double pile	Prise en charge d'IPv6 uniquement.	Points de terminaison publics prenant en charge IPv6	Les points de terminaison privés prennent en charge IPv6 1
Amazon S3	 Oui	 Non	 Oui	 Non
AWS Secrets Manager	 Oui	 Non	 Oui	 Non
AWS Shield	 Oui	 Oui	 Non	
AWS Site-to-Site VPN	 Oui	 Non	 Oui	 Non
AWS Transit Gateway	 Oui	 Non	 Oui	 Non
Amazon VPC	 Oui	 Oui	 Oui	 Non

Nom du service	Prise en charge de la double pile	Prise en charge d'IPv6 uniquement.	Points de terminaison publics prenant en charge IPv6	Les points de terminaison privés prennent en charge IPv6 [1]
AWS WAF	 Oui	 Oui	 Non	
Amazon WorkSpaces	 Oui	 Non	 Non	 Non

[1] Une cellule vide indique que le service ne s'intègre pas à AWS PrivateLink.

Prise en charge supplémentaire d'IPv6

Calcul

- Amazon EC2 prend en charge le lancement d'instances basées sur le système Nitro dans des sous-réseaux IPv6 uniquement.
- Amazon EC2 fournit des points de terminaison IPv6 pour Instance Metadata Service (IMDS) et Amazon Time Sync Service.

Réseau et diffusion de contenu

- Amazon VPC prend en charge la création de sous-réseaux IPv6 uniquement.
- Amazon VPC aide les AWS ressources IPv6 à communiquer avec les ressources IPv4 en prenant en charge le DNS64 sur vos sous-réseaux et le NAT64 sur vos passerelles NAT.

Sécurité, identité et conformité

- AWS Identity and Access Management (IAM) prend en charge les adresses IPv6 dans les politiques IAM.

- Amazon Macie prend en charge les adresses IPv6 dans des données d'identification personnelle (PII)

Gestion et gouvernance

- AWS CloudTrail les enregistrements incluent les informations IPv6 source.
- AWS CLI La version v2 prend en charge le téléchargement via des connexions IPv6 pour les clients IPv6 uniquement.

En savoir plus

- IPv6 sur AWS
- Architectures de référence Amazon VPC à double pile et IPv6 uniquement (PDF)

Clouds privés virtuels (VPC)

Un cloud privé virtuel (VPC) est un réseau virtuel dédié à votre Compte AWS. Il est logiquement isolé des autres réseaux virtuels dans le cloud AWS. Vous pouvez lancer des ressources AWS, telles que des instances Amazon EC2, dans votre VPC.

Votre compte contient un VPC par défaut pour chaque Région AWS. Vous pouvez également créer des VPC supplémentaires.

Table des matières

Principes de base des VPC

Un VPC couvre toutes les zones de disponibilité de la région. Après avoir créé un VPC, vous pouvez ajouter un ou plusieurs sous-réseaux dans chaque zone de disponibilité. Pour de plus amples informations, veuillez consulter Sous-réseaux.

Table des matières

Plage d'adresses IP de VPC

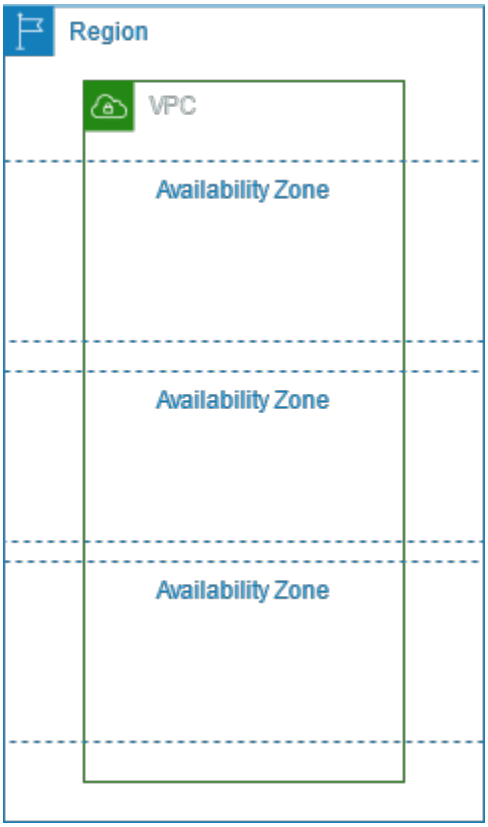
Lorsque vous créez un VPC : vous spécifiez ses adresses IP comme suit :

- IPv4 uniquement : le VPC comporte un bloc d'adresse CIDR IPv4, mais ne comporte pas de bloc d'adresse CIDR IPv6.
- Double pile : le VPC comporte à la fois un bloc d'adresse CIDR IPv4 et un bloc d'adresse CIDR IPv6.

Pour de plus amples informations, veuillez consulter Adressage IP pour vos VPC et sous-réseaux.

Diagramme VPC

Le schéma suivant illustre un VPC sans ressources VPC supplémentaires. Pour obtenir des exemples de configuration VPC, consultez Exemples.



Ressources VPC

Chaque VPC est automatiquement fourni avec les ressources suivantes :

- Jeu d'options DHCP par défaut
- Liste ACL réseau par défaut
- Groupe de sécurité par défaut
- Table de routage principale

Vous pouvez créer les ressources suivantes pour votre VPC :

- Listes ACL réseau
- Tables de routage personnalisées
- Groupes de sécurité
- Passerelle Internet
- Passerelles NAT

VPC par défaut

Lorsque vous commencez à utiliser Amazon VPC, vous disposez d'un VPC par défaut dans chaque Région AWS. Un VPC par défaut est fourni avec un sous-réseau public dans chaque zone de disponibilité, une passerelle Internet et des paramètres permettant la résolution DNS. Vous pouvez donc immédiatement lancer des instances Amazon EC2 dans un VPC par défaut. Vous pouvez également utiliser des services tels que Elastic Load Balancing, Amazon RDS et Amazon EMR dans votre VPC par défaut.

Un VPC par défaut est la solution idéale pour démarrer rapidement et lancer des instances publiques, comme un blog ou un site Internet simple. Vous pouvez modifier les composants du VPC par défaut à votre guise.

Vous pouvez ajouter des sous-réseaux à votre VPC par défaut. Pour de plus amples informations, veuillez consulter the section called “Création d’un sous-réseau”.

Table des matières

- Supprimer vos sous-réseaux par défaut et votre VPC par défaut

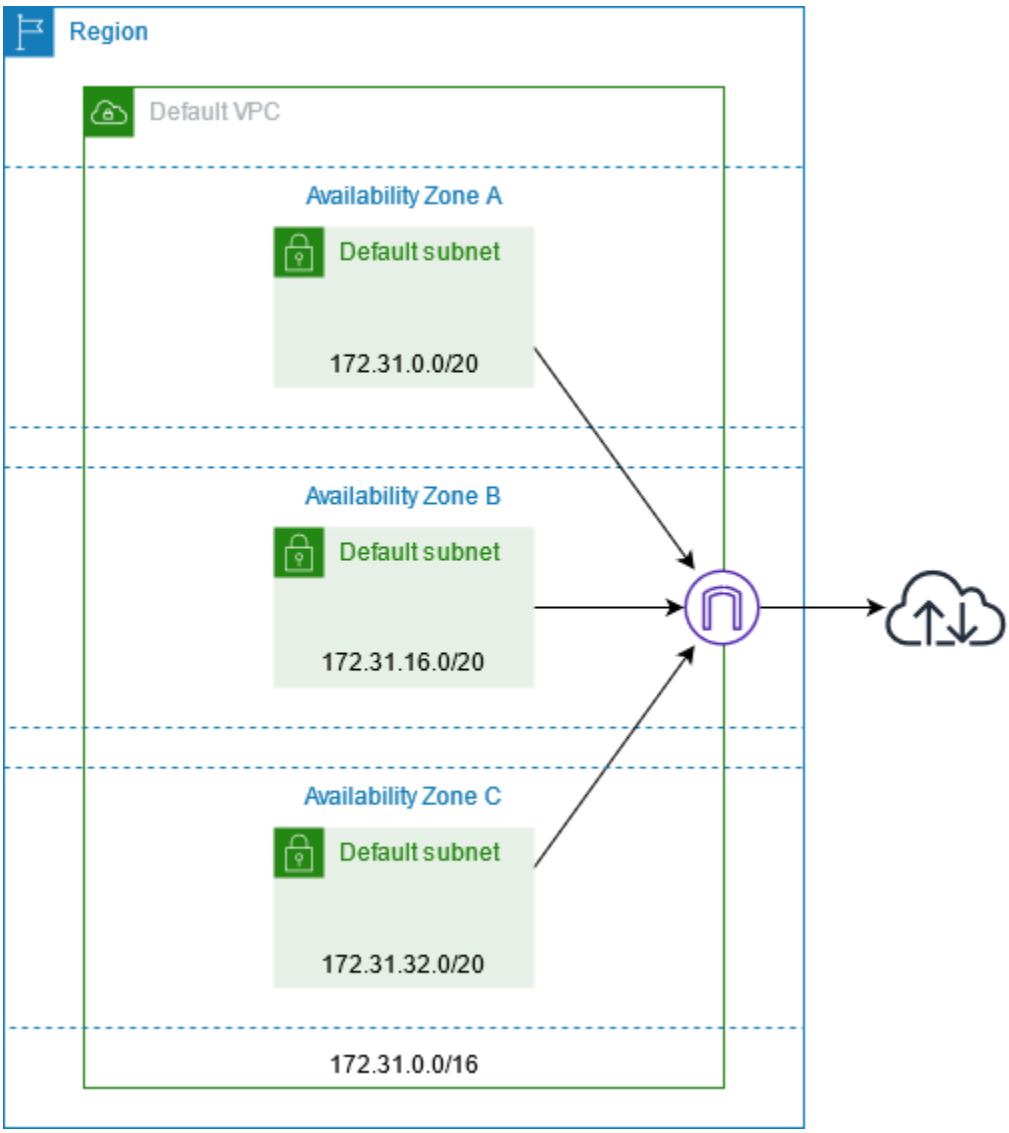
Composants du VPC par défaut

Lorsque nous créons un VPC par défaut, nous le configurons pour vous en procédant comme suit :

- Nous créons un VPC avec un bloc d'adresse CIDR IPv4 dont la taille est `/16` (`172.31.0.0/16`). Cela permet d'obtenir jusqu'à 65 536 adresses IPv4 privées.
- Nous créons un sous-réseau par défaut, de taille `/20`, dans chaque zone de disponibilité. Cela permet d'obtenir jusqu'à 4 096 adresses par sous-réseau, dont quelques-unes nous sont réservées.
- Nous créons une passerelle Internet et nous la connectons à votre VPC par défaut.
- Nous ajoutons un itinéraire dans la table de routage principale qui dirige tout le trafic (`0.0.0.0/0`) vers la passerelle Internet.
- Nous créons un groupe de sécurité par défaut et l'associons à votre VPC par défaut.
- Nous créons une liste de contrôle d'accès (ACL) réseau par défaut et l'associons à votre VPC par défaut.
- Nous associons les options DHCP par défaut définies pour votre compte AWS à votre VPC par défaut.

> **Note**
>
> Amazon crée les ressources ci-dessus pour votre compte. Les stratégies IAM ne s'appliquent pas à ces actions, car vous n'exécutez pas ces actions. Par exemple, si vous disposez d'une stratégie IAM qui vous refuse la possibilité d'appeler CreateInternetGateway et que vous appelez CreateDefaultVpc, la passerelle Internet dans le VPC par défaut est quand même créée.

La figure ci-dessous illustre les principaux composants que nous configurons pour un VPC par défaut.



Le tableau suivant montre les itinéraires dans la table de routage principale pour le VPC par défaut.

Destination	Cible
172.31.0.0/16	locale
0.0.0.0/0	*internet_gateway_id*

Un VPC par défaut s'utilise comme n'importe quel autre VPC :

- Ajoutez des sous-réseaux personnalisés supplémentaires.
- Modifiez la table de routage principale.

- Ajoutez d'autres tables de routage.
- Associez d'autres groupes de sécurité.
- Mettez à jour les règles du groupe de sécurité par défaut.
- Ajoutez des connexions AWS Site-to-Site VPN.
- Ajoutez d'autres blocs d'adresse CIDR IPv4.
- Accédez aux VPC d'une Région distante à l'aide d'une passerelle Direct Connect. Pour de plus amples informations sur les options de passerelle Direct Connect, veuillez consulter Passerelles Direct Connect dans le Guide de l'utilisateur AWS Direct Connect.

Un sous-réseau par défaut s'utilise comme n'importe quel autre sous-réseau. Ajoutez-y des tables de routage personnalisées et définissez des listes ACL réseau. Vous pouvez également spécifier un sous-réseau par défaut spécifique lorsque vous lancez une instance EC2.

Vous pouvez associer un bloc d'adresse CIDR IPv6 à votre VPC par défaut, si vous le souhaitez.

Sous-réseaux par défaut

Par défaut, un sous-réseau par défaut est public, car la table de routage principale envoie le trafic du sous-réseau destiné à Internet vers la passerelle Internet. Pour transformer un sous-réseau par défaut en sous-réseau privé, vous devez supprimer la route 0.0.0.0/0 pointant vers la passerelle Internet. Toutefois, si vous procédez ainsi, aucune instance EC2 exécutée dans ce sous-réseau ne pourra accéder à Internet.

Les instances que vous lancez dans un sous-réseau par défaut reçoivent à la fois une adresse IPv4 publique et une adresse IPv4 privée, ainsi que des noms d'hôte DNS publics et privés. Les instances que vous lancez dans un sous-réseau personnalisé d'un VPC par défaut ne reçoivent ni une adresse IPv4 publique ni un nom d'hôte DNS. Vous avez la possibilité de modifier le comportement de votre sous-réseau concernant les adresses IP publiques. Pour plus d'informations, consultez Modifier l'attribut d'adressage IPv4 public de votre sous-réseau.

De temps en temps, AWS peut ajouter une nouvelle zone de disponibilité à une Région. Dans la plupart des cas, nous créons automatiquement un sous-réseau par défaut pour votre VPC par défaut dans cette zone de disponibilité en quelques jours. Toutefois, si vous avez apporté des modifications à votre VPC par défaut, nous n'ajoutons pas de nouveau sous-réseau par défaut. Si vous avez besoin d'un sous-réseau par défaut pour la nouvelle zone de disponibilité, vous pouvez en créer un vous-même. Pour de plus amples informations, veuillez consulter Créer un sous-réseau par défaut.

Afficher votre VPC par défaut et vos sous-réseaux par défaut

Vous pouvez afficher votre VPC et vos sous-réseaux par défaut à l'aide de la console Amazon VPC or de la ligne de commande

Pour afficher votre VPC et vos sous-réseaux par défaut à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Your VPCs (Vos VPC).
3. Dans la colonne VPC par défaut, recherchez la valeur Oui. Notez l'ID du VPC par défaut.
4. Dans le volet de navigation, choisissez Subnets.
5. Dans la barre de recherche, saisissez l'ID du VPC par défaut. Les sous-réseaux renvoyés correspondent aux sous-réseaux de votre VPC par défaut.
6. Pour savoir quels sont les sous-réseaux par défaut, recherchez la valeur Oui dans la colonne Sous-réseau par défaut.

Pour décrire votre VPC par défaut à l'aide de la ligne de commande

- Utilisez la commande describe-vpcs (AWS CLI)
- Utilisez la commande Get-EC2Vpc (AWS Tools for Windows PowerShell)

Saisissez les commandes avec le filtre `isDefault`, en définissant la valeur de celui-ci sur `true`.

Pour décrire vos sous-réseaux par défaut à l'aide de la ligne de commande

- Utilisez la commande describe-subnets (AWS CLI)
- Utilisez la commande Get-EC2Subnet (AWS Tools for Windows PowerShell)

Saisissez les commandes avec le filtre `vpc-id`, en définissant la valeur de celui-ci sur l'ID du VPC par défaut. En sortie, le champ `DefaultForAz` est défini sur `true` pour les sous-réseaux par défaut.

Créer un VPC par défaut

Si vous supprimez votre VPC par défaut, vous pouvez en recréer un. Il n'est pas possible de restaurer un VPC par défaut supprimé, ni de définir un VPC personnalisé existant en tant que VPC par défaut.

Lorsque vous créez un VPC par défaut, il dispose des composants standard de tout VPC par défaut, notamment un sous-réseau par défaut dans chaque zone de disponibilité. Vous ne pouvez pas spécifier vos propres composants. Il se peut que les blocs CIDR de sous-réseau de votre nouveau VPC par défaut ne soient pas mappés sur les mêmes zones de disponibilité que votre VPC par défaut précédent. Par exemple, si le sous-réseau associé au bloc CIDR `172.31.0.0/20` avait été créé dans `us-east-2a` pour le VPC par défaut précédent, il peut être créé dans `us-east-2b` pour le nouveau VPC par défaut.

Si vous disposez déjà d'un VPC par défaut dans la Région, vous ne pouvez pas en créer un autre.

Pour créer un VPC par défaut à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Your VPCs (Vos VPC).
3. Sélectionnez Actions, puis Create Default VPC.
4. Sélectionnez Créer. Fermez l'écran de confirmation.

Pour créer un VPC par défaut à partir de la ligne de commande

Vous pouvez utiliser la commande AWS CLI create-default-vpc. Cette commande n'est dotée d'aucun paramètre d'entrée.

```
aws ec2 create-default-vpc
```

Voici un exemple de sortie.

```
{
    "Vpc": {
        "VpcId": "vpc-3f139646",
        "InstanceTenancy": "default",
        "Tags": [],
        "Ipv6CidrBlockAssociationSet": [],
        "State": "pending",
        "DhcpOptionsId": "dopt-61079b07",
        "CidrBlock": "172.31.0.0/16",
        "IsDefault": true
    }
}
```

Vous pouvez également utiliser la commande Tools for Windows PowerShell New-EC2DefaultVpc ou l'action CreateDefaultVpc de l'action d'API Amazon EC2.

Créer un sous-réseau par défaut

Vous pouvez créer un sous-réseau par défaut dans une zone de disponibilité qui n'en comporte pas un. Par exemple, il se peut que vous vouliez créer un sous-réseau par défaut si vous avez supprimé un sous-réseau par défaut, ou si AWS a ajouté une nouvelle zone de disponibilité et n'a pas créé automatiquement un sous-réseau par défaut pour cette zone dans votre VPC par défaut.

Lorsque vous créez un sous-réseau par défaut, il est créé avec un bloc d'adresses IPv4 CIDR de taille `/20` dans le prochain espace contigu disponible dans votre VPC par défaut. Les règles suivantes s'appliquent :

- Vous ne pouvez pas spécifier le bloc CIDR vous-même.
- Vous ne pouvez pas restaurer un précédent sous-réseau par défaut que vous avez supprimé.
- Vous ne pouvez avoir qu'un seul sous-réseau par défaut par zone de disponibilité.
- Vous ne pouvez pas créer de sous-réseau par défaut dans un VPC personnalisé.

S'il n'y a pas assez d'espace d'adressage dans votre VPC par défaut pour créer un bloc CIDR de taille `/20`, la demande échoue. Si vous avez besoin de plus d'espace d'adressage, vous pouvez ajouter un bloc d'adresses IPv4 CIDR à votre VPC.

Si vous avez associé un bloc d'adresses IPv6 CIDR à votre VPC par défaut, le nouveau sous-réseau par défaut ne reçoit pas automatiquement un bloc d'adresses IPv6 CIDR. À la place, vous pouvez associer un bloc d'adresses IPv6 CIDR au sous-réseau par défaut après l'avoir créé. Pour plus d'informations, consultez Ajouter un bloc d'adresse CIDR IPv6 à votre sous-réseau.

Vous ne pouvez pas créer un sous-réseau par défaut à l'aide de la AWS Management Console

Pour créer un sous-réseau par défaut à l'aide de l AWS CLI

Utilisez la commande create-default-subnet de la AWS CLI et spécifiez la zone de disponibilité dans laquelle créer le sous-réseau.

```
aws ec2 create-default-subnet --availability-zone us-east-2a
```

Voici un exemple de sortie.

```
{
    "Subnet": {
        "AvailabilityZone": "us-east-2a",
        "Tags": [],
        "AvailableIpAddressCount": 4091,
        "DefaultForAz": true,
        "Ipv6CidrBlockAssociationSet": [],
        "VpcId": "vpc-1a2b3c4d",
        "State": "available",
        "MapPublicIpOnLaunch": true,
        "SubnetId": "subnet-1122aabb",
        "CidrBlock": "172.31.32.0/20",
        "AssignIpv6AddressOnCreation": false
    }
}
```

Pour de plus amples informations sur la configuration de la AWS CLI, veuillez consulter le Guide de l'utilisateur AWS Command Line Interface.

Vous pouvez également utiliser la commande Tools for Windows PowerShell New-EC2DefaultSubnet ou l'action d'API Amazon EC2 CreateDefaultSubnet.

Supprimer vos sous-réseaux par défaut et votre VPC par défaut

Vous pouvez supprimer un sous-réseau par défaut ou un VPC par défaut comme n'importe quel sous-réseau ou VPC. Toutefois, si vous supprimez vos sous-réseaux par défaut ou votre VPC par défaut, vous devez spécifier explicitement un sous-réseau dans l'un de vos VPC lorsque vous lancerez des instances. Si vous ne disposez pas d'un autre VPC, vous devez créer un VPC avec un sous-réseau dans au moins une zone de disponibilité. Pour de plus amples informations, veuillez consulter Création d'un VPC.

Si vous supprimez votre VPC par défaut, vous pouvez en recréer un. Pour plus d'informations, consultez Créer un VPC par défaut.

Si vous supprimez un sous-réseau par défaut, vous pouvez en recréer un. Pour de plus amples informations, veuillez consulter Créer un sous-réseau par défaut. Pour faire en sorte que votre nouveau sous-réseau par défaut fonctionne comme prévu, modifiez son attribut afin d'attribuer des adresses IP publiques aux instances lancées dans ce sous-réseau. Pour plus d'informations, consultez Modifier l'attribut d'adressage IPv4 public de votre sous-réseau. Vous ne pouvez disposer que d'un seul sous-réseau par défaut par zone de disponibilité. Vous ne pouvez pas créer de sous-réseau par défaut dans un VPC personnalisé.

Création d'un VPC

Utilisez les procédures suivantes pour créer un cloud privé virtuel (VPC). Un VPC doit disposer de ressources supplémentaires, telles que des sous-réseaux, des tables de routage et des passerelles, avant de pouvoir créer des ressources AWS dans le VPC.

Table des matières

Pour en savoir plus sur l'affichage ou la modification d'un VPC, consultez the section called "Configuration de votre VPC".

Options de configuration de VPC

Vous pouvez spécifier les options de configuration suivantes lorsque vous créez un VPC.

Zones de disponibilité

> Centres de données à part entière dotés d'une alimentation, d'un réseau et d'une connectivité redondants dans une région AWS . Vous pouvez utiliser plusieurs zones de disponibilité pour exploiter des applications de production et des bases de données plus hautement disponibles, tolérantes aux pannes et évolutives que ce qui serait possible à partir d'un centre de données unique. Si vous partitionnez vos applications exécutées dans des sous-réseaux sur des AZ, vous êtes mieux isolé et protégé contre les problèmes tels que les pannes de courant, les coups de foudre, les tornades et les tremblements de terre.

Blocs CIDR

> Vous devez spécifier des plages d'adresses IP pour votre VPC et vos sous-réseaux. Pour plus d'informations, consultez Adressage IP pour vos VPC et sous-réseaux.

Options DNS

> Si vous avez besoin de noms d'hôtes DNS IPv4 publics pour les instances EC2 lancées dans vos sous-réseaux, vous devez activer les deux options DNS. Pour plus d'informations, consultez Attributs DNS pour votre VPC.

- Activer les noms d'hôte DNS : les instances EC2 lancées dans le VPC reçoivent des noms d'hôte DNS publics qui correspondent à leurs adresses IPv4 publiques.
- Activer la résolution DNS : la résolution DNS pour les noms d'hôtes DNS privés est fournie au VPC par le serveur DNS Amazon, appelé Route 53 Resolver.

Passerelle Internet

Connecte votre VPC à Internet. Les instances d'un sous-réseau public sont en mesure d'accéder à Internet, car la table de routage du sous-réseau contient une route qui envoie le trafic destiné à Internet vers la passerelle Internet. Si un serveur n'a pas besoin d'être directement accessible depuis Internet, vous ne devez pas le déployer dans un sous-réseau public. Pour plus d'informations, consultez Passerelles Internet.

Nom

Les noms que vous spécifiez pour le VPC et les autres ressources de VPC sont utilisés pour créer des balises de nom. Si vous utilisez la fonction de génération automatique de balises de nom dans la console, les valeurs des balises ont le format *nom-ressource*.

Passerelles NAT

Permet aux instances d'un sous-réseau privé d'envoyer du trafic sortant vers Internet, mais empêche les ressources sur Internet de se connecter aux instances. En production, nous vous recommandons de déployer une passerelle NAT dans chaque zone de disponibilité active. Pour plus d'informations, veuillez consulter Passerelles NAT.

Tables de routage

Contient un ensemble de règles, appelées acheminements, qui déterminent la direction du trafic réseau à partir de votre sous-réseau ou de votre passerelle. Pour de plus amples informations, consultez Tables de routage.

Sous-réseaux

Plage d'adresses IP dans votre VPC. Vous pouvez lancer AWS des ressources, telles que des instances EC2, dans vos sous-réseaux. Chaque sous-réseau réside entièrement dans une zone de disponibilité. En lançant des instances dans au moins zones de disponibilité, vous pouvez protéger vos applications contre la défaillance d'une zone de disponibilité unique.

Un sous-réseau public dispose d'une route directe vers une passerelle Internet. Les ressources d'un sous-réseau public peuvent accéder à l'Internet public. Un sous-réseau privé ne comporte pas de route vers une passerelle Internet. Les ressources d'un sous-réseau privé nécessitent un autre composant, comme un périphérique NAT, pour accéder à l'Internet public.

Pour de plus amples informations, consultez Sous-réseaux.

Location

Cette option définit si les instances EC2 que vous lancez dans le VPC s'exécuteront sur du matériel partagé avec d'autres Comptes AWS ou sur du matériel dédié à votre seul usage. Si vous choisissez la location du VPC, les instances EC2 lancées *`Default`* dans ce VPC utiliseront l'attribut de location spécifié lors du lancement de l'instance. Pour plus d'informations, consultez Lancer une instance à l'aide de paramètres définis dans le guide de l'utilisateur Amazon EC2. Si vous choisissez que la location du VPC est `Dedicated`, les instances s'exécutent toujours en tant qu'instances dédiées sur du matériel dédié à votre utilisation. Si vous utilisez des AWS Outposts, ceux-ci nécessitent une connectivité privée ; vous devez utiliser la location. `Default`

Créer un VPC et d'autres ressources VPC

Procédez comme suit pour créer un VPC ainsi que les ressources VPC supplémentaires dont vous avez besoin pour exécuter votre application, telles que des sous-réseaux, des tables de routage, des passerelles Internet et des passerelles NAT. Pour obtenir des exemples de configuration VPC, consultez Exemples.

Pour créer un VPC, des sous-réseaux et d'autres ressources VPC à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Sur le tableau de bord VPC, choisissez Create VPC (Créer un VPC).
3. Sous Ressources à créer, choisissez VPC et plus encore.
4. Maintenez la génération automatique de balises de nom sélectionnée pour créer des balises de nom pour les ressources VPC ou désactivez-la pour fournir vos propres balises de nom pour les ressources VPC.
5. Pour Bloc d'adresse CIDR IPv4, saisissez une plage d'adresses IPv4 pour le VPC. Un VPC doit avoir une plage d'adresses IPv4.
6. (Facultatif,) Pour prendre en charge le trafic IPv6, choisissez Bloc d'adresse CIDR IPv6, Bloc d'adresse CIDR IPv6 fourni par Amazon.
7. Choisissez une option de location. Cette option définit si les instances EC2 que vous lancez dans le VPC s'exécuteront sur du matériel partagé avec d'autres Comptes AWS ou sur du matériel dédié à votre seul usage. Si vous choisissez la location du VPC, les instances EC2 `Default` lancées dans ce VPC utiliseront l'attribut de location spécifié lors du lancement de l'instance. Pour plus d'informations, consultez Lancer une instance à l'aide de paramètres définis dans le

guide de l'utilisateur Amazon EC2. Si vous choisissez que la location du VPC est `Dedicated`, les instances s'exécutent toujours en tant qu'instances dédiées sur du matériel dédié à votre utilisation. Si vous utilisez des AWS Outposts, ceux-ci nécessitent une connectivité privée ; vous devez utiliser la location. `Default`

8. Pour Nombre de zones de disponibilité (AZ), nous vous recommandons de configurer des sous-réseaux dans au moins deux zones de disponibilité pour un environnement de production. Pour choisir les zones de disponibilité pour vos sous-réseaux, développez Personnaliser les AZ. Sinon, laissez-les AWS choisir pour vous.
9. Pour configurer vos sous-réseaux, choisissez des valeurs pour Nombre de sous-réseaux publics et Nombre de sous-réseaux privés. Pour choisir les plages d'adresses IP pour vos sous-réseaux, développez Personnaliser les blocs CIDR des sous-réseaux. Sinon, laissez-les AWS choisir pour vous.
10. (Facultatif) Si les ressources d'un sous-réseau privé ont besoin d'accéder à l'Internet public sur IPv4, pour Passerelles NAT, choisissez le nombre de zones de disponibilité dans lesquelles vous souhaitez créer des passerelles NAT. En production, nous vous recommandons de déployer une passerelle NAT dans chaque zone de disponibilité avec des ressources nécessitant un accès à l'Internet public. Notez que des coûts sont associés aux passerelles NAT. Pour plus d'informations, consultez Tarification.
11. (Facultatif) Si les ressources d'un sous-réseau privé doivent accéder à l'Internet public sur IPv6, pour Passerelle Internet de sortie uniquement, choisissez Oui.
12. (Facultatif) Si vous devez accéder à Amazon S3 directement depuis votre VPC, choisissez Points de terminaison d'un VPC, Passerelle S3. Cela crée un point de terminaison d'un VPC de passerelle pour Amazon S3. Pour de plus amples informations, consultez Point de terminaison d'un VPC d'une passerelle dans le Guide AWS PrivateLink .
13. (Facultatif) Pour Options DNS, les deux options de résolution des noms de domaine sont activées par défaut. Si la valeur par défaut ne répond pas à vos besoins, vous pouvez désactiver ces options.
14. (Facultatif) Pour ajouter une balise à votre VPC, développez Balises supplémentaires, choisissez Ajouter une nouvelle balise et saisissez une clé et une valeur de balise.
15. Dans le volet Aperçu, vous pouvez visualiser les relations entre les ressources VPC que vous aviez configurées. Les lignes continues représentent les relations entre les ressources. Les lignes pointillées représentent le trafic réseau vers les passerelles NAT, les passerelles Internet et les points de terminaison de passerelles. Après avoir créé le VPC, vous pouvez visualiser les ressources de votre VPC dans ce format à tout moment à l'aide de l'onglet Mappage des ressources. Pour plus d'informations, consultez Visualiser les ressources de votre VPC.

16. Une fois la configuration de votre VPC terminée, choisissez Créer VPC.

Créer un VPC uniquement

Utilisez la procédure suivante pour créer un VPC sans ressources VPC supplémentaires à l'aide de la console Amazon VPC.

Pour créer un VPC sans ressources VPC supplémentaires à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Sur le tableau de bord VPC, choisissez Create VPC (Créer un VPC).
3. Sous Ressources à créer, choisissez VPC uniquement.
4. (Facultatif) Pour Balise de nom, saisissez un nom pour votre VPC. Une identification est alors créée avec la clé `Name` et la valeur que vous spécifiez.
5. Pour IPv4 CIDR block (Bloc d'adresse CIDR IPv4), effectuez l'une des actions suivantes :
   - Choisissez la saisie manuelle de CIDR IPv4 et entrez une plage d'adresses IPv4 pour votre VPC.
   - Choisissez le bloc d'adresses CIDR IPv4 alloué par IPAM, sélectionnez votre pool d'adresses IPv4 Amazon VPC IP Address Manager (IPAM) et un masque de réseau. La taille du bloc CIDR est limitée par les règles d'allocation sur le groupe IPAM. L'IPAM est une fonctionnalité VPC qui vous permet de planifier, de suivre et de surveiller plus facilement les adresses IP pour AWS vos charges de travail. Pour plus d'informations, consultez le guide de l'utilisateur Amazon VPC IPAM.

     Si vous utilisez IPAM pour gérer vos adresses IP, nous vous recommandons de choisir cette option. Sinon, le bloc d'adresse CIDR que vous spécifiez pour votre VPC risque de se chevaucher avec une allocation d'adresse CIDR IPAM.
6. (Facultatif) Pour créer un VPC à double pile, spécifiez une plage d'adresses IPv6 pour votre VPC. Pour Bloc d'adresse CIDR IPv6, effectuez l'une des actions suivantes :
   - Choisissez Bloc d'adresse CIDR IPv6 alloué par IPAM si vous utilisez Amazon VPC IP Address Manager (IPAM) et si vous souhaitez provisionner un CIDR IPv6 à partir d'un groupe IPAM. Vous avez deux options pour provisionner une plage d'adresses IP au VPC sous le bloc d'adresse CIDR :
     - Longueur du masque réseau : choisissez cette option pour sélectionner une longueur de masque réseau pour le CIDR. Effectuez l'une des actions suivantes :

- Si une longueur de masque réseau par défaut est sélectionnée pour le groupe IPAM, vous pouvez choisir par défaut pour la longueur de masque réseau IPAM pour utiliser la longueur de masque réseau par défaut définie pour le groupe IPAM par l'administrateur IPAM. Pour plus d'informations sur la règle facultative d'allocation de longueur de masque réseau par défaut, consultez la section Création d'un groupe IPv6 régional dans le Guide de l'utilisateur Amazon VPC IPAM.
- Si aucune longueur de masque réseau par défaut n'est sélectionnée pour le groupe IPAM, choisissez une longueur de masque réseau plus spécifique que celle du CIDR du groupe IPAM. Par exemple, si le CIDR du groupe IPAM est /50, vous pouvez choisir une longueur de masque réseau comprise entre /52 et /60 pour le VPC. Les longueurs possibles des masques réseau sont comprises entre /44 et /60 par incréments de /4.

- Sélectionnez un CIDR : choisissez cette option pour saisir manuellement une adresse IPv6. Vous ne pouvez choisir qu'une longueur de masque réseau plus spécifique que la longueur du masque réseau du CIDR du groupe IPAM. Par exemple, si le CIDR du groupe IPAM est /50, vous pouvez choisir une longueur de masque réseau comprise entre /52 et /60 pour le VPC. Les longueurs possibles des masques réseau IPv6 sont comprises entre /44 et /60 par incréments de /4.

- Choisissez Bloc d'adresse CIDR IPv6 fourni par Amazon pour demander un bloc d'adresse CIDR IPv6 d'un groupe d'adresses IPv6 d'Amazon. Pour Network Border Group, sélectionnez le groupe à partir duquel les AWS adresses IP sont publiées. Amazon fournit une taille de bloc d'adresse CIDR IPv6 fixe de /56.
- Choisissez Adresses CIDR IPv6 m'appartenant pour provisionner un CIDR IPv6 que vous avez déjà apporté à AWS. Pour plus d'informations sur l'importation de vos propres plages d'adresses IP AWS, consultez la section Bring your own IP addresses (BYOIP) dans le guide de l'utilisateur Amazon EC2. Vous pouvez configurer une plage d'adresses IP pour le VPC à l'aide des options suivantes pour le bloc CIDR :
  - Aucune préférence : choisissez cette option pour utiliser une longueur de masque réseau de /56.
  - Sélectionnez un CIDR : choisissez cette option pour saisir manuellement une adresse IPv6 et choisir une longueur de masque réseau plus spécifique que la taille du CIDR BYOIP. Par exemple, si le CIDR du groupe BYOIP est /50, vous pouvez choisir une longueur de masque réseau comprise entre /52 et /60 pour le VPC. Les longueurs possibles des masques réseau IPv6 sont comprises entre /44 et /60 par incréments de /4.

7. (Facultatif) Choisissez une option de location. Cette option définit si les instances EC2 que vous lancez dans le VPC s'exécuteront sur du matériel partagé avec d'autres Comptes AWS ou

sur du matériel dédié à votre seul usage. Si vous choisissez la location du VPC, les instances EC2 lancées *Default* dans ce VPC utiliseront l'attribut de location spécifié lors du lancement de l'instance. Pour plus d'informations, consultez Lancer une instance à l'aide de paramètres définis dans le guide de l'utilisateur Amazon EC2. Si vous choisissez que la location du VPC est `Dedicated`, les instances s'exécutent toujours en tant qu'instances dédiées sur du matériel dédié à votre utilisation. Si vous utilisez des AWS Outposts, ceux-ci nécessitent une connectivité privée ; vous devez utiliser la location. `Default`

8. (Facultatif) Pour ajouter une balise à votre VPC, choisissez Ajouter une nouvelle balise et saisissez une clé et une valeur de balise.
9. Sélectionnez Create VPC (Créer un VPC).
10. Après avoir créé un VPC, vous pouvez ajouter des sous-réseaux. Pour plus d'informations, consultez Création d'un sous-réseau.

Créez un VPC à l'aide du AWS CLI

La procédure suivante contient des exemples de AWS CLI commandes permettant de créer un VPC ainsi que les ressources VPC supplémentaires nécessaires pour exécuter une application. Si vous exécutez toutes les commandes de cette procédure, vous allez créer un VPC, un sous-réseau public, un sous-réseau privé, une table de routage pour chaque sous-réseau, une passerelle Internet, une passerelle Internet de sortie uniquement et une passerelle NAT publique. Si vous n'avez pas besoin de toutes ces ressources, vous ne pouvez utiliser que les exemples de commandes dont vous avez besoin.

Prérequis

Avant de commencer, installez et configurez la AWS CLI. Lorsque vous configurez le AWS CLI, vous êtes invité à entrer des AWS informations d'identification. Les exemples de cette procédure supposent que vous avez également configuré une région par défaut. Sinon, ajoutez l'option `--region` à chaque commande. Pour plus d'informations, consultez Installation ou mise à jour de la AWS CLI et Configuration de la AWS CLI.

Identification

Vous pouvez ajouter des balises à une ressource après l'avoir créée à l'aide de la commande create-tags. Vous pouvez également ajouter l'option `--tag-specification` à la commande de création de la ressource comme suit.

```
--tag-specifications ResourceType=vpc,Tags=[{Key=Name,Value=my-project}]
```

Pour créer un VPC plus des ressources VPC à l'aide du AWS CLI

1. Utilisez la commande create-vpc suivante pour créer un VPC avec le bloc d'adresse CIDR IPv4 spécifié.

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --query Vpc.VpcId --output text
   ```

   Sinon, pour créer un VPC à double pile, ajoutez l'option `--amazon-provided-ipv6-cidr-block` permettant d'ajouter un bloc d'adresse CIDR IPv6 fourni par Amazon, comme indiqué dans l'exemple suivant.

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --amazon-provided-ipv6-cidr-block --
   query Vpc.VpcId --output text
   ```

   Ces commandes renvoient l'ID du nouveau VPC. Voici un exemple.

   ```
   vpc-1a2b3c4d5e6f1a2b3
   ```

2. [VPC à double pile] Obtenez le bloc d'adresse CIDR IPv6 qui est associé à votre VPC à l'aide de la commande describe-vpcs suivante.

   ```
   aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
    Vpcs[].Ipv6CidrBlockAssociationSet[].Ipv6CidrBlock --output text
   ```

   Voici un exemple de sortie.

   ```
   2600:1f13:cfe:3600::/56
   ```

3. Créez un ou plusieurs sous-réseaux, en fonction de votre cas d'utilisation. En production, nous vous recommandons de lancer des ressources dans au moins deux zones de disponibilité. Utilisez l'une des commandes suivantes pour créer chaque sous-réseau.

   - Sous-réseau IPv4 uniquement : pour créer un sous-réseau avec un bloc d'adresse CIDR IPv4 spécifique, utilisez la commande create-subnet suivante.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
 --availability-zone us-east-2a --query Subnet.SubnetId --output text
```

- Sous-réseau à double pile : si vous avez créé un VPC à double pile, vous pouvez utiliser l'option `--ipv6-cidr-block` pour créer un sous-réseau à double pile, comme indiqué dans la commande suivante.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
 --ipv6-cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --
query Subnet.SubnetId --output text
```

- Sous-réseau IPv6 uniquement : si vous avez créé un VPC à double pile, vous pouvez utiliser l'option `--ipv6-native` pour créer un sous-réseau IPv6 uniquement, comme indiqué dans la commande suivante.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --ipv6-native --ipv6-
cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --query
 Subnet.SubnetId --output text
```

Ces commandes renvoient l'ID du nouveau sous-réseau. Voici un exemple.

```
subnet-1a2b3c4d5e6f1a2b3
```

4. Si vous avez besoin d'un sous-réseau public pour vos serveurs Web ou d'une passerelle NAT, procédez comme suit :

   a. Créez une passerelle Internet à l'aide de la commande create-internet-gateway ci-dessous. La commande renvoie l'ID de la nouvelle passerelle Internet.

```
aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --
output text
```

   b. Attachez la passerelle Internet à votre VPC à l'aide de la commande attach-internet-gateway ci-dessous. Utilisez l'ID de passerelle Internet renvoyé à l'étape précédente.

```
aws ec2 attach-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --internet-
gateway-id igw-id
```

c. Créez une table de routage personnalisée pour votre sous-réseau public à l'aide de la commande create-route-table ci-dessous. La commande renvoie l'ID de la nouvelle table de routage.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

d. Créez une route dans la table de routage qui envoie l'ensemble du trafic IPv4 vers la passerelle Internet à l'aide de la commande create-route. Utilisez l'ID de la table de routage pour le sous-réseau public.

```
aws ec2 create-route --route-table-id rtb-id-public --destination-cidr-block
 0.0.0.0/0 --gateway-id igw-id
```

e. Associez la table de routage au sous-réseau public à l'aide de la commande associate-route-table suivante. Utilisez l'ID de la table de routage pour le sous-réseau public et l'ID du sous-réseau public.

```
aws ec2 associate-route-table --route-table-id rtb-id-public --subnet-
id subnet-id-public-subnet
```

5. [IPv6] Vous pouvez ajouter une passerelle Internet de sortie uniquement afin que les instances d'un sous-réseau privé soient en mesure d'accéder à Internet via IPv6 (par exemple, pour obtenir des mises à jour logicielles), mais les hôtes sur Internet ne peuvent pas accéder à vos instances.

a. Créez une passerelle Internet de sortie uniquement à l'aide de la commande create-egress-only-internet-gateway suivante. La commande renvoie l'ID de la nouvelle passerelle Internet.

```
aws ec2 create-egress-only-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --
query EgressOnlyInternetGateway.EgressOnlyInternetGatewayId --output text
```

b. Créez une table de routage personnalisée pour votre sous-réseau privé à l'aide de la commande create-route-table ci-dessous. La commande renvoie l'ID de la nouvelle table de routage.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

c. Créez une route dans la table de routage pour le sous-réseau privé qui envoie l'ensemble du trafic IPv6 vers la passerelle Internet de sortie uniquement à l'aide de la commande create-route ci-dessous. Utilisez l'ID de la table de routage renvoyé à l'étape précédente.

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block ::/0 --egress-only-internet-gateway eigw-id
```

d. Associez la table de routage au sous-réseau privé à l'aide de la commande associate-route-table suivante.

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

6. Si vous avez besoin d'une passerelle NAT pour vos ressources dans un sous-réseau privé, procédez comme suit :

a. Créez une adresse IP élastique pour la passerelle NAT à l'aide de la commande allocate-address suivante.

```
aws ec2 allocate-address --domain vpc --query AllocationId --output text
```

b. Créez la passerelle NAT dans le sous-réseau public à l'aide de la commande create-nat-gateway suivante. Utilisez l'ID d'allocation renvoyé à l'étape précédente.

```
aws ec2 create-nat-gateway --subnet-id subnet-id-public-subnet --allocation-
id eipalloc-id
```

c. (Facultatif) Si vous avez déjà créé une table de routage pour le sous-réseau privé à l'étape 5, ignorez cette étape. Sinon, créez une table de routage pour votre sous-réseau privé à l'aide de la commande create-route-table suivante. La commande renvoie l'ID de la nouvelle table de routage.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

d. Créez une route dans la table de routage pour le sous-réseau privé qui envoie l'ensemble du trafic IPv4 vers la passerelle NAT à l'aide de la commande create-route suivante. Utilisez l'ID de la table de routage pour le sous-réseau privé, que vous avez créé à cette étape ou à l'étape 5.

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block 0.0.0.0/0 --gateway-id nat-id
```

e. (Facultatif) Si vous avez déjà associé une table de routage avec le sous-réseau privé à l'étape 5, ignorez cette étape. Sinon, utilisez la commande associate-route-table suivante pour associer la table de routage au sous-réseau privé. Utilisez l'ID de la table de routage pour le sous-réseau privé, que vous avez créé à cette étape ou à l'étape 5.

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

Configuration de votre VPC

Utilisez les procédures suivantes pour afficher et configurer vos clouds privés virtuels (VPC).

Tâches

- Afficher des détails sur votre VPC
- Visualiser les ressources de votre VPC
- Ajouter un bloc d'adresse CIDR IPv4 à votre VPC
- Ajouter un bloc d'adresse CIDR IPv6 à votre VPC
- Supprimer un bloc d'adresse CIDR IPv4 de votre VPC
- Supprimer un bloc d'adresse CIDR IPv6 de votre VPC

Pour plus d'informations sur la création ou la suppression d'un VPC, consultez the section called "Création d'un VPC" ou the section called "Supprimer votre VPC".

Afficher des détails sur votre VPC

Utilisez les étapes suivantes pour afficher les détails concernant vos VPC.

Pour afficher les détails du VPC à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez VPCs (VPC).

3. Sélectionnez le VPC, puis Afficher les détails afin d'afficher les détails de configuration de votre VPC.

Pour décrire un VPC à l'aide du AWS CLI

Utilisez la commande describe-vpcs.

Pour afficher tous vos VPC relevant de toutes les régions

Ouvrez la console Amazon EC2 Global View à l'adresse https://console.aws.amazon.com/ec2globalview/home. Pour plus d'informations, consultez Répertorier et filtrer les ressources à l'aide d'Amazon EC2 Global View dans le guide de l'utilisateur Amazon EC2.

Visualiser les ressources de votre VPC

Suivez les étapes suivantes afin d'afficher une représentation visuelle des ressources de votre VPC à l'aide de l'onglet Mappage des ressources. Les ressources suivantes sont visibles dans le mappage des ressources :

- VPC
- Sous-réseaux
  - La zone de disponibilité est représentée par une lettre.
  - Les sous-réseaux publics sont verts.
  - Les sous-réseaux privés sont bleus.

- Tables de routage
- Passerelles Internet
- Passerelles Internet de sortie uniquement
- Passerelles NAT
- Points de terminaison de passerelle (Amazon S3 et Amazon DynamoDB)

Le mappage des ressources montre les relations entre les ressources au sein d'un VPC et la manière dont le trafic circule entre les sous-réseaux et les passerelles NAT, les passerelles Internet et les points de terminaison de passerelles.

Vous pouvez utiliser le mappage des ressources pour comprendre l'architecture d'un VPC, voir le nombre de sous-réseaux qu'il contient, les associations entre sous-réseaux et tables de routage ainsi

que les tables de routage ayant des routes vers des passerelles NAT, des passerelles Internet et des points de terminaison de passerelles.

Vous pouvez également utiliser le mappage des ressources afin de repérer les configurations indésirables ou incorrectes, telles que les sous-réseaux privés déconnectés de passerelles NAT ou ayant une route directe vers la passerelle Internet. Dans le mappage des ressources, vous pouvez sélectionner des ressources, telles que des tables de routage, pour en modifier les configurations.

Pour visualiser les ressources de votre VPC

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez VPCs (VPC).
3. Sélectionnez le VPC.
4. Sélectionnez l'onglet Carte des ressources pour afficher une visualisation des ressources.
5. Choisissez Afficher les détails pour afficher les détails en plus des ID de ressources et des zones affichés par défaut.

    - VPC : plages d'adresses CIDR IPv4 et IPv6 attribuées au VPC.
    - Sous-réseaux : plages d'adresses CIDR IPv4 et IPv6 attribuées à chaque sous-réseau.
    - Tables de routage : associations de sous-réseaux et nombre de routes dans la table de routage.
    - Connexions réseau : informations relatives à chaque type de connexion :
        - S'il existe des sous-réseaux publics dans le VPC, il existe une ressource de passerelle internet avec le nombre de routages et les sous-réseaux source et destination pour le trafic utilisant la passerelle internet.
        - S'il existe une passerelle internet de sortie uniquement, il existe une ressource de passerelle internet de sortie uniquement avec le nombre de routages et les sous-réseaux source et destination pour le trafic utilisant la passerelle internet de sortie uniquement.
        - S'il existe une passerelle NAT, il existe une ressource de passerelle NAT avec le nombre d'interfaces réseau et d'adresses IP Elastic pour la passerelle NAT.
        - S'il existe un point de terminaison de passerelle, il existe une ressource de point de terminaison de passerelle portant le nom du AWS service (Amazon S3 ou Amazon DynamoDB) à laquelle vous pouvez vous connecter à l'aide du point de terminaison.
6. Passez le curseur de votre souris sur une ressource afin d'afficher la relation entre les ressources. Les lignes continues représentent les relations entre les ressources. Les lignes pointillées représentent le trafic réseau vers les connexions réseau.

Ajouter un bloc d'adresse CIDR IPv4 à votre VPC

Votre VPC peut avoir jusqu'à cinq blocs d'adresse CIDR IPv4 par défaut, mais cette limite est réglable. Pour plus d'informations, consultez Quotas Amazon VPC. Pour plus d'informations sur les restrictions concernant les blocs d'adresse CIDR IPv4 pour un VPC, consultez Blocs CIDR VPC.

Pour ajouter un bloc d'adresse CIDR IPv4 à un VPC à l'aide de la console

1. Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Vos VPC.
3. Sélectionnez le VPC et choisissez Actions, puis Modifier les blocs d'adresse CIDR.
4. Choisissez Ajouter un nouveau bloc d'adresse CIDR IPv4.
5. Pour IPv4 CIDR block (Bloc d'adresse CIDR IPv4), effectuez l'une des actions suivantes :
   - Choisissez IPv4 CIDR manual input (Entrée manuelle CIDR IPv4) et saisissez un bloc d'adresse CIDR IPv4.
   - Choisissez IPAM-allocated IPv4 CIDR (CIDR IPv4 alloué par IPAM) et sélectionnez un CIDR à partir d'un groupe IPAM IPv4.
6. Choisissez Save, puis choisissez Close.
7. Après avoir ajouté un bloc d'adresse CIDR IPv4 à votre VPC, vous pouvez créer des sous-réseaux qui utilisent le nouveau bloc d'adresse CIDR. Pour plus d'informations, consultez Création d'un sous-réseau.

Pour associer un bloc d'adresse CIDR IPv4 à un VPC à l'aide du AWS CLI

Utilisez la commande associate-vpc-cidr-block.

Ajouter un bloc d'adresse CIDR IPv6 à votre VPC

Votre VPC peut avoir jusqu'à cinq blocs d'adresse CIDR IPv6 par défaut, mais cette limite est réglable. Pour plus d'informations, consultez Quotas Amazon VPC. Pour plus d'informations sur les restrictions concernant les blocs d'adresse CIDR IPv6 pour un VPC, consultez Blocs CIDR VPC.

Pour ajouter un bloc d'adresse CIDR IPv6 à un VPC à l'aide de la console

1. Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Vos VPC.

3. Sélectionnez le VPC et choisissez Actions, puis Modifier les blocs d'adresse CIDR.
4. Choisissez Ajouter un nouveau bloc d'adresse CIDR IPv6.
5. Pour Bloc d'adresse CIDR IPv6, effectuez l'une des actions suivantes :

   - Choisissez Bloc d'adresse CIDR IPv6 alloué par IPAM si vous utilisez Amazon VPC IP Address Manager (IPAM) et si vous souhaitez provisionner un CIDR IPv6 à partir d'un groupe IPAM. Vous avez deux options pour provisionner une plage d'adresses IP au VPC sous le bloc d'adresse CIDR :
     - Longueur du masque réseau : choisissez cette option pour sélectionner une longueur de masque réseau pour le CIDR. Effectuez l'une des actions suivantes :
       - Si une longueur de masque réseau par défaut est sélectionnée pour le groupe IPAM, vous pouvez choisir par défaut pour la longueur de masque réseau IPAM pour utiliser la longueur de masque réseau par défaut définie pour le groupe IPAM par l'administrateur IPAM. Pour plus d'informations sur la règle facultative d'allocation de longueur de masque réseau par défaut, consultez la section Création d'un groupe IPv6 régional dans le Guide de l'utilisateur Amazon VPC IPAM.
       - Si aucune longueur de masque réseau par défaut n'est sélectionnée pour le groupe IPAM, choisissez une longueur de masque réseau plus spécifique que celle du CIDR du groupe IPAM. Par exemple, si le CIDR du groupe IPAM est /50, vous pouvez choisir une longueur de masque réseau comprise entre /52 et /60 pour le VPC. Les longueurs possibles des masques réseau sont comprises entre /44 et /60 par incréments de /4.
     - Sélectionnez un CIDR : choisissez cette option pour saisir manuellement une adresse IPv6. Vous ne pouvez choisir qu'une longueur de masque réseau plus spécifique que la longueur du masque réseau du CIDR du groupe IPAM. Par exemple, si le CIDR du groupe IPAM est /50, vous pouvez choisir une longueur de masque réseau comprise entre /52 et /60 pour le VPC. Les longueurs possibles des masques réseau IPv6 sont comprises entre /44 et /60 par incréments de /4.
   - Choisissez Bloc d'adresse CIDR IPv6 fourni par Amazon pour demander un bloc d'adresse CIDR IPv6 d'un groupe d'adresses IPv6 d'Amazon. Pour Network Border Group, sélectionnez le groupe à partir duquel les AWS adresses IP sont publiées. Amazon fournit une taille de bloc d'adresse CIDR IPv6 fixe de /56.
   - Choisissez Adresses CIDR IPv6 m'appartenant pour provisionner un CIDR IPv6 que vous avez déjà apporté à AWS. Pour plus d'informations sur l'importation de vos propres plages d'adresses IP AWS, consultez la section Bring your own IP addresses (BYOIP) in Amazon

EC2 dans le guide de l'utilisateur Amazon EC2. Vous avez deux options pour provisionner une plage d'adresses IP au VPC sous le bloc d'adresse CIDR :

- Aucune préférence : choisissez cette option pour utiliser une longueur de masque réseau de /56.
- Sélectionnez un CIDR : choisissez cette option pour saisir manuellement une adresse IPv6 et choisir une longueur de masque réseau plus spécifique que la taille du CIDR BYOIP. Par exemple, si le CIDR du groupe BYOIP est /50, vous pouvez choisir une longueur de masque réseau comprise entre /52 et /60 pour le VPC. Les longueurs possibles des masques réseau IPv6 sont comprises entre /44 et /60 par incréments de /4.

6. Choisissez Sélectionner CIDR, puis Fermer.
7. Après avoir ajouté un bloc d'adresse CIDR IPv6 à votre VPC, vous pouvez créer des sous-réseaux qui utilisent le nouveau bloc d'adresse CIDR. Pour plus d'informations, consultez Création d'un sous-réseau.

Pour associer un bloc d'adresse CIDR IPv6 à un VPC à l'aide du AWS CLI

Utilisez la commande associate-vpc-cidr-block.

Supprimer un bloc d'adresse CIDR IPv4 de votre VPC

Si votre VPC est associé à plusieurs blocs d'adresse CIDR IPv4, vous pouvez supprimer un bloc d'adresse CIDR IPv4 du VPC. Vous pouvez supprimer le bloc d'adresse CIDR IPv4 principal. Vous devez supprimer un bloc d'adresse CIDR complet, mais pas un sous-ensemble d'un bloc d'adresse CIDR ou une plage fusionnée de blocs d'adresse CIDR. Vous devez commencer par supprimer tous les sous-réseaux du bloc d'adresse CIDR.

Pour supprimer un bloc d'adresse CIDR d'un VPC à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Your VPCs (Vos VPC).
3. Sélectionnez le VPC et choisissez Actions, puis Modifier les blocs CIDR.
4. Sous CIDR IPv4 VPC, supprimez le CIDR en choisissant Supprimer.
5. Choisissez Fermer.

Pour dissocier un bloc d'adresse CIDR IPv4 d'un VPC à l'aide du AWS CLI

Utilisez la commande disassociate-vpc-cidr-block.

Supprimer un bloc d'adresse CIDR IPv6 de votre VPC

Si vous ne souhaitez plus de prise en charge d'IPv6 dans votre VPC, mais que vous souhaitez continuer à utiliser votre VPC pour la création et la communication avec les ressources IPv4, vous pouvez supprimer le bloc d'adresse CIDR IPv6.

Pour supprimer un bloc d'adresse CIDR IPv6, vous devez tout d'abord annuler l'attribution des adresses IPv6 qui sont attribuées aux instances de votre sous-réseau.

La suppression d'un bloc d'adresse CIDR IPv6 ne supprime pas automatiquement les règles de groupe de sécurité, les règles ACL réseau ou les routes de table de routage que vous avez configurées pour la mise en réseau IPv6. Vous devez modifier ou supprimer manuellement ces règles ou ces routes.

Pour supprimer un bloc d'adresse CIDR IPv6 d'un VPC à l'aide de la console

1. Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Your VPCs (Vos VPC).
3. Sélectionnez votre VPC, choisissez Actions, puis Edit CIDRs.
4. Sous CIDR IPv6, supprimez le bloc d'adresse CIDR IPv6 en choisissant Supprimer.
5. Choisissez Fermer.

Pour dissocier un bloc d'adresse CIDR IPv6 d'un VPC à l'aide du AWS CLI

Utilisez la commande disassociate-vpc-cidr-block.

Jeux d'options DHCP dans Amazon VPC

Les dispositifs du réseau de votre VPC utilisent le protocole de configuration d'hôte dynamique (DHCP). Vous pouvez utiliser les jeux d'options DHCP pour contrôler les aspects suivants de la configuration réseau dans votre réseau virtuel :

- Les serveurs DNS, les noms de domaine ou les serveurs NTP (Network Time Protocol) utilisés par les dispositifs de votre VPC.
- Si la résolution DNS est activée dans votre VPC.

Table des matières

Qu'est-ce que le DHCP ?

Chaque dispositif d'un réseau TCP/IP a besoin d'une adresse IP pour communiquer sur le réseau. Auparavant, des adresses IP devaient être attribuées manuellement à chaque dispositif de votre réseau. Aujourd'hui, les adresses IP sont attribuées de manière dynamique par les serveurs DHCP en utilisant le protocole de configuration d'hôte dynamique (DHCP).

Les applications exécutées sur des instances EC2 peuvent communiquer avec les serveurs Amazon DHCP si nécessaire pour récupérer leur bail d'adresse IP ou d'autres informations de configuration réseau (telles que l'adresse IP d'un serveur Amazon DNS ou l'adresse IP du routeur dans votre VPC).

Vous pouvez spécifier les configurations réseau fournies par les serveurs DHCP Amazon à l'aide du jeu d'options DHCP.

Si vous disposez d'une configuration VPC qui nécessite que vos applications adressent des demandes directes au serveur DHCP Amazon IPv6, notez les points suivants :

- Une instance EC2 d'un sous-réseau à double pile peut uniquement récupérer son adresse IPv6 à partir du serveur DHCP IPv6. Elle ne peut pas récupérer de configurations réseau supplémentaires à partir du serveur DHCP IPv6, telles que les noms de serveurs DNS ou des noms de domaine.
- Une instance EC2 d'un sous-réseau uniquement IPv6 peut récupérer son adresse IPv6 à partir du serveur DHCP IPv6 et d'autres informations de configuration réseau, telles que les noms de serveurs DNS et les noms de domaine.
- Pour une instance EC2 dans un sous-réseau IPv6 uniquement, le serveur DHCP IPv4 renvoie 169.254.169.253 comme serveur de noms si « DNS » est explicitement mentionné dans le jeu d'options DHCP. AmazonProvided Si « AmazonProvided DNS » est absent du jeu d'options, le serveur DHCP IPv4 ne renverra pas d'adresse, que d'autres serveurs de noms IPv4 soient mentionnés ou non dans le jeu d'options.

Les serveurs Amazon DHCP peuvent également fournir un préfixe IPv4 ou IPv6 complet à une interface réseau de votre VPC à l'aide de la délégation de préfixes (voir Affectation de préfixes aux

interfaces réseau Amazon EC2 dans le guide de l'utilisateur Amazon EC2). La délégation de préfixes IPv4 n'est pas fournie dans les réponses DHCP. Les préfixes IPv4 attribués à l'interface peuvent être récupérés à l'aide de l'IMDS (voir les catégories de métadonnées des instances dans le guide de l'utilisateur Amazon EC2).

Concepts des jeux d'options DHCP

Un jeu d'options DHCP est un groupe de paramètres réseau utilisé par les ressources de votre VPC, telles que les instances EC2, pour communiquer sur votre réseau virtuel.

Chaque région possède un jeu d'options DHCP par défaut. Chaque VPC utilise le jeu d'options DHCP par défaut pour sa région, sauf si vous créez et associez un jeu d'options DHCP personnalisé au VPC ou si vous configurez le VPC sans jeu d'options DHCP.

Si aucun ensemble d'options DHCP n'est configuré pour votre VPC :

- Pour les instances EC2 créées sur le système Nitro, AWS sera configuré en `169.254.169.253` tant que serveur de noms de domaine par défaut.
- Pour les instances EC2 basées sur Xen, aucun serveur de noms de domaine ne sera configuré et, comme les instances du VPC n'ont pas accès à un serveur DNS, elles ne pourront pas accéder à Internet.

Vous pouvez associer un jeu d'options DHCP à plusieurs VPC, mais chaque VPC ne peut avoir qu'un seul jeu d'options DHCP associé.

Si vous supprimez un VPC, le jeu d'options DHCP associé au VPC est désassocié de celui-ci.

Table des matières

Jeu d'options DHCP par défaut

Le jeu d'options DHCP par défaut contient les paramètres suivants :

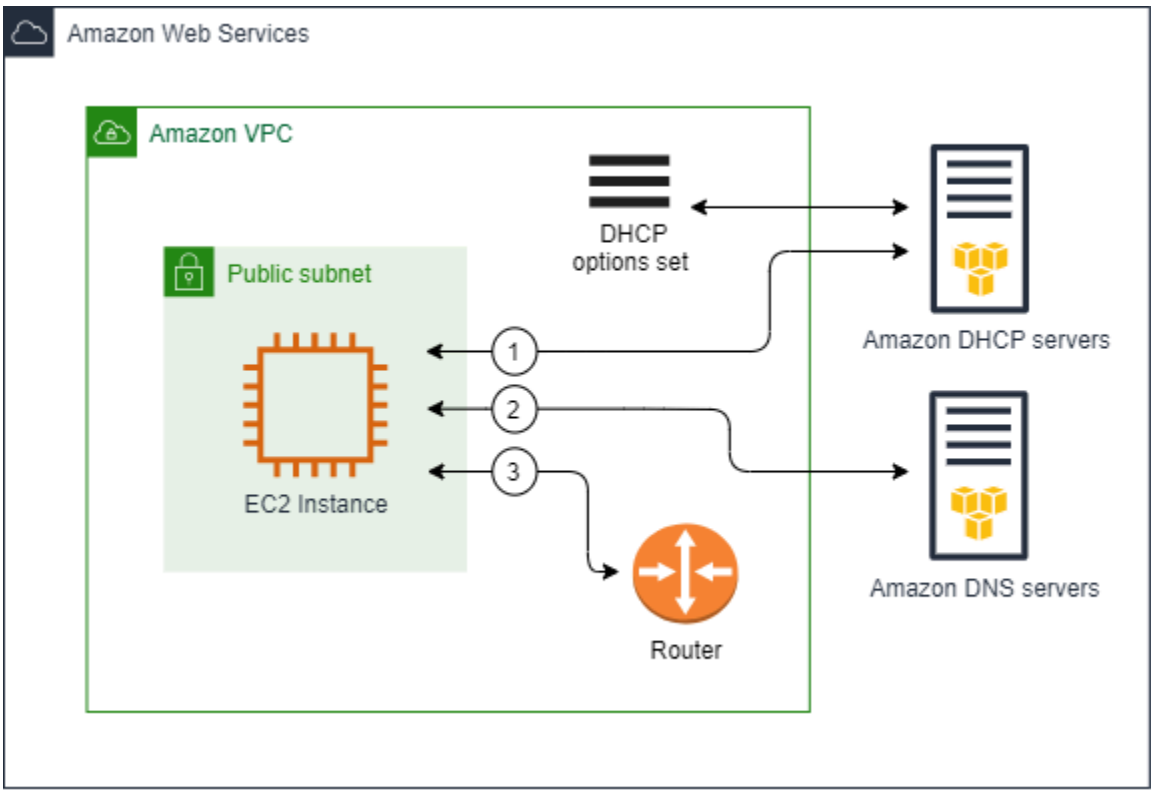
- Serveurs de noms de domaine : les serveurs DNS que vos interfaces réseau utilisent pour la résolution des noms de domaine. Pour un jeu d'options DHCP par défaut, il s'agit toujours d'`AmazonProvidedDNS`. Pour plus d'informations, consultez Serveur Amazon DNS.

- Nom de domaine : le nom de domaine qu'un client doit utiliser lors de la résolution de noms d'hôte à l'aide du système de noms de domaine (DNS). Pour en savoir plus sur les noms de domaine utilisés pour des instances EC2, consultez la section Noms d'hôtes d'instances Amazon EC2.
- Durée de location préférée IPv6 : fréquence à laquelle une instance en cours d'exécution à laquelle un IPv6 est attribué est renouvelée par le protocole DHCPv6. La durée de bail par défaut est de 140 secondes. Le renouvellement du bail a généralement lieu lorsque la moitié de la durée du bail est écoulée.

Lorsque vous utilisez un jeu d'options DHCP par défaut, les paramètres suivants ne sont pas utilisés, mais il existe des paramètres par défaut pour les instances EC2 :

- Serveurs NTP : par défaut, les instances EC2 utilisent le Service de synchronisation temporelle d'Amazon pour récupérer l'heure.
- Serveurs de nom NetBIOS : pour les instances EC2 exécutant Windows, le nom de l'ordinateur NetBIOS est un nom convivial attribué à l'instance pour l'identifier sur le réseau. Le serveur de nom NetBIOS gère une liste de mappages entre les noms d'ordinateurs NetBIOS et les adresses réseau pour les réseaux qui utilisent NetBIOS comme service de dénomination.
- Type de nœud NetBIOS : pour les instances EC2 exécutant Windows, c'est la méthode utilisée par les instances pour résoudre les noms NetBIOS en adresses IP.

Lorsque vous utilisez le jeu d'options par défaut, le serveur Amazon DHCP utilise les paramètres réseau du jeu d'options par défaut. Lorsque vous lancez des instances dans votre VPC, elles effectuent les opérations suivantes, comme indiqué dans le schéma : (1) interagissent avec le serveur DHCP, (2) interagissent avec le serveur Amazon DNS et (3) se connectent à d'autres dispositifs du réseau via le routeur de votre VPC. Les instances peuvent interagir avec le serveur DHCP d'Amazon à tout moment pour obtenir leur bail d'adresse IP et leurs paramètres réseau supplémentaires.



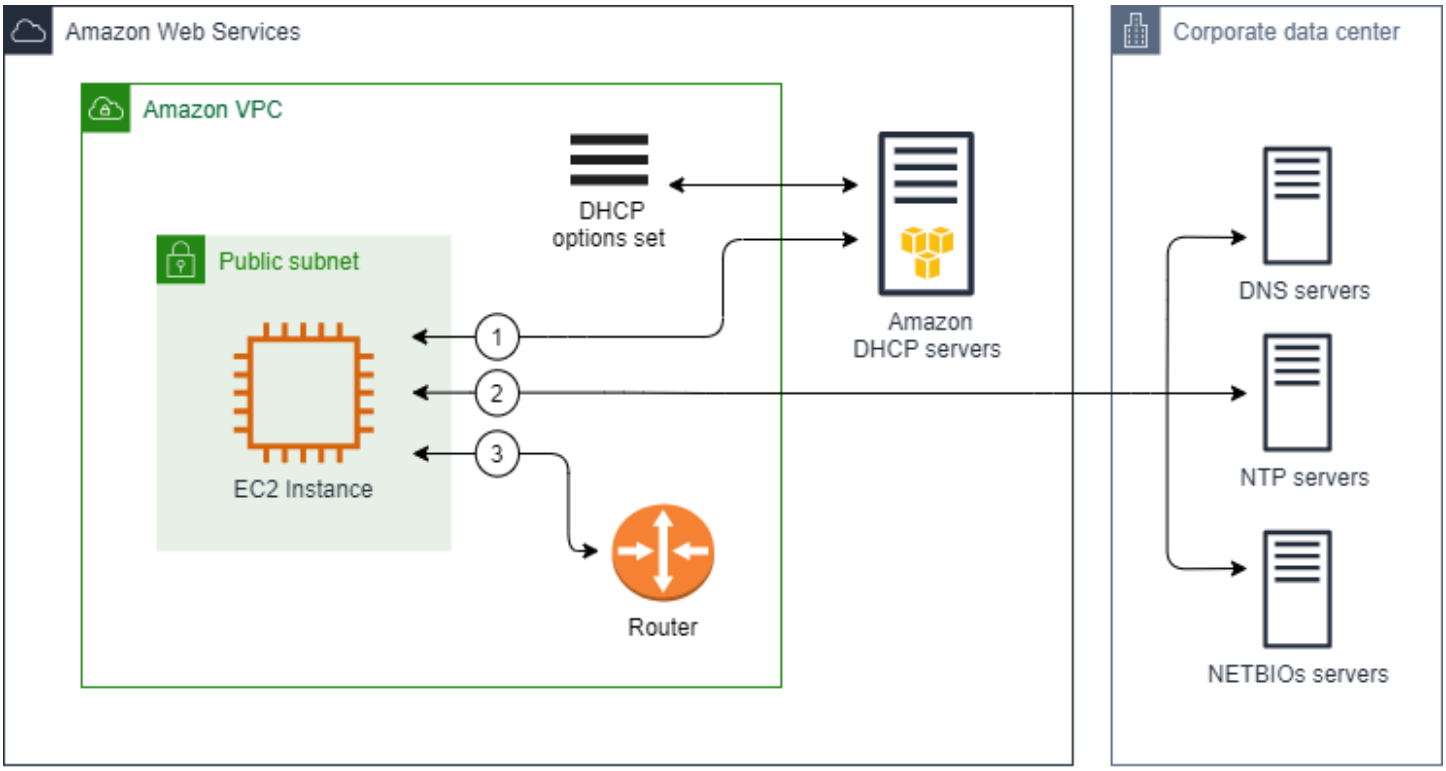
Jeu d'options DHCP personnalisé

Vous pouvez créer un jeu d'options DHCP personnalisé avec les paramètres suivants, puis l'associer à un VPC :

- Serveurs de noms de domaine : les serveurs DNS que vos interfaces réseau utilisent pour la résolution des noms de domaine.
- Nom de domaine : le nom de domaine qu'un client utilise lors de la résolution de noms d'hôte à l'aide du système de noms de domaine (DNS).
- Serveurs NTP : les serveurs NTP qui fournissent le temps aux instances.
- Serveurs de nom NetBIOS : pour les instances EC2 exécutant Windows, le nom de l'ordinateur NetBIOS est un nom convivial attribué à l'instance pour l'identifier sur le réseau. Un serveur de noms NetBIOS gère une liste de mappages entre les noms d'ordinateurs NetBIOS et les adresses réseau pour les réseaux qui utilisent NetBIOS comme service de dénomination.
- Type de nœud NetBIOS : pour les instances EC2 exécutant Windows, la méthode utilisée par les instances pour résoudre les noms NetBIOS en adresses IP.
- Durée de location préférée IPv6 (facultatif) : valeur (en secondes, minutes, heures ou années) indiquant la fréquence à laquelle une instance en cours d'exécution à laquelle un IPv6 est attribué est renouvelée par le protocole DHCPv6. Les valeurs acceptables sont comprises entre 140 et

4294967295 secondes (environ 138 ans). Si aucune valeur n'est saisie, la durée du bail par défaut est de 140 secondes. Si vous utilisez l'adressage à long terme pour les instances EC2, vous pouvez augmenter la durée du bail et éviter de fréquentes demandes de renouvellement de bail. Le renouvellement du bail a généralement lieu lorsque la moitié de la durée du bail est écoulée.

Lorsque vous utilisez un jeu d'options personnalisé, les instances lancées dans votre VPC effectuent les opérations suivantes, comme indiqué dans le schéma : (1) utilisent les paramètres réseau du jeu d'options DHCP personnalisé, (2) interagissent avec les serveurs DNS, NTP et NetBIOS spécifiés dans le jeu d'options DHCP personnalisé et (3) se connectent à d'autres dispositifs du réseau via le routeur de votre VPC.



Tâches associées

- Créer un jeu d'options DHCP
- Modifier le jeu d'options associé à un VPC

Travailler avec des jeux d'options DHCP

Utilisez les procédures suivantes pour afficher et travailler avec des jeux d'options DHCP. Pour plus d'informations sur le fonctionnement des jeux d'options DHCP, consultez the section called “Concepts des jeux d'options DHCP”.

Tâches

Afficher vos jeux d'options DHCP

Vous pouvez afficher vos jeux d'options DHCP comme suit. Pour un jeu d'options DHCP par défaut, les seuls paramètres comportant des valeurs sont le nom de domaine et les serveurs de noms de domaine.

Pour afficher vos jeux d'options DHCP à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez DHCP Option Sets (Jeux d'options DHCP).
3. Sélectionnez l'ID d'un jeu d'options DHCP pour ouvrir sa page de détails.

Pour afficher vos jeux d'options DHCP à l'aide de la ligne de commande

Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Utilisation d'Amazon VPC.

- describe-dhcp-options (AWS CLI)
- Get-EC2DhcpOption (AWS Tools for Windows PowerShell)

Créer un jeu d'options DHCP

Un jeu d'options DHCP personnalisé vous permet de personnaliser votre VPC avec votre propre serveur DNS, nom de domaine, etc. Vous pouvez créer autant de jeux d'options DHCP

supplémentaires que vous le souhaitez. Cependant, vous ne pouvez associer qu'un seul jeu d'options DHCP à la fois à un VPC.

> **Note**
>
> Après avoir créé un jeu d'options DHCP, vous ne pouvez pas le modifier. Pour mettre à jour les options DHCP de votre VPC, vous devez créer un nouveau jeu d'options DHCP, puis l'associer à votre VPC.

Pour créer un jeu d'options DHCP à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez DHCP Option Sets (Jeux d'options DHCP).
3. Choisissez Create DHCP options set (Créer un jeu d'options DHCP).
4. Pour Tag settings (Paramètres d'identification), saisissez en option un nom pour le jeu d'options DHCP. Si vous saisissez une valeur, elle crée automatiquement une identification Name (Nom) pour le jeu d'options DHCP.
5. Pour le options DHCP, indiquez les paramètres de configuration dont vous avez besoin.

   - Domain name (facultatif) : saisissez le nom de domaine qu'un client devrait utiliser lors de la résolution de noms d'hôte via le système de noms de domaine. Si vous n'utilisez pas le AmazonProvided DNS, vos serveurs de noms de domaine personnalisés doivent résoudre le nom d'hôte comme il convient. Si vous utilisez une zone hébergée privée Amazon Route 53, vous pouvez utiliser le AmazonProvided DNS. Pour plus d'informations, consultez Attributs DNS pour votre VPC.

     Certains systèmes d'exploitation Linux acceptent plusieurs noms de domaines séparés par des espaces. Cependant, Windows et les autres systèmes d'exploitation Linux traitent la valeur comme un domaine unique, ce qui entraîne un comportement inattendu. Si votre jeu d'options DHCP est associé à un VPC dont les instances exécutent des systèmes d'exploitation qui traitent la valeur comme un domaine unique, spécifiez un seul nom de domaine.
   - Domain name servers (Serveurs de nom de domaine) (facultatif) : saisissez les serveurs DNS qui seront utilisés pour résoudre l'adresse IP de l'hôte à partir d'un nom d'hôte précédent.

Vous pouvez saisir soit **AmazonProvidedDNS**, soit des serveurs de noms de domaine personnalisés. L'utilisation des deux peut entraîner un comportement inattendu. Vous pouvez saisir les adresses IP de quatre serveurs de noms de domaine IPv4 au maximum (ou jusqu'à trois serveurs de noms de domaine IPv4 et **AmazonProvidedDNS**) et quatre serveurs de noms de domaine IPv6 séparés par des virgules. Bien que vous puissiez spécifier jusqu'à huit serveurs de noms de domaine, certains systèmes d'exploitation pourraient imposer des limites inférieures. Pour plus d'informations sur le AmazonProvidedDNS et le serveur DNS Amazon, consultezServeur Amazon DNS.

> **Important**
>
> Si votre VPC possède une passerelle Internet, veillez à spécifier votre propre serveur DNS ou un serveur DNS Amazon (AmazonProvidedDNS) pour la valeur des serveurs de noms de domaine. Sinon, les instances du VPC n'auront pas accès au DNS, ce qui désactive l'accès à Internet.

- NTP servers (facultatif) : Saisissez les adresses IP de huit serveurs NTP (Network Time Protocol) au maximum (quatre adresses IPv4 et quatre adresses IPv6).

  Les serveurs NTP fournissent le temps à votre réseau. Vous pouvez spécifier Amazon Time Sync Service à l'adresse IPv4 `169.254.169.123` ou à l'adresse IPv6 `fd00:ec2::123`. Les instances communiquent par défaut avec Amazon Time Sync Service. Notez que l'adresse IPv6 n'est accessible que sur les Instances EC2 reposant sur le système Nitro.

  Pour plus d'informations sur les options des serveurs NTP, consultez RFC 2132. Pour plus d'informations sur le service Amazon Time Sync, consultez Définir l'heure pour votre instance dans le guide de l'utilisateur Amazon EC2.

- Serveurs de noms NetBIOS (facultatif) : entrez les adresses IP de quatre serveurs de noms NetBIOS au maximum.

  Pour les instances EC2 exécutant un Windows OS, le nom de l'ordinateur NetBIOS est un nom convivial attribué à l'instance pour l'identifier sur le réseau. Le serveur de nom NetBIOS gère une liste de mappages entre les noms d'ordinateurs NetBIOS et les adresses réseau pour les réseaux qui utilisent NetBIOS comme service de dénomination.

- NetBIOS node type (Type de nœud NetBIOS) (facultatif) : Saisissez **1**, **2**, **4**, ou **8**. Nous vous recommandons de spécifier **2** (point-to-point ou P-node). La diffusion et le multicast ne sont

pas pris en charge pour l'instant. Pour plus d'informations sur ces types de nœud, consultez la section 8.7 de la page RFC 2132 et la section 10 de la page RFC 1001.

Pour les instances EC2 exécutant un Windows OS, c'est la méthode utilisée par les instances pour résoudre les noms NetBIOS en adresses IP. Dans le jeu d'options par défaut, il n'y a aucune valeur pour le type de nœud NetBIOS.

- Durée de location préférée IPv6 (facultatif) : valeur (en secondes, minutes, heures ou années) indiquant la fréquence à laquelle une instance en cours d'exécution à laquelle un IPv6 est attribué est renouvelée par le protocole DHCPv6. Les valeurs acceptables sont comprises entre 140 et 2147483647 secondes (environ 68 ans). Si aucune valeur n'est saisie, la durée du bail par défaut est de 140 secondes. Si vous utilisez l'adressage à long terme pour les instances EC2, vous pouvez augmenter la durée du bail et éviter de fréquentes demandes de renouvellement de bail. Le renouvellement du bail a généralement lieu lorsque la moitié de la durée du bail est écoulée.

6. Ajoutez des balises.
7. Choisissez Create DHCP options set (Créer un jeu d'options DHCP). Notez le nom ou l'ID du nouveau jeu d'options DHCP.
8. Pour configurer un VPC afin d'utiliser le nouveau jeu d'options, consultez Modifier le jeu d'options associé à un VPC.

Pour créer un jeu d'options DHCP pour votre VPC à l'aide de la ligne de commande

Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Utilisation d'Amazon VPC.

- create-dhcp-options (AWS CLI)
- New-EC2DhcpOption (AWS Tools for Windows PowerShell)

Modifier le jeu d'options associé à un VPC

Après avoir créé un jeu d'options DHCP, vous pouvez l'associer à un ou plusieurs VPC. Vous ne pouvez associer qu'un seul jeu d'options DHCP à la fois à un VPC. Si vous n'associez aucun jeu d'options DHCP à un VPC, cela désactive la résolution des noms de domaine dans le VPC.

Lorsque vous associez un nouveau jeu d'options DHCP à un VPC, toutes les instances existantes et toutes les nouvelles instances que vous lancez dans ce VPC utilisent les nouvelles options. Vous ne devez pas redémarrer ni relancer vos instances. Les instances récupèrent automatiquement les

changements en quelques heures, selon la fréquence à laquelle elles renouvellent leur bail DHCP. Si vous préférez, vous pouvez explicitement renouveler le bail grâce au système d'exploitation sur l'instance.

Pour modifier le jeu d'options DHCP associé à un VPC à l'aide de la console

1. Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Your VPCs (Vos VPC).
3. Sélectionnez la case à cocher du VPC, puis choisissez Actions, Edit VPC Settings (Modifier les paramètres du VPC).
4. Pour DHCP options set (jeu d'options DHCP), choisissez un nouveau jeu d'options DHCP. Vous pouvez également choisir Aucun jeu d'options DHCP pour désactiver la résolution de nom de domaine pour le VPC.
5. Choisissez Enregistrer.

Pour modifier le jeu d'options DHCP associé à un VPC à l'aide de la ligne de commande

Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Utilisation d'Amazon VPC.

- associate-dhcp-options (AWS CLI)
- Register-EC2DhcpOption (AWS Tools for Windows PowerShell)

Supprimer un jeu d'options DHCP

Quand vous n'avez plus besoin d'un jeu d'options DHCP, utilisez la procédure suivante pour le supprimer. Vous ne pouvez pas supprimer un jeu d'options DHCP s'il est en cours d'utilisation. Pour chaque VPC associé au jeu d'options DHCP à supprimer, vous devez associer un jeu d'options DHCP différent au VPC ou configurer le VPC pour qu'il n'utilise aucun jeu d'options DHCP. Pour plus d'informations, consultez the section called "Modifier le jeu d'options associé à un VPC".

Pour supprimer un jeu d'options DHCP à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez DHCP Option Sets (Jeux d'options DHCP).
3. Sélectionnez le bouton radio du jeu d'options DHCP à supprimer, puis choisissez Actions, Supprimer le jeu d'options DHCP.

4. Dans la boîte de dialogue de confirmation, entrez **`delete`**, puis choisissez Supprimer le jeu d'options DHCP.

Pour supprimer un jeu d'options DHCP à l'aide de la ligne de commande

Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Utilisation d'Amazon VPC.

- delete-dhcp-options (AWS CLI)
- Remove-EC2DhcpOption (AWS Tools for Windows PowerShell)

Attributs DNS pour votre VPC

Le DNS (Domain Name System) est une norme permettant la résolution des noms utilisés sur Internet en leurs adresses IP correspondantes. Un nom d'hôte DNS est un nom attribué de façon unique et absolue à un ordinateur. Il est composé d'un nom d'hôte et d'un nom de domaine. Les serveurs DNS résolvent les noms d'hôte DNS en adresses IP correspondantes.

Les adresses IPv4 publiques permettent de communiquer sur Internet, tandis que les adresses IPv4 privées permettent de communiquer au sein du réseau de l'instance. Pour plus d'informations, veuillez consulter Adressage IP pour vos VPC et sous-réseaux.

Amazon fournit un serveur DNS (Amazon Route 53 Resolver) pour votre VPC. Pour utiliser votre propre serveur DNS, créez un jeu d'options DHCP pour votre VPC. Pour plus d'informations, veuillez consulter Jeux d'options DHCP dans Amazon VPC.

Table des matières

Serveur Amazon DNS

Le résolveur Route 53 (également appelé « serveur DNS Amazon » ou « AmazonProvided DNS ») est un service de résolution DNS intégré à chaque zone de disponibilité d'une AWS région. Route 53 Resolver se localise aux adresses `169.254.169.253` (IPv4) et `fd00:ec2::253` (IPv6), ainsi que dans la plage CIDR IPv4 privée principale fournie à votre VPC plus deux. Par exemple, si vous disposez d'un VPC avec une adresse CIDR IPv4 `10.0.0.0/16` et une adresse CIDR IPv6 `fd00:ec2::253`, vous pouvez accéder à Route 53 Resolver à l'adresse `169.254.169.253` (IPv4), `fd00:ec2::253` (IPv6) ou `10.0.0.2` (IPv4). Les ressources d'un VPC utilisent une adresse locale de lien pour les requêtes DNS. Ces requêtes sont transportées vers le résolveur Route 53 en privé et ne sont pas visibles sur le réseau. Dans un sous-réseau uniquement IPv6, l'adresse locale du lien IPv4 (169.254.169.253) est toujours accessible tant que « DNS » est le serveur de noms dans le jeu d'options DHCP. AmazonProvided

Lorsque vous lancez une instance dans un VPC, nous fournissons l'instance avec un nom d'hôte DNS privé. Nous fournissons également un nom d'hôte DNS public si l'instance est configurée avec une adresse IPv4 publique et que les attributs DNS VPC sont activés.

Le format du nom d'hôte DNS privé dépend de la façon dont vous configurez l'instance EC2 lorsque vous la lancez. Pour plus d'informations sur les types de noms d'hôtes DNS privés, consultez Dénomination d'instances EC2.

Le serveur Amazon DNS dans votre VPC est utilisé pour résoudre les noms de domaine DNS que vous spécifiez dans une zone hébergée privée dans Route 53. Pour de plus amples informations sur les zones hébergées privées, veuillez consulter Utilisation des zones hébergées privées dans le Guide du développeur Amazon Route 53.

Règles et considérations

Lors de l'utilisation du serveur Amazon DNS, les règles et considérations suivantes s'appliquent.

- Il n'est pas possible de filtrer le trafic vers ou depuis le serveur Amazon DNS à l'aide de groupes de sécurité ou de liste de contrôle d'accès réseau.
- Les services qui utilisent le framework Hadoop, tels que Amazon EMR, ont besoin d'instances pour résoudre leurs propres noms de domaine complets (FQDN). Dans de tels cas, une résolution DNS peut échouer si l'option `domain-name-servers` est définie comme valeur personnalisée. Pour garantir une résolution DNS appropriée, pensez à ajouter un redirecteur conditionnel à votre serveur DNS pour faire suivre les requêtes pour le domaine *`region-name`*`.compute.internal`

vers le serveur Amazon DNS. Pour plus d'informations, veuillez consulter Configuration d'un VPC pour héberger des clusters dans le Guide de gestion Amazon EMR.

- Amazon Route 53 Resolver ne prend en charge que les requêtes DNS récursives.

Noms d'hôte DNS

Lorsque vous lancez une instance, elle reçoit toujours une adresse IPv4 privée et un nom d'hôte DNS privé qui correspond à son adresse IPv4 privée. Si votre instance possède une adresse IPv4 publique, les attributs DNS de son VPC déterminent si elle reçoit un nom d'hôte DNS public qui correspond à l'adresse IPv4 publique. Pour plus d'informations, veuillez consulter Attributs DNS dans votre VPC.

Lorsque le serveur DNS fourni par Amazon est activé, les noms d'hôte DNS sont attribués et résolus comme suit.

Private IP DNS name (IPv4 only) (Nom DNS de l'adresse IP privée [IPv4 uniquement])

Vous pouvez utiliser le nom d'hôte DNS de l'adresse IP privée (IPv4 uniquement) pour les communications entre les instances du même VPC. Vous pouvez résoudre les noms d'hôte DNS IP privés (IPv4 uniquement) d'autres instances dans d'autres VPC à condition que les instances se trouvent dans la même AWS région et que le nom d'hôte de l'autre instance se situe dans la plage d'espaces d'adressage privés définie par la RFC 1918 :, et. `10.0.0.0 - 10.255.255.255 (10/8 prefix)` `172.16.0.0 - 172.31.255.255 (172.16/12 prefix)` `192.168.0.0 - 192.168.255.255 (192.168/16 prefix)`

Private resource DNS name (Nom DNS de la ressource privée)

Nom DNS basé sur RBN qui peut se traduire par les enregistrements DNS A et AAAA sélectionnés pour cette instance. Ce nom d'hôte DNS est visible dans les détails des instances des sous-réseaux à double pile et IPv6 uniquement. Pour de plus amples informations sur RBN, veuillez consulter Types de noms d'hôte des instances Amazon EC2.

Public IPv4 DNS (DNS IPv4 public)

Un nom d'hôte DNS IPv4 public (externe) prend la forme `ec2-`*`public-ipv4-address`*`.compute-1.amazonaws.com` pour la région `us-east-1` et `ec2-`*`public-ipv4-address`*`.`*`region`*`.compute.amazonaws.com` pour les autres régions. Le DNS Amazon résout un nom d'hôte DNS public en adresse IPv4 publique de l'instance en dehors du réseau de cette dernière et nous la résolvons en adresse IPv4 privée de l'instance depuis son réseau. Pour plus

d'informations, consultez la section Adresses IPv4 publiques et noms d'hôte DNS externes dans le guide de l'utilisateur Amazon EC2.

Attributs DNS dans votre VPC

Les attributs VPC suivants déterminent la prise en charge DNS fournie pour votre VPC. Si les deux attributs sont activés, une instance lancée dans le VPC reçoit un nom d'hôte DNS public si une adresse IPv4 publique ou une adresse IP Elastic lui est attribuée à la création. Si vous activez les deux attributs pour un VPC qui ne l'était pas auparavant, les instances qui ont déjà été lancées dans ce VPC reçoivent des noms d'hôtes DNS publics si elles ont une adresse IPv4 publique ou une adresse IP Elastic.

Pour vérifier si votre VPC est activé pour ces attributs, veuillez consulter Afficher et mettre à jour les attributs DNS pour votre VPC.

Attribut	Description
`enableDnsHostnames`	Détermine si le VPC prend en charge l'attribution de noms d'hôtes DNS publics à des instances avec des adresses IP publiques. La valeur par défaut de cet attribut est `false`, sauf si le VPC est un VPC par défaut. Notez les règles et considérations relatives à cet attribut ci-dessous.
`enableDnsSupport`	Détermine si le VPC prend en charge la résolution DNS via le serveur DNS fourni par Amazon. Si cet attribut est `true`, les requêtes adressées au serveur DNS fourni par Amazon aboutissent. Pour plus d'informations, consultez Serveur Amazon DNS. La valeur par défaut de cet attribut est `true`. Notez les règles et considérations relatives à cet attribut ci-dessous.

Règles et considérations

- Si les deux attributs sont définis sur `true`, les actions suivantes ont lieu :

  - Les instances avec une adresse IP publique reçoivent les noms d'hôte DNS publics correspondants.
  - Le Amazon Route 53 Resolver serveur peut résoudre les noms d'hôte DNS privés fournis par Amazon.
- Si au moins un des attributs est défini sur `false`, les actions suivantes se produisent :
  - Les instances avec une adresse IP publique ne reçoivent pas de noms d'hôte DNS publics correspondants.
  - Amazon Route 53 Resolver Impossible de résoudre les noms d'hôte DNS privés fournis par Amazon.
  - Les instances reçoivent des noms d'hôte DNS privés personnalisés si le jeu d'options DHCP contient un nom de domaine personnalisé. Si vous n'utilisez pas le serveur Amazon Route 53 Resolver , vos serveurs de noms de domaine personnalisés doivent résoudre le nom d'hôte si nécessaire.
- Si vous utilisez des noms de domaine DNS personnalisés définis dans une zone hébergée privée dans Amazon Route 53 ou un DNS privé avec des points de terminaison de VPC d'interface (AWS PrivateLink), vous devez définir les attributs `enableDnsHostnames` et `enableDnsSupport` sur `true`.
- Ils Amazon Route 53 Resolver peuvent convertir les noms d'hôte DNS privés en adresses IPv4 privées pour tous les espaces d'adressage, y compris lorsque la plage d'adresses IPv4 de votre VPC se situe en dehors des plages d'adresses IPv4 privées spécifiées par la RFC 1918. Toutefois, si vous avez créé votre VPC avant octobre 2016, le Amazon Route 53 Resolver ne résout pas les noms d'hôtes DNS privés si la plage d'adresses IPv4 de votre VPC se situe en dehors de ces plages. Pour activer la prise en charge correspondante, contactez AWS Support.
- Si vous utilisez l'appairage de VPC, vous devez activer les deux attributs pour les deux VPC et vous devez activer la résolution DNS pour la connexion d'appairage. Pour plus d'informations, consultez Activation de la résolution DNS pour une connexion d'appairage de VPC.

Quotas DNS

Chaque instance EC2 peut envoyer 1024 paquets par seconde par interface réseau au Route 53 Resolver (spécifiquement l'adresse .2, telle que 10.0.0.2 et 169.254.169.253). Ce quota ne peut pas être augmenté. Le nombre de requêtes DNS par seconde prises en charge par Route 53 Resolver varie selon le type de requête, la taille de la réponse et le protocole utilisé. Pour plus d'informations

sur les recommandations relatives à une architecture DNS évolutive, veuillez consulter le Guide technique DNS hybride AWS avec Active Directory.

Si vous atteignez le quota, le Route 53 Resolver rejette le trafic. Certaines des causes de l'atteinte du quota peuvent être un problème de limitation DNS ou des requêtes de métadonnées d'instance qui utilisent l'interface réseau du Route 53 Resolver. Pour plus d'informations sur la résolution des problèmes de limitation DNS VPC, consultez Comment puis-je déterminer si mes requêtes DNS envoyées vers le serveur DNS fourni par Amazon échouent en raison de limitations DNS du VPC ? Pour plus d'informations sur la récupération des métadonnées d'instance, consultez la section Récupérer les métadonnées d'instance dans le guide de l'utilisateur Amazon EC2.

Afficher les noms d'hôte DNS de votre instance EC2

Vous pouvez afficher les noms d'hôte DNS pour une instance en cours d'exécution ou une interface réseau à l'aide de la console Amazon EC2 ou de la ligne de commande.

Les champs DNS public (IPv4) et DNS privé sont disponibles lorsque les options DNS sont activées pour le VPC associé à l'instance. Pour plus d'informations, consultez the section called "Attributs DNS dans votre VPC".

Instance

Pour afficher les noms d'hôte DNS d'une instance à l'aide de la console :

1. Ouvrez la console Amazon EC2 sur https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez votre instance dans la liste.
4. Dans le volet des détails, les noms d'hôte DNS s'affichent dans les champs DNS public (IPv4) et DNS privé, le cas échéant.

Pour afficher les noms d'hôte DNS d'une instance à l'aide de la ligne de commande :

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Utilisation d'Amazon VPC.

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

Interface réseau

Pour afficher le nom d'hôte DNS privé d'une interface réseau à l'aide de la console :

1. Ouvrez la console Amazon EC2 sur https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Dans la liste, sélectionnez l'interface réseau.
4. Dans le volet des détails, le nom d'hôte DNS privé s'affiche dans le champ Private DNS (IPv4) (DNS privé (IPv4)).

Pour afficher les noms d'hôte DNS d'une interface réseau à l'aide de la ligne de commande :

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Utilisation d'Amazon VPC.

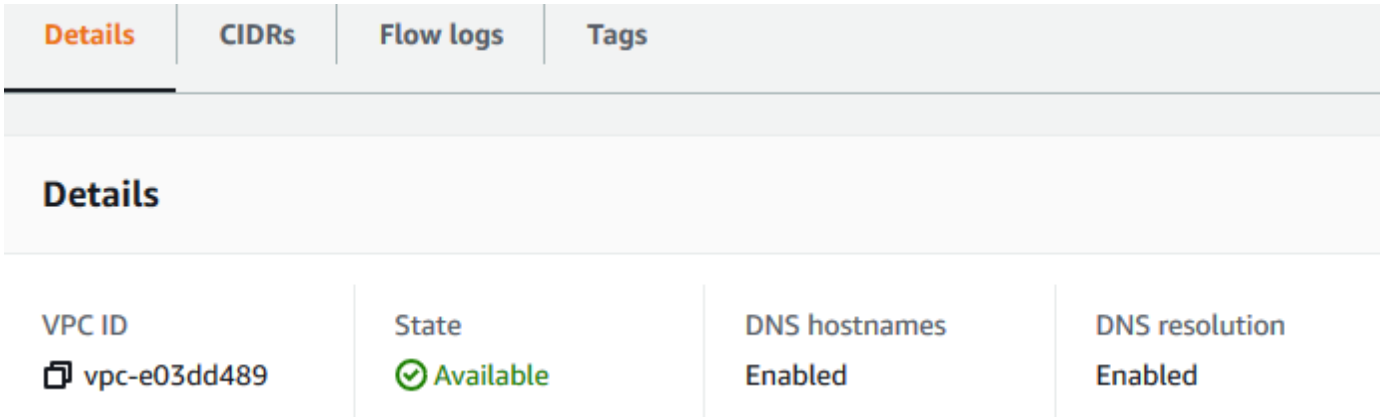
- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Afficher et mettre à jour les attributs DNS pour votre VPC

Vous pouvez afficher et mettre à jour les attributs de support DNS pour votre VPC à l'aide de la console Amazon VPC.

Pour décrire et mettre à jour la prise en charge de DNS pour un VPC à l'aide de la console :

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Vos VPC.
3. Cochez la case correspondant au VPC.
4. Examinez le informations contenues dans Détails). Dans cet exemple, Noms d'hôte DNS et Résolution DNS sont activés.



5. Pour mettre à jour ces paramètres, choisissez Actions, puis Edit VPC Settings (Modifier les paramètres du VPC). Sélectionnez ou déselectionnez Enable (Activer) sur l'attribut DNS approprié et choisissez Save changes (Enregistrer les modifications).

Pour décrire la prise en charge de DNS pour un VPC à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Utilisation d'Amazon VPC.

- describe-vpc-attribute (AWS CLI)
- Get-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Pour mettre à jour la prise en charge de DNS pour un VPC à l'aide de la ligne de commande :

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Utilisation d'Amazon VPC.

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Zones hébergées privées

Pour accéder aux ressources de votre VPC à l'aide de noms de domaine DNS personnalisés, par exemple`example.com`, au lieu d'utiliser des adresses IPv4 privées ou des noms d'hôte DNS privés AWS fournis, vous pouvez créer une zone hébergée privée dans Route 53. Une zone hébergée privée est un conteneur qui comporte des informations sur la façon dont vous souhaitez acheminer le trafic pour un domaine et ses sous-domaines dans un ou plusieurs VPC, sans

exposer vos ressources à Internet. Vous pouvez ensuite créer des ensembles d'enregistrements de ressource Route 53, qui déterminent de quelle manière Route 53 répond aux requêtes pour votre domaine et vos sous-domaines. Par exemple, si vous souhaitez que les requêtes du navigateur pour exemple.com soient acheminées vers un serveur Web dans votre VPC, vous devez créer un enregistrement A dans votre zone hébergée privée et spécifier l'adresse IP de ce serveur Web. Pour de plus amples informations sur la création d'une zone hébergée privée, veuillez consulter Utilisation de zones hébergées privées dans le Guide du développeur Amazon Route 53.

Pour accéder aux ressources à l'aide de noms de domaine DNS personnalisés, vous devez être connecté à une instance au sein de votre VPC. À partir de votre instance, vous pouvez tester si la ressource incluse dans votre zone hébergée privée est accessible depuis son nom DNS personnalisé, à l'aide de la commande `ping` (par exemple, `ping mywebserver.example.com`). Assurez-vous que les règles de groupe de sécurité de votre instance autorisent le trafic ICMP entrant pour que la commande `ping` fonctionne.

Les zones hébergées privées ne prennent pas en charge les relations transitives en dehors du VPC. Par exemple, vous ne pouvez pas accéder à vos ressources à l'aide de leurs noms DNS privés personnalisés depuis l'autre extrémité d'une connexion VPN.

> **Important**
>
> Si vous utilisez des noms de domaine DNS personnalisés définis dans une zone hébergée privée dans Amazon Route 53, vous devez définir les attributs `enableDnsHostnames` et `enableDnsSupport` sur `true`.

Utilisation des adresses réseau pour votre VPC

Network Address Usage (NAU) est une métrique appliquée aux ressources de votre réseau virtuel pour vous permettre de planifier et de surveiller la taille de votre VPC. Chaque unité NAU contribue à un total qui représente la taille de votre VPC.

Il est important de connaître le nombre total d'unités qui constituent la NAU de votre VPC, car les quotas de VPC suivants limitent la taille d'un VPC :

- Utilisation des adresses réseau : nombre maximum d'unités NAU qu'un VPC peut avoir. Chaque VPC peut avoir jusqu'à 64 000 unités NAU par défaut. Vous pouvez également demander une augmentation de quota jusqu'à 256 000.

- Utilisation des adresses réseau appairées : nombre maximum d'unités NAU pour un VPC et tous ses VPC appairés. Si un VPC est appairé à d'autres VPC de la même région, les VPC combinés peuvent avoir jusqu'à 128 000 unités NAU par défaut. Vous pouvez également demander une augmentation de quota jusqu'à 512 000. Les VPC qui sont appairés à des régions différentes ne contribuent pas à cette limite.

Vous pouvez utiliser la NAU selon les manières suivantes :

- Avant de créer votre réseau virtuel, calculez les unités NAU pour déterminer si vous devez répartir les charges de travail sur plusieurs VPC.
- Une fois que vous avez créé votre VPC, utilisez Amazon CloudWatch pour surveiller l'utilisation du VPC au titre du NAU afin qu'elle ne dépasse pas les limites de quota NAU. Pour plus d'informations, consultez the section called "Métriques CloudWatch".

Comment la NAU est calculée

Si vous comprenez comment la NAU est calculée, cela peut vous aider à planifier la mise à l'échelle de vos VPC.

Le tableau suivant explique quelles ressources constituent le nombre de NAU dans un VPC et le nombre d'unités NAU utilisées par chaque ressource. Certaines AWS ressources sont représentées sous forme d'unités NAU uniques, tandis que d'autres ressources sont représentées sous forme d'unités NAU multiples. Vous pouvez utiliser le tableau pour savoir comment la NAU est calculée.

Ressource	Unités NAU
Chaque adresse IPv4 privée ou publique et chaque adresse IPv6 assignée à une interface réseau pour une instance EC2 dans le VPC	1
Interfaces réseau supplémentaires attachées à une instance EC2	1
Préfixe attribué à une interface réseau	1
Network Load Balancer par zone de disponibilité	6
Gateway Load Balancer pour AZ	6
Point de terminaison d'un VPC par zone de disponibilité	6

Ressource	Unités NAU
Réseaux de transit par passerelle	6
Fonction Lambda	6
Passerelle NAT	6
Cible de montage EFS	6

Exemples de NAU

Les exemples suivants montrent comment calculer la NAU.

Exemple 1 : deux VPC connectés via l'appairage de VPC

Les VPC appairés dans la même région contribuent à un quota NAU combiné.

- VPC 1
  - 50 équilibreurs de charge Network Load Balancer répartis en 2 sous-réseaux dans des zones de disponibilité distinctes : 600 unités NAU
  - 5 000 instances (chacune avec une adresse IPv4 et une adresse IPv6) dans un sous-réseau et 5 000 instances (chacune avec une adresse IPv4 et une adresse IPv6) dans un autre sous-réseau - 20 000 unités
  - 100 fonctions Lambda – 600 unités NAU
- VPC 2
  - 50 équilibreurs de charge Network Load Balancer répartis en 2 sous-réseaux dans des zones de disponibilité distinctes : 600 unités NAU
  - 5 000 instances (chacune avec une adresse IPv4 et une adresse IPv6) dans un sous-réseau et 5 000 instances (chacune avec une adresse IPv4 et une adresse IPv6) dans un autre sous-réseau - 20 000 unités
  - 100 fonctions Lambda – 600 unités NAU
- Nombre total d'unités NAU d'appairage : 42 400 unités
- Quota NAU d'appairage par défaut : 128 000 unités

Exemple 2 : deux VPC connectés à l'aide d'une passerelle de transit

Les VPC connectés via une passerelle de transit ne contribuent pas à un quota NAU combiné comme c'est le cas pour les VPC appairés.

- VPC 1
  - 50 équilibreurs de charge Network Load Balancer répartis en 2 sous-réseaux dans des zones de disponibilité distinctes : 600 unités NAU
  - 5 000 instances (chacune avec une adresse IPv4 et une adresse IPv6) dans un sous-réseau et 5 000 instances (chacune avec une adresse IPv4 et une adresse IPv6) dans un autre sous-réseau - 20 000 unités
  - 100 fonctions Lambda – 600 unités NAU
- VPC 2
  - 50 équilibreurs de charge Network Load Balancer répartis en 2 sous-réseaux dans des zones de disponibilité distinctes : 600 unités NAU
  - 5 000 instances (chacune avec une adresse IPv4 et une adresse IPv6) dans un sous-réseau et 5 000 instances (chacune avec une adresse IPv4 et une adresse IPv6) dans un autre sous-réseau - 20 000 unités
  - 100 fonctions Lambda – 600 unités NAU
- Nombre total de NAU par VPC : 21 200 unités
- Quota NAU par défaut par VPC : 64 000 unités

Partager votre VPC avec d'autres comptes

Le partage VPC permet Comptes AWS à plusieurs utilisateurs de créer leurs ressources applicatives, telles que les instances Amazon EC2, les bases de données Amazon Relational Database Service (RDS), les clusters AWS Lambda Amazon Redshift et les fonctions, dans des clouds privés virtuels (VPC) partagés et gérés de manière centralisée. Dans ce modèle, le compte propriétaire du VPC (propriétaire) partage un ou plusieurs sous-réseaux avec d'autres comptes (participants) appartenant à la même organisation. AWS Organizations Une fois un sous-réseau partagé, les participants peuvent afficher, créer, modifier et supprimer leurs ressources d'application contenues dans les sous-réseaux partagés avec eux. Ils ne peuvent toutefois pas afficher, modifier ou supprimer des ressources appartenant à d'autres participants ou au propriétaire du VPC.

Vous pouvez partager vos VPC afin de tirer parti du routage implicite au sein d'un VPC au profit d'applications nécessitant un niveau élevé d'interconnectivité et comprises dans les mêmes limites de confiance. Cela permet de réduire le nombre de VPC que vous créez et gérez, tout en utilisant

des comptes distincts pour la facturation et le contrôle d'accès. Vous pouvez simplifier les topologies de réseau en interconnectant des Amazon VPC partagés à l'aide de fonctionnalités de connectivité AWS PrivateLink, telles que les passerelles de transit et le peering VPC. Pour plus d'informations sur les avantages du partage de VPC, consultez Partage de VPC : une nouvelle approche des comptes multiples et de la gestion des VPC.

Table des matières

Conditions préalables relatives aux VPC partagés

- Les comptes du propriétaire et du participant du VPC doivent être gérés par. AWS Organizations
- Vous devez activer le partage des ressources dans la AWS RAM console à partir du compte de gestion de votre organisation. Pour plus d'informations, voir Activer le partage des ressources AWS Organizations dans le Guide de AWS RAM l'utilisateur.
- Vous devez créer un partage de ressources. Vous pouvez spécifier les sous-réseaux à partager lorsque vous créez le partage de ressources, ou ajouter les sous-réseaux au partage de ressources ultérieurement en suivant la procédure décrite dans la section suivante. Pour de plus amples informations, veuillez consulter Création d'un partage de ressources dans le Guide de l'utilisateur AWS RAM .

Partager un sous-réseau

Vous pouvez partager des sous-réseaux autres que ceux par défaut avec d'autres comptes au sein de votre organisation comme suit.

Pour partager un sous-réseau à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Subnets.
3. Sélectionnez votre sous-réseau, choisissez Actions, puis Share subnet (Partager un sous-réseau).
4. Sélectionnez partage de ressources, puis choisissez Share subnet (Partager un sous-réseau).

Pour partager un sous-réseau à l'aide du AWS CLI

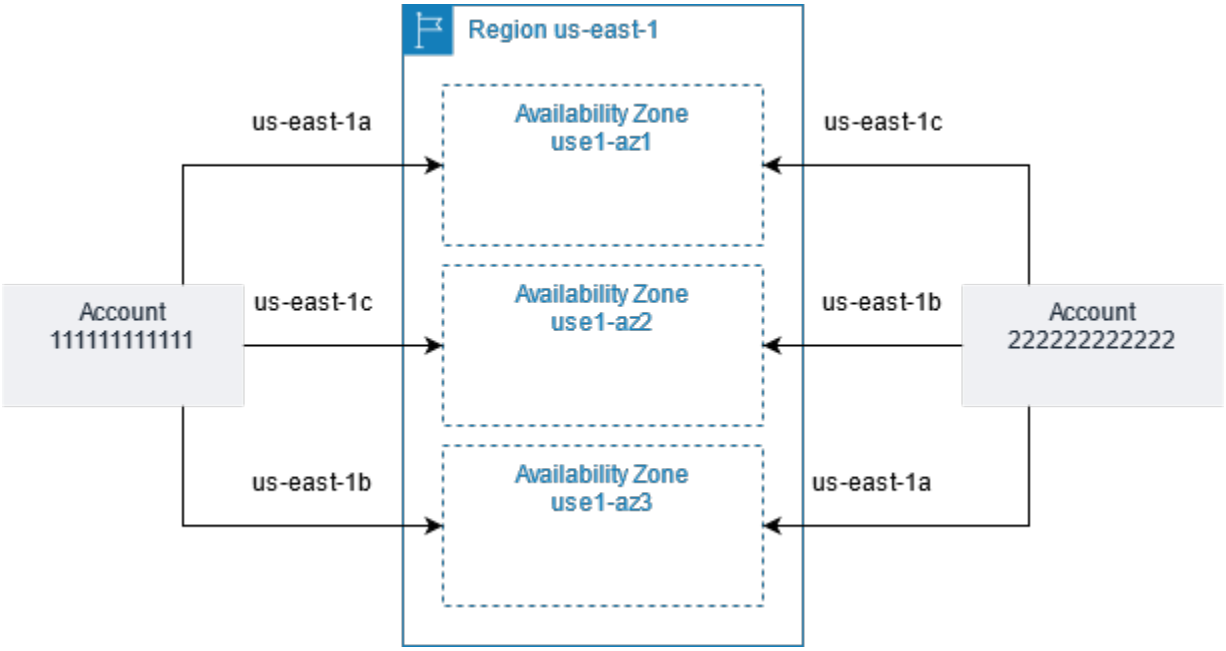
Utilisez les associate-resource-sharecommandes create-resource-shareet.

Mapper des sous-réseaux entre les zones de disponibilité

Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une Région, nous mappons indépendamment les zones de disponibilité aux noms de chaque compte. Par exemple, il est possible que la zone `us-east-1a` de disponibilité de votre AWS compte ne soit pas la même que celle `us-east-1a` d'un autre AWS compte.

Pour coordonner les zones de disponibilité entre les comptes pour le partage de VPC, vous devez utiliser un ID de zone de disponibilité, qui représente l'identifiant unique et cohérent d'une zone de disponibilité. Par exemple, `use1-az1` est l'ID de zone de disponibilité de l'une des zones de disponibilité de la région `us-east-1`. Utilisez les ID de zone de disponibilité pour déterminer l'emplacement des ressources dans un compte par rapport à un autre compte. Vous pouvez afficher l'ID de zone de disponibilité pour chaque sous-réseau dans la console Amazon VPC.

Le diagramme suivant illustre deux comptes avec des mappages différents entre le code de la zone de disponibilité et l'ID de zone de disponibilité.



Annuler le partage d'un sous-réseau partagé

Le propriétaire peut annuler le partage d'un sous-réseau avec des participants à tout moment. Lorsque le propriétaire a annulé le partage d'un sous-réseau, les règles suivantes doivent être respectées :

- Les ressources existantes des participants continuent de s'exécuter dans le sous-réseau non partagé. AWS les services gérés (par exemple, Elastic Load Balancing) dotés de flux de travail automatisés/gérés (tels que le dimensionnement automatique ou le remplacement de nœuds) peuvent nécessiter un accès continu au sous-réseau partagé pour certaines ressources.
- Les participants ne peuvent plus créer de ressources dans le sous-réseau dont le partage a été annulé.
- Les participants peuvent modifier, décrire et supprimer leurs ressources contenues dans le sous-réseau.
- Si les participants possèdent toujours des ressources dans le sous-réseau dont le partage a été annulé, le propriétaire ne peut pas supprimer le sous-réseau partagé ou le VPC de sous-réseau partagé. Il peut supprimer le sous-réseau partagé ou le VPC de sous-réseau partagé uniquement une fois que les participants ont supprimé toutes les ressources dans le sous-réseau dont le partage a été annulé.

Pour annuler le partage d'un sous-réseau à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Subnets.
3. Sélectionnez votre sous-réseau, choisissez Actions, puis Share subnet (Partager un sous-réseau).
4. Choisissez Actions, Stop sharing (Arrêter le partage).

Pour annuler le partage d'un sous-réseau à l'aide du AWS CLI

Utilisez la commande disassociate-resource-share.

Identifier le propriétaire d'un sous-réseau partagé

Les participants peuvent afficher les sous-réseaux partagés avec eux en utilisant la console Amazon VPC ou l'outil de ligne de commande.

Pour identifier le propriétaire d'un sous-réseau à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Subnets. La colonne Propriétaire indique le propriétaire du sous-réseau.

Pour identifier le propriétaire d'un sous-réseau à l'aide du AWS CLI

Utilisez les commandes describe-subnets et describe-vpcs, qui comprennent l'ID du propriétaire dans leur sortie.

Gestion des ressources VPC

Les propriétaires et les participants sont responsables des ressources VPC qu'ils possèdent.

Ressources des propriétaires

Les propriétaires des VPC sont responsables de la création, la gestion, et la suppression des ressources associées à un VPC partagé. Il s'agit notamment des sous-réseaux, des tables de routage, des listes ACL réseau, des connexions d'appairage, des points de terminaison de

passerelle, des points de terminaison d'interface, des points de terminaison Amazon Route 53 Resolver , des passerelles Internet, des passerelles NAT, des passerelles réseau privé virtuel et des attachements de la passerelle de transit.

Ressources des participants

Les participants peuvent créer un ensemble limité de ressources VPC dans un VPC partagé. Par exemple, les participants peuvent créer des interfaces réseau et des groupes de sécurité et activer des journaux de flux VPC pour les interfaces réseau dont ils sont propriétaires. Les ressources VPC qu'un participant crée sont prises en compte dans les quotas de VPC du compte du participant, et non du compte propriétaire. Pour plus d'informations, consultez Partage de VPC.

Facturation et mesure pour le propriétaire et les participants

- Dans un VPC partagé, chaque participant paie pour les ressources de son application, notamment les instances Amazon EC2, les bases de données Amazon Relational Database Service, les clusters Amazon Redshift et les fonctions. AWS Lambda Les participants paient également les frais de transfert de données associés au transfert de données dans les zones d'interdisponibilité ainsi qu'au transfert de données via des connexions de peering VPC, via des passerelles Internet et entre des passerelles. AWS Direct Connect
- Les propriétaires de VPC paient des frais horaires (le cas échéant), ainsi que des frais de traitement et de transfert de données entre les passerelles NAT, les passerelles privées virtuelles, les passerelles de transit et les points de terminaison VPC. AWS PrivateLink En outre, les adresses IPv4 publiques utilisées dans les VPC partagés sont facturées aux propriétaires de VPC. Pour plus d'informations sur la tarification des adresses IPv4 publiques, consultez l'onglet Adresse IPv4 publique sur la page de tarification d'Amazon VPC.
- Le transfert de données au sein d'une même zone de disponibilité (identifiée par son ID de zone de disponibilité) est gratuit, quel que soit le propriétaire du compte des ressources qui communiquent.

Responsabilités et autorisations des propriétaires et des participants

Les responsabilités et autorisations suivantes s'appliquent aux ressources VPC lorsque vous travaillez avec des sous-réseaux VPC partagés :

Journaux de flux

- Les participants ne peuvent pas créer, supprimer ou décrire des journaux de flux dans un sous-réseau VPC partagé dont ils ne sont pas propriétaires.

- Les participants peuvent créer, supprimer et décrire des journaux de flux dans un sous-réseau VPC partagé dont ils sont propriétaires.
- Les propriétaires de VPC ne peuvent pas décrire ou supprimer les journaux de flux créés par un participant.

Passerelles Internet et passerelles Internet de sortie uniquement

- Les participants ne peuvent pas créer, attacher ou supprimer des passerelles Internet et des passerelles Internet de sortie uniquement dans un sous-réseau VPC partagé. Les participants peuvent décrire les passerelles Internet d'un sous-réseau VPC partagé. Les participants ne peuvent pas décrire les passerelles Internet de sortie uniquement dans un sous-réseau VPC partagé.

Passerelles NAT

- Les participants ne peuvent pas créer, supprimer ou décrire des passerelles NAT dans un sous-réseau VPC partagé.

Listes de contrôle d'accès réseau (NACL)

- Les participants ne peuvent pas créer, supprimer ou remplacer des passerelles NACL dans un sous-réseau VPC partagé. Les participants peuvent décrire les NACL créées par les propriétaires de VPC dans un sous-réseau VPC partagé.

Interfaces réseau

- Les participants peuvent créer des interfaces réseau dans un sous-réseau VPC partagé. Les participants ne peuvent utiliser les interfaces réseau créées par les propriétaires de VPC dans un sous-réseau VPC partagé d'une autre manière, par exemple en attachant, en détachant ou en modifiant les interfaces réseau. Les participants peuvent modifier ou supprimer les interfaces réseau d'un VPC partagé qu'ils ont créé. Par exemple, les participants peuvent associer ou dissocier des adresses IP aux interfaces réseau qu'ils ont créées.
- Les propriétaires de VPC peuvent décrire les interfaces réseau détenues par les participants d'un sous-réseau VPC partagé. Les propriétaires de VPC ne peuvent pas travailler avec les interfaces réseau détenues par les participants d'une autre manière, par exemple en attachant, détachant ou modifiant les interfaces réseau détenues par les participants dans un sous-réseau VPC partagé.

Tables de routage

- Les participants ne peuvent pas utiliser des tables de routage (par exemple, créer, supprimer ou associer des tables de routage) dans un sous-réseau VPC partagé. Les participants peuvent décrire les tables de routage dans un sous-réseau VPC partagé.

Groupes de sécurité

- Les participants peuvent travailler avec (créer, supprimer, décrire, modifier ou créer des règles d'entrée et de sortie pour) les groupes de sécurité dont ils sont propriétaires dans un sous-réseau VPC partagé. Les participants ne peuvent en aucun cas travailler avec les groupes de sécurité créés par les propriétaires de VPC.
- Les participants peuvent créer des règles dans les groupes de sécurité dont ils sont propriétaires et qui font référence à des groupes de sécurité appartenant à d'autres participants ou au propriétaire du VPC comme suit : numéro de compte/ security-group-id
- Les participants ne peuvent pas lancer d'instances en utilisant des groupes de sécurité appartenant au propriétaire du VPC ou à d'autres participants. Les participants ne peuvent pas lancer d'instances en utilisant le groupe de sécurité par défaut du VPC, car il appartient au propriétaire.
- Les propriétaires de VPC peuvent décrire les groupes de sécurité créés par les participants dans un sous-réseau VPC partagé. Les propriétaires de VPC ne peuvent pas travailler avec les groupes de sécurité créés par les participants d'aucune autre manière. Par exemple, les propriétaires de VPC ne peuvent pas lancer d'instances à l'aide de groupes de sécurité créés par les participants.

Sous-réseaux

- Les participants ne peuvent pas modifier les sous-réseaux partagés ni leurs attributs associés. Seul le propriétaire du VPC peut le faire. Les participants peuvent décrire les sous-réseaux dans un sous-réseau VPC partagé.
- Les propriétaires de VPC ne peuvent partager des sous-réseaux qu'avec d'autres comptes ou unités organisationnelles appartenant à la même organisation qu'Organizations. AWS Les propriétaires de VPC ne peuvent pas partager des sous-réseaux se trouvant dans un VPC par défaut.

Passerelles de transit

- Seul le propriétaire d'un VPC peut attacher une passerelle de transit à un sous-réseau VPC partagé. Les participants ne le peuvent pas.

VPC

- Les participants ne peuvent pas modifier les VPC ni leurs attributs associés. Seul le propriétaire du VPC peut le faire. Les participants peuvent décrire les VPC, leurs attributs et les ensembles d'options DHCP.
- Les balises de VPC et les balises pour les ressources dans le VPC partagé ne sont pas partagées avec les participants.

AWS ressources et sous-réseaux VPC partagés

Les ressources de Services AWS support suivantes dans les sous-réseaux VPC partagés. Pour plus d'informations sur la façon dont le service prend en charge les sous-réseaux VPC partagés, consultez les liens vers la documentation du service correspondant.

- Amazon Aurora
- AWS CodeBuild
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Kubernetes Service
- Elastic Load Balancing
  - Application Load Balancers
  - Équilibreurs de charge de passerelle
  - Network Load Balancers
- Amazon EMR
- AWS Glue
- AWS Lambda
- AWS Network Manager
  - AWS Réseau WAN dans le cloud
  - Analyseur d'accès réseau

  - Reachability Analyzer
- AWS PrivateLink†
- Amazon Relational Database Service (RDS)
- Amazon Redshift
- Amazon Route 53
- AWS Transit Gateway
- Accès vérifié par AWS
- Amazon VPC
  - Appairage
  - Mise en miroir du trafic
- Amazon VPC Lattice

† Vous pouvez vous connecter à tous les AWS services qui prennent PrivateLink en charge l'utilisation d'un point de terminaison VPC dans un VPC partagé. Pour obtenir la liste des services compatibles PrivateLink, reportez-vous à la section AWS Services intégrés AWS PrivateLink dans le AWS PrivateLink Guide.

Quotas de partage de VPC

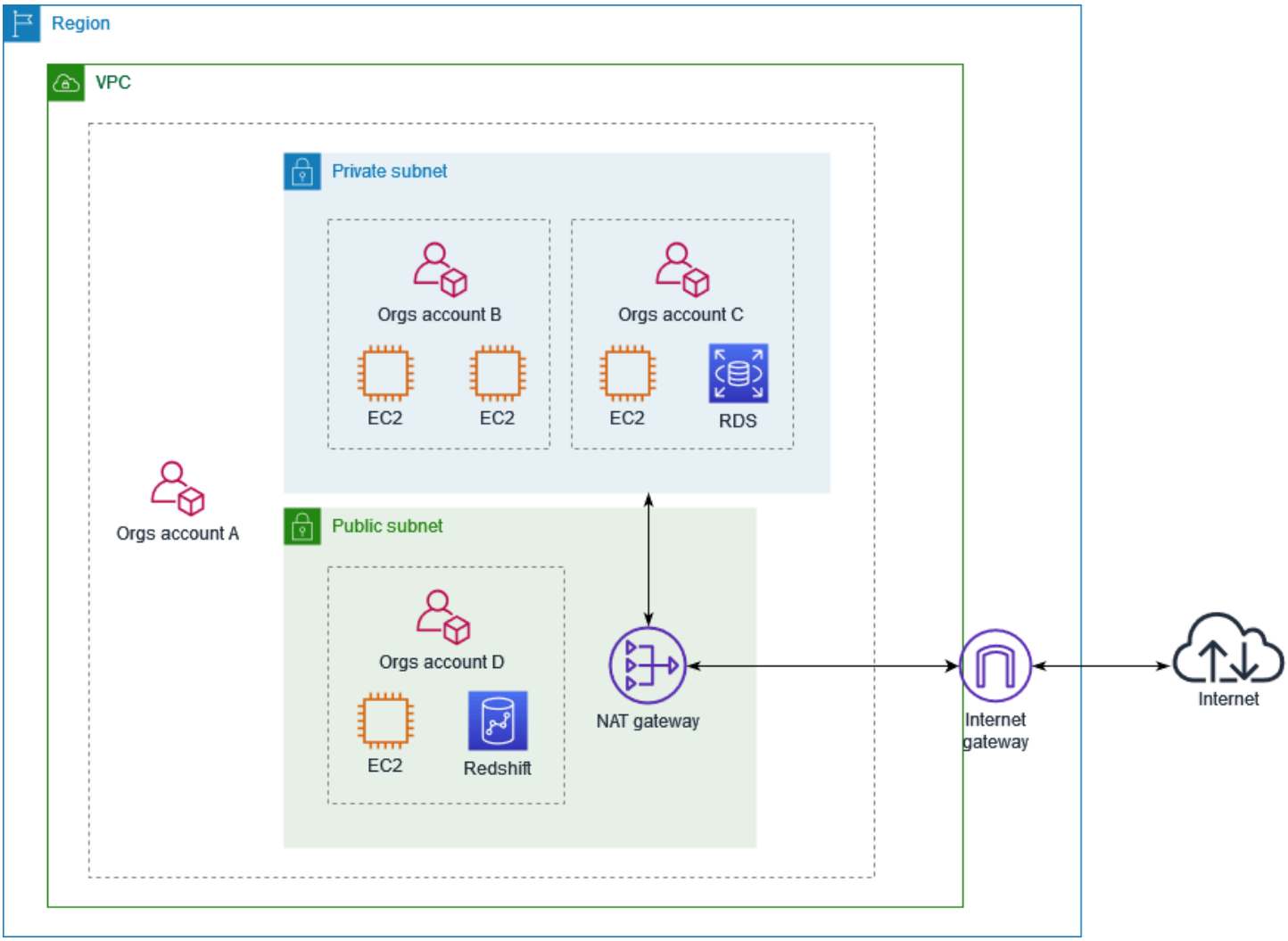
Il existe des quotas liés au partage de VPC. Pour plus d'informations, voir Partage de VPC.

Exemple : partage de sous-réseaux publics et de sous-réseaux privés

Imaginez ce scénario où vous souhaitez qu'un compte (compte A) gère l'infrastructure, y compris les VPC, les sous-réseaux, les tables de routage, les passerelles et les plages CIDR, et que d'autres comptes membres utilisent les sous-réseaux pour leurs applications. Le compte D contient des applications qui doivent se connecter à Internet. Le compte B et le compte C contiennent des applications qui n'ont pas besoin de se connecter à Internet.

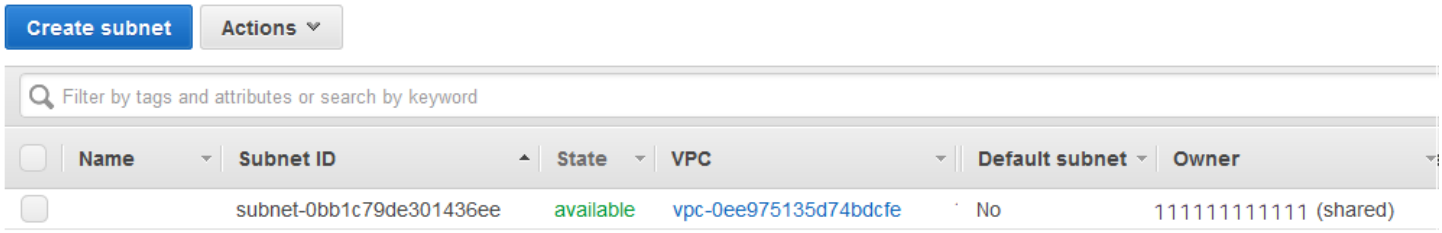
Le compte A utilise AWS Resource Access Manager pour créer un partage de ressources pour les sous-réseaux et partage le sous-réseau public avec le compte D ainsi que le sous-réseau privé avec le compte B et le compte C. Le compte B, le compte C et le compte D peuvent créer des ressources dans les sous-réseaux. Chaque compte peut uniquement voir et créer des ressources dans les sous-réseaux qui sont partagés avec le compte en question. Chaque compte peut contrôler les ressources qu'il crée dans ces sous-réseaux (par exemple, les instances EC2 et les groupes de sécurité).

Aucune configuration supplémentaire n'est requise pour les sous-réseaux partagés, les tables de routage sont donc les mêmes que les tables de routage des sous-réseaux non partagés.



Le compte A (111111111111) partage le sous-réseau public avec le compte D (444444444444). Le compte D voit les sous-réseaux suivants et la colonne Propriétaire fournit deux indicateurs montrant que le sous-réseau est partagé.

- L'ID de compte du propriétaire est le compte A (111111111111) et non le compte D (444444444444).
- Le mot « partagé » apparaît en regard de l'ID de compte du propriétaire.



Étendre un VPC à une zone locale, une zone Wavelength ou Outpost

Vous pouvez héberger des ressources VPC telles que des sous-réseaux dans plusieurs emplacements dans le monde. Ces emplacements sont composés de régions, de zones de disponibilité, de Local Zones et de zones Wavelength. Chaque région constitue une zone géographique séparée.

- Les zones de disponibilité sont des emplacements multiples isolés dans chaque région.
- Les Local Zones vous permettent de placer des ressources, telles que calcul et stockage, dans plusieurs emplacements plus proches de vos utilisateurs finaux.
- AWS Outposts offre les services, l'infrastructure et les modèles d'exploitation AWS natifs à la quasi-totalité de centres de données, d'espaces de colocalisation d'infrastructures ou d'installations sur site.
- Les zones Wavelength permettent aux développeurs de créer des applications qui offrent des latences ultra-faibles aux appareils 5G et aux utilisateurs finaux. Wavelength déploie des services de calcul et de stockage AWS standard à la périphérie des réseaux 5G des opérateurs de télécommunications.

AWS gère des centres de données à la pointe de la technologie et hautement disponibles. Bien qu'elles soient rares, des pannes touchant la disponibilité des instances se trouvant au même emplacement peuvent se produire. Si vous hébergez toutes vos instances dans un seul emplacement touché par une panne, aucune de vos instances ne sera disponible.

Pour vous aider à déterminer le déploiement qui vous convient le mieux, consultez les Questions fréquentes (FAQ) AWS Wavelength.

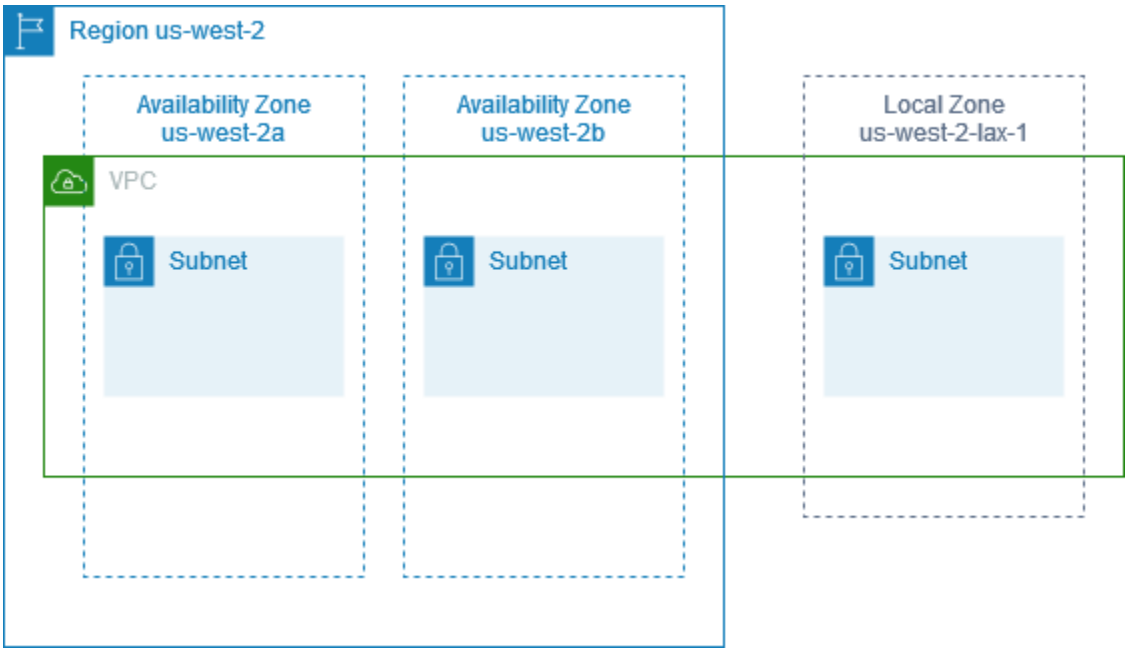
Sous-réseaux dans AWS Local Zones

Les AWS Local Zones vous permettent de placer des ressources plus près de vos utilisateurs et de vous connecter sans difficulté à la gamme complète des services de la Région AWS en utilisant des API et des outils familiers. Lorsque vous créez un sous-réseau dans une Local Zone, vous étendez le VPC à cette dernière.

Pour utiliser une zone locale, vous suivez le processus suivant :

- Inscrivez-vous à la zone locale.
- Créez un sous-réseau dans la zone locale.
- Lancez des ressources dans le sous-réseau de la zone locale, afin que vos applications soient plus proches de vos utilisateurs.

Le schéma suivant illustre un VPC dans la région USA Ouest (Oregon) (`us-west-2`) qui couvre des zones de disponibilité et une zone locale.



Lorsque vous créez un VPC, vous pouvez choisir d'attribuer un ensemble d'adresses IP publiques fournies par Amazon au VPC. Vous pouvez également définir un groupe de bordure réseau pour les adresses afin de limiter les adresses au groupe. Lorsque vous définissez un groupe de bordure réseau, les adresses IP ne peuvent pas se déplacer entre les groupes de bordure réseau. Le trafic réseau de la zone locale ira directement vers Internet ou vers des points de présence (PoP) sans traverser la région parente de la zone locale, ce qui permet d'accéder à des fonctionnalités

informatiques à faible latence. Pour obtenir la liste complète des zones locales et des régions parentes correspondantes, consultez la section Zones locales disponibles dans le Guide de l'utilisateur des zones locales AWS.

Les règles suivantes s'appliquent aux Local Zones :

- Les sous-réseaux Locale Zone suivent les mêmes règles de routage que les sous-réseaux de zone de disponibilité, notamment pour les tables de routage, les groupes de sécurité et les listes ACL réseau.
- Le trafic Internet sortant quitte une Local Zone à partir de la Local Zone.
- Vous devez provisionner des adresses IP publiques à utiliser dans une Local Zone. Lorsque vous allouez des adresses, vous pouvez spécifier l'emplacement à partir duquel l'adresse IP est annoncée. Nous appelons cela un groupe de bordure réseau et vous pouvez définir ce paramètre pour limiter les adresses à cet emplacement. Après avoir provisionné fourni les adresses IP, vous ne pouvez pas les déplacer entre la Local Zone e et la région parente (par exemple, de `us-west-2-lax-1a` à `us-west-2`).
- Si la zone locale prend en charge IPv6, vous pouvez demander des adresses IP fournies par Amazon pour IPv6 et les associer au groupe périphérique du réseau pour un VPC nouveau ou existant. Pour obtenir la liste des zones locales qui prennent en charge IPv6, consultez la section Considérations dans le Guide de l'utilisateur des zones locales AWS
- Vous ne pouvez pas créer de points de terminaison d'un VPC dans les sous-réseaux de la zone locale.

Pour plus d'informations sur l'utilisation des zones locales, consultez le Guide de l'utilisateur des zones locales AWS.

Considérations relatives aux passerelles Internet

Lorsque vous utilisez des passerelles Internet (dans la région parente) dans des Local Zones, tenez compte des informations suivantes :

- Vous pouvez utiliser des passerelles Internet dans des Local Zones avec des adresses IP Elastic ou des adresses IP publiques attribuées automatiquement par Amazon. Les adresses IP Elastic que vous associez doivent inclure le groupe de bordure réseau de la Local Zone. Pour plus d'informations, consultez the section called “Adresses IP Elastic”.

  Vous ne pouvez pas associer une adresse IP élastique définie pour la région.

- Les adresses IP élastiques utilisées dans les Local Zones ont les mêmes quotas que les adresses IP élastiques d'une région. Pour plus d'informations, consultez the section called "Adresses IP Elastic".
- Vous pouvez utiliser des passerelles Internet dans les tables de routage associées aux ressources de la Local Zone. Pour plus d'informations, consultez the section called "Routage vers une passerelle Internet".

Accéder aux Local Zones à l'aide d'une passerelle Direct Connect

Considérez le scénario dans lequel vous souhaitez qu'un centre de données sur site accède aux ressources qui se trouvent dans une Local Zone. Vous utilisez une passerelle réseau privé virtuel pour le VPC associé à la Local Zone afin de vous connecter à une passerelle Direct Connect. La passerelle Direct Connect se connecte à un emplacement AWS Direct Connect dans une région. Le centre de données local dispose d'une connexion AWS Direct Connect à l'emplacement AWS Direct Connect.

> **Note**
>
> Le trafic aux États-Unis qui est destiné à un sous-réseau dans une zone locale utilisant Direct Connect ne passe pas par la région mère de la zone locale. Au lieu de cela, la trafic emprunte le chemin le plus court vers la zone locale. Cela permet de réduire la latence et d'augmenter la réactivité de vos applications.

Vous configurez les ressources suivantes pour cette configuration :

- Une passerelle réseau privé virtuel pour le VPC associé au sous-réseau de Local Zone. Vous pouvez afficher le VPC du sous-réseau sur la page d'informations du sous-réseau dans la Amazon Virtual Private Cloud Console ou utiliser describe-subnets.

  Pour en savoir plus sur la création d'une passerelle réseau privé virtuel, consultez Création d'une passerelle cible dans le Guide de l'utilisateur AWS Site-to-Site VPN.
- Une connexion Direct Connect. Pour obtenir les meilleures performances de latence, AWS vous recommande d'utiliser l'emplacement Direct Connect le plus proche de la zone locale à laquelle vous allez étendre votre sous-réseau.

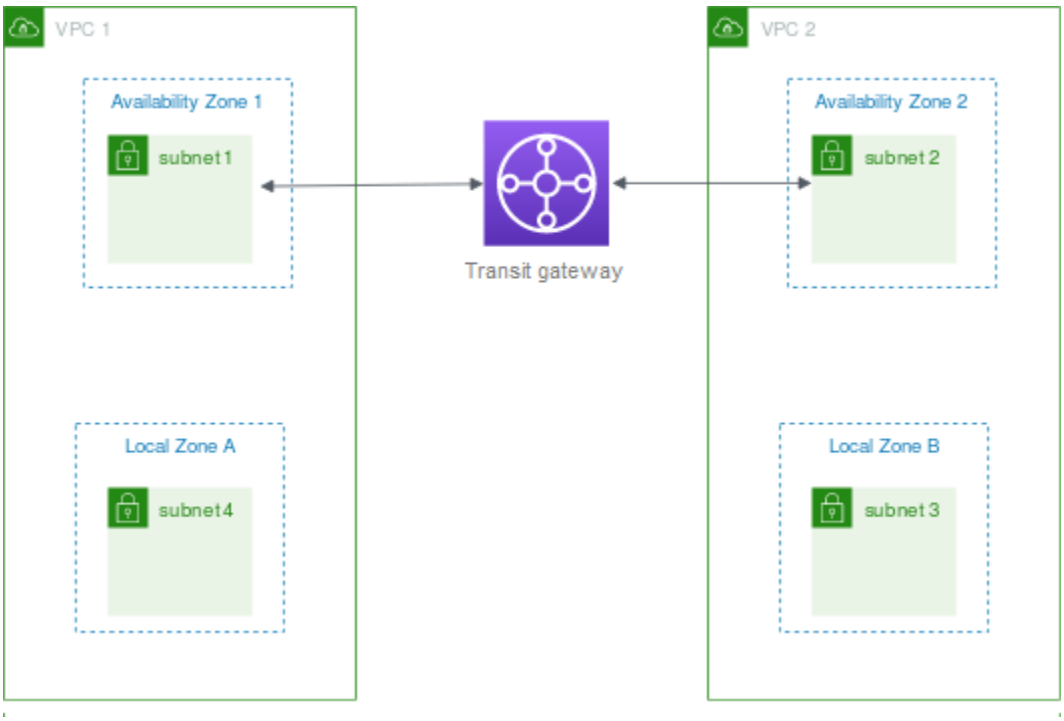
  Pour plus d'informations sur la façon de commander une connexion, consultez Connexions croisées dans le Guide de l'utilisateur AWS Direct Connect.

- Une passerelle Direct Connect. Pour plus d'informations sur la création d'une passerelle Direct Connect, consultez Création d'une passerelle Direct Connect dans le Guide de l'utilisateur AWS Direct Connect.
- Une association de passerelle réseau privé virtuel permettant de connecter le VPC à la passerelle Direct Connect. Pour en savoir plus sur la création d'une association de passerelle réseau privé virtuel, consultez Association et dissociation de passerelles privées virtuelles dans le Guide de l'utilisateur AWS Direct Connect.
- Une interface virtuelle privée sur la connexion depuis l'emplacement AWS Direct Connect au centre de données sur site. Pour plus d'informations sur la création d'une passerelle Direct Connect, consultez Création d'une interface virtuelle privée vers la passerelle Direct Connect dans le Guide de l'utilisateur AWS Direct Connect.

Connecter des sous-réseaux Local Zone à une passerelle Transit Gateway

Vous ne pouvez pas créer de réseau Transit Gateway pour un sous-réseau dans une Local Zone. Le diagramme suivant montre comment configurer votre réseau de sorte que les sous-réseaux de la Local Zone se connectent à une passerelle Transit Gateway via la zone de disponibilité parente. Créez des sous-réseaux dans les Local Zones et dans les zones de disponibilité parentes. Connectez les sous-réseaux dans les zones de disponibilité parentes à la passerelle de transit, puis créez une route dans la table de routage pour chaque VPC qui achemine le trafic destiné à l'autre CIDR VPC vers l'interface réseau du réseau de transit par passerelle.

> **Note**
>
> Le trafic destiné à un sous-réseau dans une zone locale qui provient d'une passerelle de transit traversera d'abord la région mère.



Pour ce scénario, créez les ressources suivantes :

- Un sous-réseau dans chaque zone de disponibilité parente. Pour de plus amples informations, veuillez consulter the section called "Création d'un sous-réseau".
- Une passerelle de transit. Pour plus d'informations, consultez Créer une passerelle de transit dans Passerelles de transit Amazon VPC.
- Un réseau de transit par passerelle pour le VPC qui inclut la zone de disponibilité parente. Pour plus d'informations, consultez Créer un réseau de transit par passerelle dans Passerelles de transit Amazon VPC.
- Vous pouvez associer une table de routage de passerelle de transit au réseau de transit par passerelle. Pour plus d'informations, consultez Tables de routage de passerelles de transit dans Passerelles de transit Amazon VPC.
- Pour chaque VPC, une entrée dans la table de routage VPC qui a l'autre CIDR VPC comme destination et l'ID d'interface de réseau pour l'attachement de la passerelle de transit comme cible. Pour trouver l'interface réseau du réseau de transit par passerelle, recherchez dans les descriptions de vos interfaces réseau l'ID du réseau de transit par passerelle. Pour de plus amples informations, veuillez consulter the section called "Routage pour une passerelle de transit".

Voici un exemple de table de routage pour le VPC 1.

Destination	Cible
CIDR VPC 1	*local*
CIDR VPC 2	*vpc1-attachment-network-interface-id*

Voici un exemple de table de routage pour le VPC 2.

Destination	Cible
CIDR VPC 2	*local*
CIDR VPC 1	*vpc2-attachment-network-interface-id*

Voici un exemple de table de routage de passerelle de transit. Les blocs d'adresse CIDR de chaque VPC sont propagés vers la table de routage de la passerelle Transit Gateway.

CIDR	Réseau de transit par passerelle	Type de routage
CIDR VPC 1	*Réseau de transit par passerelle pour le VPC 1*	propagée
CIDR VPC 2	*Réseau de transit par passerelle pour le VPC 2*	propagée

Sous-réseaux dans AWS Wavelength

AWS Wavelength permet aux développeurs de créer des applications qui offrent des latences ultra-faibles aux appareils mobiles et aux utilisateurs finaux. Wavelength déploie des services de calcul et de stockage AWS standard à la périphérie des réseaux 5G des opérateurs de télécommunications. Les développeurs peuvent étendre un cloud privé virtuel (VPC) à une ou plusieurs zones Wavelength, puis utiliser des ressources AWS comme les instances Amazon EC2 pour exécuter des applications nécessitant une latence ultra-faible et se connectant aux Services AWS dans la région.

Pour utiliser une zone Wavelength, vous devez d'abord vous inscrire à la zone. Ensuite, créez un sous-réseau dans la zone Wavelength. Vous pouvez créer des instances Amazon EC2, des volumes Amazon EBS, des sous-réseaux d'Amazon VPC et des passerelles d'opérateur dans les zones Wavelength. Vous pouvez également utiliser des services qui gèrent ou utilisent EC2, EBS et VPC tels qu'Amazon EC2 Auto Scaling, les clusters Amazon EKS, les clusters Amazon ECS, Amazon EC2 Systems Manager, Amazon CloudWatch, AWS CloudTrail et AWS CloudFormation. Les services dans Wavelength font partie d'un VPC qui est connecté par le biais d'une connexion à haut débit fiable à une région AWS pour un accès facile à des services tels qu'Amazon DynamoDB et Amazon RDS.

Les règles suivantes s'appliquent aux zones Wavelength :

- Un VPC s'étend à une zone Wavelength lorsque vous créez un sous-réseau dans le VPC et l'associez à la zone Wavelength.
- Par défaut, chaque sous-réseau que vous créez dans un VPC qui couvre une zone Wavelength hérite de la table de routage principale du VPC, y compris le routage local.
- Lorsque vous lancez une instance EC2 dans un sous-réseau dans une zone Wavelength, vous lui attribuez une adresse IP d'opérateur. La passerelle d'opérateur utilise l'adresse pour le trafic depuis l'interface vers Internet ou les appareils mobiles. La passerelle d'opérateur utilise NAT pour traduire l'adresse, puis envoie le trafic vers la destination. Le trafic provenant du réseau de l'opérateur de télécommunications passe par la passerelle de l'opérateur.
- Vous pouvez définir la cible d'une table de routage de VPC ou d'une table de routage de sous-réseau dans une zone Wavelength sur une passerelle d'opérateur, ce qui autorise le trafic entrant à partir d'un réseau d'opérateur à un emplacement spécifique, et le trafic sortant vers le réseau d'opérateur et Internet. Pour plus d'informations sur les options de routage dans une zone Wavelength, consultez Routage dans le Guide du développeur AWS Wavelength.

- Les sous-réseaux des zones Wavelength ont les mêmes composants réseau que les sous-réseaux des zones de disponibilité, y compris les adresses IPv4, les ensembles d'options DHCP et les listes ACL réseau.
- Vous ne pouvez pas créer de réseau Transit Gateway pour un sous-réseau situé dans une zone Wavelength. Au lieu de cela, créez le réseau via un sous-réseau situé dans la zone de disponibilité parent, puis acheminez le trafic vers les destinations souhaitées via la passerelle Transit Gateway. Pour obtenir un exemple, veuillez consulter la section suivante.

Considérations relatives aux zones Wavelength multiples

Les instances EC2 qui se trouvent dans des zones Wavelength différentes dans le même VPC ne sont pas autorisées à communiquer entre elles. Si vous avez besoin d'une communication de zone Wavelength à zone Wavelength, AWS vous recommande d'utiliser plusieurs VPC, un pour chaque zone Wavelength. Vous pouvez utiliser une passerelle de transit pour connecter les VPC. Cette configuration permet la communication entre les instances dans les zones Wavelength.

Itinéraires de trafic entre zones Wavelength dans la région AWS. Pour plus d'informations, consultez AWS Transit Gateway.

Le diagramme suivant montre comment configurer votre réseau afin que les instances de deux zones Wavelength différentes puissent communiquer. Vous disposez de deux zones Wavelength (zone Wavelength A et zone Wavelength B). Vous devez créer les ressources suivantes pour activer la communication :

- Pour chaque zone Wavelength, un sous-réseau dans une zone de disponibilité qui est la zone de disponibilité parente de la zone Wavelength. Dans l'exemple, vous créez un sous-réseau 1 et un sous-réseau 2. Pour de plus amples informations sur la création des sous-réseaux, veuillez consulter the section called “Création d'un sous-réseau”. Utilisez describe-availability-zones pour trouver la zone parente.
- Une passerelle de transit La passerelle de transit relie les VPC. Pour plus d'informations sur la création d'une passerelle de transit, consultez Création d'une passerelle de transit dans le Guide Amazon VPC Transit Gateways.
- Pour chaque VPC, un attachement de VPC à la passerelle Transit Gateway dans la zone de disponibilité parent de la zone Wavelength. Pour plus d'informations, consultez Attachements de passerelle Transit Gateway vers un VPC dans le Guide Passerelles de transit Amazon VPC.

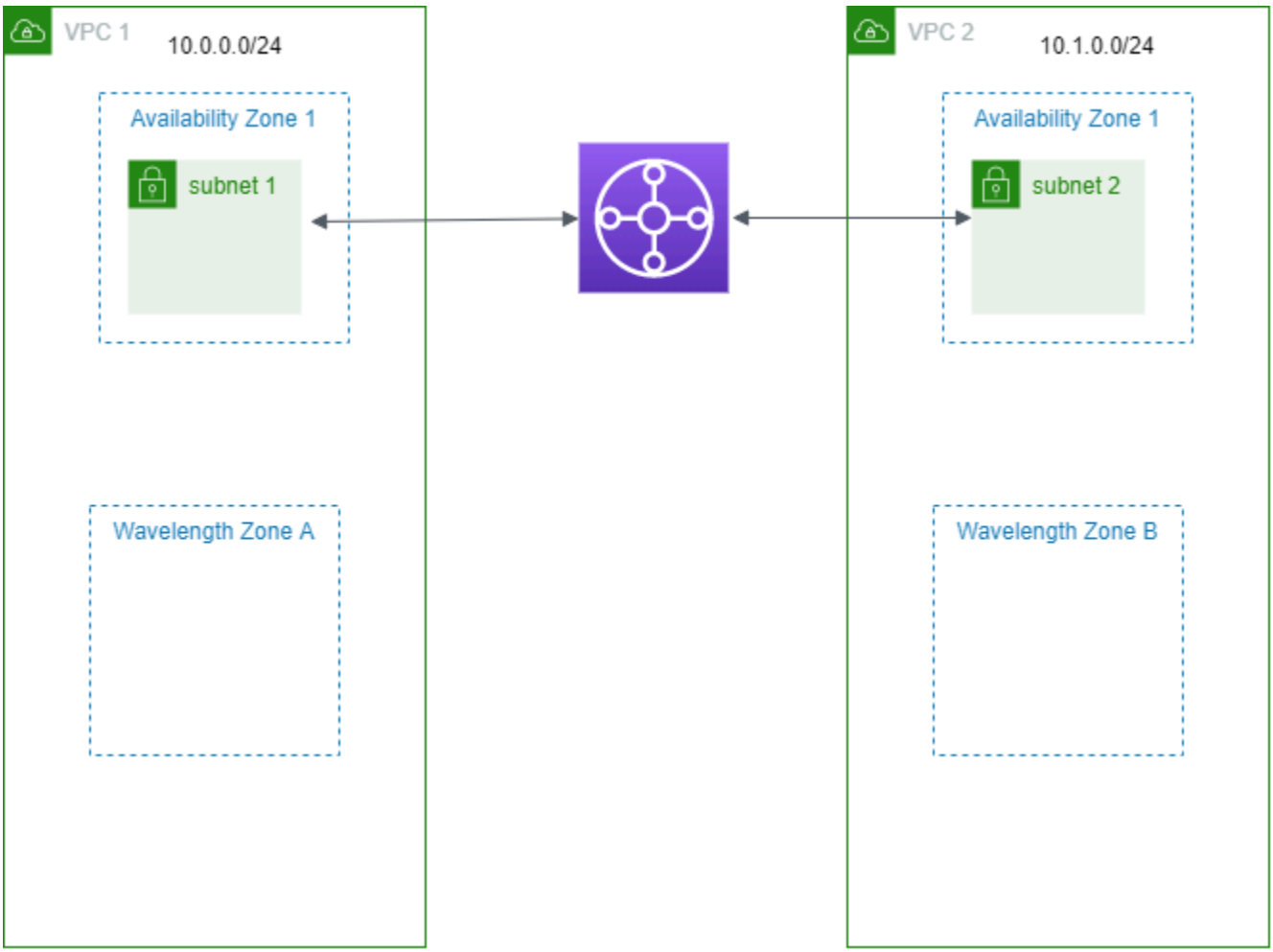
- Entrées pour chaque VPC dans la table de routage de passerelle de transit. Pour plus d'informations sur la création de routes de passerelle de transit, consultez Tables de routage de passerelle de transit dans le Guide Amazon VPC Transit Gateways.
- Pour chaque VPC, une entrée dans la table de routage VPC qui a l'autre CIDR VPC en tant que destination et l'ID de passerelle de transit en tant que cible. Pour plus d'informations, consultez the section called "Routage pour une passerelle de transit".

  Dans l'exemple, la table de routage pour VPC 1 comporte l'entrée suivante :

Destination	Target
10.1.0.0/24	tgw-22222222222222222

  La table de routage pour VPC 2 a l'entrée suivante :

Destination	Target
10.0.0.0/24	tgw-22222222222222222



Sous-réseaux dans AWS Outposts

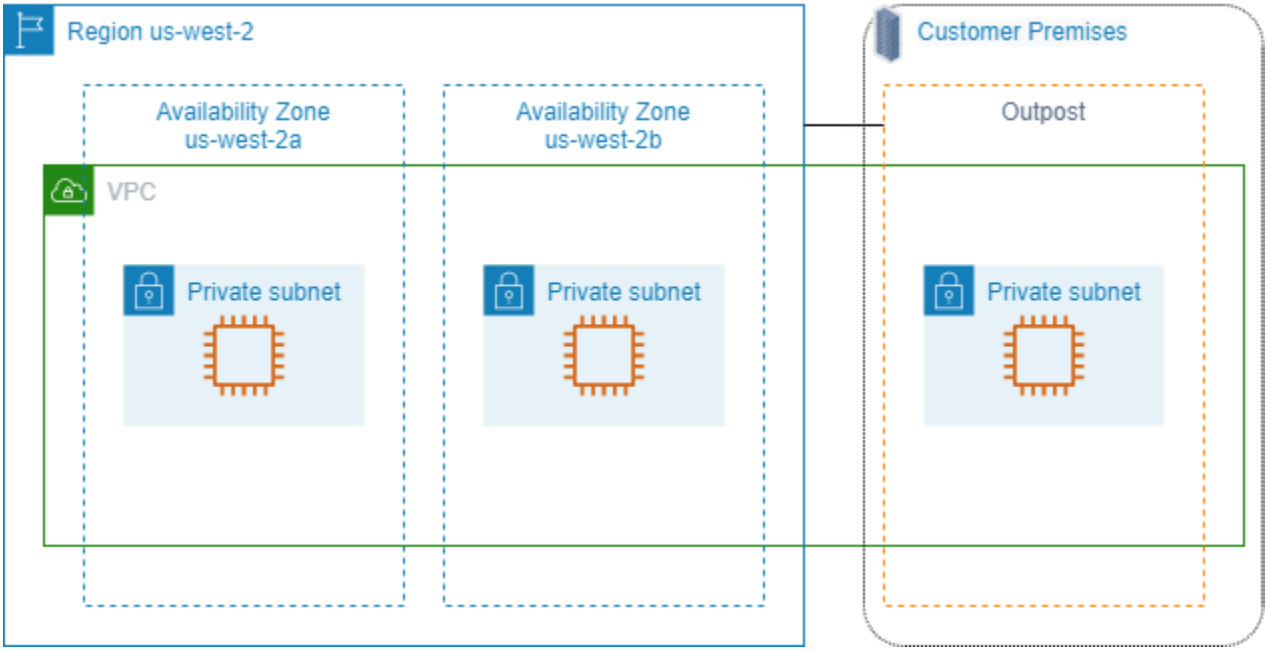
AWS Outposts vous offre les mêmes infrastructure matérielle, services, API et outils AWS pour créer et exécuter vos applications sur site et dans le cloud. AWS Outposts est idéal pour les charges de travail nécessitant un accès à faible latence aux applications ou systèmes sur site, et pour celles ayant besoin de stocker et traiter des données en local. Pour plus d'informations sur AWS Outposts, consultez AWS Outposts.

Un VPC couvre toutes les zones de disponibilité d'une Région AWS. Après avoir connecté votre Outpost à sa région parent, vous pouvez étendre n'importe quel VPC de la région à votre Outpost en créant un sous-réseau pour l'Outpost de ce VPC.

Les règles suivantes s'appliquent à AWS Outposts :

- Les sous-réseaux doivent résider dans un emplacement Outpost.

- Vous créez un sous-réseau pour un Outpost en spécifiant l'Amazon Resource Name (ARN) de l'Outpost lorsque vous créez le sous-réseau.
- Rack d'Outposts : une passerelle locale gère la connectivité réseau entre votre VPC et les réseaux sur site. Pour plus d'informations, veuillez consulter la rubrique Passerelles locales dans le Guide de l'utilisateur AWS Outposts du rack Outposts.
- Serveurs d'Outposts : une interface réseau locale gère la connectivité réseau entre votre VPC et les réseaux sur site. Pour plus d'informations, veuillez consulter la rubrique Interfaces réseau locales dans le Guide de l'utilisateur AWS Outposts des serveurs Outposts.
- Par défaut, chaque sous-réseau que vous créez dans un VPC, y compris les sous-réseaux de vos Outposts, est associé de manière implicite à la table de routage principale de votre VPC. Sinon, vous pouvez associer explicitement une table de routage personnalisée aux sous-réseaux de votre VPC et disposer d'une passerelle locale comme cible « next hop » pour tout le trafic à destination de votre réseau sur site.



Supprimer votre VPC

Lorsque vous avez terminé avec une VPC, vous pouvez le supprimer.

Exigence

Avant de supprimer un VPC, vous devez commencer par résilier ou supprimer toutes les ressources qui ont créé une interface réseau gérées par demandeur dans le VPC. Par exemple, vous devez

résilier à vos instances EC2 et supprimer vos équilibreurs de charge, passerelles NAT, attachements de VPC de passerelle de transit et points de terminaison de VPC d'interface.

Table des matières

Supprimer un VPC à l'aide de la console

Si vous supprimez un VPC à l'aide de la console Amazon VPC, nous supprimons également les composants du VPC suivants pour vous :

- Options DHCP
- Passerelles Internet de sortie uniquement
- Points de terminaison de passerelle
- Passerelles Internet
- Listes ACL réseau
- Tables de routage
- Groupes de sécurité
- Sous-réseaux

Pour supprimer votre VPC à l'aide de la console

1. Ouvrez la console Amazon EC2 sur https://console.aws.amazon.com/ec2/.
2. Mettez fin à toutes les instances dans le VPC. Pour plus d'informations, consultez la section Résiliation de votre instance dans le guide de l'utilisateur Amazon EC2.
3. Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/.
4. Dans le panneau de navigation, sélectionnez Your VPCs (Vos VPC).
5. Sélectionnez le VPC à supprimer, choisissez Actions, puis Supprimer le VPC.
6. Si vous devez supprimer certaines ressources ou les résilier avant de pouvoir supprimer le VPC, nous les affichons. Supprimez ou résiliez ces ressources, puis réessayez. Sinon, nous affichons les ressources que nous allons supprimer en plus du VPC. Consultez la liste, puis passez à l'étape suivante.

7. (Facultatif) Si vous avez une connexion Site-to-Site VPN, vous pouvez sélectionner l'option qui permet de la supprimer. Si vous prévoyez d'utiliser la passerelle client avec un autre VPC, nous vous recommandons de conserver la connexion Site-to-Site VPN et les passerelles. Sinon, vous devrez configurer à nouveau votre périphérique de passerelle client après avoir créé une nouvelle connexion Site-to-Site VPN.
8. Lorsque vous êtes invité à confirmer, entrez **delete**, puis choisissez Delete (Supprimer).

Supprimer un VPC à l'aide de la ligne de commande

Avant de supprimer un VPC à l'aide de la ligne de commande, vous devez résilier ou supprimer toutes les ressources qui ont créé une interface réseau gérée par demandeur dans le VPC. Vous devez également supprimer ou détacher toutes les ressources VPC que vous avez créées, telles que les sous-réseaux, les groupes de sécurités personnalisés, les ACL réseau, les tables de routage, les passerelles Internet et les passerelles Internet de sortie uniquement. Vous n'avez pas besoin de supprimer le groupe de sécurité, la table de routage ou la liste d'accès du réseau par défaut.

La procédure suivante décrit les commandes à utiliser pour supprimer des ressources VPC communes, puis pour supprimer votre VPC. Vous devez utiliser ces commandes dans cet ordre. Si vous avez créé des ressources VPC supplémentaires, vous devez également utiliser leur commande de suppression correspondante avant de pouvoir supprimer le VPC.

Pour supprimer un VPC à l'aide du AWS CLI

1. Supprimez votre groupe de sécurité à l'aide la commande delete-security-group.

```
aws ec2 delete-security-group --group-id sg-id
```

2. Supprimez chaque ACL réseau à l'aide de la commande delete-network-acl.

```
aws ec2 delete-network-acl --network-acl-id acl-id
```

3. Supprimez chaque sous-réseau à l'aide de la commande delete-subnet.

```
aws ec2 delete-subnet --subnet-id subnet-id
```

4. Supprimez chaque table de routage personnalisée à l'aide de la commande delete-route-table.

```
aws ec2 delete-route-table --route-table-id rtb-id
```

5. Détachez votre passerelle Internet de votre VPC à l'aide de la commande detach-internet-gateway.

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-id --vpc-id vpc-id
```

6. Supprimez votre passerelle Internet à l'aide de la commande delete-internet-gateway.

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-id
```

7. [VPC à double pile] Supprimez votre passerelle Internet de sortie uniquement à l'aide de la commande delete-egress-only-internet-gateway.

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-id eigw-id
```

8. Supprimez votre VPC à l'aide de la commande delete-vpc.

```
aws ec2 delete-vpc --vpc-id vpc-id
```

Sous-réseaux de votre VPC

Un sous-réseau est une plage d'adresses IP dans votre VPC. Vous pouvez créer des AWS ressources, telles que des instances EC2, dans des sous-réseaux spécifiques.

Table des matières

Principes de base des sous-réseaux

Chaque sous-réseau doit résider entièrement dans une zone de disponibilité et ne peut pas s'étendre sur plusieurs zones. En lançant AWS des ressources dans des zones de disponibilité distinctes, vous pouvez protéger vos applications contre la défaillance d'une seule zone de disponibilité.

Table des matières

Plage d'adresses IP du sous-réseau

Lorsque vous créez un sous-réseau, vous spécifiez ses adresses IP, en fonction de la configuration du VPC :

- IPv4 uniquement : le sous-réseau comporte un bloc d'adresse CIDR IPv4, mais ne comporte pas de bloc d'adresse CIDR IPv6. Les ressources d'un sous-réseau IPv4 uniquement doivent communiquer via IPv4.
- Double pile : le sous-réseau comporte à la fois un bloc d'adresse CIDR IPv4 et un bloc d'adresse CIDR IPv6. Le VPC doit comporter à la fois un bloc d'adresse CIDR IPv4 et un bloc d'adresse CIDR IPv6. Les ressources d'un sous-réseau à double pile peuvent communiquer via IPv4 et IPv6.
- IPv6 uniquement : le sous-réseau comporte un bloc d'adresse CIDR IPv6, mais ne comporte pas de bloc d'adresse CIDR IPv4. Le VPC doit avoir un bloc d'adresse CIDR IPv6. Les ressources d'un sous-réseau IPv6 uniquement doivent communiquer via IPv6.

> **Note**
>
> Les ressources des sous-réseaux IPv6 uniquement se voient attribuer des adresses locales de liaison IPv4 à partir du bloc CIDR `169.254.0.0/16`. Ces adresses sont utilisées pour communiquer avec les services VPC tels que le service de métadonnées d'instance (IMDS).

Pour plus d'informations, consultez Adressage IP pour vos VPC et sous-réseaux.

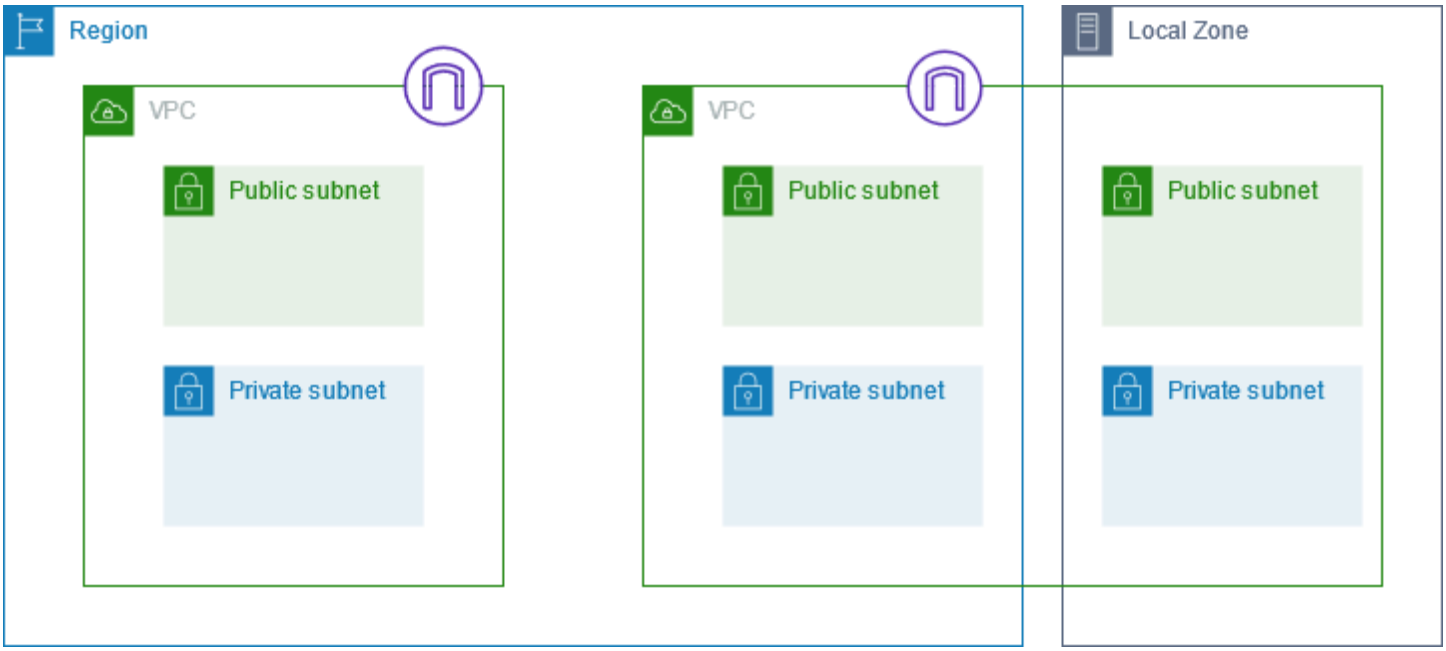
Types de sous-réseaux

Le type de sous-réseau est déterminé par la façon dont vous configurez le routage pour vos sous-réseaux. Par exemple :

- Sous-réseau public : le sous-réseau possède une route directe vers une passerelle Internet. Les ressources d'un sous-réseau public peuvent accéder à l'Internet public.
- Sous-réseau privé : le sous-réseau ne comporte pas de route vers une passerelle Internet. Les ressources d'un sous-réseau privé nécessitent un périphérique NAT pour accéder à l'Internet public.
- Sous-réseau VPN uniquement : le sous-réseau possède une route vers une connexion Site-to-Site VPN via une passerelle réseau privé virtuel. Le sous-réseau ne dispose pas d'un acheminement vers une passerelle Internet.
- Sous-réseau isolé : le sous-réseau ne possède aucune route vers des destinations en dehors de son VPC. Les ressources d'un sous-réseau isolé ne peuvent accéder ou être accessibles que par d'autres ressources du même VPC.

Diagramme de sous-réseau

Le diagramme suivant montre deux VPC dans une région. Chaque VPC possède des sous-réseaux publics et privés et une passerelle Internet. Vous pouvez éventuellement ajouter des sous-réseaux dans une zone locale, comme indiqué dans le diagramme. Une zone locale est un déploiement d' AWS infrastructure qui rapproche les services de calcul, de stockage et de base de données de vos utilisateurs finaux. Lorsque vous utilisez une zone locale, vos utilisateurs finaux peuvent exécuter des applications qui nécessitent des latences de l'ordre de la milliseconde. Pour plus d'informations, consultez Local Zones AWS.



Routage des sous-réseaux

Chaque sous-réseau doit être associé à une table de routage, qui indique les routes autorisées pour le trafic sortant quittant le sous-réseau. Chaque sous-réseau que vous créez est automatiquement associé à la table de routage principale de votre VPC. Vous pouvez modifier cette association, mais aussi le contenu de la table de routage principale. Pour plus d'informations, consultez Configuration des tables de routage.

Paramètres du sous-réseau

Tous les sous-réseaux disposent d'un attribut modifiable qui détermine si une interface réseau créée dans ce sous-réseau se voit attribuer une adresse IPv4 publique et, le cas échéant, une adresse IPv6. Cela inclut l'interface réseau principale (eth0) qui est créée pour une instance lorsque vous

lancez une instance dans ce sous-réseau. Quel que soit l'attribut du sous-réseau, vous pouvez toujours remplacer ce paramètre pour une instance spécifique lors du lancement.

Après avoir créé un sous-réseau, vous pouvez modifier les paramètres suivants pour le sous-réseau :

- Auto-assign IP settings (Paramètres d'attribution automatique des adresses IP) : vous permet de configurer les paramètres d'attribution automatique des adresses IP pour demander automatiquement une adresse IPv4 ou IPv6 publique pour une nouvelle interface réseau dans ce sous-réseau.
- Resource-based Name (RBN) settings (Paramètres de nom basé sur les ressources [RBN]) : vous permet de spécifier le type de nom d'hôte pour les instances EC2 dans ce sous-réseau et de configurer la façon dont les requêtes d'enregistrement DNS A et AAAA sont traitées. Pour plus d'informations, consultez les types de noms d'hôte des instances Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

Sécurité des sous-réseaux

Pour protéger vos AWS ressources, nous vous recommandons d'utiliser des sous-réseaux privés. Utilisez un hôte bastion ou un périphérique NAT pour fournir un accès Internet aux ressources, telles que les instances EC2, dans un sous-réseau privé.

AWS fournit des fonctionnalités que vous pouvez utiliser pour renforcer la sécurité des ressources de votre VPC. Les groupes de sécurité autorisent le trafic entrant et sortant des ressources associées, telles que les instances EC2. Listes ACL réseau : les listes ACL réseau autorisent ou refusent le trafic entrant et sortant au niveau du sous-réseau. Dans la plupart des cas, les groupes de sécurité peuvent répondre à vos besoins. Vous pouvez utiliser les ACL réseau si vous souhaitez ajouter une couche de sécurité supplémentaire. Pour plus d'informations, consultez the section called “Comparer les groupes de sécurité et les listes ACL réseau”.

Dans sa conception, chaque sous-réseau doit être associé à une liste ACL réseau. Chaque sous-réseau que vous créez est automatiquement associé à l'ACL réseau par défaut du VPC. L'ACL réseau par défaut permet tout le trafic entrant et sortant. Vous pouvez mettre à jour l'ACL réseau par défaut ou créer des ACL réseau personnalisées et les associer à vos sous-réseaux. Pour plus d'informations, consultez Contrôle du trafic vers les sous-réseaux avec des listes ACL réseau.

Vous pouvez créer un journal de flux sur votre VPC ou sous-réseau pour capturer ces flux vers et en provenance des interfaces réseau dans votre VPC ou sous-réseau. Vous pouvez aussi créer un

journal de flux sur une interface réseau individuelle. Pour plus d'informations, voir Journalisation du trafic IP à l'aide des journaux de flux VPC.

Création d'un sous-réseau

Utiliser les procédures suivantes pour créer des sous-réseaux pour votre cloud privé virtuel (VPC). Selon la connectivité dont vous avez besoin, vous devriez peut-être ajouter également des passerelles et des tables de routage.

Considérations

- Vous devez spécifier un bloc d'adresse CIDR IPv4 pour le sous-réseau de la plage de votre VPC. Le cas échéant, vous pouvez spécifier un bloc d'adresse CIDR IPv6 pour un sous-réseau si un bloc d'adresse CIDR IPv6 est associé au VPC. Pour plus d'informations, consultez Adressage IP pour vos VPC et sous-réseaux.
- Si vous créez uniquement un sous-réseau IPv6, veuillez tenir compte des éléments suivants. Une instance EC2 lancée dans un sous-réseau IPv6 uniquement reçoit une adresse IPv6 mais pas d'adresse IPv4. Toute instance que vous lancez dans un sous-réseau IPv6 uniquement, doit être une instance reposant sur le système Nitro.
- Pour créer le sous-réseau dans une zone locale ou une zone Wavelength, vous devez activer la zone. Pour plus d'informations, veuillez consulter la rubrique Régions et zones dans le Guide de l'utilisateur Amazon EC2.

Pour ajouter un sous-réseau à votre VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
3. Choisissez Create subnet (Créer un sous-réseau).
4. Sous l'ID du VPC, choisissez le VPC pour le sous-réseau.
5. (Facultatif) Pour Subnet name (Nom du sous-réseau), tapez un nom pour votre sous-réseau. Une identification est alors créée avec la clé `Name` et la valeur que vous spécifiez.
6. Pour la zone de disponibilité, vous pouvez choisir une zone pour votre sous-réseau ou laisser la valeur Aucune préférence par défaut pour en AWS choisir une pour vous.
7. Pour le bloc d'adresse CIDR IPv4, sélectionnez Saisie manuelle pour saisir un bloc d'adresse CIDR IPv4 pour votre sous-réseau (par exemple, `10.0.1.0/24`) ou sélectionnez Aucune

adresse CIDR IPv4. Si vous utilisez Amazon VPC IP Address Manager (IPAM) pour planifier, suivre et surveiller les adresses IP de vos AWS charges de travail, lorsque vous créez un sous-réseau, vous avez la possibilité d'allouer un bloc CIDR depuis IPAM (alloué par IPAM). Pour plus d'informations sur la planification de l'espace d'adresse IP VPC pour les allocations IP de sous-réseau, consultez le didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau dans le Guide de l'utilisateur Amazon VPC IPAM.

8. Pour le bloc d'adresse CIDR IPv6, sélectionnez Saisie manuelle pour choisir l'adresse CIDR IPv6 du VPC dans laquelle vous souhaitez créer un sous-réseau. Cette option est uniquement disponible si le VPC a un bloc d'adresse CIDR IPv6 associé. Si vous utilisez le Gestionnaire d'adresses IP (IPAM) Amazon VPC pour planifier, suivre et contrôler les adresses IP pour vos charges de travail AWS , lorsque vous créez un sous-réseau, vous avez la possibilité d'allouer un bloc CIDR à partir l'IPAM (alloué par IPAM). Pour plus d'informations sur la planification de l'espace d'adresse IP VPC pour les allocations IP de sous-réseau, consultez le didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau dans le Guide de l'utilisateur Amazon VPC IPAM.
9. Choisissez un bloc d'adresse CIDR IPv6 VPC.
10. Pour le bloc CIDR du sous-réseau IPv6, choisissez un CIDR pour le sous-réseau égal ou plus spécifique que le CIDR VPC. Par exemple, si le CIDR du groupe VPC est /50, vous pouvez choisir une longueur de masque réseau comprise entre /50 et /64 pour le sous-réseau. Les longueurs possibles des masques réseau IPv6 sont comprises entre /44 et /64 par incréments de /4.
11. Choisissez Create subnet (Créer un sous-réseau).

Pour ajouter un sous-réseau à votre VPC à l'aide du AWS CLI

Utilisez la commande create-subnet.

Étapes suivantes

Une fois que vous avez créé un sous-réseau, vous pouvez le configurer comme suit :

- Configuration du routage. Vous pouvez ensuite créer une table de routage et un routage personnalisés qui envoient du trafic vers une passerelle associée au VPC, telle qu'une passerelle Internet. Pour plus d'informations, consultez Configuration des tables de routage.
- Modifiez les adresses IP du sous-réseau. Pour plus d'informations, consultez the section called "Configurer vos sous-réseaux".

- Modification du comportement d'adressage IP. Vous pouvez spécifier que toutes les instances lancées dans ce sous-réseau reçoivent une adresse IPv4 publique, ou une adresse IPv6, ou les deux. Pour plus d'informations, consultez Paramètres du sous-réseau.
- Modifiez les paramètres de nom basé sur les ressources (RBN). Pour de plus amples informations, veuillez consulter Types de noms d'hôte des instances Amazon EC2.
- Créez ou modifiez vos ACL de réseau. Pour plus d'informations, consultez Contrôle du trafic vers les sous-réseaux avec des listes ACL réseau.
- Partager le sous-réseau avec d'autres comptes. Pour plus d'informations, voir ???.

Configurer vos sous-réseaux

Utiliser les procédures suivantes pour configurer des sous-réseaux pour votre cloud privé virtuel (VPC).

Tâches

- Afficher vos sous-réseaux
- Ajouter un bloc d'adresse CIDR IPv6 à votre sous-réseau
- Supprimer un bloc d'adresse CIDR IPv6 de votre sous-réseau
- Modifier l'attribut d'adressage IPv4 public de votre sous-réseau
- Modifier l'attribut d'adressage IPv6 de votre sous-réseau

Afficher vos sous-réseaux

Utilisez les étapes de cette section pour afficher les détails de votre sous-réseau.

Pour afficher les détails du sous-réseau à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
3. Cochez la case correspondant au sous-réseau ou choisissez l'ID de sous-réseau pour ouvrir la page détaillée.

Pour décrire un sous-réseau à l'aide du AWS CLI

Utilisez la commande describe-subnets.

Pour afficher vos sous-réseaux relevant de toutes les régions

Ouvrez la console Amazon EC2 Global View à l'adresse https://console.aws.amazon.com/ec2globalview/home. Pour plus d'informations, consultez Répertorier et filtrer les ressources à l'aide d'Amazon EC2 Global View dans le guide de l'utilisateur Amazon EC2.

Ajouter un bloc d'adresse CIDR IPv6 à votre sous-réseau

Vous pouvez associer un bloc d'adresses CIDR IPv6 à un sous-réseau existant de votre VPC. Le sous-réseau ne doit pas posséder de bloc d'adresse CIDR IPv6 existant associé à celui-ci.

Pour ajouter un bloc d'adresse CIDR IPv6 à un sous-réseau

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
3. Sélectionnez votre sous-réseau et choisissez Actions, Edit IPv6 CIDRs (Modifier les blocs d'adresses CIDR IPv6).
4. Choisissez Ajoutez un bloc d'adresse CIDR IPv6.
5. Choisissez un bloc d'adresse CIDR VPC, saisissez un bloc d'adresse CIDR de sous-réseau et choisissez une longueur de masque réseau égale ou plus spécifique que la longueur de masque réseau de l'adresse CIDR VPC. Par exemple, si le CIDR du groupe VPC est /50, vous pouvez choisir une longueur de masque réseau comprise entre /50 et /64 pour le sous-réseau. Les longueurs possibles des masques réseau IPv6 sont comprises entre /44 et /64 par incréments de /4.
6. Choisissez Enregistrer.

Pour associer un bloc d'adresse CIDR IPv6 à un sous-réseau à l'aide du AWS CLI

Utilisez la commande associate-subnet-cidr-block.

Supprimer un bloc d'adresse CIDR IPv6 de votre sous-réseau

Si vous ne souhaitez plus prendre en charge IPv6 dans votre sous-réseau, mais que vous souhaitez continuer à utiliser votre sous-réseau pour la création et la communication avec les ressources IPv4, vous pouvez supprimer le bloc d'adresse CIDR IPv6.

Avant de pouvoir supprimer un bloc d'adresse CIDR IPv6, vous devez tout d'abord annuler l'attribution des adresses IPv6 qui sont attribuées aux instances de votre sous-réseau.

Pour supprimer un bloc d'adresse CIDR IPv6 d'un sous-réseau

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
3. Sélectionnez le sous-réseau et choisissez Actions, Edit IPv6 CIDRs (Modifier les blocs d'adresses CIDR IPv6).
4. Trouvez le bloc d'adresse CIDR IPv6 et choisissez Remove (Supprimer).
5. Choisissez Enregistrer.

Pour dissocier un bloc d'adresse CIDR IPv6 d'un sous-réseau à l'aide du AWS CLI

Utilisez la commande disassociate-subnet-cidr-block.

Modifier l'attribut d'adressage IPv4 public de votre sous-réseau

Par défaut, l'attribut d'adressage public IPv4 est configuré sur `false` pour les sous-réseaux personnalisés, et sur `true` pour les sous-réseaux par défaut. Une exception existe pour un sous-réseau personnalisé créé par l'assistant de lancement d'instance Amazon EC2 où l'assistant détermine l'attribut comme `true`. Vous pouvez modifier cet attribut à l'aide de la console Amazon VPC.

Pour modifier le comportement de l'adressage IPv4 public de votre sous-réseau

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
3. Sélectionnez votre sous-réseau, choisissez Actions, puis Edit subnet settings (Modifier les paramètres du sous-réseau).
4. Si elle est activée, la case à cocher Enable auto-assign public IPv4 address demande une adresse IPv4 publique pour toutes les instances lancées dans le sous-réseau sélectionné. Activez ou désactivez la case à cocher si nécessaire, puis choisissez Edit.

Pour modifier un attribut de sous-réseau à l'aide du AWS CLI

Utilisez la commande modify-subnet-attribute.

Modifier l'attribut d'adressage IPv6 de votre sous-réseau

Par défaut, tous les sous-réseaux disposent d'un attribut d'adressage IPv6 défini sur `false`. Vous pouvez modifier cet attribut à l'aide de la console Amazon VPC. Si vous activez l'attribut d'adressage IPv6 de votre sous-réseau, les interfaces réseau créées dans le sous-réseau reçoivent une adresse IPv6 à partir de la plage du sous-réseau. Les instances lancées dans le sous-réseau reçoivent une adresse IPv6 sur l'interface réseau principale.

Votre sous-réseau dispose d'un bloc d'adresse CIDR IPv6 associé.

> **Note**
>
> Si vous activez la fonctionnalité d'adressage IPv6 pour votre sous-réseau, votre interface ou instance réseau ne reçoit une adresse IPv6 que si elle est créée à l'aide de la version `2016-11-15` ou ultérieure de l'API Amazon EC2. La console Amazon EC2 utilise la dernière version de l'API.

Pour modifier le comportement de l'adressage IPv6 de votre sous-réseau

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
3. Sélectionnez votre sous-réseau, choisissez Actions, puis Edit subnet settings (Modifier les paramètres du sous-réseau).
4. Si elle est activée, la case à cocher Enable auto-assign IPv6 address demande une adresse IPv6 pour toutes les interfaces réseau créées dans le sous-réseau sélectionné. Activez ou désactivez la case à cocher si nécessaire, puis choisissez Edit (Modifier).

Pour modifier un attribut de sous-réseau à l'aide du AWS CLI

Utilisez la commande modify-subnet-attribute.

Réservation de bloc d'adresse CIDR de sous-réseau

Une réservation CIDR de sous-réseau est une plage d'adresses IPv4 ou IPv6 que vous mettez de côté afin de ne pas AWS pouvoir les attribuer à vos interfaces réseau. Cela vous permet de

réserver des blocs d'adresse CIDR IPv4 ou IPv6 (également appelés « préfixes ») à utiliser avec vos interfaces réseau.

Lorsque vous créez un sous-réseau CIDR, vous spécifiez comment vous allez utiliser l'adresse IP réservée. Les options suivantes sont disponibles :

- Préfixe : AWS attribue les adresses de la plage d'adresses IP réservée aux interfaces réseau. Pour plus d'informations, consultez la section Attribuer des préfixes aux interfaces réseau Amazon EC2 dans le guide de l'utilisateur Amazon EC2.
- Explicite — Vous attribuez manuellement des adresses IP aux interfaces réseau.

Les règles suivantes s'appliquent aux réservations de bloc d'adresse CIDR de sous-réseau :

- Lorsque vous créez une réservation CIDR de sous-réseau, la plage d'adresses IP peut inclure des adresses déjà utilisées. Créer une réservation de sous-réseau n'annule pas l'attribution des adresses IP déjà utilisées.
- Vous pouvez réserver plusieurs plages de blocs d'adresse CIDR par sous-réseau. Lorsque vous réservez plusieurs plages de blocs d'adresse CIDR dans le même VPC, elles ne peuvent pas se chevaucher.
- Lorsque vous réservez plusieurs plages dans un sous-réseau pour la délégation de préfixes et que cette dernière est configurée pour l'affectation automatique, nous choisissons de manière aléatoire les adresses IP à attribuer aux interfaces réseau.
- Lorsque vous supprimez une réservation de sous-réseau, les adresses IP non utilisées peuvent AWS être attribuées à vos interfaces réseau. Supprimer une réservation de sous-réseau n'annule pas l'attribution des adresses IP utilisées.

Pour plus d'informations sur la notation CIDR (Routage inter-domaines sans classe), consultez Adressage IP.

Utiliser les réservations de bloc d'adresse CIDR de sous-réseau en utilisant la console

Vous pouvez créer et gérer les réservations de bloc d'adresse CIDR de sous-réseau comme suit.

Pour modifier les réservations de bloc d'adresse CIDR de sous-réseau

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.

2. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
3. Sélectionnez le sous-réseau.
4. Choisissez l'onglet Réservations CIDR pour obtenir des informations sur les réservations existantes d'adresse CIDR de sous-réseau.
5. Pour ajouter ou supprimer des réservations CIDR de sous-réseau, choisissez Actions, Modifier les réservations de bloc d'adresse CIDR puis procédez comme suit :
   - Pour ajouter une réservation de bloc d'adresse CIDR IPv4, choisissez IPv4, Ajouter une réservation de bloc d'adresse CIDR IPv4. Choisissez le type de réservation, entrez la plage de blocs d'adresse CIDR, puis choisissez Ajouter.
   - Pour ajouter une réservation de bloc d'adresse CIDR IPv6, choisissez IPv6, Ajouter une réservation d'adresse CIDR IPv6. Choisissez le type de réservation, entrez la plage de blocs d'adresse CIDR, puis choisissez Ajouter.
   - Pour supprimer une réservation de bloc d'adresse CIDR, choisissez Supprimer pour la réservation de bloc d'adresse CIDR du sous-réseau.

Travaillez avec les réservations CIDR de sous-réseau à l'aide du AWS CLI

Vous pouvez utiliser le AWS CLI pour créer et gérer des réservations CIDR de sous-réseau.

Tâches

- Créer une réservation de bloc d'adresse CIDR de sous-réseau
- Afficher les réservations de bloc d'adresse CIDR de sous-réseau
- Supprimer une réservation de bloc d'adresse CIDR de sous-réseau

Créer une réservation de bloc d'adresse CIDR de sous-réseau

Vous pouvez utiliser create-subnet-cidr-reservation pour créer une réservation de bloc d'adresse CIDR de sous-réseau.

```
aws ec2 create-subnet-cidr-reservation --subnet-id subnet-03c51e2eEXAMPLE --
reservation-type prefix --cidr 2600:1f13:925:d240:3a1b::/80
```

Voici un exemple de sortie.

```
{
```

```
    "SubnetCidrReservation": {
        "SubnetCidrReservationId": "scr-044f977c4eEXAMPLE",
        "SubnetId": "subnet-03c51e2ef5EXAMPLE",
        "Cidr": "2600:1f13:925:d240:3a1b::/80",
        "ReservationType": "prefix",
        "OwnerId": "123456789012"
    }
}
```

Afficher les réservations de bloc d'adresse CIDR de sous-réseau

Vous pouvez utiliser get-subnet-cidr-reservations pour afficher les détails d'une réservation de bloc d'adresse CIDR de sous-réseau.

```
aws ec2 get-subnet-cidr-reservations --subnet-id subnet-05eef9fb78EXAMPLE
```

Supprimer une réservation de bloc d'adresse CIDR de sous-réseau

Vous pouvez utiliser delete-subnet-cidr-reservation pour supprimer une réservation de bloc d'adresse CIDR de sous-réseau.

```
aws ec2 delete-subnet-cidr-reservation --subnet-cidr-reservation-
id scr-044f977c4eEXAMPLE
```

Configuration des tables de routage

Une table de routage contient un ensemble de règles, appelées acheminements, qui déterminent la direction du trafic réseau à partir de votre sous-réseau ou de votre passerelle.

Table des matières

- Exemples d'options de routage
- Utiliser des tables de routage
- Assistant de routage middlebox

Concepts liés aux tables de routage

Voici les concepts clés relatifs aux tables de routage :

- Table de routage principale : il s'agit de la table de routage qui est associée automatiquement à votre VPC. Location : choisissez l'option de location pour ce VPC.
- Table de routage personnalisée : il s'agit de la table de routage que vous créez pour votre VPC.
- Destination : il s'agit de la plage d'adresses IP vers laquelle vous souhaitez acheminer le trafic (CIDR de destination). Par exemple, un réseau d'entreprise externe avec le CIDR `172.16.0.0/12`.
- Cible : il s'agit de la passerelle, de l'interface réseau ou de la connexion permettant d'envoyer le trafic de destination ; par exemple, une passerelle Internet.
- Association de table de routage : il s'agit de l'association entre une table de routage et un sous-réseau, une passerelle Internet ou une passerelle réseau privé virtuel.
- Table de routage de sous-réseau : il s'agit d'une table de routage associée à un sous-réseau.
- Route locale : il s'agit de l'acheminement de la communication par défaut dans le VPC.
- Propagation : si vous avez attaché une passerelle privée virtuelle à votre VPC et activé la propagation du routage, nous ajoutons automatiquement des routes pour votre connexion VPN à vos tables de routage de sous-réseau. Ainsi, vous n'avez pas besoin d'ajouter ou supprimer manuellement des routes VPN. Pour plus d'informations, veuillez consulter la section Options de routage Site-to-Site VPN du Guide de l'utilisateur Site-to-Site VPN.
- Table de routage de passerelle : il s'agit d'une table de routage associée à une passerelle Internet ou à une passerelle réseau privé virtuel.
- Association périphérique : il s'agit de la table de routage que vous utilisez pour acheminer le trafic VPC entrant vers une appliance. Vous associez une table de routage à la passerelle Internet ou à la passerelle réseau privé virtuel, et vous spécifiez l'interface réseau de votre appliance comme cible pour le trafic VPC.
- Table de routage de passerelle de transit : il s'agit d'une table de routage associée à une passerelle de transit. Pour plus d'informations, consultez Tables de routage de passerelle de transit dans Passerelle de transit Amazon VPC.

- Table de routage de passerelle locale : il s'agit d'une table de routage associée à une passerelle locale Outposts. Pour plus d'informations, veuillez consulter la rubrique Passerelles locales dans le Guide de l'utilisateur AWS Outposts .

Tables de routage des sous-réseaux

Votre VPC dispose d'un routeur implicite, et vous utilisez des tables de routage pour contrôler où le trafic réseau est dirigé. Chaque sous-réseau de votre VPC doit être associé à une table de routage, qui contrôle le routage pour ce sous-réseau (table de routage de sous-réseau). Vous pouvez associer explicitement un sous-réseau à une table de routage particulière. Sinon, le sous-réseau est implicitement associé à la table de routage principale. Un sous-réseau peut être associé à une seule table de routage à la fois, mais vous pouvez associer plusieurs sous-réseaux à une même table de routage.

Table des matières

Acheminements

Chaque acheminement d'une table spécifie une destination et une cible. Par exemple, pour permettre à votre sous-réseau d'accéder à Internet via une passerelle Internet, ajoutez l'acheminement suivant dans la table de routage de votre sous-réseau. La destination de l'acheminement est `0.0.0.0/0`, qui représente toutes les adresses IPv4. La cible est la passerelle Internet qui est attachée à votre VPC.

Destination	Cible
0.0.0.0/0	*igw-id*

Les blocs d'adresse CIDR IPv4 et IPv6 sont traités séparément. Par exemple, une route dotée du CIDR de destination `0.0.0.0/0` n'inclut pas automatiquement toutes les adresses IPv6. Vous devez créer un acheminement avec le bloc d'adresse CIDR de destination `::/0` pour toutes les adresses IPv6.

Si vous référencez fréquemment le même ensemble de blocs CIDR dans toutes vos AWS ressources, vous pouvez créer une liste de préfixes gérée par le client pour les regrouper. Vous pouvez ensuite spécifier la liste de préfixes comme destination dans votre entrée de table de routage.

Chaque table de routage contient un acheminement local pour la communication au sein du VPC. Cette route est ajoutée par défaut à toutes les tables de routage. Si votre VPC est associé à plusieurs blocs d'adresse CIDR IPv4, les tables de routage contiennent une route locale pour chaque bloc d'adresse CIDR IPv4. Si vous avez associé un bloc d'adresse CIDR IPv6 avec votre VPC, les tables de routage contiennent une route locale pour le bloc d'adresse CIDR IPv6. Vous pouvez remplacer ou restaurer la cible de chaque acheminement local si nécessaire.

Règles et considérations

- Vous pouvez ajouter à vos tables de routage un acheminement plus spécifique que l'acheminement local. La destination doit correspondre au bloc d'adresse CIDR IPv4 ou IPv6 complet d'un sous-réseau de votre VPC. La cible doit être une passerelle NAT, une interface réseau ou un point de terminaison d'équilibreur de charge de passerelle.
- Si votre table de routage contient plusieurs acheminements, nous utilisons l'acheminement le plus spécifique correspondant au trafic (correspondance de préfixe le plus long) pour déterminer comment acheminer le trafic.
- Vous ne pouvez pas ajouter d'acheminements aux adresses IPv4 qui sont une correspondance exacte ou un sous-ensemble de la plage suivante : 169.254.168.0/22. Cette plage se trouve dans l'espace d'adressage lien-local et est réservée à l'usage des AWS services. Par exemple, Amazon EC2 utilise des adresses de cette plage pour les services accessibles uniquement à partir d'instances EC2, tels que le service de métadonnées d'instance (IMDS) et le serveur Amazon DNS. Vous pouvez utiliser un bloc d'adresse CIDR qui dépasse, mais chevauche 169.254.168.0/22, mais les paquets destinés aux adresses de 169.254.168.0/22 ne seront pas transférés.
- Vous ne pouvez pas ajouter d'itinéraires aux adresses IPv6 correspondant exactement ou à un sous-ensemble de la plage suivante : fd00:ec2::/32. Cette plage se situe dans l'espace d'adresse locale unique (ULA) et est réservée à l'usage des AWS services. Par exemple, Amazon EC2 utilise des adresses de cette plage pour les services accessibles uniquement à partir d'instances EC2, tels que le service de métadonnées d'instance (IMDS) et le serveur DNS d'Amazon. Vous pouvez utiliser un bloc d'adresse CIDR qui est plus grand que, mais chevauche fd00:ec2::/32, mais les paquets destinés aux adresses de fd00:ec2::/32 ne seront pas transférés.
- Vous pouvez ajouter des appliances middlebox dans les chemins de routage de votre VPC. Pour en savoir plus, consultez the section called "Routage pour une appliance middlebox".

Exemple

Dans l'exemple suivant, supposez que le VPC comporte à la fois un bloc d'adresse CIDR IPv4 et un bloc d'adresse CIDR IPv6. Les trafics IPv4 et IPv6 sont traités séparément, comme le montre la table de routage suivante.

Destination	Cible
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567
::/0	eigw-aabbccddee1122334

- Le trafic IPv4 à acheminer au sein du VPC (10.0.0.0/16) est couvert par la route Local.
- Le trafic IPv6 à acheminer au sein du VPC (2001:db8:1234:1a00::/56) est couvert par la route Local.
- La route pour 172.31.0.0/16 envoie le trafic vers une connexion d'appairage.
- La route pour l'ensemble du trafic IPv4 (0.0.0.0/0) envoie le trafic vers une passerelle Internet. Par conséquent, tout le trafic IPv4, à l'exception du trafic à l'intérieur du VPC et de la connexion d'appairage, est acheminé vers la passerelle Internet.
- La route pour l'ensemble du trafic IPv6 (::/0) envoie le trafic vers une passerelle Internet de sortie uniquement. Par conséquent, tout le trafic IPv6, à l'exception du trafic à l'intérieur du VPC, est acheminé vers la passerelle Internet de sortie uniquement.

Table de routage principale

Lorsque vous créez un VPC, il est automatiquement associé à une table de routage principale. Si un sous-réseau n'est pas associé explicitement à une table de routage, la table de routage principale est utilisée par défaut. Sur la page Route Tables (Tables de routage) de la console Amazon VPC, vous pouvez afficher la table de routage principale d'un VPC en recherchant Oui dans la colonne Principale.

Par défaut, lorsque vous créez un VPC personnalisé, la table de routage principale contient seulement une route locale. Si vous Création d'un VPC et choisissez une passerelle NAT, Amazon VPC ajoute automatiquement des acheminements à la table de routage principale pour les passerelles.

Les règles suivantes s'appliquent à la table de routage principale :

- Vous pouvez ajouter, supprimer et modifier des acheminements dans la table de routage principale.
- Vous ne pouvez pas supprimer la table de routage principale.
- Vous ne pouvez pas définir une table de routage de passerelle comme table de routage principale.
- Vous pouvez remplacer la table de routage principale en associant une table de routage personnalisée à un sous-réseau.
- Vous pouvez associer explicitement un sous-réseau à la table de routage principale, même s'il est déjà associé implicitement.

  Vous pouvez procéder ainsi si vous changez la table faisant office de table de routage principale. Lorsque vous changez la table faisant office de table de routage principale, cela change également la table par défaut des nouveaux sous-réseaux ajoutés et des réseaux qui ne sont associés explicitement à aucune autre table de routage. Pour plus d'informations, consultez Remplacer la table de routage principale.

Tables de routage personnalisées

Par défaut, une table de routage contient une route locale pour la communication au sein du VPC. Si vous Création d'un VPC et choisissez un sous-réseau public, Amazon VPC crée une table de routage personnalisée et ajoute un acheminement qui pointe vers la passerelle Internet. Une façon de protéger votre VPC consiste à laisser la table de routage principale dans son état par défaut d'origine. Ensuite, associez explicitement chaque nouveau sous-réseau que vous créez à l'une des tables de routage personnalisées que vous avez créées. Vous vous assurez ainsi de contrôler explicitement la façon dont chaque sous-réseau route le trafic.

Vous pouvez ajouter, supprimer et modifier des acheminements dans une table de routage personnalisée. Vous pouvez supprimer une table de routage personnalisée seulement si elle n'a aucune association.

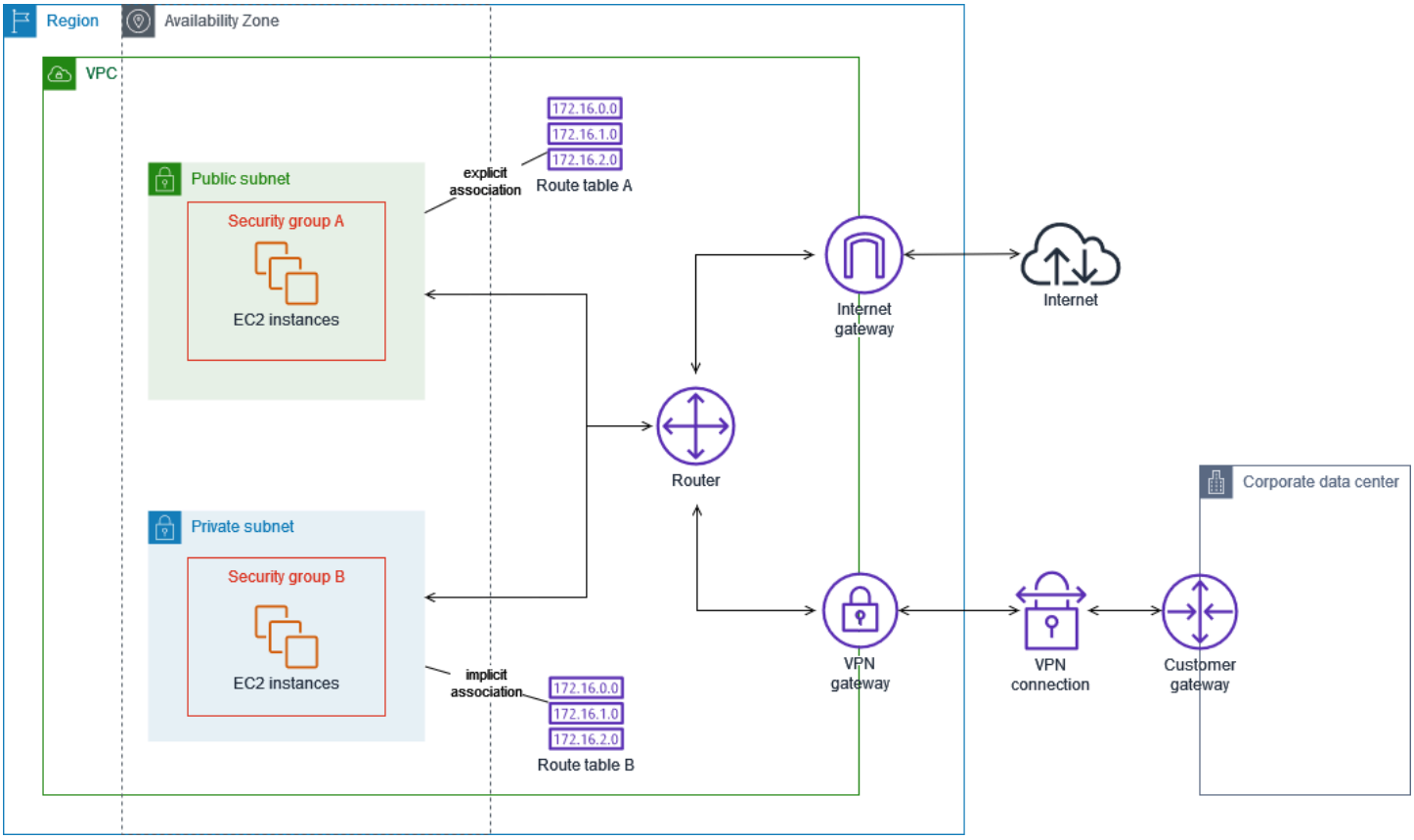
Association de la table de routage du sous-réseau

Chaque sous-réseau de votre VPC doit être associé à une table de routage. Un sous-réseau peut être associé explicitement à une table de routage personnalisée, ou associé implicitement ou explicitement à la table de routage principale. Pour de plus amples informations sur l'affichage de vos associations entre sous-réseaux et table de routage, veuillez consulter Déterminer quels sous-réseaux et/ou les passerelles sont explicitement associés.

Les sous-réseaux qui se trouvent dans des VPC associés à Outposts peuvent avoir un type de cible supplémentaire d'une passerelle locale. Il s'agit de la seule différence de routage par rapport aux sous-réseaux autres qu'Outposts.

Exemple 1 : Associations implicite et explicite de sous-réseau

Le schéma ci-après illustre le routage pour un VPC comportant une passerelle Internet, une passerelle réseau privé virtuel, un sous-réseau public et un sous-réseau VPN unique.



La table de routage A est une table de routage personnalisée qui est associée explicitement au sous-réseau public. Elle dispose d'une route qui envoie tout le trafic vers la passerelle Internet, ce qui fait du sous-réseau un sous-réseau public.

Destination	Cible
Bloc d'adresse du VPC	Local
0.0.0.0/0	*igw-id*

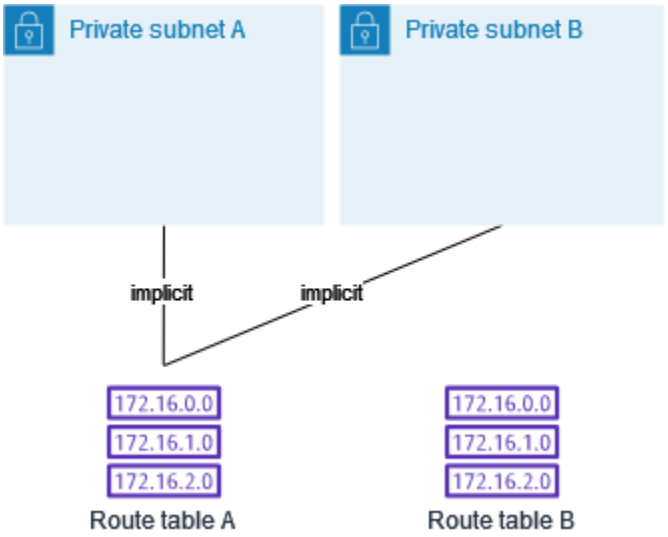
La table de routage B est la table de routage principale. Elle est implicitement associée au sous-réseau privé. Elle dispose d'une route qui envoie tout le trafic vers la passerelle privée virtuelle, mais aucune route vers la passerelle Internet, ce qui fait du sous-réseau un sous-réseau VPN uniquement. Si vous créez un autre sous-réseau dans ce VPC et que vous n'y associez pas de table de routage personnalisée, le sous-réseau sera également associé implicitement à cette table de routage, car il s'agit de la table de routage principale.

Destination	Cible
Bloc d'adresse du VPC	Local
0.0.0.0/0	*vgw-id*

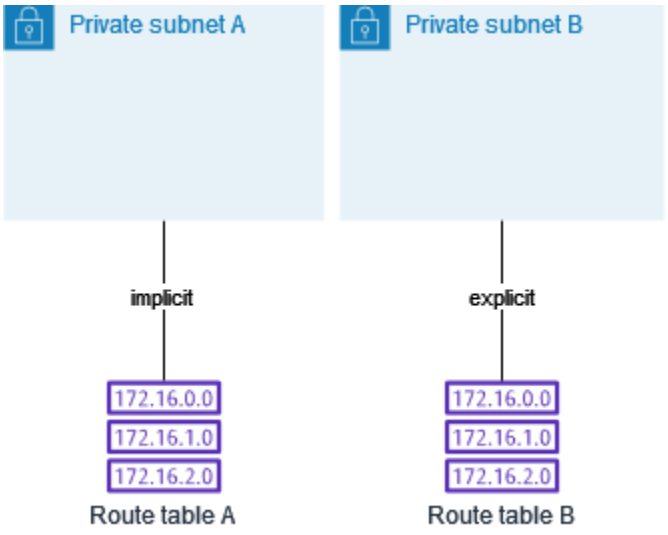
Exemple 2 : Remplacement de la table de routage principale

Vous pouvez apporter des modifications à la table de routage principale. Pour éviter toute interruption de trafic, nous vous recommandons de commencer par tester les changements de route à l'aide d'une table de routage personnalisée. Une fois satisfait des résultats du test, vous pouvez remplacer la table de routage principale par la nouvelle table personnalisée.

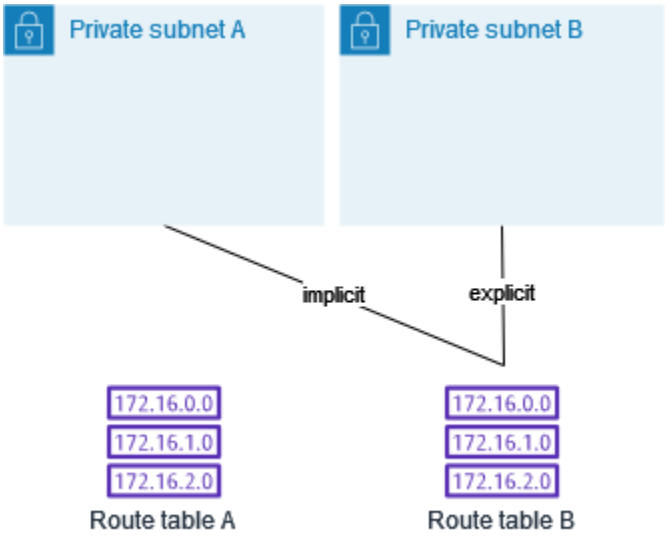
Le schéma suivant montre deux sous-réseaux et deux tables de routage. Le sous-réseau A est implicitement associé à la table de routage A, la table de routage principale. Le sous-réseau B est implicitement associé à la table de routage A. La table de routage B, une table de routage personnalisée, n'est associée à aucun des deux sous-réseaux.



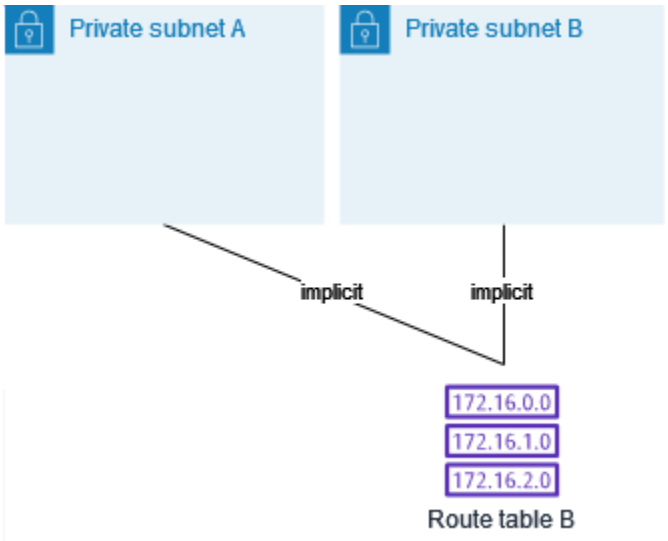
Pour remplacer la table de routage principale, commencez par créer une association explicite entre le sous-réseau B et la table de routage B. Testez la table de routage B.



Après avoir testé la table de routage B, définissez-la en tant que table de routage principale. Le sous-réseau B comporte toujours une association explicite à la table de routage B. Cependant, le sous-réseau A comporte une association implicite à la table de routage B, car il s'agit de la nouvelle table de routage principale. La table de routage A n'est plus associée à aucun des deux sous-réseaux.



(Facultatif) Si vous dissociez le sous-réseau B de la table de routage B, il y a toujours une association implicite entre le sous-réseau B et la table de routage B. Si vous n'avez plus besoin de la table de routage A, vous pouvez la supprimer.



Tables de routage de passerelle

Vous pouvez associer une table de routage à une passerelle Internet ou à une passerelle réseau privé virtuel. Lorsqu'une table de routage est associée à une passerelle, elle est appelée table de routage de passerelle. Vous pouvez créer une table de routage de passerelle pour bénéficier d'un contrôle précis du chemin de routage du trafic entrant dans votre VPC. Par exemple, vous pouvez intercepter le trafic qui entre dans votre VPC par une passerelle Internet en redirigeant ce trafic vers une appliance middlebox (telle qu'une appliance de sécurité) dans votre VPC.

Table des matières

Acheminements des tables de routage de passerelle

Une table de routage de passerelle associée à une passerelle Internet prend en charge les acheminements ayant les cibles suivantes :

- L'acheminement local par défaut
- Un point de terminaison Gateway Load Balancer
- Une interface réseau pour une appliance middlebox

Une table de routage de passerelle associée à une passerelle privée virtuelle prend en charge les acheminements ayant les cibles suivantes :

- L'acheminement local par défaut
- Un point de terminaison Gateway Load Balancer
- Une interface réseau pour une appliance middlebox

Lorsque la cible est un point de terminaison d'équilibreur de charge de passerelle ou une interface réseau, les destinations suivantes sont autorisées :

- L'ensemble du bloc d'adresse CIDR IPv4 ou IPv6 de votre VPC. Dans ce cas, vous remplacez la cible de la route locale par défaut.
- L'ensemble du bloc d'adresse CIDR IPv4 ou IPv6 d'un sous-réseau dans votre VPC. Il s'agit d'une route plus spécifique que la route locale par défaut.

Si vous remplacez la cible de la route locale dans une table de routage de passerelle par une interface réseau dans votre VPC, vous pourrez restaurer ultérieurement la cible `local` par défaut. Pour plus d'informations, consultez Remplacer ou restaurer la cible d'un acheminement local.

Exemple

Dans la table de routage de passerelle suivante, le trafic destiné à un sous-réseau contenant le bloc d'adresse CIDR `172.31.0.0/20` est routé vers une interface réseau spécifique. Le trafic destiné à tout autre sous-réseau du VPC utilise la route locale.

Destination	Cible
172.31.0.0/16	Locale
172.31.0.0/20	*eni-id*

Exemple

Dans la table de routage de passerelle suivante, la cible de la route locale est remplacée par un ID d'interface réseau. Le trafic destiné à tous les sous-réseaux du VPC est routé vers cette interface réseau.

Destination	Cible
172.31.0.0/16	*eni-id*

Règles et considérations

Vous ne pouvez pas associer une table de routage à une passerelle si l'une des situations suivantes s'applique :

- La table de routage contient les acheminements existants avec des cibles autres qu'une interface réseau, un point de terminaison de l'équilibreur de charge de passerelle ou l'acheminement local par défaut.
- La table de routage contient des routes existantes vers des blocs d'adresse CIDR en dehors des plages de votre VPC.
- La propagation du routage est activée pour la table de routage.

En outre, les règles et considérations suivantes s'appliquent :

- Vous ne pouvez pas ajouter de routes vers des blocs d'adresse CIDR en dehors des plages incluses dans votre VPC, y compris vers des plages plus grandes que les blocs d'adresse CIDR individuels du VPC.
- Vous pouvez uniquement spécifier `local`, un point de terminaison de l'équilibreur de charge de passerelle ou une interface réseau en tant que cible. Vous ne pouvez pas spécifier d'autres types de cibles, y compris des adresses IP d'hôtes individuels. Pour plus d'informations, consultez the section called "Exemples d'options de routage".
- Vous ne pouvez pas spécifier de liste de préfixes comme destination.
- Vous ne pouvez pas utiliser une table de routage de passerelle pour contrôler ni intercepter le trafic en dehors de votre VPC, tel que le trafic via une passerelle de transit attachée. Vous pouvez intercepter le trafic qui entre dans votre VPC et le rediriger vers une autre cible dans le même VPC uniquement.
- Pour vous assurer que le trafic atteint votre appliance middlebox, l'interface réseau cible doit être connectée à une instance en cours d'exécution. Pour le trafic qui passe par une passerelle Internet, l'interface réseau cible doit également avoir une adresse IP publique.
- Lors de la configuration de votre appliance middlebox, prenez note des considérations relatives à l'appliance.
- Lorsque vous acheminez le trafic via une appliance middlebox, le trafic de retour du sous-réseau de destination doit être acheminé via la même appliance. Le routage asymétrique n'est pas pris en charge.
- Les règles de table de routage s'appliquent à l'ensemble du trafic qui quitte un sous-réseau. Le trafic qui quitte un sous-réseau est défini comme étant destiné à l'adresse MAC du routeur de passerelle de ce sous-réseau. Le trafic destiné à l'adresse MAC d'une autre interface réseau du sous-réseau utilise un routage (de couche 2) de liaison de données et non de réseau (couche 3), si bien que les règles ne s'appliquent pas à ce trafic.
- Les zones locales ne prennent pas toutes en charge l'association périphérique avec des passerelles privées virtuelles. Pour plus d'informations sur les zones disponibles, consultez la section Considérations dans le Guide de l'utilisateur des zones locales AWS .

Priorité d'acheminement

En général, nous dirigeons le trafic en utilisant l'acheminement le plus spécifique qui correspond au trafic. C'est ce qu'on appelle la correspondance du préfixe le plus long. Si votre table de routage comporte des acheminements qui se chevauchent ou correspondent, les règles suivantes s'appliquent :

Table des matières

Correspondance du préfixe le plus long

Les acheminements vers des adresses IPv4 et IPv6 ou des blocs d'adresse CIDR sont indépendantes les unes des autres. Nous utilisons l'acheminement le plus spécifique correspondant au trafic IPv4 ou au trafic IPv6 pour déterminer comment acheminer le trafic.

Par exemple, la table de routage de sous-réseau ci-après comporte un acheminement pour le trafic Internet IPv4 (`0.0.0.0/0`) qui pointe vers une passerelle Internet, et un acheminement pour le trafic IPv4 (`172.31.0.0/16`) qui pointe vers une connexion d'appairage (`pcx-11223344556677889`). Tout le trafic en provenance du sous-réseau qui est destiné à la plage d'adresses IP `172.31.0.0/16` utilise la connexion d'appairage, car cet acheminement est plus spécifique que l'acheminement vers la passerelle Internet. Tout trafic destiné à une cible au sein du VPC (`10.0.0.0/16`) est couvert par la route `local` et, par conséquent, routé au sein du VPC. Tout autre trafic en provenance du sous-réseau utilise la passerelle Internet.

Destination	Cible
10.0.0.0/16	local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567

Priorité des acheminements et acheminements propagés

Si vous avez attaché une passerelle réseau privé virtuel à votre VPC et activé la propagation d'acheminement sur votre table de routage de sous-réseau, les acheminements représentant votre connexion Site-to-Site VPN apparaissent automatiquement comme des acheminements propagés dans votre table de routage.

Si la destination d'un acheminement propagé chevauche un acheminement statique, l'acheminement statique est prioritaire.

Si la destination d'un acheminement propagé est identique à la destination d'un acheminement statique, l'acheminement statique est prioritaire si la cible est l'une des cibles suivantes :

- Passerelle Internet
- Passerelle NAT
- Interface réseau
- ID d'instance
- Point de terminaison d'un VPC de passerelle
- Passerelle de transit
- Connexion d'appairage de VPC
- Point de terminaison d'équilibreur de charge de passerelle

Pour de plus amples informations, consultez Tables de routage et priorité d'acheminement VPN dans le Guide de l'utilisateur AWS Site-to-Site VPN .

L'exemple de table de routage suivant a un acheminement statique vers une passerelle Internet et un acheminement propagé vers une passerelle réseau privé virtuel. Les deux acheminements ont pour destination : `172.31.0.0/24`. Étant donné qu'un acheminement statique vers une passerelle Internet est prioritaire, tout le trafic destiné à `172.31.0.0/24` est acheminé vers la passerelle Internet.

Destination	Cible	Propagé
10.0.0.0/16	local	Non
172.31.0.0/24	vgw-11223344556677889	Oui
172.31.0.0/24	igw-12345678901234567	Non

Listes des priorités et des préfixes d'acheminement

Si votre table de routage fait référence à une liste de préfixes, les règles suivantes s'appliquent :

- Si votre table de routage contient un acheminement statique qui chevauche un autre acheminement faisant référence à une liste de préfixes, l'acheminement statique avec le bloc d'adresse CIDR de destination est prioritaire.

- Si votre table de routage contient un acheminement propagé qui correspond à un acheminement qui fait référence à une liste de préfixes, l'acheminement qui fait référence à la liste de préfixes est prioritaire. Veuillez noter que pour les acheminements qui se chevauchent, les acheminements plus spécifiques sont toujours prioritaires, qu'il s'agisse d'acheminements propagés, d'acheminements statiques ou d'acheminements faisant référence à des listes de préfixes.
- Si votre table de routage fait référence à plusieurs listes de préfixes dont les blocs d'adresse CIDR se chevauchent vers des cibles différentes, nous choisissons aléatoirement le chevauchement prioritaire. Par la suite, le même acheminement est toujours prioritaire.

Quotas des tables de routage

Le nombre de tables de routage que vous pouvez créer par VPC est limité. Il existe également un quota pour le nombre de routes que vous pouvez ajouter par table de routage. Pour plus d'informations, consultez Quotas Amazon VPC.

Résoudre les problèmes d'accessibilité

Reachability Analyzer est un outil d'analyse de configuration statique. Utilisez Reachability Analyzer pour analyser et déboguer l'accessibilité réseau entre deux ressources de votre VPC. Reachability Analyzer hop-by-hop fournit des détails sur le chemin virtuel entre ces ressources lorsqu'elles sont accessibles, et identifie le composant bloquant dans le cas contraire. Par exemple, il peut identifier les itinéraires de table de routage manquants ou mal configurés.

Pour plus d'informations, reportez-vous au Guide de l'Analyseur d'accessibilité.

Exemples d'options de routage

Les rubriques ci-après décrivent le routage pour des passerelles ou des connexions spécifiques au sein de votre VPC.

Table des matières

- Routage vers une connexion d'appairage de VPC
- Routage vers un point de terminaison d'un VPC de passerelle
- Routage vers une passerelle Internet de sortie uniquement
- Routage pour une passerelle de transit
- Routage pour une appliance middlebox
- Routage à l'aide d'une liste de préfixes
- Routage vers un point de terminaison d'équilibreur de charge de passerelle

Routage vers une passerelle Internet

Vous pouvez faire d'un sous-réseau un sous-réseau public en ajoutant une route dans votre table de routage de sous-réseau vers une passerelle Internet. Pour ce faire, créez et attachez une passerelle Internet à votre VPC, puis ajoutez une route avec comme destination l'adresse `0.0.0.0/0` pour le trafic IPv4 ou l'adresse `::/0` pour le trafic IPv6, et comme cible l'ID de la passerelle Internet (`igw-xxxxxxxxxxxxxxxxx`).

Destination	Cible
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Pour plus d'informations, consultez Connecter à l'Internet à l'aide d'une passerelle Internet.

Routage vers un périphérique NAT

Pour permettre aux instances d'un sous-réseau privé de se connecter à Internet, vous pouvez créer une passerelle NAT ou lancer une instance NAT dans un sous-réseau public. Ensuite, ajoutez une route pour la table de routage du sous-réseau privé afin de router le trafic Internet IPv4 (`0.0.0.0/0`) vers le périphérique NAT.

Destination	Cible
0.0.0.0/0	*nat-gateway-id*

Vous pouvez également créer des routes plus spécifiques vers d'autres cibles pour éviter des frais inutiles de traitement de données liés à l'utilisation d'une passerelle NAT ou pour router un certain trafic de manière privée. Dans l'exemple suivant, le trafic Amazon S3 (pl-xxxxxxxx, une liste de préfixes qui contient les plages d'adresses IP pour Amazon S3 dans une région spécifique) est acheminé vers un point de terminaison d'un VPC de passerelle et le trafic 10.25.0.0/16 est acheminé vers une connexion d'appairage de VPC. Ces plages d'adresses IP sont plus spécifiques que 0.0.0.0/0. Lorsque des instances envoient du trafic vers Amazon S3 ou le VPC d'appairage, le trafic est envoyé vers le point de terminaison VPC de passerelle ou la connexion d'appairage de VPC. Tout autre trafic est envoyé à la passerelle NAT.

Destination	Cible
0.0.0.0/0	*nat-gateway-id*
pl-*xxxxxxxx*	*vpce-id*
10.25.0.0/16	*pcx-id*

Pour plus d'informations, consultez Périphériques NAT.

Routage vers une passerelle réseau privé virtuel

Vous pouvez utiliser une AWS Site-to-Site VPN connexion pour permettre aux instances de votre VPC de communiquer avec votre propre réseau. Pour ce faire, créez et attachez une passerelle réseau privé virtuel à votre VPC. Ensuite, ajoutez une route dans votre table de routage de sous-réseau avec la destination de votre réseau et une cible correspondant à la passerelle réseau privé virtuel (`vgw-xxxxxxxxxxxxxxxxx`).

Destination	Cible
10.0.0.0/16	*vgw-id*

Vous pouvez ensuite créer et configurer votre connexion Site-to-Site VPN. Pour plus d'informations, consultez Qu'est-ce qu' AWS Site-to-Site VPN ? et Tables de routage et priorité de route VPN dans le Guide de l'utilisateur AWS Site-to-Site VPN .

Une connexion Site-to-Site VPN sur une passerelle réseau privé virtuel n'est pas compatible avec le trafic IPv6. Toutefois, nous prenons en charge le trafic IPv6 acheminé via une passerelle réseau privé virtuel vers une connexion AWS Direct Connect . Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS Direct Connect.

Routage vers une passerelle AWS Outposts locale

Cette section décrit les configurations des tables de routage pour le routage vers une passerelle AWS Outposts locale.

Table des matières

Activer le trafic entre les sous-réseaux de l'Outpost et votre réseau sur site

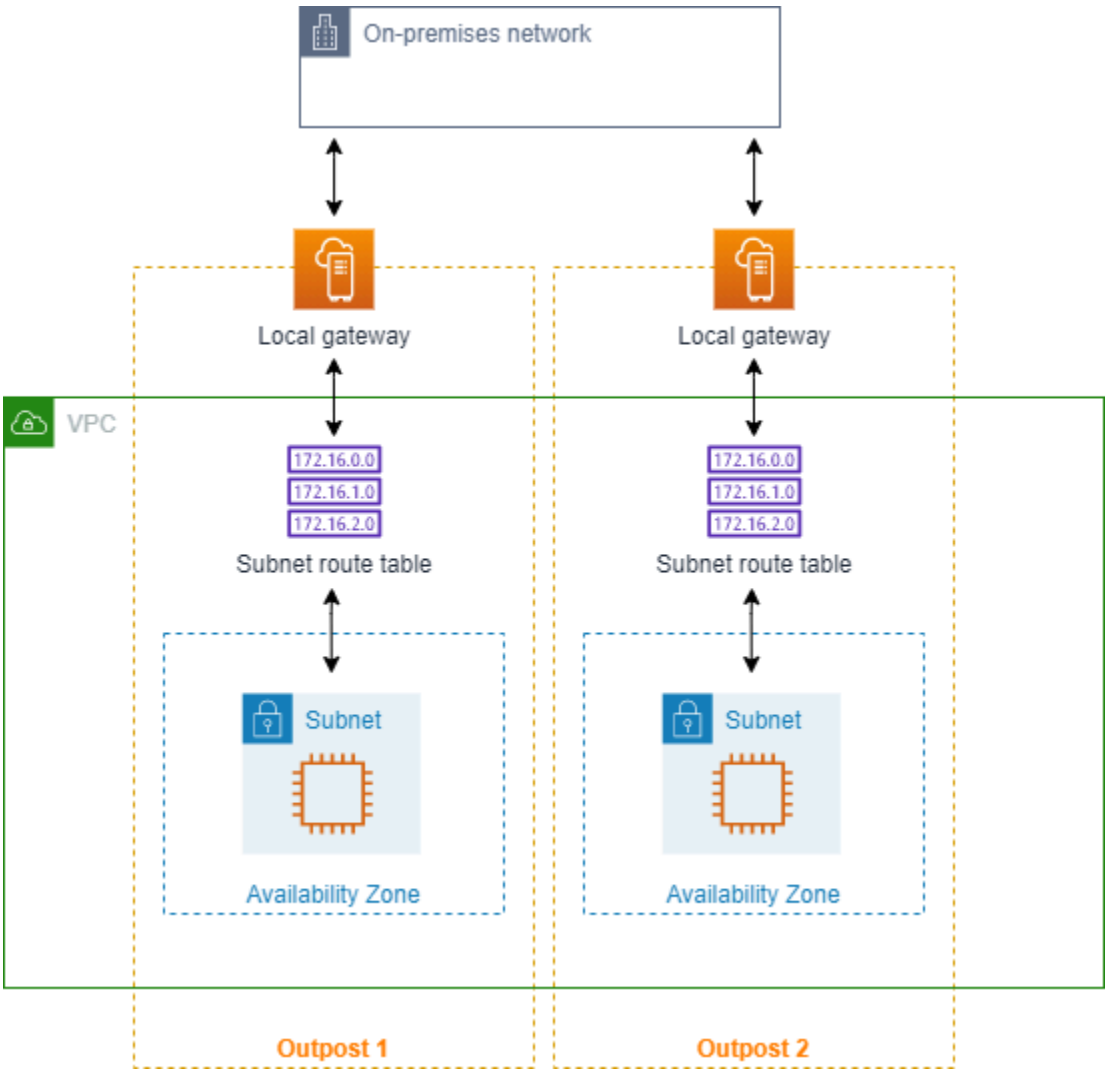
Les sous-réseaux situés dans des VPC associés à AWS Outposts peuvent avoir un type de cible supplémentaire, à savoir une passerelle locale. Considérez le cas où vous souhaitez que la passerelle locale route le trafic avec une adresse de destination 192.168.10.0/24 vers le réseau client. Pour ce faire, ajoutez la route suivante avec le réseau de destination et une cible de la passerelle locale (`lgw-xxxx`).

Destination	Cible
192.168.10.0/24	*lgw-id*

Permettre le trafic entre les sous-réseaux du même VPC à travers les Outposts

Vous pouvez établir une communication entre des sous-réseaux qui sont dans le même VPC à travers différents Outposts en utilisant les passerelles locales Outpost et votre réseau sur site.

Vous pouvez utiliser cette fonctionnalité pour créer des architectures similaires aux architectures de zones de disponibilité (AZ) multiples pour vos applications sur site exécutées sur des racks d'Outposts en établissant une connectivité entre les racks d'Outposts qui sont ancrés à différentes AZ.



Pour activer cette fonctionnalité, ajoutez un routage à la table de routage du sous-réseau de votre rack Outpost qui soit plus spécifique que le routage local dans cette table de routage et qui ait un type de cible de passerelle locale. La destination du routage doit correspondre à l'intégralité du bloc IPv4 du sous-réseau de votre VPC qui se trouve dans un autre Outpost. Répétez cette configuration pour tous les sous-réseaux de l'Outpost qui doivent communiquer.

Important

- Pour utiliser cette fonctionnalité, vous devez utiliser le routage direct VPC. Vous ne pouvez pas utiliser vos propres adresses IP appartenant au client.
- Votre réseau sur site auquel les passerelles locales des Outposts sont connectées doit disposer du routage nécessaire pour que les sous-réseaux puissent accéder l'un à l'autre.

- Si vous voulez utiliser des groupes de sécurité pour les ressources des sous-réseaux, vous devez utiliser des règles qui incluent des plages d'adresses IP comme source ou destination dans les sous-réseaux des Outposts. Vous ne pouvez pas utiliser d'ID de groupe de sécurité.
- Les racks Outposts existants peuvent nécessiter une mise à jour pour permettre la prise en charge de la communication intra-VPC entre plusieurs Outposts. Si cette fonctionnalité ne vous convient pas, contactez AWS Support.

Example Exemple

Pour un VPC avec un CIDR de 10.0.0.0/16, un sous-réseau Outpost 1 avec un CIDR de 10.0.1.0/24, et un sous-réseau Outpost 2 avec un CIDR de 10.0.2.0/24, l'entrée de la table de routage du sous-réseau Outpost 1 serait la suivante :

Destination	Cible
10.0.0.0/16	Locale
10.0.2.0/24	*lgw-1-id*

L'entrée de la table de routage du sous-réseau Outpost 2 serait la suivante :

Destination	Cible
10.0.0.0/16	Locale
10.0.1.0/24	*lgw-2-id*

Routage vers une connexion d'appairage de VPC

Une connexion d'appairage de VPC est une connexion de mise en réseau entre deux VPC qui permet d'acheminer le trafic entre ces derniers à l'aide d'adresses IPv4 privées. Les instances des deux VPC peuvent communiquer entre elles comme si elles faisaient partie du même réseau.

Pour activer le routage du trafic entre des VPC dans une connexion d'appairage de VPC, vous devez ajouter une route dans une ou plusieurs tables de routage de sous-réseau qui pointe vers la

connexion d'appairage de VPC. Cela vous permet d'accéder à tout ou partie du bloc d'adresse CIDR de l'autre VPC dans la connexion d'appairage. De même, le propriétaire de l'autre VPC doit ajouter une route dans sa table de routage de sous-réseau afin de router le trafic en retour vers votre VPC.

Par exemple, vous disposez d'une connexion d'appairage VPC (`pcx-11223344556677889`) entre deux VPC, avec les informations suivantes :

- VPC A : le bloc d'adresse CIDR est 10.0.0.0/16
- VPC B : le bloc d'adresse CIDR est 172.31.0.0/16

Pour permettre le trafic entre les VPC et autoriser l'accès à l'intégralité du bloc d'adresse CIDR IPv4 de chaque VPC, la table de routage VPC A est configurée comme suit.

Destination	Cible
10.0.0.0/16	Local
172.31.0.0/16	pcx-11223344556677889

La table de routage VPC B est configurée comme suit.

Destination	Cible
172.31.0.0/16	Local
10.0.0.0/16	pcx-11223344556677889

Votre connexion d'appairage de VPC peut également prendre en charge la communication IPv6 entre les instances dans les VPC, si les VPC et les instances sont activés pour la communication IPv6. Pour activer le routage du trafic IPv6 entre les VPC, vous devez ajouter une route vers votre table de routage qui pointe vers la connexion d'appairage de VPC pour accéder à tout ou partie du bloc d'adresse CIDR IPv6 du VPC pair.

Par exemple, à l'aide de la même connexion d'appairage de VPC (`pcx-11223344556677889`) ci-dessus, supposez que les VPC disposent des informations suivantes :

- VPC A : le bloc d'adresse CIDR IPv6 est `2001:db8:1234:1a00::/56`

- VPC B : le bloc d'adresse CIDR IPv6 est `2001:db8:5678:2b00::/56`

Pour activer la communication IPv6 via la connexion d'appairage de VPC, ajoutez la route suivante dans la table de routage de sous-réseau pour VPC A.

Destination	Cible
10.0.0.0/16	Local
172.31.0.0/16	pcx-11223344556677889
2001:db8:5678:2b00::/56	pcx-11223344556677889

Ajoutez la route suivante dans la table de routage pour VPC B.

Destination	Cible
172.31.0.0/16	Local
10.0.0.0/16	pcx-11223344556677889
2001:db8:1234:1a00::/56	pcx-11223344556677889

Pour de plus amples informations sur les connexions d'appairage de VPC, veuillez consulter le Guide de l'appairage Amazon VPC.

Routage vers un point de terminaison d'un VPC de passerelle

Un point de terminaison VPC de passerelle vous permet de créer une connexion privée entre votre VPC et un autre service. AWS Lorsque vous créez un point de terminaison de passerelle, vous spécifiez les tables de routage de sous-réseau dans votre VPC qui sont utilisées par le point de terminaison de passerelle. Une route est automatiquement ajoutée pour chacune des tables de routage avec une destination qui spécifie l'ID de liste des préfixes du service (`pl-`*`xxxxxxxx`*) et une cible avec l'ID point de terminaison (`vpce-`*`xxxxxxxxxxxxxxxxx`*). Vous ne pouvez pas supprimer ou modifier explicitement la route du point de terminaison, mais vous pouvez modifier les tables de routage qui sont utilisées par le point de terminaison.

Pour plus d'informations sur le routage pour les points de terminaison et les implications pour les routes vers les services AWS , veuillez consulter Routage des points de terminaison de passerelle.

Routage vers une passerelle Internet de sortie uniquement

Vous pouvez créer une passerelle Internet de sortie uniquement pour votre VPC afin de permettre aux instances figurant dans un sous-réseau privé d'initier une communication sortante vers Internet, mais d'empêcher Internet d'établir des connexions avec les instances. Une passerelle Internet de sortie uniquement est utilisée pour le trafic IPv6 uniquement. Pour configurer le routage pour une passerelle Internet de sortie uniquement, ajoutez une route dans la table de routage du sous-réseau privé afin de router le trafic Internet IPv6 (`::/0`) vers la passerelle Internet de sortie uniquement.

Destination	Target
::/0	*eigw-id*

Pour plus d'informations, consultez Activer le trafic sortant IPv6 à l'aide de passerelles Internet de sortie uniquement.

Routage pour une passerelle de transit

Lorsque vous associez un VPC à une passerelle de transit, vous devez ajouter une route à votre table de routage de sous-réseau pour que le trafic passe par la passerelle de transit.

Examinez le scénario suivant où nous disposons de trois VPC associés à une passerelle de transit. Dans ce scénario, tous les attachements sont associés à la table de routage de la passerelle de transit et propage vers elle. Par conséquent, tous les attachements peuvent s'acheminer des paquets respectivement, la passerelle de transit servant de simple hub d'IP de couche 3.

Par exemple, vous disposez de deux VPC avec les informations suivantes :

- VPC A : 10.1.0.0/16, ID d'attachement tgw-attach-11111111111111111
- VPC B : 10.2.0.0/16, ID d'attachement tgw-attach-22222222222222222

Pour permettre le trafic entre les VPC et autoriser l'accès à la passerelle de transit, la table de routage VPC A est configurée comme suit.

Destination	Cible
10.1.0.0/16	Local
10.0.0.0/8	*tgw-id*

Voici un exemple des entrées de table de routage de la passerelle de transit pour les attachements de VPC.

Destination	Cible
10.1.0.0/16	tgw-attach-11111111111111111
10.2.0.0/16	tgw-attach-22222222222222222

Pour de plus amples informations sur les tables de routage de passerelle de transit, veuillez consulter Routage dans Passerelle de transit Amazon VPC

Routage pour une appliance middlebox

Vous pouvez ajouter des appliances middlebox dans les chemins de routage de votre VPC. Voici des cas d'utilisation possibles :

- Interception du trafic qui entre dans votre VPC via une passerelle Internet ou une passerelle réseau privé virtuel en le dirigeant vers une appliance middlebox dans votre VPC. Vous pouvez utiliser l'assistant de routage du boîtier intermédiaire pour configurer AWS automatiquement les tables de routage appropriées pour votre passerelle, votre boîtier intermédiaire et votre sous-réseau de destination. Pour plus d'informations, consultez the section called "Assistant de routage middlebox".
- Direction du trafic entre deux sous-réseaux vers une appliance middlebox. Pour ce faire, vous pouvez créer un acheminement pour une table de routage de sous-réseau qui correspond au CIDR de sous-réseau de l'autre sous-réseau et spécifie un point de terminaison Gateway Load Balancer, une passerelle NAT, un point de terminaison Network Firewall ou l'interface réseau d'une appliance en tant que cible. Sinon, pour rediriger l'ensemble du trafic du sous-réseau vers un autre sous-réseau, remplacez la cible de l'acheminement local par un point de terminaison Gateway Load Balancer, une passerelle NAT ou une interface réseau.

Vous pouvez configurer l'appliance en fonction de vos besoins. Par exemple, vous pouvez configurer une appliance de sécurité pour filtrer tout le trafic, ou une appliance d'accélération WAN. L'appliance est déployée en tant qu'instance Amazon EC2 dans un sous-réseau de votre VPC et est représentée par une interface réseau Elastic (interface réseau) dans votre sous-réseau.

Si vous activez la propagation du routage pour la table de routage du sous-réseau de destination, vous devez tenir compte de la priorité de routage. Nous donnons la priorité à l'acheminement le plus spécifique, et, en cas de correspondance des acheminements, nous donnons la priorité aux acheminements statiques plutôt qu'aux acheminements propagés. Vérifiez vos itinéraires pour vous assurer que le trafic est correctement acheminé et qu'il n'y a aucune conséquence imprévue si vous activez ou désactivez la propagation des itinéraires (par exemple, la propagation des itinéraires est requise pour une AWS Direct Connect connexion qui prend en charge les trames jumbo).

Pour acheminer le trafic VPC entrant vers une appliance, vous associez une table de routage à la passerelle Internet ou à la passerelle réseau privé virtuel, et vous spécifiez l'interface réseau de votre appliance comme cible pour le trafic VPC. Pour plus d'informations, consultez Tables de routage de passerelle. Vous pouvez également acheminer le trafic sortant de votre sous-réseau vers une appliance middlebox figurant dans un autre sous-réseau.

Pour obtenir des exemples de routage middlebox, consultez Scénarios middlebox.

Table des matières

Considérations relatives aux appliances

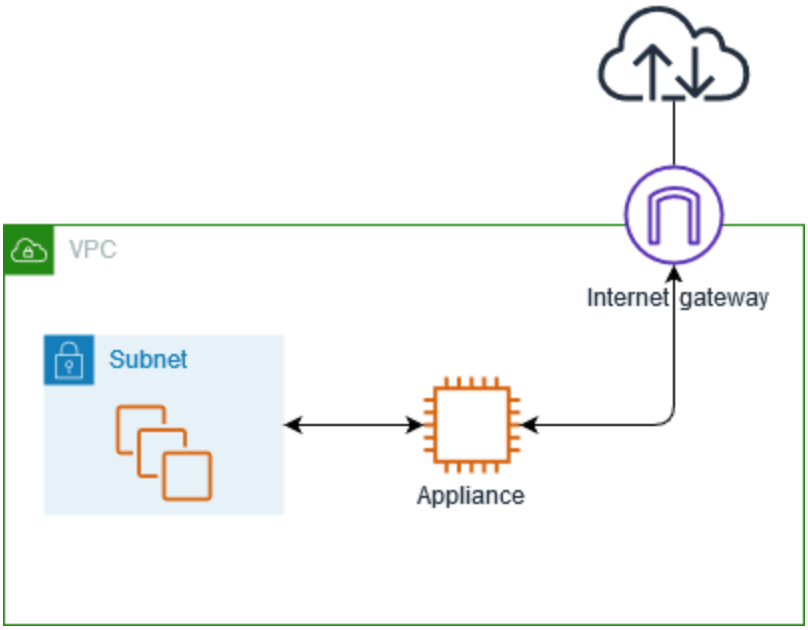
Vous pouvez choisir une appliance tierce provenant de AWS Marketplace ou configurer votre propre appliance. Lorsque vous créez ou configurez une appliance, prenez en compte les éléments suivants :

- L'appliance doit être configurée dans un sous-réseau distinct du trafic source ou de destination.
- Vous devez désactiver la vérification origine/destination sur l'appliance. Pour plus d'informations, consultez la section Modification de la vérification de la source ou de la destination dans le guide de l'utilisateur Amazon EC2.
- Vous ne pouvez pas acheminer le trafic entre les hôtes du même sous-réseau via une appliance.

- L'appliance n'est pas tenue d'effectuer la traduction d'adresses réseau (NAT).
- Vous pouvez ajouter à vos tables de routage un acheminement plus spécifique que l'acheminement local. Vous pouvez utiliser des acheminements plus spécifiques pour rediriger le trafic entre les sous-réseaux d'un VPC (trafic Est-Ouest) vers une appliance middlebox. La destination de l'acheminement doit correspondre au bloc d'adresse CIDR IPv4 ou IPv6 complet d'un sous-réseau de votre VPC.
- Pour intercepter le trafic IPv6, vérifiez que votre VPC, votre sous-réseau et l'appliance prennent en charge IPv6. Les passerelles réseau privé virtuel ne prennent pas en charge le trafic IPv6.

Acheminement du trafic entre une passerelle et une appliance

Pour acheminer le trafic VPC entrant vers une appliance, vous associez une table de routage à la passerelle Internet ou à la passerelle réseau privé virtuel, et vous spécifiez l'interface réseau de votre appliance comme cible pour le trafic VPC. Dans l'exemple suivant, le VPC dispose d'une passerelle Internet, d'une appliance et d'un sous-réseau avec des instances. Le trafic en provenance d'Internet est acheminé via une appliance.



Associez cette table de routage à votre passerelle Internet ou passerelle réseau privé virtuel. La première entrée est l'acheminement local. La deuxième entrée envoie le trafic IPv4 destiné au sous-réseau vers l'interface réseau de l'appliance. Cet acheminement est plus spécifique que l'acheminement local.

Destination	Cible
Bloc d'adresse du VPC	Local
Bloc d'adresse CIDR du sous-réseau	*ID d'interface réseau de l'appliance*

Vous pouvez également remplacer la cible de l'acheminement local par l'interface réseau de l'appliance. Vous pouvez procéder ainsi pour faire en sorte que l'ensemble du trafic soit acheminé automatiquement vers l'appliance, y compris le trafic destiné aux sous-réseaux que vous ajouterez dans l'avenir au VPC.

Destination	Cible
Bloc d'adresse CIDR du VPC	*ID d'interface réseau de l'appliance*

Pour acheminer le trafic de votre sous-réseau vers une appliance figurant dans un autre sous-réseau, ajoutez un acheminement dans votre table de routage de sous-réseau, afin d'acheminer le trafic vers l'interface réseau de l'appliance. La destination doit être moins spécifique que la destination de la route locale. Par exemple, pour du trafic destiné à Internet, spécifiez `0.0.0.0/0` (toutes les adresses IPv4) comme destination.

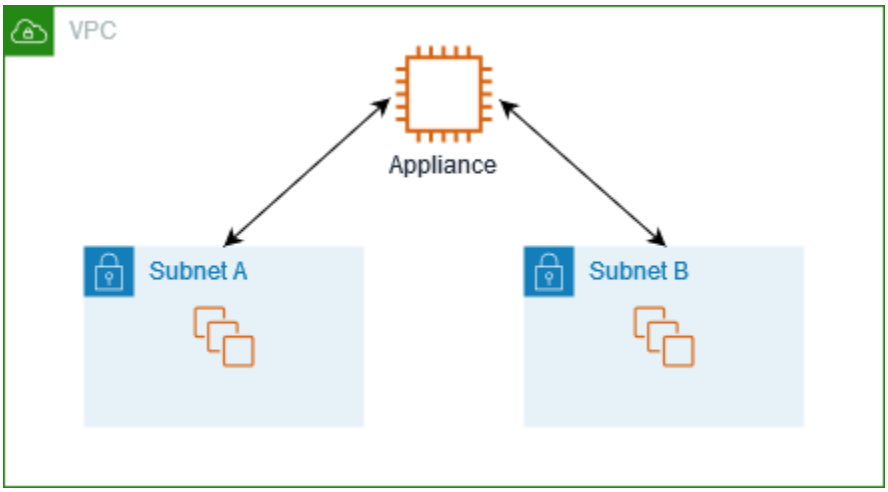
Destination	Cible
Bloc d'adresse du VPC	Local
0.0.0.0/0	*ID d'interface réseau de l'appliance*

Ensuite, dans la table de routage associée au sous-réseau de l'appliance, ajoutez un acheminement qui renvoie le trafic à la passerelle Internet ou à la passerelle réseau privé virtuel.

Destination	Cible
Bloc d'adresse du VPC	Local
0.0.0.0/0	*igw-id*

Acheminement du trafic inter-sous-réseaux vers une appliance

Vous pouvez acheminer le trafic destiné à un sous-réseau spécifique vers l'interface réseau d'une appliance. Dans l'exemple suivant, le VPC contient deux sous-réseaux et une appliance. Le trafic entre les sous-réseaux est acheminé via une appliance.



Groupes de sécurité

Lorsque vous acheminez le trafic entre les instances de différents sous-réseaux via une appliance middlebox, les groupes de sécurité des deux instances doivent autoriser le trafic à transiter entre les instances. Le groupe de sécurité de chaque instance doit référencer l'adresse IP privée de l'autre instance ou la plage d'adresses CIDR du sous-réseau qui contient l'autre instance en tant que source. Si vous référencez le groupe de sécurité de l'autre instance en tant que source, cela n'autorise pas le trafic à transiter entre les instances.

Routage

Voici un exemple de table de routage pour le sous-réseau A. La première entrée autorise les instances du VPC à communiquer entre elles. La deuxième entrée achemine l'ensemble du trafic du sous-réseau A au sous-réseau B vers l'interface réseau de l'appliance.

Destination	Cible
Bloc d'adresse du VPC	Local
CIDR du sous-réseau B	*ID d'interface réseau de l'appliance*

Voici un exemple de table de routage pour le sous-réseau B. La première entrée autorise les instances du VPC à communiquer entre elles. La deuxième entrée achemine l'ensemble du trafic du sous-réseau B au sous-réseau A vers l'interface réseau de l'appliance.

Destination	Cible
Bloc d'adresse du VPC	Local
CIDR du sous-réseau A	*ID d'interface réseau de l'appliance*

Vous pouvez également remplacer la cible de l'acheminement local par l'interface réseau de l'appliance. Vous pouvez procéder ainsi pour faire en sorte que l'ensemble du trafic soit acheminé automatiquement vers l'appliance, y compris le trafic destiné aux sous-réseaux que vous ajouterez dans l'avenir au VPC.

Destination	Cible
Bloc d'adresse CIDR du VPC	*ID d'interface réseau de l'appliance*

Routage à l'aide d'une liste de préfixes

Si vous référencez fréquemment le même ensemble de blocs CIDR dans toutes vos AWS ressources, vous pouvez créer une liste de préfixes gérée par le client pour les regrouper. Vous pouvez ensuite spécifier la liste de préfixes comme destination dans votre entrée de table de routage. Vous pouvez ajouter ou supprimer ultérieurement des entrées pour la liste de préfixes sans avoir à mettre à jour vos tables de routage.

Par exemple, vous disposez d'une passerelle de transit avec plusieurs pièces jointes VPC. Les VPC doivent pouvoir communiquer avec deux pièces jointes VPC spécifiques qui ont les blocs CIDR suivants :

- 10.0.0.0/16
- 10.2.0.0/16

Vous créez une liste de préfixes avec les deux entrées. Dans vos tables de routage de sous-réseau, vous créez un itinéraire et spécifiez la liste de préfixes comme destination, et la passerelle de transit comme cible.

Destination	Cible
172.31.0.0/16	Local
pl-123abc123abc123ab	*tgw-id*

Le nombre maximal d'entrées pour les listes de préfixes est égal au même nombre d'entrées dans la table de routage.

Routage vers un point de terminaison d'équilibreur de charge de passerelle

Un équilibreur de charge de passerelle vous permet de distribuer le trafic vers un parc d'appliances virtuelles, tels que des pare-feu. Vous pouvez configurer l'équilibreur de charge en tant que service en créant une configuration de service de point de terminaison d'un VPC. Créez ensuite un point de terminaison d'équilibreur de charge de passerelle dans votre VPC pour connecter votre VPC au service.

Pour acheminer votre trafic vers l'équilibreur de charge de passerelle (par exemple, pour une inspection de sécurité), spécifiez le point de terminaison de l'équilibreur de charge de passerelle comme cible dans vos tables de routage.

Pour obtenir un exemple d'appliances de sécurité derrière un Gateway Load Balancer, consultez the section called “Inspectez le trafic à l'aide d'appliances de sécurité”.

Pour spécifier le point de terminaison de l'équilibreur de charge de passerelle dans la table de routage, utilisez l'ID du point de terminaison d'un VPC. Par exemple, pour acheminer le trafic destiné à 10.0.1.0/24 vers un point de terminaison Gateway Load Balancer, ajoutez l'acheminement suivant.

Destination	Cible
10.0.1.0/24	*vpc-endpoint-id*

Pour plus d'informations, consultez Gateway Load Balancers.

Utiliser des tables de routage

Cette section décrit comment utiliser les tables de routage.

Table des matières

Déterminer la table de routage associée à un sous-réseau

Vous pouvez déterminer la table de routage à laquelle est associé un sous-réseau en examinant les informations de celui-ci dans la console Amazon VPC.

Pour déterminer la table de routage d'un sous-réseau

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.

2. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
3. Sélectionnez le sous-réseau.
4. Choisissez l'onglet Route Table (Table de routage) pour afficher des informations sur la table de routage et ses routes. Pour déterminer si l'association est à la table de routage principale et si cette association est explicite, voir Déterminer quels sous-réseaux et/ou les passerelles sont explicitement associés.

Déterminer quels sous-réseaux et/ou les passerelles sont explicitement associés

Vous pouvez déterminer le nombre et la nature des sous-réseaux ou passerelles qui sont explicitement associés à une table de routage.

La table de routage principale peut comporter des associations de sous-réseau explicites et implicites. Les tables de routage personnalisées comportent uniquement des associations explicites.

Les sous-réseaux qui ne sont pas explicitement associés à une table de routage comportent une association implicite à la table de routage principale. Vous pouvez associer explicitement un sous-réseau à la table de routage principale. Veuillez consulter afin de visualiser un exemple de la raison de cette actio Remplacer la table de routage principale.

Pour déterminer les sous-réseaux explicitement associés à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Route tables (Tables de routage).
3. Vérifiez la colonne Association de sous-réseau explicite pour déterminer les sous-réseaux explicitement associés et la colonne Principal pour déterminer s'il s'agit de la table de routage principale.
4. Sélectionnez la table de routage et choisissez l'onglet Subnet associations (Associations de sous-réseaux).
5. Les sous-réseaux sous Associations de sous-réseaux explicites sont explicitement associés à la table de routage. Les sous-réseaux sous Sous-réseaux sans association explicite appartiennent au même VPC que la table de routage, mais ne sont associés à aucune table de routage. Par conséquent, ils sont implicitement associés à la table de routage principale du VPC.

Pour déterminer les passerelles explicitement associées à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, choisissez Route tables (Tables de routage).
3. Sélectionnez la table de routage et choisissez l'onglet Edge associations (Associations périphériques).

Pour décrire une ou plusieurs tables de routage, et afficher leurs associations à l'aide de la ligne de commande

- describe-route-tables (AWS CLI)
- Get-EC2RouteTable (AWS Tools for Windows PowerShell)

Créer une table de routage personnalisée

Vous pouvez créer une table de routage personnalisée pour votre VPC à l'aide de la console Amazon VPC.

Pour créer une table de routage personnalisée à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Route tables (Tables de routage).
3. Choisissez Créer une table de routage.
4. (Facultatif) Pour Nom, entrez un nom pour votre table de routage.
5. Pour VPC, choisissez votre VPC.
6. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
7. Choisissez Créer une table de routage.

Pour créer une table de routage personnalisée à l'aide de la ligne de commande

- créer une table de routage (AWS CLI)
- New-EC2RouteTable (AWS Tools for Windows PowerShell)

Ajouter et supprimer des routes d'une table de routage

Vous pouvez ajouter, supprimer et modifier des routes dans vos tables de routage. Vous pouvez uniquement modifier les routes que vous avez ajoutées.

Pour plus d'informations sur l'utilisation des acheminements statiques pour une connexion Site-to-Site VPN, consultez Modification des acheminements statiques pour une connexion Site-to-Site VPN dans le Guide de l'utilisateur AWS Site-to-Site VPN .

Pour mettre à jour les routes pour une table de routage à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage et sélectionnez la table de routage.
3. Choisissez Actions, Modifier les routes.
4. Pour ajouter une route, choisissez Add route (Ajouter une route). Pour Destination, entrez le bloc CIDR de destination, une adresse IP unique ou l'ID d'une liste de préfixes.
5. Pour modifier une route, pour Destination, remplacez le bloc d'adresse CIDR de destination ou l'adresse IP unique. Pour Cible, choisissez une cible.
6. Pour supprimer une route, sélectionnez Remove (Supprimer).
7. Sélectionnez Enregistrer les modifications.

Pour mettre à jour les routes pour une table de routage à l'aide de la ligne de commande

- create-route (AWS CLI)
- replace-route (AWS CLI)
- delete-route (AWS CLI)
- New-EC2Route (AWS Tools for Windows PowerShell)
- Set-EC2Route (AWS Tools for Windows PowerShell)
- Remove-EC2Route (AWS Tools for Windows PowerShell)

> **Note**
>
> Si vous ajoutez une route à l'aide d'un outil de ligne de commande ou de l'API, le bloc d'adresse CIDR de destination est automatiquement ramené à sa forme canonique. Par exemple, si vous spécifiez `100.68.0.18/18` pour le bloc CIDR, nous créons une route avec un bloc d'adresse CIDR de destination de `100.68.0.0/18`.

Activer ou désactiver la propagation du routage

La propagation du routage permet à une passerelle privée virtuelle de propager automatiquement des routes vers vos tables de routage. Ainsi, vous n'avez pas besoin d'ajouter ou supprimer manuellement des routes VPN.

Pour exécuter ce processus, vous devez disposer d'une passerelle réseau privé virtuel.

Pour plus d'informations, veuillez consulter la section Options de routage Site-to-Site VPN du Guide de l'utilisateur Site-to-Site VPN.

Pour activer la propagation de route avec la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la table de routage.
3. Choisissez Actions, Edit route propagation (Modifier la propagation des itinéraires).
4. Sélectionnez la case à cocher Enable (Activer) en regard de la passerelle réseau privé virtuel, puis choisissez Save (Enregistrer).

Pour activer la propagation du routage à l'aide de la ligne de commande

- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Pour désactiver la propagation de route avec la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la table de routage.
3. Choisissez Actions, Edit route propagation (Modifier la propagation des acheminements).
4. Désélectionnez la case à cocher Enable (Activer) en regard de la passerelle réseau privé virtuel, puis choisissez Save (Enregistrer).

Pour désactiver la propagation du routage à l'aide de la ligne de commande

- disable-vgw-route-propagation (AWS CLI)

- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Associer un sous-réseau à une table de routage

Pour appliquer des routes de table de routage à un sous-réseau spécifique, vous devez associer la table de routage au sous-réseau. Une table de routage peut être associée à plusieurs sous-réseaux. Toutefois, un sous-réseau peut être associé à une seule table de routage à la fois. Tout sous-réseau non associé explicitement à une table est associé implicitement à la table de routage principale par défaut.

Pour associer une table de routage à un sous-réseau à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la table de routage.
3. Sous l'onglet Subnet associations (Associations de sous-réseau), choisissez Edit subnet associations (Modifier les associations de sous-réseau).
4. Sélectionnez la case à cocher pour le sous-réseau à associer à la table de routage.
5. Choisissez Save associations (Enregistrer les associations).

Pour associer un sous-réseau à une table de routage à l'aide de la ligne de commande

- associate-route-table (AWS CLI)
- Register-EC2RouteTable (AWS Tools for Windows PowerShell)

Changer le tableau de routage associé à un sous-réseau

Vous pouvez changer l'association de table de routage d'un sous-réseau.

Lorsque vous modifiez la table de routage, vos connexions existantes dans le sous-réseau sont supprimées, sauf si la nouvelle table de routage contient une route pour le même trafic vers la même cible.

Pour modifier une association de table de routage et de sous-réseau à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Subnets, puis sélectionnez le sous-réseau.

3. Sur l'onglet Table de routage, choisissez Edit route table association (Modifier l'association de table de routage).
4. Pour ID de table de routage, sélectionnez la nouvelle table de routage.
5. Choisissez Enregistrer.

Pour modifier la table de routage associée à un sous-réseau à l'aide de la ligne de commande

- replace-route-table-association (AWS CLI)
- Set-EC2RouteTableAssociation (AWS Tools for Windows PowerShell)

Dissocier un sous-réseau d'une table de routage

Vous pouvez dissocier un sous-réseau d'une table de routage. Tant que vous n'associez pas le sous-réseau à une autre table de routage, il est associé implicitement à la table de routage principale.

Pour dissocier un sous-réseau d'une table de routage à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la table de routage.
3. Sur l'onglet Associations de sous-réseau, choisissez Modifier les associations de sous-réseau.
4. Désélectionnez la case à cocher pour le sous-réseau.
5. Choisissez Save associations (Enregistrer les associations).

Pour dissocier un sous-réseau d'une table de routage à l'aide de la ligne de commande

- disassociate-route-table (AWS CLI)
- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

Remplacer la table de routage principale

Vous pouvez modifier la table de routage qui est la table de routage principale dans votre VPC.

Pour remplacer la table de routage principale à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.

2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la nouvelle table de routage principale.
3. Choisissez Actions, Définir la table de routage principale.
4. Lorsque vous êtes invité à confirmer, saisissez **`set`**, puis choisissez OK.

Pour remplacer la table de routage principale à l'aide de la ligne de commande

- replace-route-table-association (AWS CLI)
- Set-EC2RouteTableAssociation (AWS Tools for Windows PowerShell)

La procédure ci-après explique comment retirer une association explicite entre un sous-réseau et la table de routage principale. Le résultat est une association implicite entre le sous-réseau et la table de routage principale. Le processus est identique à la dissociation d'un sous-réseau d'une table de routage.

Pour retirer une association explicite à la table de routage principale

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la table de routage.
3. Sur l'onglet Associations de sous-réseau, choisissez Modifier les associations de sous-réseau.
4. Désélectionnez la case à cocher pour le sous-réseau.
5. Choisissez Save associations (Enregistrer les associations).

Associer une passerelle à une table de routage

Vous pouvez associer une passerelle Internet ou une passerelle réseau privé virtuel à une table de routage. Pour plus d'informations, consultez Tables de routage de passerelle.

Pour associer une passerelle à une table de routage à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la table de routage.
3. Sur l'onglet Associations périphériques, choisissez Modifier les associations périphériques.

4. Cochez la case correspondante à la passerelle.
5. Sélectionnez Enregistrer les modifications.

Pour associer une passerelle à une table de routage à l'aide du AWS CLI

Utilisez la commande associate-route-table. L'exemple suivant associe la passerelle Internet `igw-11aa22bb33cc44dd1` à la table de routage `rtb-01234567890123456`.

```
aws ec2 associate-route-table --route-table-id rtb-01234567890123456 --gateway-id
 igw-11aa22bb33cc44dd1
```

Dissocier une passerelle d'une table de routage

Vous pouvez dissocier une passerelle Internet ou une passerelle réseau privé virtuel d'une table de routage.

Pour associer une passerelle à une table de routage à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la table de routage.
3. Sur l'onglet Associations périphériques, choisissez Modifier les associations périphériques.
4. Désactivez la case correspondante à la passerelle.
5. Sélectionnez Enregistrer les modifications.

Pour dissocier une passerelle d'une table de routage à l'aide de la ligne de commande

- disassociate-route-table (AWS CLI)
- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

Remplacer ou restaurer la cible d'un acheminement local

Vous pouvez modifier la cible de l'acheminement local par défaut. Si vous remplacez la cible d'un acheminement local, vous pouvez la restaurer ultérieurement et rétablir la cible `local` par défaut. Si votre VPC a plusieurs blocs d'adresse CIDR, vos tables de routage disposent de plusieurs routes locales : une par bloc d'adresse CIDR. Vous pouvez remplacer ou restaurer la cible de chacun des acheminements locaux si nécessaire.

Pour mettre à jour la route locale à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la table de routage.
3. Sur l'onglet Routes, choisissez Edit routes (Modifier les routes).
4. Pour la route locale, désélectionnez Cible, puis choisissez une nouvelle cible.
5. Sélectionnez Enregistrer les modifications.

Pour restaurer la cible d'une route locale à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la table de routage.
3. Choisissez Actions, Modifier les routes.
4. Pour l'acheminement, décochez Cible, puis choisissez locale.
5. Sélectionnez Enregistrer les modifications.

Pour remplacer la cible d'un itinéraire local à l'aide du AWS CLI

Utilisez la commande replace-route. L'exemple suivant remplace la cible de la route locale par `eni-11223344556677889`.

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block
 10.0.0.0/16 --network-interface-id eni-11223344556677889
```

Pour restaurer la cible d'un itinéraire local à l'aide du AWS CLI

L'exemple suivant restaure la cible locale de la table de routage `rtb-01234567890123456`.

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block
 10.0.0.0/16 --local-target
```

Supprimer une table de routage

Vous ne pouvez supprimer une table de routage que si elle n'est associée à aucun sous-réseau. Vous ne pouvez pas supprimer la table de routage principale.

Pour supprimer une table de routage à l'aide de la console

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la table de routage.
3. Choisissez Actions, Supprimer une table de routage.
4. Lorsque vous êtes invité à confirmer, saisissez **`delete`**, puis choisissez Delete (Supprimer).

Pour supprimer une table de routage à l'aide de la ligne de commande

- delete-route-table (AWS CLI)
- Remove-EC2RouteTable (AWS Tools for Windows PowerShell)

Assistant de routage middlebox

Si vous souhaitez configurer un contrôle précis du chemin de routage du trafic entrant ou sortant de votre VPC, par exemple en redirigeant le trafic vers une appliance de sécurité, vous pouvez utiliser l'assistant de routage middlebox dans la console VPC. L'assistant de routage middlebox vous aide en créant automatiquement les tables de routage et les acheminements (sauts) nécessaires pour rediriger le trafic selon les besoins.

L'assistant de routage middlebox peut vous aider à configurer le routage pour les scénarios suivants :

- Acheminement du trafic vers une appliance middlebox, par exemple une instance Amazon EC2 configurée en tant qu'appliance de sécurité.
- Acheminement du trafic vers un équilibreur de charge de passerelle. Pour plus d'informations, consultez le Guide de l'utilisateur des équilibreurs de charge de passerelle.

Pour plus d'informations, consultez the section called "Scénarios middlebox".

Table des matières

Prérequis de l'assistant de routage middlebox

Consultez the section called “Considérations relatives à l'assistant de routage middlebox”. Vérifiez ensuite que vous disposez des informations suivantes avant d'utiliser l'assistant de routage middlebox.

- Le VPC.
- La ressource d'où le trafic provient ou entre dans le VPC, par exemple, une passerelle Internet, une passerelle privée virtuelle ou une interface réseau.
- L'interface réseau middlebox ou le point de terminaison Gateway Load Balancer.
- Le sous-réseau de destination du trafic.

Gérer les acheminements middlebox

L'assistant de routage middlebox est disponible dans la Amazon Virtual Private Cloud Console.

Sommaire

Création d'acheminements à l'aide de l'assistant de routage middlebox

Pour créer des acheminements à l'aide de l'assistant de routage middlebox

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Vos VPC.
3. Sélectionnez votre VPC, puis choisissez Actions et Manage middlebox routes (Gérer les acheminements middlebox).
4. Choisissez Create routes (Créer des acheminements).
5. Dans la page Specify routes (Spécifier des acheminements), procédez comme suit :

    - Pour Source, choisissez la source de votre trafic. Si vous choisissez une passerelle réseau privé virtuel, pour Destination IPv4 CIDR (CIDR IPv4 de destination), entrez le CIDR pour le trafic sur site entrant dans le VPC à partir de la passerelle privée virtuelle.

- Pour Middlebox, choisissez l'ID d'interface réseau associé à votre appliance middlebox, ou si vous utilisez un point de terminaison Gateway Load Balancer, choisissez l'ID de point de terminaison du VPC.
- Pour Destination subnet (Sous-réseau de destination), choisissez le sous-réseau de destination.

6. (Facultatif) Pour ajouter un autre sous-réseau de destination, sélectionnez Add additional subnet (Ajouter un sous-réseau supplémentaire), puis procédez comme suit :

   - Pour Middlebox, choisissez l'ID d'interface réseau associé à votre appliance middlebox, ou si vous utilisez un point de terminaison Gateway Load Balancer, choisissez l'ID de point de terminaison du VPC.

     Vous devez utiliser la même appliance middlebox pour plusieurs sous-réseaux.
   - Pour Destination subnet (Sous-réseau de destination), choisissez le sous-réseau de destination.

7. (Facultatif) Pour ajouter une autre source, choisissez Add source (Ajouter une source), puis répétez les étapes précédentes.
8. Choisissez Suivant.
9. Dans la page Review and create (Vérifier et créer), vérifiez les acheminements, puis choisissez Create routes (Créer des acheminements).

Modification d'acheminements middlebox

Vous pouvez modifier la configuration de vos acheminements en changeant de passerelle, de middlebox ou de sous-réseau de destination.

Lorsque vous apportez des modifications, l'assistant de routage middlebox effectue automatiquement les opérations suivantes :

- Création de tables de routage pour la passerelle, le middlebox et le sous-réseau de destination.
- Ajout des acheminements nécessaires aux nouvelles tables de routage.
- Dissociation des tables de routage actuelles que l'assistant de routage middlebox milieu a associées aux ressources.
- Association des nouvelles tables de routage créées par l'assistant de routage middlebox aux ressources.

Pour modifier des acheminements middlebox à l'aide de l'assistant de routage middlebox

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Vos VPC.
3. Sélectionnez votre VPC, puis choisissez Actions et Manage middlebox routes (Gérer les acheminements middlebox).
4. Choisissez Edit routes (Modifier des routes).
5. Pour changer de passerelle, pour Source, choisissez la passerelle par laquelle le trafic entre dans votre VPC. Si vous choisissez une passerelle réseau privé virtuel, pour Destination IPv4 CIDR (CIDR IPv4 de destination), entrez le CIDR du sous-réseau de destination.
6. Pour ajouter un autre sous-réseau de destination, choisissez Add additional subnet (Ajouter un sous-réseau supplémentaire), puis procédez comme suit :

   - Pour Middlebox, choisissez l'ID d'interface réseau associé à votre appliance middlebox, ou si vous utilisez un point de terminaison Gateway Load Balancer, choisissez l'ID de point de terminaison du VPC.

     Vous devez utiliser la même appliance middlebox pour plusieurs sous-réseaux.
   - Pour Destination subnet (Sous-réseau de destination), choisissez le sous-réseau de destination.
7. Choisissez Suivant.
8. La liste des tables de routage et leurs acheminements qui seront créés par l'assistant de routage middlebox s'affichent dans la page Review and update (Vérifier et mettre à jour). Vérifiez les acheminements puis, dans la boîte de dialogue de confirmation, choisissez Update routes (Mettre à jour les acheminements).

Affichage des tables de routage de l'assistant de routage middlebox

Pour afficher les tables de routage de l'assistant de routage middlebox

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/
2. Dans le panneau de navigation, sélectionnez Vos VPC.
3. Sélectionnez votre VPC, puis choisissez Actions et Manage middlebox routes (Gérer les acheminements middlebox).

4. Sous Middlebox route tables (Tables de routage middlebox), le nombre indique combien d'acheminements ont été créés par l'assistant de routage middlebox. Sélectionnez le numéro pour afficher les acheminements.

Les acheminements de l'assistant de routage middlebox s'affichent dans une page de table de routage distincte.

Suppression de la configuration de l'assistant de routage middlebox

Si vous estimez que vous n'avez plus besoin de la configuration de l'assistant de routage middlebox, vous devez supprimer les tables de routage manuellement.

Pour supprimer la configuration de l'assistant de routage middlebox

1. Affichez les tables de routage de l'assistant de routage middlebox. Pour de plus amples informations, veuillez consulter the section called “Affichage des tables de routage de l'assistant de routage middlebox”.

   Après avoir effectué l'opération, les tables de routage créées par l'assistant de routage middlebox s'affichent dans une page de table de routage distincte.
2. Supprimez chaque table de routage affichée. Pour de plus amples informations, veuillez consulter the section called “Supprimer une table de routage”.

Considérations relatives à l'assistant de routage middlebox

Tenez compte des points suivants lorsque vous utilisez l'assistant de routage middlebox :

- Si vous souhaitez inspecter le trafic, vous pouvez utiliser une passerelle Internet ou une passerelle réseau privé virtuel pour la source.
- Si vous utilisez le même middlebox dans une configuration à plusieurs middlebox au sein du même VPC, assurez-vous que le middlebox se trouve dans la même position de saut pour les deux sous-réseaux.
- L'appliance doit être configurée dans un sous-réseau distinct du sous-réseau source ou de destination.
- Vous devez désactiver la vérification origine/destination sur l'appliance. Pour plus d'informations, consultez la section Modification de la vérification de la source ou de la destination dans le guide de l'utilisateur Amazon EC2.

- Les tables de routage et les acheminements créés par l'assistant de routage middlebox sont comptabilisés au titre de vos quotas. Pour de plus amples informations, veuillez consulter the section called "Tables de routage".
- Si vous supprimez une ressource, par exemple une interface réseau, ses associations à des tables de routage sont supprimées. Si la ressource est une cible, la destination de l'acheminement est définie sur Blackhole. Les tables de routage ne sont pas supprimées.
- Le sous-réseau middlebox et le sous-réseau de destination doivent être associés à une table de routage qui n'est pas une table de routage par défaut.

> **Note**
>
> Nous vous recommandons d'utiliser l'assistant de routage middlebox pour modifier ou supprimer les tables de routage que vous avez créées à l'aide de l'assistant de routage middlebox.

Scénarios middlebox

Les exemples suivants décrivent des scénarios pour l'assistant de routage middlebox.

Table des matières

Inspection du trafic destiné à un sous-réseau

Imaginez un scénario où le trafic entrant du VPC passe par une passerelle Internet et où vous souhaitez inspecter l'ensemble du trafic destiné à un sous-réseau, que nous appellerons « sous-réseau B », avec une appliance de pare-feu installée sur une instance EC2. L'appliance de pare-feu doit être installée et configurée sur une instance EC2 dans un sous-réseau distinct du sous-réseau B de votre VPC, par exemple le sous-réseau C. Vous pouvez ensuite utiliser l'assistant de routage middlebox pour configurer des acheminements pour le trafic entre le sous-réseau B et la passerelle Internet.

L'assistant de routage middlebox effectue automatiquement les opérations suivantes :

- Crée les tables de routage suivantes :
  - Une table de routage pour la passerelle Internet
  - Une table de routage pour le sous-réseau de destination
  - Une table de routage pour le sous-réseau middlebox
- Ajout des acheminements nécessaires aux nouvelles tables de routage comme décrit dans les sections suivantes.
- Dissociation des tables de routage actuellement associées à la passerelle Internet, au sous-réseau B et au sous-réseau C.
- Association de la table de routage A à la passerelle Internet (la Source dans l'assistant de routage middlebox), de la table de routage C au sous-réseau C (le Middlebox dans l'assistant de routage middlebox) et de la table de routage B au sous-réseau B (la Destination dans l'assistant de routage middlebox).
- Création d'une étiquette indiquant qu'elle a été créée par l'assistant de routage middlebox et d'une étiquette indiquant la date de création.

L'assistant de routage middlebox ne modifie pas vos tables de routage existantes. Il crée des tables de routage et les associe à vos ressources de passerelle et de sous-réseau. Si vos ressources sont déjà explicitement associées à des tables de routage existantes, ces dernières sont d'abord dissociées et les nouvelles tables de routage sont ensuite associées à vos ressources. Vos tables de routage existantes ne sont pas supprimées.

Si vous n'utilisez pas l'assistant de routage middlebox, vous devez configurer manuellement les tables de routage et les affecter aux sous-réseaux et à la passerelle Internet.

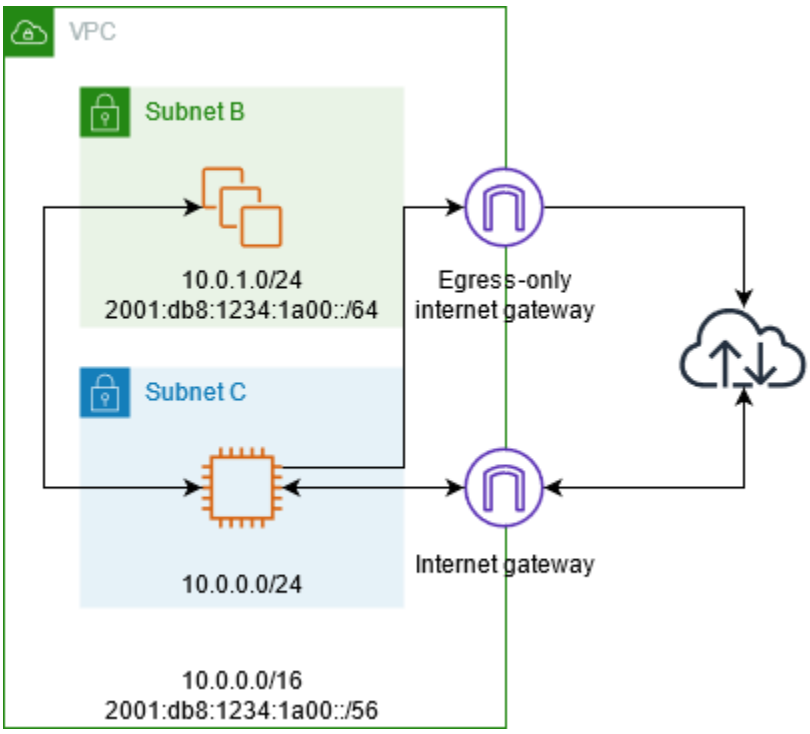


Table de routage de la passerelle Internet

Ajouter les acheminements suivants à la table de routage de la passerelle Internet.

Destination	Cible	Objectif
10.0.0.0/16	Locale	Acheminement local pour IPv4
10.0.1.0/24	*appliance-eni*	Achemine le trafic IPv4 destiné au sous-réseau B vers le middlebox
2001:db8:1234:1a00::/56	Local	Acheminement local pour IPv6
2001:db8:1234:1a00::/64	*appliance-eni*	Achemine le trafic IPv6 destiné au sous-réseau B vers le middlebox

Il existe une association de périphérie entre la passerelle Internet et le VPC.

Lorsque vous utilisez l'assistant de routage middlebox, il associe les balises suivantes à la table de routage :

- La clé est « Origin (Origine) » et la valeur est « Middlebox wizard (Assistant middlebox) »
- La clé est « date_created » et la valeur est l'heure de création (par exemple « 2021-02-18T 22:25:49 .137Z »)

Table de routage de sous-réseau de destination

Ajoutez les acheminements suivants à la table de routage du sous-réseau de destination (sous-réseau B dans l'exemple de diagramme).

Destination	Cible	Objectif
10.0.0.0/16	Locale	Acheminement local pour IPv4
0.0.0.0/0	*appliance-eni*	Achemine le trafic IPv4 destiné à Internet vers le middlebox
2001:db8:1234:1a00::/56	Local	Acheminement local pour IPv6
::/0	*appliance-eni*	Achemine le trafic IPv6 destiné à Internet vers le middlebox

Il existe une association de sous-réseau avec le sous-réseau middlebox.

Lorsque vous utilisez l'assistant de routage middlebox, il associe les balises suivantes à la table de routage :

- La clé est « Origin (Origine) » et la valeur est « Middlebox wizard (Assistant middlebox) »
- La clé est « date_created » et la valeur est l'heure de création (par exemple « 2021-02-18T 22:25:49 .137Z »)

Table de routage de sous-réseau middlebox

Ajoutez les acheminements suivants à la table de routage du sous-réseau middlebox (sous-réseau C dans l'exemple de diagramme).

Destination	Cible	Objectif
10.0.0.0/16	Locale	Acheminement local pour IPv4
0.0.0.0/0	*igw-id*	Acheminement du trafic IPv4 vers la passerelle Internet
2001:db8:1234:1a00::/56	Local	Acheminement local pour IPv6
::/0	*eigw-id*	Acheminer le trafic IPv6 vers la passerelle Internet de sortie seulement.

Il existe une association de sous-réseau avec le sous-réseau de destination.

Lorsque vous utilisez l'assistant de routage middlebox, il associe les balises suivantes à la table de routage :

- La clé est « Origin (Origine) » et la valeur est « Middlebox wizard (Assistant middlebox) »
- La clé est « date_created » et la valeur est l'heure de création (par exemple « 2021-02-18T 22:25:49 .137Z »)

Inspectez le trafic à l'aide d'appliances dans un VPC de sécurité

Considérez le scénario dans lequel vous devez inspecter le trafic entrant dans un VPC à partir de la passerelle Internet vers un sous-réseau en utilisant une flotte d'appliances de sécurité configurée derrière un Gateway Load Balancer. Le propriétaire du VPC des utilisateurs du service crée un point de terminaison Gateway Load Balancer dans un sous-réseau de son VPC (représenté par une interface réseau de point de terminaison). Tout le trafic entrant dans le VPC via la passerelle Internet est d'abord acheminé vers le point de terminaison de l'équilibreur de charge de passerelle pour inspection avant d'être acheminé vers le sous-réseau de l'application. De même, l'ensemble du trafic sortant du sous-réseau de l'application est d'abord acheminé vers le point de terminaison Gateway Load Balancer pour inspection avant d'être acheminé vers Internet.

L'assistant de routage middlebox effectue automatiquement les opérations suivantes :

- Création des tables de routage.
- Ajout des acheminements nécessaires aux nouvelles tables de routage.

- Dissociation des tables de routage actuellement associées aux sous-réseaux.
- Association des tables de routage créées par l'assistant de routage middlebox aux sous-réseaux.
- Création d'une étiquette indiquant qu'elle a été créée par l'assistant de routage middlebox et d'une étiquette indiquant la date de création.

L'assistant de routage middlebox ne modifie pas vos tables de routage existantes. Il crée des tables de routage et les associe à vos ressources de passerelle et de sous-réseau. Si vos ressources sont déjà explicitement associées à des tables de routage existantes, ces dernières sont d'abord dissociées et les nouvelles tables de routage sont ensuite associées à vos ressources. Vos tables de routage existantes ne sont pas supprimées.

Si vous n'utilisez pas l'assistant de routage middlebox, vous devez configurer manuellement les tables de routage et les affecter aux sous-réseaux et à la passerelle Internet.

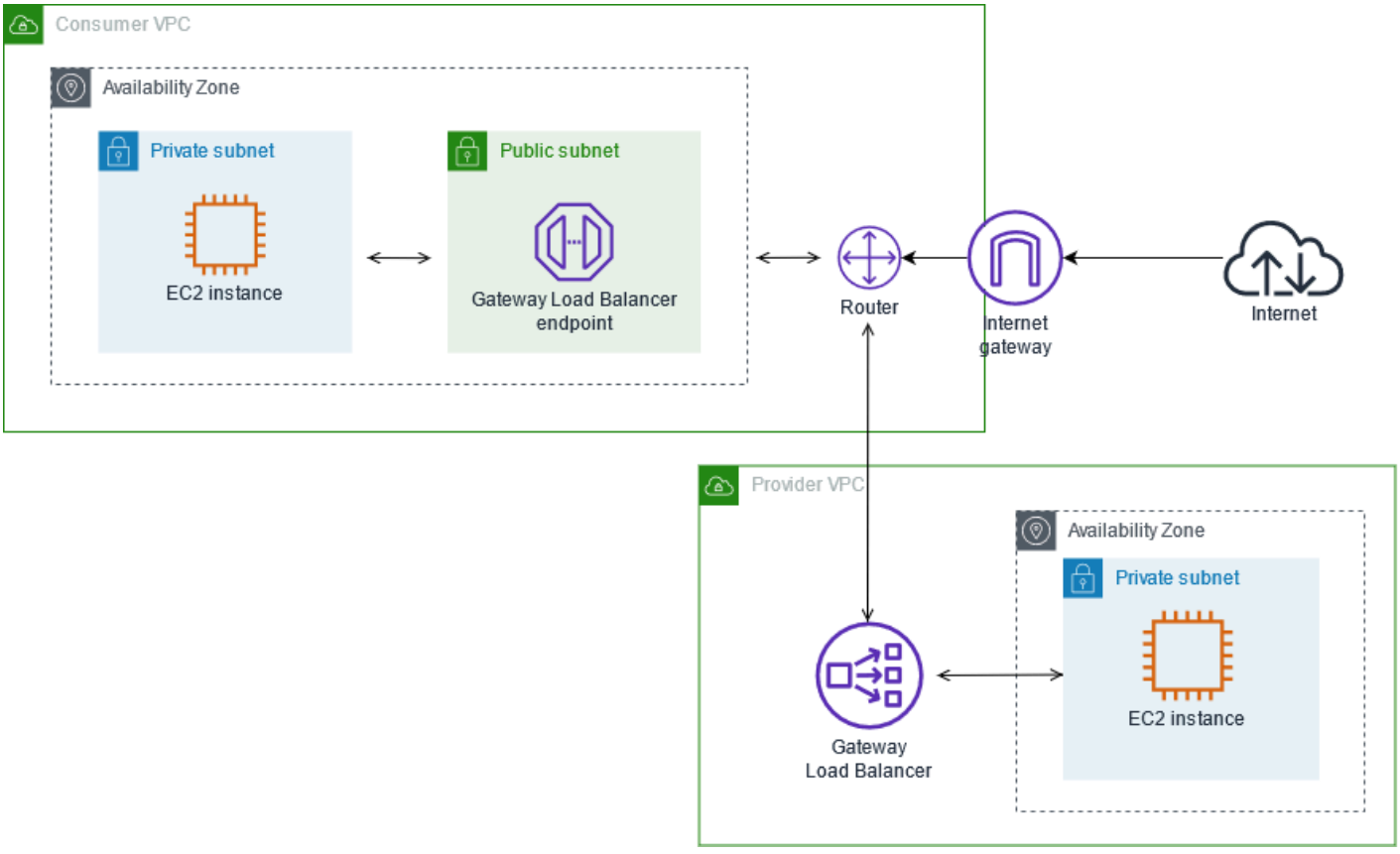


Table de routage de la passerelle Internet

La table de routage de la passerelle Internet comporte les acheminements suivants.

Destination	Cible	Objectif
CIDR VPC consummateur	Local	Acheminement local
CIDR du sous-réseau d'application	*ID du point de terminaison*	Achemine le trafic destiné au sous-rése au d'application vers le point de terminais on Gateway Load Balancer.

Il existe une association de périphérie avec la passerelle.

Lorsque vous utilisez l'assistant de routage middlebox, il associe les balises suivantes à la table de routage :

- La clé est « Origin (Origine) » et la valeur est « Middlebox wizard (Assistant middlebox) »
- La clé est « date_created » et la valeur est l'heure de création (par exemple « 2021-02-18T 22:25:49 .137Z »)

Table de routage de sous-réseau d'application

La table de routage du sous-réseau d'application comporte les acheminements suivants.

Destination	Cible	Objectif
CIDR VPC consummateur	Local	Acheminement local
0.0.0.0/0	*ID du point de terminaison*	Acheminez le trafic depuis les serveurs d'application vers le point de terminais on Gateway Load Balancer avant d'être acheminé vers Internet.

Lorsque vous utilisez l'assistant de routage middlebox, il associe les balises suivantes à la table de routage :

- La clé est « Origin (Origine) » et la valeur est « Middlebox wizard (Assistant middlebox) »
- La clé est « date_created » et la valeur est l'heure de création (par exemple « 2021-02-18T 22:25:49 .137Z »)

Table de routage de sous-réseau fournisseur

La table de routage du sous-réseau fournisseur comporte les acheminements suivants.

Destination	Cible	Objectif
CIDR VPC fournisseur	Local	Acheminement local. Garantit que le trafic provenant d'Internet est acheminé vers les serveurs d'application.
0.0.0.0/0	*igw-id*	Achemine l'ensemble du trafic vers la passerelle Internet.

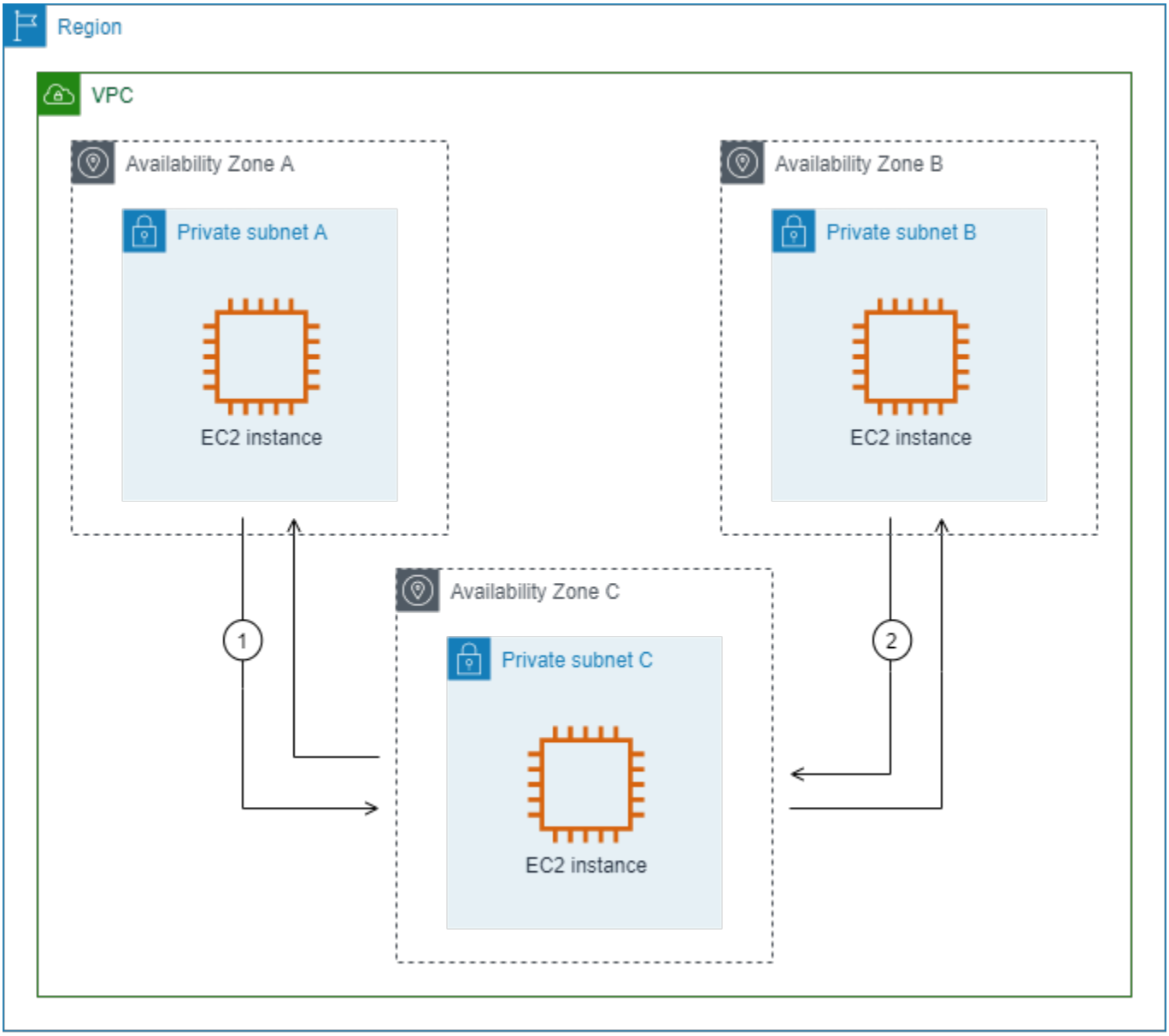
Lorsque vous utilisez l'assistant de routage middlebox, il associe les balises suivantes à la table de routage :

- La clé est « Origin (Origine) » et la valeur est « Middlebox wizard (Assistant middlebox) »
- La clé est « date_created » et la valeur est l'heure de création (par exemple « 2021-02-18T 22:25:49 .137Z »)

Inspection du trafic entre les sous-réseaux

Imaginez un scénario où il existe plusieurs sous-réseaux dans un VPC et où vous souhaitez inspecter le trafic entre eux à l'aide d'une appliance de pare-feu. Configurez et installez l'appliance de pare-feu sur une instance EC2 dans un sous-réseau distinct dans votre VPC.

Le schéma suivant montre une appliance de pare-feu installée sur une instance EC2 du sous-réseau C. L'appliance inspecte tout le trafic qui passe du sous-réseau A au sous-réseau B (voir 1) et du sous-réseau B au sous-réseau A (voir 2).



Vous utilisez la table de routage principale pour le VPC et le sous-réseau middlebox. Les sous-réseaux A et B ont chacun une table de routage personnalisée.

L'assistant de routage middlebox effectue automatiquement les opérations suivantes :

- Création des tables de routage.
- Ajout des acheminements nécessaires aux nouvelles tables de routage.
- Dissociation des tables de routage actuellement associées aux sous-réseaux.
- Association des tables de routage créées par l'assistant de routage middlebox aux sous-réseaux.

- Création d'une étiquette indiquant qu'elle a été créée par l'assistant de routage middlebox et d'une étiquette indiquant la date de création.

L'assistant de routage middlebox ne modifie pas vos tables de routage existantes. Il crée des tables de routage et les associe à vos ressources de passerelle et de sous-réseau. Si vos ressources sont déjà explicitement associées à des tables de routage existantes, ces dernières sont d'abord dissociées et les nouvelles tables de routage sont ensuite associées à vos ressources. Vos tables de routage existantes ne sont pas supprimées.

Si vous n'utilisez pas l'assistant de routage middlebox, vous devez configurer manuellement les tables de routage et les affecter aux sous-réseaux et à la passerelle Internet.

Table de routage personnalisée pour le sous-réseau A

La table de routage du sous-réseau A comporte les acheminements suivants.

Destination	Cible	Objectif
Bloc d'adresse du VPC	Local	Acheminement local
CIDR du sous-réseau B	*appliance-eni*	Achemine le trafic destiné au sous-réseau B vers le middlebox

Lorsque vous utilisez l'assistant de routage middlebox, il associe les balises suivantes à la table de routage :

- La clé est « Origin (Origine) » et la valeur est « Middlebox wizard (Assistant middlebox) »
- La clé est « date_created » et la valeur est l'heure de création (par exemple « 2021-02-18T 22:25:49 .137Z »)

Table de routage personnalisée pour le sous-réseau B

La table de routage pour la sous-réseau B comporte les acheminements suivants.

Destination	Cible	Objectif
Bloc d'adresse du VPC	Local	Acheminement local
CIDR du sous-réseau A	*appliance-eni*	Achemine le trafic destiné au sous-réseau A vers le middlebox

Lorsque vous utilisez l'assistant de routage middlebox, il associe les balises suivantes à la table de routage :

- La clé est « Origin (Origine) » et la valeur est « Middlebox wizard (Assistant middlebox) »
- La clé est « date_created » et la valeur est l'heure de création (par exemple « 2021-02-18T 22:25:49 .137Z »)

Table de routage principale

Le sous-réseau C utilise la table de routage principale. La table de routage principale comporte la route suivante.

Destination	Cible	Objectif
Bloc d'adresse du VPC	Local	Acheminement local

Lorsque vous utilisez l'assistant de routage middlebox, il associe les balises suivantes à la table de routage :

- La clé est « Origin (Origine) » et la valeur est « Middlebox wizard (Assistant middlebox) »
- La clé est « date_created » et la valeur est l'heure de création (par exemple « 2021-02-18T 22:25:49 .137Z »)

Delete un subnet.

Si vous n'avez plus besoin d'un sous-réseau, vous pouvez le supprimer. Vous ne pouvez pas supprimer un sous-réseau s'il contient des interfaces réseau. Par exemple, vous devez mettre fin à toutes les instances dans un sous-réseau avant de pouvoir le supprimer.

Pour supprimer un sous-réseau à l'aide de la console

1. Ouvrez la console Amazon EC2 sur https://console.aws.amazon.com/ec2/.
2. Mettez fin à toutes les instances dans le sous-réseau. Pour de plus amples informations, veuillez consulter Résilier une instance dans le Guide de l'utilisateur Amazon EC2.
3. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
4. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
5. Sélectionnez le sous-réseau, puis choisissez Actions, Delete subnet (Supprimer le sous-réseau).
6. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

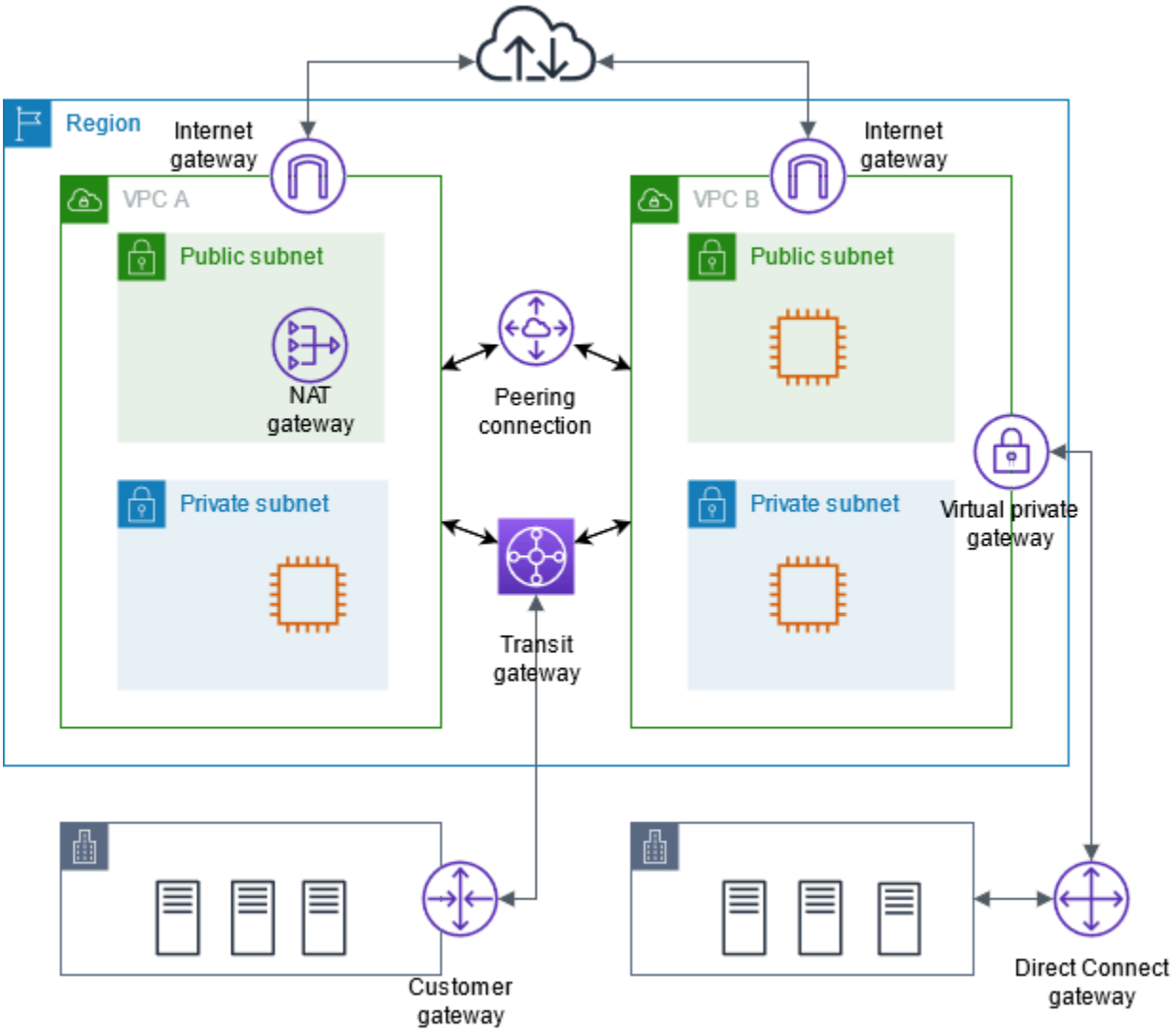
Pour supprimer un sous-réseau à l'aide de la AWS CLI

Utilisez la commande delete-subnet.

Connexion de votre VPC à des réseaux distants

Vous pouvez connecter votre cloud privé virtuel (VPC) à d'autres réseaux. Par exemple, d'autres VPC, Internet ou votre réseau local.

Le diagramme suivant illustre certaines de ces options de connectivité. Le VPC A est connecté à l'Internet via une passerelle Internet. L'instance EC2 du sous-réseau privé du VPC A peut se connecter à l'Internet à l'aide de la passerelle NAT du sous-réseau public du VPC A. Le VPC B est connecté à l'Internet via une passerelle Internet. L'instance EC2 du sous-réseau public du VPC B peut se connecter à l'Internet via la passerelle Internet. Le VPC A et le VPC B sont connectés entre eux à travers une connexion d'appairage de VPC et une passerelle de transit. La passerelle de transit dispose d'une connexion VPN à un centre de données. Le VPC B dispose d'une AWS Direct Connect connexion à un centre de données.



Pour en savoir plus, consultez Cloud privé virtuel d'Amazon Connectivity Options (Options de connectivité de cloud privé virtuel d'Amazon).

Table des matières

Connecter à l'Internet à l'aide d'une passerelle Internet

Une passerelle Internet est un composant de VPC dimensionné horizontalement, redondant et hautement disponible qui permet la communication entre votre VPC et Internet. Elle prend en charge le trafic IPv4 et IPv6. Elle ne génère pas de risques de disponibilité ou de contraintes de bande passante sur votre trafic réseau.

Une passerelle Internet active des ressources de vos sous-réseaux publics (telles que les instances EC2) pour se connecter à l'Internet si elles comportent une adresse IPv4 publique ou une adresse IPv6. De même, les ressources sur Internet peuvent établir une connexion à des ressources de votre sous-réseau à l'aide de l'adresse IPv4 publique ou de l'adresse IPv6. Par exemple, une passerelle Internet vous permet de vous connecter à une instance EC2 en AWS utilisant votre ordinateur local.

Une passerelle Internet fournit une cible dans vos tables de routage VPC pour le trafic routable par Internet. Pour la communication via IPv4, la passerelle Internet effectue la traduction d'adresses réseau (NAT). Pour les communications utilisant IPv6, le NAT n'est pas nécessaire car les adresses IPv6 sont publiques. Pour plus d'informations, consultez Adresses IP et NAT.

Configuration pour l'accès à Internet

Pour permettre à vos instances de recevoir ou d'envoyer du trafic depuis Internet, procédez comme suit :

- Créez une passerelle Internet et attachez-la à votre VPC.

- Ajoutez une route à la table de routage pour le sous-réseau qui dirige le trafic lié à Internet vers la passerelle Internet.
- Assurez-vous que les instances de votre sous-réseau ont une adresse IPv4 publique ou une adresse IPv6. Pour plus d'informations, consultez la section Adressage IP des instances dans le guide de l'utilisateur Amazon EC2.
- Assurez-vous que vos groupes de sécurité et listes de contrôle d'accès réseau autorisent l'acheminement du trafic souhaité vers et en provenance de vos instances.

Pour fournir un accès Internet à vos instances sans leur attribuer d'adresses IP publiques, utilisez un périphérique NAT à la place. Un périphérique NAT permet aux instances d'un sous-réseau privé de se connecter à Internet, mais empêche les hôtes sur Internet d'initier des connexions avec les instances. Pour plus d'informations, consultez Périphériques NAT.

Sous-réseaux publics et privés

Si un sous-réseau est associé à une table de routage comportant une route vers une passerelle Internet, il est reconnu comme un sous-réseau public. Si un sous-réseau est associé à une table de routage ne comportant pas de route vers une passerelle Internet, il est reconnu comme un sous-réseau privé.

Dans votre table de routage de sous-réseau public, vous pouvez spécifier une route pour la passerelle Internet vers toutes les destinations qui ne sont pas explicitement connues de la table de routage (`0.0.0.0/0` pour IPv4 ou `::/0` pour IPv6). Vous pouvez également définir l'itinéraire vers une gamme plus restreinte d'adresses IP ; par exemple, les adresses IPv4 publiques des points de terminaison publics de votre entreprise situés en dehors de votre VPC ou les adresses IP élastiques d' AWS autres instances Amazon EC2 situées en dehors de votre VPC.

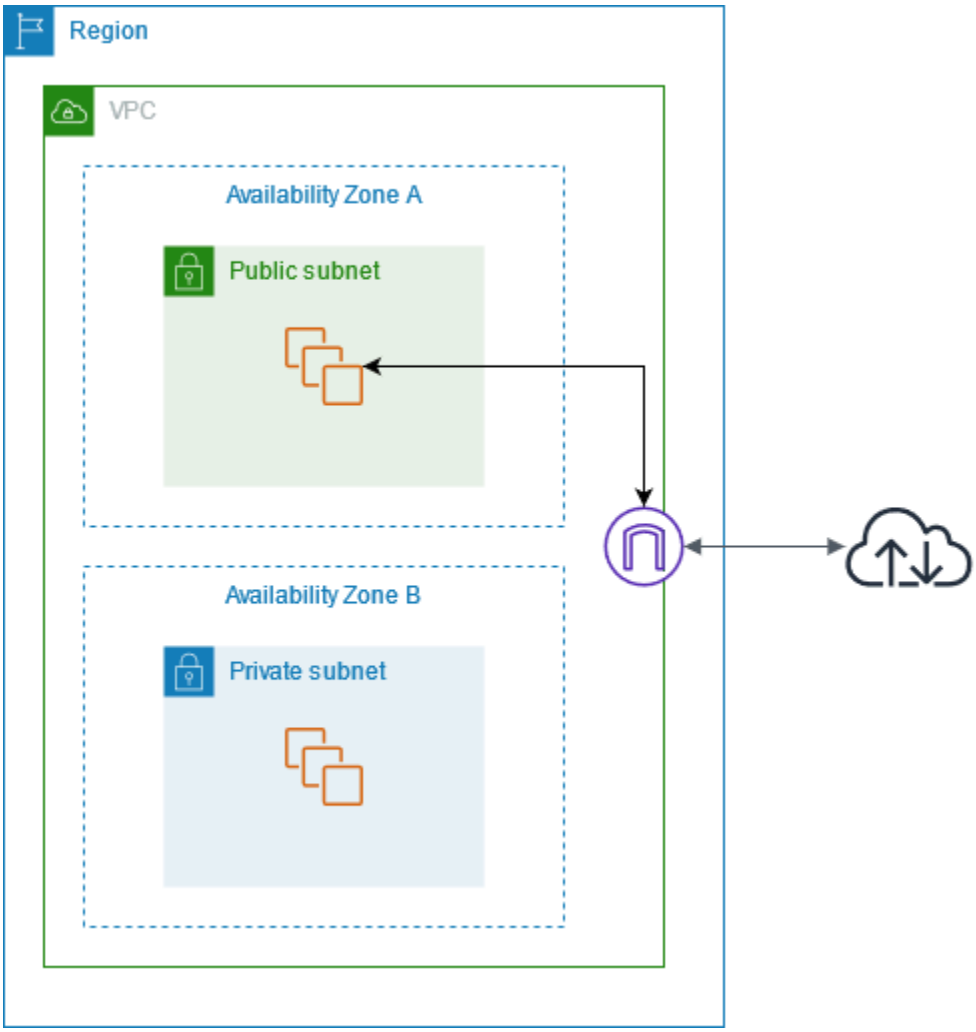
Adresses IP et NAT

Pour permettre la communication via Internet pour IPv4, votre instance doit comporter une adresse IPv4 publique. Vous pouvez soit configurer votre VPC pour affecter automatiquement des adresses IPv4 publiques à vos instances, soit affecter des adresses IP Elastic à vos instances. Votre instance ne connaît que l'espace d'adresse IP privée (interne) défini au sein du VPC et du sous-réseau. La passerelle Internet fournit logiquement le one-to-one NAT au nom de votre instance, de sorte que lorsque le trafic quitte votre sous-réseau VPC pour se rendre sur Internet, le champ d'adresse de réponse est défini sur l'adresse IPv4 publique ou l'adresse IP élastique de votre instance, et non sur son adresse IP privée. Inversement, l'adresse de destination du trafic qui est destiné pour l'adresse

IPv4 publique ou l'adresse IP Elastic de votre instance est convertie en adresse IPv4 privée de l'instance avant que le trafic ne soit distribué au VPC.

Pour permettre la communication via Internet pour IPv6, votre VPC et un sous-réseau doivent avoir un bloc d'adresse CIDR IPv6 associé et une adresse IPv6 doit être attribuée à votre instance à partir de la plage du sous-réseau. Les adresses IPv6 sont globalement uniques et par conséquent publiques par défaut.

Dans le diagramme suivant, le sous-réseau de la zone de disponibilité A est un sous-réseau public. La table de routage de ce sous-réseau a un acheminement qui envoie tout le trafic IPv4 lié à Internet à la passerelle Internet. Les instances du sous-réseau public doivent avoir des adresses IP publiques ou des adresses IP Elastic pour permettre la communication avec Internet via la passerelle Internet. À titre de comparaison, le sous-réseau de la zone de disponibilité B est un sous-réseau privé, car sa table de routage n'a pas d'acheminement vers la passerelle Internet. Comme il n'existe aucune route menant à la passerelle Internet, les instances du sous-réseau privé ne peuvent pas communiquer avec Internet même si elles possèdent des adresses IP publiques.



Accès Internet pour les VPC par défaut et personnalisés

Le tableau suivant fournit une vue d'ensemble qui indique si votre VPC est automatiquement associé aux composants requis pour l'accès Internet via IPv4 ou IPv6.

Composant	VPC par défaut	VPC personnalisé
Passerelle Internet	Oui	Non
Table de routage avec route vers une passerelle Internet pour le trafic IPv4 (0.0.0.0/0)	Oui	Non
Table de routage avec route vers une passerelle Internet pour le trafic IPv6 (::/0)	Non	Non
Adresse IPv4 publique attribuée automatiquement à l'instance lancée dans le sous-réseau	Oui (sous-réseau par défaut)	Non (sous-réseau personnalisé)
Adresse IPv6 attribuée automatiquement à l'instance lancée dans le sous-réseau	Non (sous-réseau par défaut)	Non (sous-réseau personnalisé)

Pour plus d'informations sur les VPC par défaut, consultez VPC par défaut. Pour plus d'informations sur la création d'un VPC, consultez Création d'un VPC.

Utiliser des passerelles Internet

La section suivante décrit comment prendre en charge l'accès Internet à partir d'un sous-réseau dans votre VPC à l'aide d'une passerelle Internet. Pour supprimer l'accès à Internet, vous pouvez détacher la passerelle Internet de votre VPC, puis la supprimer.

Tâches

- Création d'une passerelle Internet
- Attachement d'une passerelle Internet à un VPC

- Détacher une passerelle Internet de votre VPC
- Suppression d'une passerelle Internet

Création d'une passerelle Internet

Utilisez la procédure suivante pour créer une passerelle Internet.

Pour créer une passerelle Internet

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Passerelles Internet.
3. Choisissez Créer une passerelle Internet.
4. (Facultatif) Saisissez un nom pour votre passerelle Internet.
5. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
6. Choisissez Créer une passerelle Internet.
7. (Facultatif) Pour attacher la passerelle Internet à un VPC maintenant, choisissez Attacher à un VPC dans la bannière en haut de l'écran, sélectionnez un VPC disponible, puis choisissez Attacher une passerelle Internet. Sinon, vous pouvez attacher votre passerelle Internet à un VPC à un autre moment.

Attachement d'une passerelle Internet à un VPC

Pour utiliser une passerelle Internet, vous devez l'associer à un VPC.

Pour attacher une passerelle Internet à un VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Passerelles Internet.
3. Cochez la case pour la passerelle Internet.
4. Choisissez Actions, Attacher au VPC.
5. Sélectionnez un VPC disponible.
6. Choisissez Attacher une passerelle Internet.

Détacher une passerelle Internet de votre VPC

Si vous n'avez plus besoin d'un accès Internet pour les instances que vous lancez dans un VPC, vous pouvez détacher une passerelle Internet d'un VPC. Vous ne pouvez pas détacher une passerelle Internet si le VPC comporte des ressources avec des adresses IP publiques ou des adresses IP Elastic associées.

Pour détacher une passerelle Internet

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Passerelles Internet.
3. Cochez la case pour la passerelle Internet.
4. Choisissez Actions, Détacher du VPC.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Détacher la passerelle Internet.

Suppression d'une passerelle Internet

Si vous n'avez plus besoin d'une passerelle Internet, vous pouvez la supprimer. Vous ne pouvez pas supprimer une passerelle Internet si elle est encore attachée à un VPC.

Pour supprimer une passerelle Internet

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Passerelles Internet.
3. Cochez la case pour la passerelle Internet.
4. Choisissez Actions, Supprimer la passerelle Internet.
5. Lorsque vous êtes invité à confirmer, saisissez **`delete`**, puis choisissez Supprimer la passerelle Internet.

Présentation des API et des commandes

Vous pouvez exécuter les tâches décrites sur cette page à l'aide de la ligne de commande ou d'un API. Pour plus d'informations sur les interfaces de ligne de commande et la liste des actions liées aux API disponibles, consultez Utilisation d'Amazon VPC.

Création d'une passerelle Internet

- create-internet-gateway (AWS CLI)
- New-EC2InternetGateway (AWS Tools for Windows PowerShell)

Attachement d'une passerelle Internet à un VPC

- attach-internet-gateway (AWS CLI)
- Add-EC2InternetGateway (AWS Tools for Windows PowerShell)

Description d'une passerelle Internet

- describe-internet-gateways (AWS CLI)
- Get-EC2InternetGateway (AWS Tools for Windows PowerShell)

Détachement d'une passerelle Internet d'un VPC

- detach-internet-gateway (AWS CLI)
- Dismount-EC2InternetGateway (AWS Tools for Windows PowerShell)

Suppression d'une passerelle Internet

- delete-internet-gateway (AWS CLI)
- Remove-EC2InternetGateway (AWS Tools for Windows PowerShell)

Tarification

Il n'y a pas de frais pour une passerelle Internet, mais il y a des frais de transfert de données pour les instances EC2 qui utilisent des passerelles Internet. Pour plus d'informations, consultez Amazon EC2 On-Demand Pricing (Tarification à la demande EC2 d'Amazon).

Activer le trafic sortant IPv6 à l'aide de passerelles Internet de sortie uniquement

Une passerelle Internet de sortie uniquement est un composant de VPC dimensionnés horizontalement, redondant et hautement disponible qui permet la communication sortante via IPv6 des instances de votre VPC à Internet, et empêche Internet d'initier une connexion IPv6 avec vos instances.

> **Note**
>
> Une passerelle Internet de sortie doit être utilisée avec le trafic IPv6 uniquement. Pour activer la communication Internet sortante uniquement via IPv4, utilisez plutôt une passerelle NAT. Pour de plus amples informations, veuillez consulter Passerelles NAT.

Table des matières

Principes de base sur la passerelle Internet de sortie uniquement

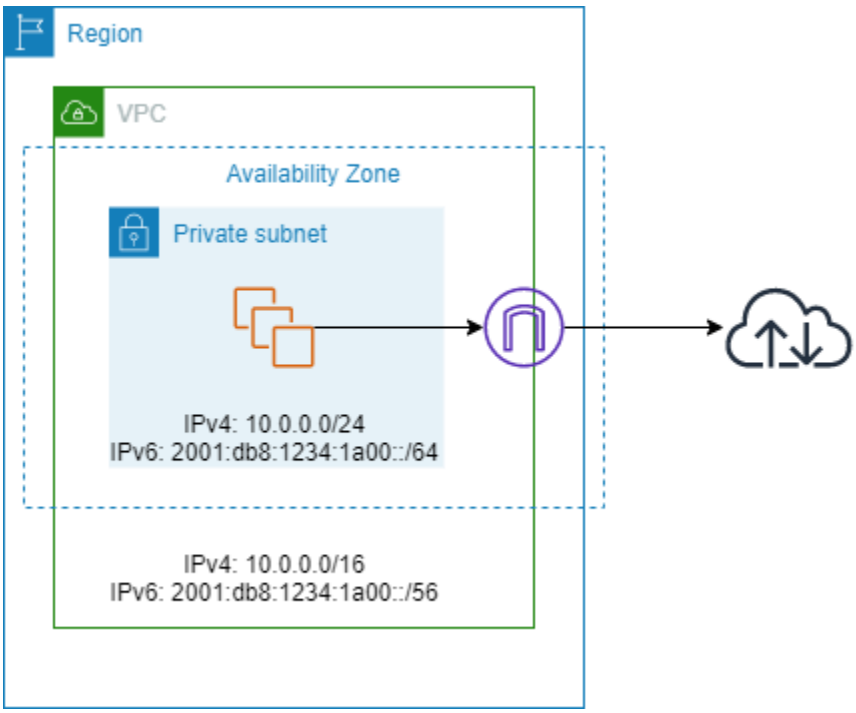
Les adresses IPv6 sont globalement uniques, et par conséquent publiques par défaut. Si vous souhaitez que votre instance puisse accéder à Internet, mais que vous voulez empêcher les ressources sur Internet d'initier la communication avec votre instance, vous pouvez utiliser une passerelle Internet de sortie uniquement. Pour ce faire, créez une passerelle Internet de sortie uniquement dans votre VPC, puis ajoutez une route vers votre table de routage qui dirige tout le trafic IPv6 (`::/0`) ou une plage spécifique de l'adresse IPv6 vers la passerelle Internet de sortie uniquement. Le trafic IPv6 du sous-réseau associé à la table de routage est acheminé vers la passerelle Internet de sortie uniquement.

Une passerelle Internet de sortie uniquement est dynamique : elle transmet le trafic des instances du sous-réseau vers Internet ou d'autres AWS services, puis renvoie la réponse aux instances.

Une passerelle Internet de sortie uniquement présente les caractéristiques suivantes :

- Vous ne pouvez pas associer un groupe de sécurité à une passerelle Internet de sortie uniquement. Vous pouvez utiliser des groupes de sécurité pour vos instances dans le sous-réseau privé pour contrôler le trafic à destination et en provenance de ces instances.
- Vous pouvez utiliser une liste ACL réseau pour contrôler le trafic à destination et en provenance du sous-réseau pour lequel la passerelle Internet de sortie uniquement achemine le trafic.

Dans le diagramme suivant, le VPC comporte des blocs CIDR IPv4 et IPv6, et le sous-réseau des blocs CIDR IPv4 et IPv6. Le VPC a une passerelle Internet de sortie uniquement.



Voici un exemple de table de routage associée au sous-réseau. Il y a une route qui envoi tout le trafic IPv6 Internet (::/0) vers une passerelle Internet de sortie uniquement.

Destination	Cible
10.0.0.0/16	Locale
2001:db8:1234:1a00::/64	Local
::/0	*eigw-id*

Utiliser des passerelles Internet de sortie uniquement

Les tâches suivantes décrivent comment créer une passerelle Internet de sortie (sortante) uniquement pour votre sous-réseau privé, et configurer le routage du sous-réseau.

Tâches

Création d'une passerelle Internet de sortie uniquement

Vous pouvez créer une passerelle Internet de sortie uniquement pour votre VPC à l'aide de la console Amazon VPC.

Pour créer une passerelle Internet de sortie uniquement

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Egress Only Internet Gateways.
3. Choisissez Create Egress Only Internet Gateway.
4. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une balise] Choisissez Ajouter une nouvelle balise et procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Value (Valeur), saisissez la valeur de clé.

   [Remove a tag] Choisissez Remove (Supprimer) à la droite de la clé et de la valeur de la balise.
5. Sélectionnez le VPC dans lequel créer la passerelle Internet de sortie uniquement.
6. Choisissez Créer.

Afficher votre passerelle Internet de sortie uniquement

Vous pouvez afficher les informations concernant votre passerelle Internet de sortie uniquement dans la console Amazon VPC.

Pour afficher les informations sur une passerelle Internet de sortie uniquement

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Egress Only Internet Gateways.
3. Sélectionnez la passerelle Internet de sortie uniquement pour afficher ses informations dans le volet des détails.

Créer une table de routage personnalisée

Pour envoyer le trafic destiné à l'extérieur du VPC vers la passerelle Internet de sortie uniquement, vous devez créer une table de routage personnalisée, ajouter une route qui envoie le trafic vers la passerelle, puis l'associer à votre sous-réseau.

Pour créer une table de routage personnalisée et ajouter une route à la passerelle Internet de sortie uniquement

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Route Tables (Tables de routage), puis Create route table (Créer une table de routage).
3. Dans la boîte de dialogue Create route table (Créer une table de routage), nommez si vous le souhaitez votre table de routage, puis sélectionnez votre VPC, puis choisissez Create route table (Créer une table de routage).
4. Sélectionnez la table de routage personnalisée que vous venez de créer. Le volet des détails affiche des onglets pour utiliser ses routes, ses associations et la propagation du routage.
5. Sous l'onglet Routes, choisissez Edit routes (Modifier les routes), spécifiez `::/0` dans la zone Destination, sélectionnez l'ID de passerelle Internet de sortie uniquement dans la liste Target (Cible), puis choisissez Save changes (Enregistrer les modifications).
6. Sous l'onglet Subnet associations (Associations de sous-), choisissez Edit subnet associations (Modifier les associations de sous-réseau), puis sélectionnez la case à cocher pour le sous-réseau. Choisissez Enregistrer.

Sinon, vous pouvez ajouter une route vers une table de routage existante qui est associée à votre sous-réseau. Sélectionnez votre table de routage existante et suivez les étapes 5 et 6 ci-dessus pour ajouter une route vers la passerelle Internet de sortie uniquement.

Pour plus d'informations sur les tables de routage, consultez Configuration des tables de routage.

Suppression d'une passerelle Internet de sortie uniquement

Si vous n'avez plus besoin de passerelle Internet de sortie uniquement, vous pouvez la supprimer. Toute route d'une table de routage qui pointe vers la passerelle Internet de sortie uniquement supprimée reste dans un état `blackhole` tant que vous n'avez pas supprimé ni mis à jour manuellement la route.

Pour supprimer une passerelle Internet de sortie uniquement

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Passerelles Internet de sortie uniquement et sélectionnez la passerelle Internet de sortie uniquement.
3. Sélectionnez Supprimer.
4. Choisissez Delete Egress Only Internet Gateway dans la boîte de dialogue de confirmation.

Présentation des API et de l'interface de ligne de commande (CLI)

Vous pouvez exécuter les tâches décrites sur cette page à l'aide de la ligne de commande ou d'un API. Pour plus d'informations sur les interfaces de ligne de commande et la liste des actions liées aux API disponibles, consultez Utilisation d'Amazon VPC.

Création d'une passerelle Internet de sortie uniquement

- create-egress-only-internet-passerelle ()AWS CLI
- New-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

Description d'une passerelle Internet de sortie uniquement

- describe-egress-only-internet-passerelles ()AWS CLI
- Get-EC2EgressOnlyInternetGatewayList (AWS Tools for Windows PowerShell)

Suppression d'une passerelle Internet de sortie uniquement

- delete-egress-only-internet-passerelle ()AWS CLI
- Remove-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

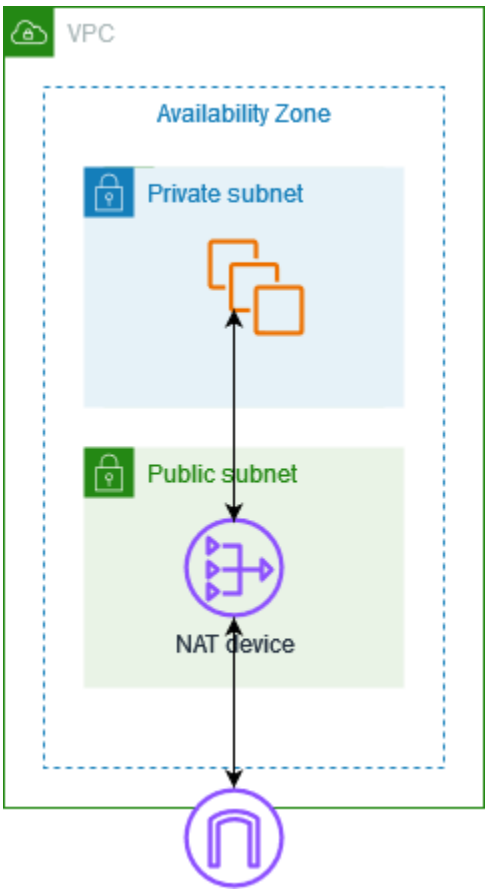
Tarification

Il n'y a pas de frais pour une passerelle internet de sortie uniquement, mais il y a des frais de transfert de données pour les instances EC2 qui utilisent des passerelles internet. Pour plus d'informations, consultez Amazon EC2 On-Demand Pricing (Tarification à la demande EC2 d'Amazon).

Connectez-vous à Internet ou à d'autres réseaux à l'aide de périphériques NAT

Vous pouvez utiliser un périphérique NAT pour autoriser des ressources dans des sous-réseaux privés à se connecter à Internet, à d'autres VPC ou à des réseaux sur site. Ces instances peuvent communiquer avec des services extérieurs au VPC, mais ne peuvent pas recevoir de demandes de connexion non sollicitées.

Par exemple, le schéma suivant montre un périphérique NAT dans un sous-réseau public qui permet aux instances EC2 d'un sous-réseau privé de se connecter à Internet via une passerelle Internet. Le périphérique NAT remplace l'adresse IPv4 source des instances par l'adresse du périphérique NAT. Lors de l'envoi du trafic de réponse aux instances, le périphérique NAT retraduit les adresses en adresses IPv4 sources d'origine.



Important

- Nous utilisons le terme NAT dans cette documentation pour suivre les pratiques informatiques courantes, bien que le véritable rôle d'un périphérique NAT soit la traduction d'adresse et la traduction d'adresse port (PAT).
- Vous pouvez utiliser un périphérique NAT géré proposé par AWS, appelé passerelle NAT, ou vous pouvez créer votre propre périphérique NAT sur une instance EC2, appelée instance NAT. Nous vous recommandons d'utiliser des passerelles NAT car elles offrent une disponibilité et une bande passante supérieures, et nécessitent moins d'efforts d'administration de votre part.

Table des matières

Passerelles NAT

Une passerelle NAT est un service de traduction d'adresses réseau (NAT). Vous pouvez utiliser une passerelle NAT, afin que les instances d'un sous-réseau privé puissent se connecter à des services en dehors de votre VPC, mais que les services externes ne puissent pas initier une connexion avec ces instances.

Lorsque vous créez une passerelle NAT, vous spécifiez l'un des types de connectivité suivants :

- Publique (par défaut) : des instances dans des sous-réseaux privés peuvent se connecter à Internet via une passerelle NAT publique, mais ne peuvent pas recevoir de connexions entrantes non sollicitées à partir d'Internet. Vous créez une passerelle NAT publique dans un sous-réseau public, et devez associer une adresse IP Elastic à la passerelle NAT lors de sa création. Vous acheminez le trafic de la passerelle NAT vers la passerelle Internet pour le VPC. Vous pouvez également utiliser une passerelle NAT publique pour vous connecter à d'autres VPC ou à votre réseau local. Dans ce cas, vous acheminez le trafic de la passerelle NAT via une passerelle de transit ou une passerelle réseau privé virtuel.
- Privée : des instances dans des sous-réseaux privés peuvent se connecter à d'autres VPC ou à votre réseau local via une passerelle NAT privée. Vous pouvez acheminer le trafic de la passerelle NAT via une passerelle de transit ou une passerelle réseau privé virtuel. Vous pouvez associer une adresse IP Elastic à une passerelle NAT privée. Vous pouvez attacher une passerelle Internet à un VPC avec une passerelle NAT privée, mais si vous acheminez le trafic de la passerelle NAT privée à la passerelle Internet, cette dernière laisse tomber le trafic.

Les passerelles NAT privées et publiques mappent l'adresse IPv4 privée source des instances à l'adresse IPv4 privée de la passerelle NAT. Dans le cas d'une passerelle NAT publique, la passerelle Internet mappe ensuite l'adresse IPv4 privée de la passerelle NAT publique à l'adresse IP Elastic associée à la passerelle NAT. Lors de l'envoi du trafic de réponse aux instances, qu'il s'agisse d'une passerelle NAT publique ou privée, la passerelle NAT retraduit l'adresse en adresse IP source d'origine.

> **Important**
>
> Vous pouvez utiliser une passerelle NAT publique ou privée pour acheminer le trafic vers des passerelles de transit et des passerelles privées virtuelles.

Si vous utilisez une passerelle NAT privée pour vous connecter à une passerelle de transit ou à une passerelle privée virtuelle, le trafic vers la destination proviendra de l'adresse IP privée de la passerelle NAT privée.
Si vous utilisez une passerelle NAT publique pour vous connecter à une passerelle de transit ou à une passerelle privée virtuelle, le trafic vers la destination proviendra de l'adresse IP privée de la passerelle NAT publique, à moins que vous n'utilisiez une passerelle Internet.
La passerelle NAT publique n'utilisera que son EIP comme adresse IP source lorsqu'elle est utilisée conjointement avec une passerelle Internet.

Table des matières

Principes de base d'une passerelle NAT

Chaque passerelle NAT est créée dans une zone de disponibilité spécifique et implémentée de manière redondante dans cette zone. Le nombre de passerelles NAT que vous pouvez créer dans chaque zone de disponibilité est régi par un quota. Pour plus d'informations, consultez Quotas Amazon VPC.

Si vous avez des ressources dans plusieurs zones de disponibilité et qu'elles partagent une passerelle NAT, si une panne affecte la zone de disponibilité de la passerelle NAT, les ressources des autres zones de disponibilité perdent leur accès à Internet. Pour améliorer la résilience, créez une passerelle NAT dans chaque zone de disponibilité et configurez votre routage pour vous assurer que les ressources utilisent la passerelle NAT dans la même zone de disponibilité.

Les caractéristiques et règles suivantes s'appliquent aux passerelles NAT :

- Une passerelle NAT prend en charge les protocoles suivants : TCP, UDP et ICMP.
- Les passerelles NAT sont prises en charge pour le trafic IPv4 ou IPv6. Pour le trafic IPv6, la passerelle NAT exécute NAT64. Si vous l'utilisez conjointement avec DNS64 (disponible sur le résolveur Route 53), vos charges de travail IPv6 dans un sous-réseau Amazon VPC peuvent communiquer avec les ressources IPv4. Ces services IPv4 peuvent être présents dans le même VPC (dans un sous-réseau distinct) ou dans un autre VPC, dans votre environnement sur site ou sur Internet.
- Une passerelle NAT prend en charge jusqu'à 5 Gbit/s de bande passante et augmente automatiquement jusqu'à 100 Gbit/s. Si vous avez besoin de plus de bande passante, vous pouvez diviser vos ressources en plusieurs sous-réseaux et créer une passerelle NAT dans chaque sous-réseau.
- Une passerelle NAT peut traiter un million de paquets par seconde et augmenter automatiquement jusqu'à dix millions de paquets par seconde. Au-delà de cette limite, une passerelle NAT supprime les paquets. Pour éviter une perte de paquets, fractionnez vos ressources en plusieurs sous-réseaux et créez une passerelle NAT distincte pour chacun d'eux.
- Chaque adresse IPv4 peut prendre en charge jusqu'à 55 000 connexions simultanées vers chaque destination unique. Une destination unique est identifiée par une combinaison unique d'adresse IP de destination, de port de destination et de protocole (TCP/UDP/ICMP). Vous pouvez augmenter cette limite en associant jusqu'à huit adresses IPv4 à vos passerelles NAT (une principale et sept secondaires). Par défaut, vous ne pouvez associer que deux adresses IP Elastic à votre passerelle NAT publique. Vous pouvez augmenter cette limite en sollicitant un ajustement de quota. Pour plus d'informations, consultez Adresses IP Elastic.
- Vous pouvez choisir l'adresse IPv4 privée à attribuer à la passerelle NAT ou la faire attribuer automatiquement à partir de la plage d'adresses IPv4 du sous-réseau. L'adresse IPv4 privée attribuée persiste jusqu'à ce que vous supprimiez la passerelle NAT privée. Vous ne pouvez ni détacher l'adresse IPv4 privée ni attacher d'adresses IPv4 privées supplémentaires.
- Vous ne pouvez pas associer de groupe de sécurité à une passerelle NAT. Vous pouvez associer des groupes de sécurité à vos instances afin de contrôler le trafic entrant et sortant.
- Vous pouvez utiliser une ACL réseau pour contrôler le trafic entrant et sortant du sous-réseau pour votre passerelle NAT. Les passerelles NAT utilisent les ports 1024–65535. Pour plus d'informations, consultez Contrôle du trafic vers les sous-réseaux avec des listes ACL réseau.
- Une passerelle NAT reçoit une interface réseau. Vous pouvez choisir l'adresse IPv4 privée à attribuer à l'interface ou la faire attribuer automatiquement à partir de la plage d'adresses IPv4 du sous-réseau. Vous pouvez afficher l'interface réseau pour la passerelle NAT à l'aide de la console

Amazon EC2. Pour de plus amples d'informations, consultezAffichage des informations relatives à une interface réseau. Vous ne pouvez pas modifier les attributs de cette interface réseau.

- Vous ne pouvez pas acheminer le trafic vers une passerelle NAT via une connexion d'appairage VPC. Vous ne pouvez pas acheminer le trafic via une passerelle NAT lorsque le trafic arrive via une connexion hybride (VPN de site à site ou Direct Connect) via une passerelle privée virtuelle. Vous pouvez acheminer le trafic via une passerelle NAT lorsque le trafic arrive via une connexion hybride (VPN de site à site ou Direct Connect) via une passerelle de transit.
- Les passerelles NAT prennent en charge le trafic avec une unité de transmission maximale (MTU) de 8500, mais il est important de noter ce qui suit :
  - Pour éviter toute perte de paquets potentielle lors de la communication avec des ressources via Internet via une passerelle NAT publique, le paramètre MTU de vos instances EC2 ne doit pas dépasser 1 500 octets. Pour plus d'informations sur la vérification et le paramétrage du MTU sur une instance, consultez Vérifier et définir le MTU sur votre instance Linux dans le guide de l'utilisateur Amazon EC2.
  - Les passerelles NAT prennent en charge la découverte de Path MTU (PMTUD) via les paquets ICMPv4 FRAG_NEEDED et les paquets ICMPv6 Packet Too Big (PTB).
  - Les passerelles NAT appliquent le blocage de la taille maximale de segment (MSS) pour tous les paquets. Pour de plus amples informations, veuillez consulter RFC879.

Contrôler l'utilisation des passerelles NAT

Par défaut, les utilisateurs ne sont pas autorisés à utiliser des passerelles NAT. Vous pouvez créer un rôle IAM avec une politique qui autorise les utilisateurs à créer, décrire et supprimer des passerelles NAT. Pour plus d'informations, consultez Identity and Access Management pour Amazon VPC.

Utiliser des passerelles NAT

Vous pouvez utiliser la console Amazon VPC pour créer et gérer vos passerelles NAT.

Tâches

- Créer une passerelle NAT
- Modification des associations d'adresses IP secondaires
- Baliser une passerelle NAT
- Supprimer une passerelle NAT

Créer une passerelle NAT

Utilisez la procédure suivante pour créer une passerelle NAT.

Quotas associés

- Vous ne pourrez pas créer de passerelle NAT publique si vous avez épuisé le nombre d'EIP alloués à votre compte. Pour plus d'informations sur les quotas EIP et sur la façon de les ajuster, consultez Adresses IP Elastic.
- Vous pouvez attribuer jusqu'à huit adresses IPv4 privées à votre passerelle NAT privée. Cette limite n'est pas réglable.
- Par défaut, vous ne pouvez associer que deux adresses IP Elastic à votre passerelle NAT publique. Vous pouvez augmenter cette limite en sollicitant un ajustement de quota. Pour plus d'informations, consultez Adresses IP Elastic.

Créer une passerelle NAT

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Passerelles NAT.
3. Sélectionnez Créer une passerelle NAT.
4. (Facultatif) Spécifiez un nom pour la passerelle NAT. Cela crée une identification où la clé est **`Name`** et la valeur est le nom que vous spécifiez.
5. Sélectionnez le sous-réseau public dans lequel créer la passerelle NAT.
6. Pour Type de connectivité, conservez la valeur Publique sélectionnée par défaut afin de créer une passerelle NAT publique, ou sélectionnez Privée pour créer une passerelle NAT privée. Pour plus d'informations sur la différence entre une passerelle NAT publique et privée, veuillez consulter la section Passerelles NAT.
7. Si vous avez sélectionné Public, procédez comme suit ; sinon, passez à l'étape 8 :

    1. Sélectionnez un ID d'allocation d'adresses IP Elastic pour attribuer une EIP à la passerelle NAT, ou Allouer une adresse IP Elastic afin d'attribuer automatiquement une EIP à la passerelle NAT publique. Par défaut, vous ne pouvez associer que deux adresses IP Elastic à votre passerelle NAT publique. Vous pouvez augmenter cette limite en sollicitant un ajustement de quota. Pour plus d'informations, consultez Adresses IP Elastic.

> **Important**
>
> Lorsque vous attribuez une adresse IP élastique (EIP) à une passerelle NAT publique, le groupe périphérique du réseau de l'EIP doit correspondre au groupe périphérique du réseau de la zone de disponibilité (AZ) dans laquelle vous lancez la passerelle NAT publique. Si ce n'est pas le cas, la passerelle NAT ne pourra pas être lancée. Vous pouvez voir le groupe périphérique du réseau pour la zone de disponibilité (AZ) du sous-réseau en consultant les détails du sous-réseau. De même, vous pouvez voir le groupe périphérique du réseau d'une EIP en consultant les détails de l'adresse EIP. Pour en savoir plus sur les groupes périphériques du réseau et les EIP, consultez allouer une adresse IP Elastic ;.

2. (Facultatif) Sélectionnez Paramètres supplémentaires et, sous Adresse IP privée - facultatif, entrez une adresse IPv4 privée pour la passerelle NAT. Si vous n'entrez pas d'adresse, une adresse IPv4 privée AWS sera automatiquement attribuée à votre passerelle NAT de manière aléatoire à partir du sous-réseau dans lequel se trouve votre passerelle NAT.
3. Passez à l'étape 11.

8. Si vous avez sélectionné Privé, cliquez sur Paramètres supplémentaires, Méthode d'attribution d'adresse IPv4 privée, puis sélectionnez l'une des options suivantes :

   - Attribution automatique : AWS choisit l'adresse IPv4 privée principale pour la passerelle NAT. Pour Nombre d'adresses IPv4 privées attribuées automatiquement, vous pouvez éventuellement spécifier le nombre d'adresses IPv4 privées secondaires pour la passerelle NAT. AWS choisit ces adresses IP au hasard dans le sous-réseau de votre passerelle NAT.
   - Personnalisé : pour Adresse IPv4 privée principale, choisissez l'adresse IPv4 privée principale pour la passerelle NAT. Pour Adresses IPv4 privées secondaires, vous pouvez éventuellement spécifier jusqu'à sept adresses IPv4 privées secondaires pour la passerelle NAT.

9. Si vous avez sélectionné Personnalisée à l'étape 8, ignorez cette étape. Si vous avez choisi Attribuer automatiquement, sous Nombre d'adresses IP privées attribuées automatiquement, choisissez le nombre d'adresses IPv4 secondaires que vous souhaitez AWS attribuer à cette passerelle NAT privée. Ce nombre ne peut pas être supérieur à sept adresses IPv4.

> **Note**
>
> Les adresses IPv4 secondaires sont facultatives et doivent être attribuées ou allouées lorsque vos charges de travail utilisant une passerelle NAT dépassent

55 000 connexions simultanées vers une seule destination (la même adresse IP de destination, le même port de destination et le même protocole). Les adresses IPv4 secondaires augmentent le nombre de ports disponibles et, par conséquent, la limite du nombre de connexions simultanées que vos charges de travail peuvent établir à l'aide d'une passerelle NAT.

10. Si vous avez sélectionné Attribuer automatiquement à l'étape 9, ignorez cette étape. Si vous avez sélectionné Personnalisée, procédez comme suit :
    1. Sous Adresse IPv4 privée principale, saisissez une adresse IPv4 privée.
    2. Sous Adresse IPv4 privée secondaire, entrez jusqu'à sept adresses IPv4 privées secondaires.
11. (Facultatif) Pour ajouter une balise à la passerelle NAT, choisissez Add new tag (Ajouter une nouvelle balise) et saisissez la clé et entrez le nom et la valeur de la clé. Vous pouvez ajouter jusqu'à 50 balises.
12. Sélectionnez Créer une passerelle NAT.
13. Le statut initial de la passerelle NAT est `Pending`. Dès que le statut devient `Available`, la passerelle NAT est prête à être utilisée. Veillez à mettre à jour vos tables de routage si nécessaire. Pour obtenir des exemples, consultez the section called "Cas d'utilisation".

Si le statut de la passerelle NAT devient `Failed`, une erreur s'est produite pendant la création. Pour plus d'informations, consultez Échec de la création d'une passerelle NAT.

Modification des associations d'adresses IP secondaires

Chaque adresse IPv4 peut prendre en charge jusqu'à 55 000 connexions simultanées vers chaque destination unique. Une destination unique est identifiée par une combinaison unique d'adresse IP de destination, de port de destination et de protocole (TCP/UDP/ICMP). Vous pouvez augmenter cette limite en associant jusqu'à huit adresses IPv4 à vos passerelles NAT (une principale et sept secondaires). Par défaut, vous ne pouvez associer que deux adresses IP Elastic à votre passerelle NAT publique. Vous pouvez augmenter cette limite en sollicitant un ajustement de quota. Pour plus d'informations, consultez Adresses IP Elastic.

Vous pouvez utiliser les CloudWatchmétriques de passerelle NAT ErrorPort Allocation et PacketsDropCount pour déterminer si votre passerelle NAT génère des erreurs d'allocation de port ou supprime des paquets. Afin de résoudre ce problème, ajoutez des adresses IPv4 secondaires à votre passerelle NAT.

Considérations

- Vous pouvez ajouter des adresses IPv4 privées secondaires lorsque vous créez une passerelle NAT privée ou après sa création en suivant la procédure décrite dans cette section. Vous pouvez ajouter des adresses EIP secondaires aux passerelles NAT publiques uniquement après avoir créé la passerelle NAT en suivant la procédure décrite dans cette section.
- Jusqu'à huit adresses IPv4 peuvent être associées à votre passerelle NAT (une principale et sept secondaires). Vous pouvez attribuer jusqu'à huit adresses IPv4 privées à votre passerelle NAT privée. Par défaut, vous ne pouvez associer que deux adresses IP Elastic à votre passerelle NAT publique. Vous pouvez augmenter cette limite en sollicitant un ajustement de quota. Pour plus d'informations, consultez Adresses IP Elastic.

Pour modifier des associations d'adresses IPv4 secondaires

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Passerelles NAT.
3. Sélectionnez la passerelle NAT dont vous souhaitez modifier les associations d'adresses IPv4 secondaires.
4. Sélectionnez Actions, puis Modifier les associations d'adresses IP secondaires.
5. Si vous modifiez les associations d'adresses IPv4 secondaires d'une passerelle NAT privée, sous Action, sélectionnez Attribuer de nouvelles adresses IPv4 ou Annuler l'attribution d'adresses IPv4 existantes. Si vous modifiez les associations d'adresses IPv4 secondaires d'une passerelle NAT publique, sous Action, sélectionnez Associer de nouvelles adresses IPv4 ou Dissocier les adresses IPv4 existantes.
6. Effectuez l'une des actions suivantes :

   - Si vous avez choisi d'attribuer ou d'associer de nouvelles adresses IPv4, procédez comme suit :

     1. Cette étape est obligatoire. Vous devez sélectionner une adresse IPv4 privée. Sélectionnez la méthode d'attribution d'adresse IPv4 privée :

        - Attribution automatique : choisit AWS automatiquement une adresse IPv4 privée principale et vous choisissez si vous souhaitez attribuer jusqu' AWS à 7 adresses IPv4 privées secondaires à attribuer à la passerelle NAT. AWS les choisit et vous les attribue automatiquement au hasard à partir du sous-réseau dans lequel se trouve votre passerelle NAT.

- Personnalisée : pour Adresse IPv4 privée primaire, choisissez l'adresse IPv4 privée primaire pour la passerelle NAT. Pour Adresses IPv4 privées secondaires, vous pouvez optionnellement spécifier jusqu'à sept adresses IPv4 privées secondaires pour la passerelle NAT.

2. Sous ID d'allocation d'adresses IP Elastic, sélectionnez une EIP à ajouter en tant qu'adresse IPv4 secondaire. Cette étape est obligatoire. Vous devez sélectionner une EIP avec une adresse IPv4 privée. Si vous avez sélectionné Personnalisée comme méthode d'attribution d'adresse IP privée, vous devez également saisir une adresse IPv4 privée pour chaque EIP que vous ajoutez.

> **Important**
>
> Lorsque vous attribuez une EIP secondaire à une passerelle NAT publique, le groupe périphérique du réseau de l'EIP doit correspondre au groupe périphérique du réseau de la zone de disponibilité (AZ) dans laquelle se trouve la passerelle NAT publique. Si ce n'est pas le cas, l'EIP ne sera pas attribuée. Vous pouvez voir le groupe périphérique du réseau pour la zone de disponibilité (AZ) du sous-réseau en consultant les détails du sous-réseau. De même, vous pouvez voir le groupe périphérique du réseau d'une EIP en consultant les détails de l'adresse EIP. Pour en savoir plus sur les groupes périphériques du réseau et les EIP, consultez allouer une adresse IP Elastic ;.

Jusqu'à huit adresses IP peuvent être associées à votre passerelle NAT. S'il s'agit d'une passerelle NAT publique, il existe une limite de quota par défaut pour les EIP par région. Pour plus d'informations, consultez Adresses IP Elastic.

- Si vous avez choisi d'annuler l'attribution ou de dissocier de nouvelles adresses IPv4, procédez comme suit :

  1. Sous Adresse IP secondaire existante pour laquelle annuler l'attribution, sélectionnez les adresses IP secondaires dont vous souhaitez annuler l'attribution.
  2. (Facultatif) Sous Durée de drainage de la connexion, entrez la durée maximale d'attente (en secondes) avant de libérer de force les adresses IP si les connexions sont toujours en cours. Si vous ne spécifiez aucune valeur, la valeur par défaut est 350 secondes.

7. Sélectionnez Enregistrer les modifications.

Si le statut de la passerelle NAT devient `Failed`, une erreur s'est produite pendant la création. Pour plus d'informations, consultez Échec de la création d'une passerelle NAT.

Baliser une passerelle NAT

Vous pouvez baliser votre passerelle NAT afin de l'identifier ou de la classer en fonction des besoins de votre organisation. Pour plus d'informations sur l'utilisation des balises, consultez la section Marquage de vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

Les balises d'allocation des coûts sont prises en charge pour les passerelles NAT. Par conséquent, vous pouvez également utiliser des balises pour organiser votre AWS facture et refléter votre propre structure de coûts. Pour plus d'informations, veuillez consulter Utilisation des étiquettes de répartition des coûts dans le AWS Billing Guide de l'utilisateur. Pour plus d'informations sur la configuration d'un rapport de répartition des coûts avec des balises, voir Rapport de répartition des coûts mensuel dans À propos de la facturation du AWS compte.

Pour baliser une passerelle NAT

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Passerelles NAT.
3. Sélectionnez la passerelle NAT que vous souhaitez baliser, puis Actions. Ensuite, sélectionnez Gérer les balises.
4. Sélectionnez Ajouter une nouvelle balise, puis définissez une clé ainsi qu'une valeur pour la balise. Vous pouvez ajouter jusqu'à 50 balises.
5. Choisissez Enregistrer.

Supprimer une passerelle NAT

Si vous n'avez plus besoin d'une passerelle NAT, vous pouvez la supprimer. Après que vous avez supprimé une passerelle NAT, son entrée reste visible dans la console Amazon VPC pendant environ une heure, après quoi elle est automatiquement supprimée. Vous ne pouvez pas supprimer cette entrée vous-même.

Supprimer une passerelle NAT dissocie son adresse IP Elastic mais ne libère pas l'adresse de votre compte. Si vous supprimez une passerelle NAT, les routes de la passerelle NAT restent en statut `blackhole` jusqu'à ce que vous supprimiez ou mettiez les routes à jour.

Supprimer une passerelle NAT

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez NAT Gateways.
3. Sélectionnez le bouton radio de la passerelle NAT, puis choisissez Actions, Supprimer la passerelle NAT.
4. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).
5. Si vous n'avez plus besoin de l'adresse IP Elastic associée à la passerelle NAT publique, nous vous recommandons de la libérer. Pour plus d'informations, consultez Libérer une adresse IP Elastic.

Présentation des API et de l'interface de ligne de commande (CLI)

Vous pouvez exécuter les tâches décrites sur cette page à l'aide de la ligne de commande ou de l'API. Pour plus d'informations sur les interfaces de ligne de commande et une liste des opérations de l'API disponibles, consultez Utilisation d'Amazon VPC.

Attribuer une adresse IPv4 privée à une passerelle NAT privée

- assign-private-nat-gateway-address (AWS CLI)
- Register-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)
- AssignPrivateNatGatewayAdresse (API de requête Amazon EC2)

Associer des adresses IP Elastic (EIP) et des adresses IPv4 privées à une passerelle NAT publique

- associate-nat-gateway-address (AWS CLI)
- Register-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)
- AssociateNatGatewayAddress(API de requête Amazon EC2)

Créer une passerelle NAT

- create-nat-gateway (AWS CLI)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)
- CreateNatPasserelle (API de requête Amazon EC2)

Supprimer une passerelle NAT

- delete-nat-gateway (AWS CLI)
- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)
- DeleteNatPasserelle (API de requête Amazon EC2)

Décrire une passerelle NAT

- describe-nat-gateways (AWS CLI)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)
- DescribeNatPasserelles (API de requête Amazon EC2)

Dissocier des adresses IP Elastic (EIP) secondaires d'une passerelle NAT publique

- disassociate-nat-gateway-address (AWS CLI)
- Unregister-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)
- DisassociateNatGatewayAddress(API de requête Amazon EC2)

Baliser une passerelle NAT

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)
- CreateTags(API de requête Amazon EC2)

Annuler l'attribution d'adresses IPv4 secondaires d'une passerelle NAT privée

- unassign-private-nat-gateway-address (AWS CLI)
- Unregister-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)
- UnassignPrivateNatGatewayAdresse (API de requête Amazon EC2)

Cas d'utilisation de la passerelle NAT

Voici des exemples de cas d'utilisation de passerelles NAT publiques et privées.

Scénarios

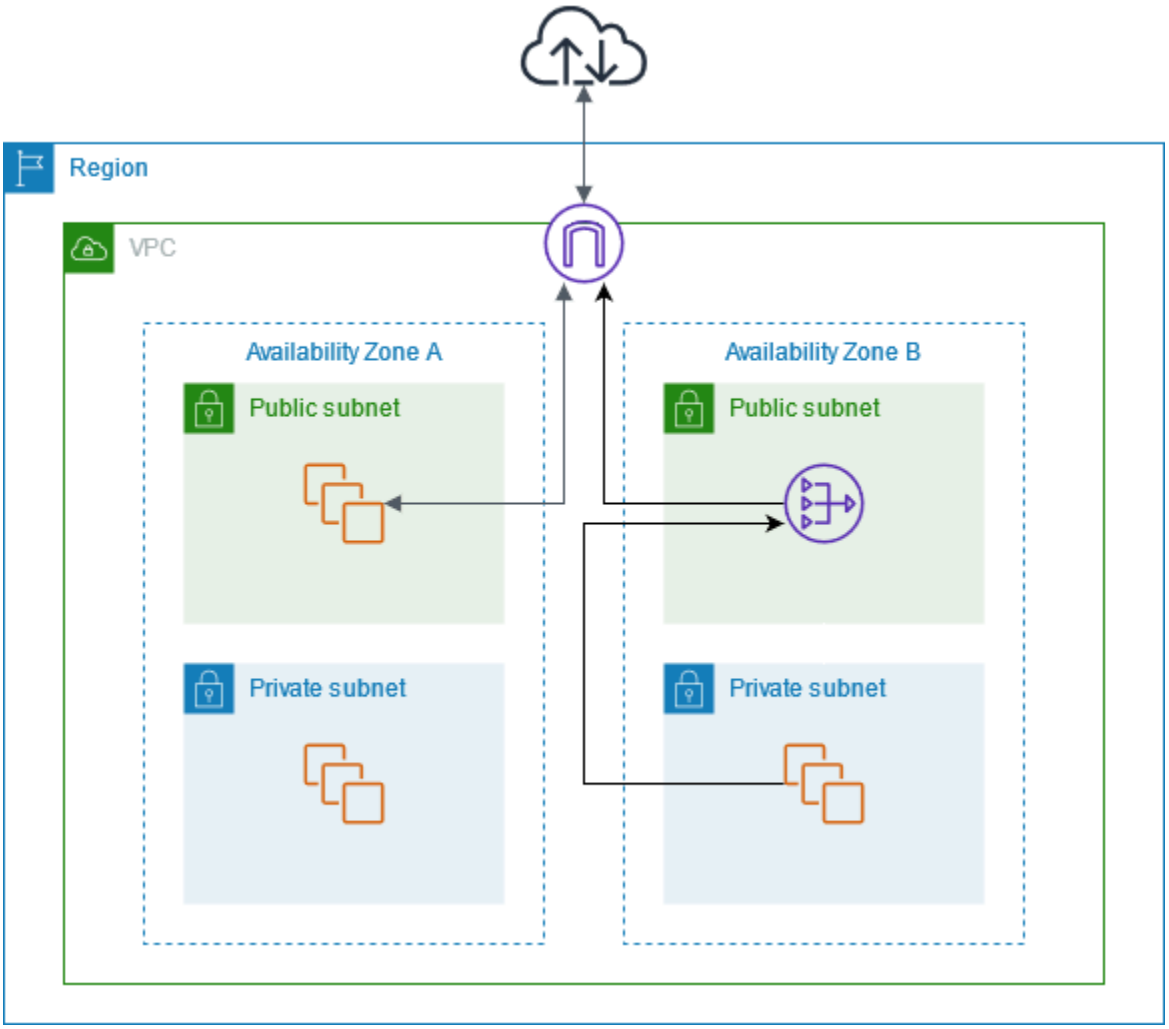
Accéder à Internet à partir d'un sous-réseau privé

Vous pouvez utiliser une passerelle NAT publique pour permettre aux instances d'un sous-réseau privé d'envoyer du trafic sortant vers Internet, tout en empêchant Internet d'établir des connexions avec les instances.

Table des matières

Présentation

Le diagramme suivant illustre ce cas d'utilisation. Il existe deux zones de disponibilité, avec deux sous-réseaux dans chaque zone de disponibilité. La table de routage de chaque sous-réseau détermine la manière dont le trafic est acheminé. Dans la zone de disponibilité A, les instances du sous-réseau public peuvent accéder à Internet via un acheminement vers la passerelle Internet, tandis que les instances du sous-réseau privé n'ont aucun acheminement vers Internet. Dans la zone de disponibilité B, le sous-réseau public contient une passerelle NAT et les instances du sous-réseau privé peuvent accéder à Internet via un acheminement vers la passerelle NAT du sous-réseau public. Les passerelles NAT privées et publiques mappent l'adresse IPv4 privée source des instances à l'adresse IPv4 privée de la passerelle NAT privée. Dans le cas d'une passerelle NAT publique, la passerelle Internet mappe ensuite l'adresse IPv4 privée de la passerelle NAT publique à l'adresse IP Elastic associée à la passerelle NAT. Lors de l'envoi du trafic de réponse aux instances, qu'il s'agisse d'une passerelle NAT publique ou privée, la passerelle NAT retraduit l'adresse en adresse IP source d'origine.



Notez que si les instances du sous-réseau privé de la zone de disponibilité A doivent également accéder à Internet, vous pouvez créer une route à partir de ce sous-réseau vers la passerelle NAT de la zone de disponibilité B. Vous pouvez également améliorer la résilience en créant une passerelle NAT dans chaque zone de disponibilité contenant des ressources qui nécessitent un accès à Internet. Pour obtenir un exemple de diagramme, consultez the section called “Serveurs privés”.

Routage

Voici la table de routage associée au sous-réseau public dans la zone de disponibilité A. La première entrée est l'acheminement local ; cela permet aux instances du sous-réseau de communiquer avec d'autres instances du VPC à l'aide d'adresses IP privées. La deuxième entrée envoie tout le reste du trafic de sous-réseau à la passerelle Internet, ce qui permet aux instances du sous-réseau d'accéder à Internet.

Destination	Cible
Bloc d'adresse du VPC	locale
0.0.0.0/0	*internet-gateway-id*

Voici la table de routage associée au sous-réseau privé dans la zone de disponibilité A. L'entrée est l'acheminement local, qui permet aux instances du sous-réseau de communiquer avec d'autres instances du VPC à l'aide d'adresses IP privées. Les instances de ce sous-réseau n'ont pas accès à Internet.

Destination	Cible
Bloc d'adresse du VPC	local

Voici la table de routage associée au sous-réseau public dans la zone de disponibilité B. La première entrée est l'acheminement local ; cela permet aux instances du sous-réseau de communiquer avec d'autres instances du VPC à l'aide d'adresses IP privées. La deuxième entrée envoie tout le reste du trafic de sous-réseau à la passerelle Internet, ce qui permet à la passerelle NAT du sous-réseau d'accéder à Internet.

Destination	Cible
Bloc d'adresse du VPC	locale
0.0.0.0/0	*internet-gateway-id*

Voici la table de routage associée au sous-réseau privé dans la zone de disponibilité B. La première entrée est l'itinéraire local ; cela permet aux instances du sous-réseau de communiquer avec d'autres instances du VPC à l'aide d'adresses IP privées. La deuxième entrée envoie tout le reste du trafic du sous-réseau vers la passerelle NAT.

Destination	Cible
Bloc d'adresse du VPC	locale

Destination	Cible
0.0.0.0/0	*nat-gateway-id*

Pour plus d'informations, consultez the section called "Utiliser des tables de routage".

Tester la passerelle NAT publique

Après avoir créé votre passerelle NAT et mis à jour vos tables de routage, vous pouvez effectuer un test ping d'adresses distantes à partir d'une instance de votre sous-réseau privé afin de vérifier s'il peut se connecter à Internet. Pour obtenir un exemple montrant la façon de procéder, consultez Tester la connexion Internet.

Si vous ne pouvez pas vous connecter à Internet, vous pouvez également tester si le trafic Internet est acheminé via la passerelle NAT :

- Tracez la route du trafic à partir d'une instance dans votre sous-réseau privé. Pour ce faire, exécutez la commande `traceroute` depuis une instance Linux dans votre sous-réseau privé. A la sortie, vous devez voir l'adresse IP privée de la passerelle NAT dans un des sauts (généralement le premier).
- Utilisez un site Web ou un outil tiers qui affiche l'adresse IP source quand vous vous y connectez depuis une instance dans votre sous-réseau privé. L'adresse IP source doit être l'adresse IP Elastic de la passerelle NAT.

Si ces tests échouent, veuillez consulter Résoudre les problèmes des passerelles NAT.

Tester la connexion Internet

L'exemple suivant montre comment tester si une instance dans un sous-réseau privé peut se connecter à Internet.

1. Lancez une instance dans votre sous-réseau public (utilisez-la comme hôte bastion). Dans l'assistant de lancement, assurez-vous de sélectionner une AMI Amazon Linux et d'assigner une adresse IP publique à votre instance. Assurez-vous que les règles de votre groupe de sécurité autorisent le trafic SSH entrant depuis la plage d'adresses IP pour votre réseau local, et le trafic SSH sortant vers la plage d'adresses IP de votre sous-réseau privé (vous pouvez également utiliser `0.0.0.0/0` pour le trafic SSH entrant et sortant pour ce test).

2. Lancez une instance dans votre sous-réseau privé. Dans l'assistant de lancement, assurez-vous de sélectionner une AMI Amazon Linux. N'assignez pas d'adresse IP publique à votre instance. Assurez-vous que les règles de votre groupe de sécurité autorisent le trafic SSH entrant depuis l'adresse IP privée de votre instance que vous avez lancée dans le sous-réseau public, et tout le trafic ICMP sortant. Vous devez choisir la même paire de clés que vous avez utilisée pour lancer votre instance dans un sous-réseau public.
3. Configurez le transfert de l'agent SSH sur votre ordinateur local et connectez-vous à votre hôte bastion dans le sous-réseau public. Pour plus d'informations, consultez Pour configurer le transfert de l'agent SSH pour Linux ou macOS ou Configurer le transfert de l'agent SSH pour Windows.
4. Depuis votre hôte bastion, connectez-vous à votre instance du sous-réseau privé, puis testez la connexion Internet depuis votre instance du sous-réseau privé. Pour plus d'informations, consultez Pour tester la connexion Internet.

Pour configurer le transfert de l'agent SSH pour Linux ou macOS

1. Depuis votre machine locale, ajoutez votre clé privée à l'agent d'authentification.

   Pour Linux, utilisez la commande suivante.

   ```
   ssh-add -c mykeypair.pem
   ```

   Pour macOS, utilisez la commande suivante.

   ```
   ssh-add -K mykeypair.pem
   ```

2. Connectez-vous à votre instance dans le sous-réseau public à l'aide de l'option `-A` pour activer le transfert de l'agent SSH et utilisez l'adresse publique de l'instance, comme dans l'exemple suivant :

   ```
   ssh -A ec2-user@54.0.0.123
   ```

Configurer le transfert de l'agent SSH pour Windows

Vous pouvez utiliser le client OpenSSH disponible sous Windows ou installer votre client SSH préféré (par exemple, PuTTY).

OpenSSH

Installez OpenSSH pour Windows comme décrit dans cet article : Bien démarrer avec OpenSSH pour Windows. Ajoutez ensuite votre clé à l'agent d'authentification. Pour plus d'informations, consultez Authentification basée sur une clé dans OpenSSH pour Windows.

PuTTY

1. Téléchargez et installez Pageant depuis la page de téléchargement PuTTY, s'il n'est pas déjà installé.
2. Convertissez votre clé privée au format .ppk. Pour plus d'informations, consultez la section Conversion de votre clé privée à l'aide de PuttyGen dans le guide de l'utilisateur Amazon EC2.
3. Démarrez Pageant, cliquez avec le bouton droit sur l'icône Pageant de la barre des tâches (il peut être masqué) et choisissez Add Key. Sélectionnez le fichier .ppk que vous avez créé, entrez la phrase secrète si nécessaire, puis choisissez Ouvrir.
4. Démarrez une session PuTTY et connectez-vous à votre instance dans le sous-réseau public à l'aide de son adresse IP publique. Pour de plus ample informations, veuillez consulter Connexion à votre instance Linux. Dans la catégorie Auth, assurez-vous d'avoir sélectionné l'option Allow agent forwarding, puis laissez la zone Private key file for authentication vide.

Pour tester la connexion Internet

1. Depuis votre instance dans le sous-réseau public, connectez-vous à votre instance dans votre sous-réseau privé en utilisant son adresse IP privée, comme illustré dans l'exemple suivant.

```
ssh ec2-user@10.0.1.123
```

2. Depuis votre instance privée, vérifiez que vous pouvez vous connecter à Internet en exécutant la commande `ping` pour un site web dont l'ICMP est activé.

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=47 time=86.0 ms
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=47 time=75.6 ms
...
```

Appuyez sur Ctrl+C sur votre clavier pour annuler la commande `ping`. Si la commande `ping` échoue, consultez Les instances ne peuvent pas accéder à Internet.

3. (Facultatif) Si vous n'avez plus besoin de vos instances, mettez-les hors service. Pour de plus amples informations, veuillez consulter Résilier une instance dans le Guide de l'utilisateur Amazon EC2.

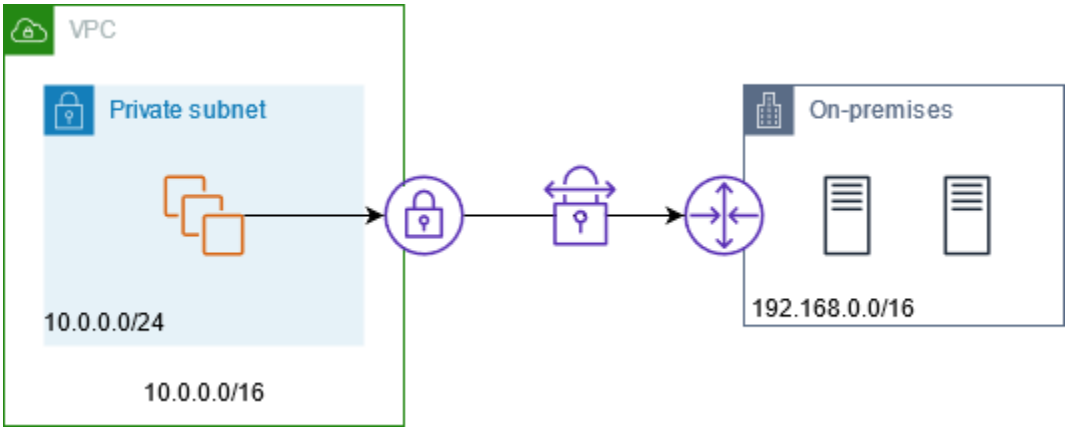
Accédez à votre réseau à l'aide d'adresses IP autorisées

Vous pouvez utiliser une passerelle NAT privée pour activer la communication entre vos VPC et votre réseau sur site à l'aide d'un groupe d'adresses autorisées. Au lieu d'attribuer à chaque instance une adresse IP distincte dans la plage d'adresses IP autorisées, vous pouvez acheminer le trafic du sous-réseau destiné au réseau interne via une passerelle NAT privée dotée d'une adresse IP dans la plage d'adresses IP autorisées.

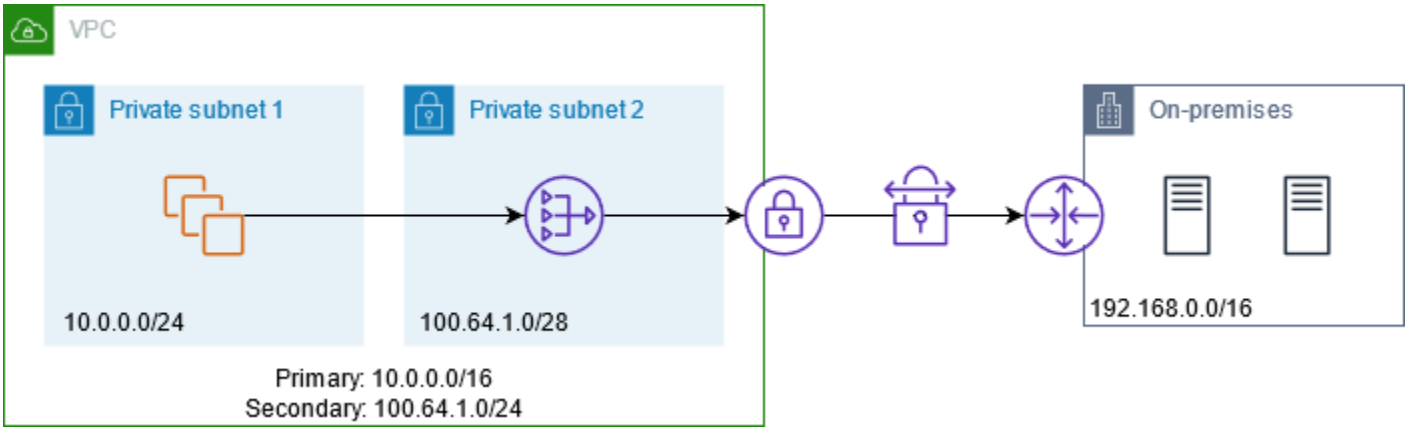
Table des matières

Présentation

Le schéma suivant montre comment les instances peuvent accéder aux ressources locales via AWS VPN. Le trafic provenant des instances est acheminé vers une passerelle réseau privé virtuel, via la connexion VPN, vers la passerelle client, puis vers la destination dans le réseau sur site. Cependant, supposons que la destination n'autorise le trafic qu'à partir d'une plage d'adresses IP spécifique, telle que 100.64.1.0/28. Cela empêcherait le trafic de ces instances d'atteindre le réseau sur site.



Le schéma suivant illustre les principaux composants pour la configuration de ce scénario. Le VPC a sa plage d'adresses IP d'origine plus la plage d'adresses IP autorisée. Le VPC possède un sous-réseau de la plage d'adresses IP autorisée avec une passerelle NAT privée. Le trafic des instances destiné au réseau sur site est envoyé à la passerelle NAT avant d'être acheminé vers la connexion VPN. Le réseau sur site reçoit le trafic des instances avec l'adresse IP source de la passerelle NAT, qui provient de la plage d'adresses IP autorisée.



Ressources

Créez ou mettez à jour des ressources comme suit :

- Associez la plage d'adresses IP autorisées au VPC.
- Créez un sous-réseau dans le VPC à partir de la plage d'adresses IP autorisée.
- Créez une passerelle NAT privée dans le nouveau sous-réseau.
- Mettez à jour la table de routage du sous-réseau avec les instances pour envoyer le trafic destiné au réseau sur site à la passerelle NAT. Ajoutez un acheminement à la table de routage pour le sous-réseau avec la passerelle NAT privée qui envoie le trafic destiné au réseau sur site à la passerelle réseau privé virtuel.

Routage

Voici la table de routage associée au premier sous-réseau. Il existe un acheminement local pour chaque CIDR de VPC. Les acheminements locaux permettent aux ressources du sous-réseau de communiquer avec d'autres ressources du VPC à l'aide d'adresses IP privées. La troisième entrée envoie le trafic destiné au réseau sur site à la passerelle NAT privée.

Destination	Cible
10,0.0.0/16	locale
100,64,1,0/24	local
192.168.0.0/16	*nat-gateway-id*

Voici la table de routage associée au deuxième sous-réseau. Il existe un acheminement local pour chaque CIDR de VPC. Les acheminements locaux permettent aux ressources du sous-réseau de communiquer avec d'autres ressources du VPC à l'aide d'adresses IP privées. La troisième entrée envoie le trafic destiné au réseau sur site à la passerelle réseau privé virtuel.

Destination	Cible
10,0.0.0/16	locale
100,64,1,0/24	local
192.168.0.0/16	*vgw-id*

Activer la communication entre des réseaux qui se chevauchent

Vous pouvez utiliser une passerelle NAT privée pour activer la communication entre les réseaux même s'ils ont des plages d'adresses CIDR qui se chevauchent. Par exemple, supposons que les instances du VPC A aient besoin d'accéder aux services fournis par les instances du VPC B.

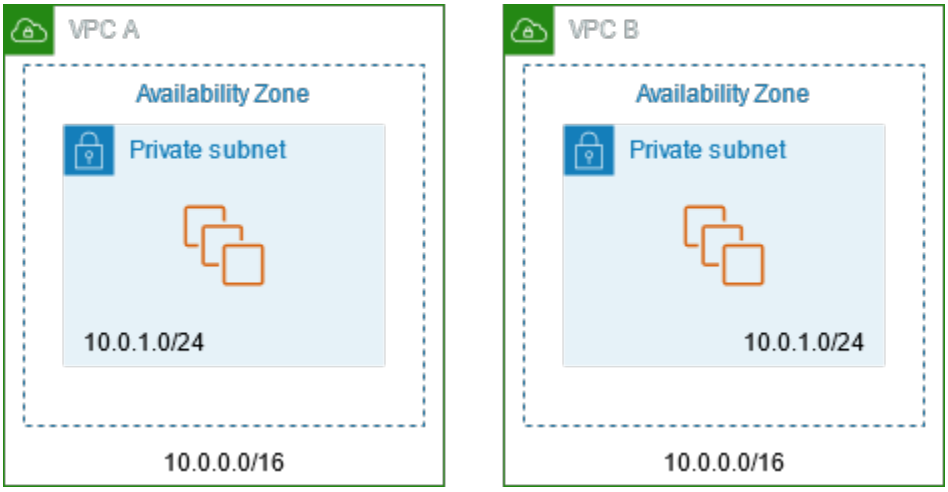


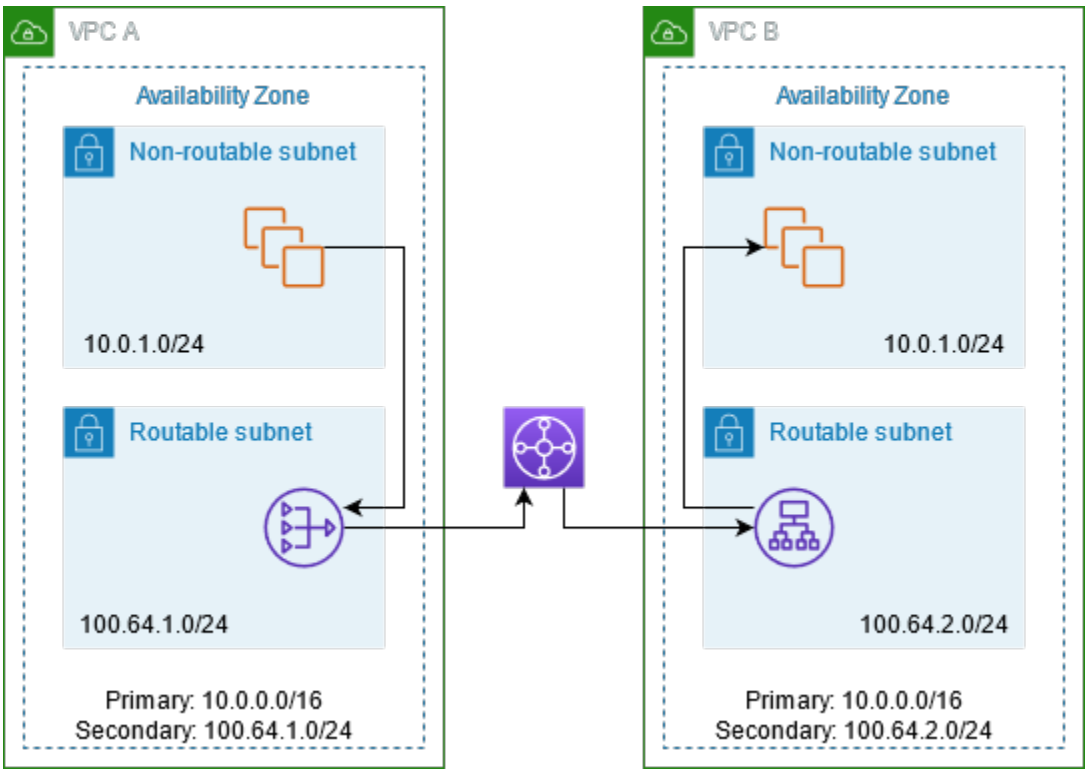
Table des matières

Présentation

Le schéma suivant illustre les principaux composants pour la configuration de ce scénario. Tout d'abord, votre équipe de gestion des adresses IP détermine quelles plages d'adresses peuvent se chevaucher (plages d'adresses non routables) et lesquelles ne le peuvent pas (plages d'adresses routables). L'équipe de gestion des adresses IP alloue des plages d'adresses du groupe de plages d'adresses routables aux projets à la demande.

Chaque VPC a sa plage d'adresses IP d'origine, qui n'est pas routable, plus la plage d'adresses IP routables qui lui est attribuée par l'équipe de gestion des adresses IP. Le VPC A possède un sous-réseau de sa plage routable avec une passerelle NAT privée. La passerelle NAT privée obtient son adresse IP à partir de son sous-réseau. Le VPC B possède un sous-réseau provenant de sa plage routable avec un Application Load Balancer. L'Application Load Balancer obtient ses adresses IP à partir de ses sous-réseaux.

Le trafic d'une instance du sous-réseau non routable du VPC A destiné aux instances du sous-réseau non routable du VPC B est envoyé via la passerelle NAT privée, puis acheminé vers la passerelle de transit. La Transit Gateway envoie le trafic à l'Application Load Balancer, qui achemine le trafic vers l'une des instances cibles dans le sous-réseau non routable de VPC B. Le trafic de la Transit Gateway à l'Application Load Balancer a l'adresse IP source de la passerelle NAT privée. Par conséquent, le trafic de réponse de l'équilibreur de charge utilise l'adresse de la passerelle NAT privée comme destination. Le trafic de réponse est envoyé à la passerelle de transit, puis acheminé vers la passerelle NAT privée, qui traduit la destination vers l'instance dans le sous-réseau non routable du VPC A.



Ressources

Créez ou mettez à jour des ressources comme suit :

- Associez les plages d'adresses IP routables attribuées à leurs VPC respectifs.
- Créez un sous-réseau dans le VPC A à partir de sa plage d'adresses IP routables et créez une passerelle NAT privée dans ce nouveau sous-réseau.
- Créez un sous-réseau dans le VPC B à partir de sa plage d'adresses IP routables et créez un Application Load Balancer dans ce nouveau sous-réseau. Enregistrez les instances dans le sous-réseau non routable avec le groupe cible pour l'équilibreur de charge.
- Créez une passerelle de transit pour connecter les VPC. Assurez-vous de désactiver la propagation de l'acheminement. Lorsque vous attachez chaque VPC à la passerelle de transit, utilisez la plage d'adresses routables du VPC.
- Mettez à jour la table de routage du sous-réseau non routable dans le VPC A pour envoyer tout le trafic destiné à la plage d'adresses routables du VPC B vers la passerelle NAT privée. Mettez à jour la table de routage du sous-réseau routable dans le VPC A pour envoyer tout le trafic destiné à la plage d'adresses routables du VPC B vers la passerelle de transit.
- Mettez à jour la table de routage du sous-réseau routable dans le VPC B pour envoyer tout le trafic destiné à la plage d'adresses routables du VPC A vers la passerelle de transit.

Routage

Voici la table de routage pour le sous-réseau non routable dans le VPC A.

Destination	Cible
10,0.0.0/16	locale
100,64,1,0/24	local
100,64,2,0/24	*nat-gateway-id*

Voici la table de routage pour le sous-réseau routable dans le VPC A.

Destination	Cible
10,0.0.0/16	locale
100,64,1,0/24	local
100,64,2,0/24	*transit-gateway-id*

Voici la table de routage pour le sous-réseau non routable dans le VPC B.

Destination	Cible
10,0.0.0/16	locale
100,64,2,0/24	local

Voici la table de routage pour le sous-réseau routable dans le VPC B.

Destination	Cible
10,0.0.0/16	locale
100,64,2,0/24	local

Destination	Cible
100,64,1,0/24	*transit-gateway-id*

Voici la table de routage de passerelle de transit.

CIDR	Réseau de transit par passerelle	Type de routage
100,64,1,0/24	*Attachement pour le VPC A*	Statique
100,64,2,0/24	*Attachement pour le VPC B*	Statique

DNS64 et NAT64

La passerelle NAT A prend en charge la traduction d'adresses réseau de IPv6 vers IPv4, communément appelée NAT64. NAT64 permet à vos AWS ressources IPv6 de communiquer avec les ressources IPv4 du même VPC ou d'un autre VPC, sur votre réseau local ou sur Internet. Vous pouvez utiliser NAT64 avec DNS64 sur Amazon Route 53 Resolver ou utiliser votre propre serveur DNS64.

Table des matières

Qu'est-ce que DNS64 ?

Vos charges de travail IPv6 uniquement exécutées dans des VPC peuvent uniquement envoyer et recevoir des paquets réseau IPv6. Sans DNS64, une requête DNS pour un service IPv4 uniquement produira une adresse de destination IPv4 en réponse et votre service IPv6 uniquement ne peut pas communiquer avec. Pour combler ce manque de communication, vous pouvez activer le DNS64 pour un sous-réseau et il s'applique à toutes les AWS ressources de ce sous-réseau. Avec DNS64, Amazon Route 53 Resolver recherche l'enregistrement DNS du service que vous avez interrogé et effectue l'une des opérations suivantes :

- Si l'enregistrement contient une adresse IPv6, il renvoie l'enregistrement d'origine et la connexion est établie sans aucune traduction via IPv6.
- S'il n'y a pas d'adresse IPv6 associée à la destination dans l'enregistrement DNS, Route 53 Resolver en synthétise une en ajoutant le préfixe `/96` bien connu, défini dans RFC6052 (`64:ff9b::/96`), à l'adresse IPv4 de l'enregistrement. Votre service IPv6 uniquement envoie des paquets réseau à l'adresse IPv6 synthétisée. Vous devrez ensuite acheminer ce trafic via la passerelle NAT, qui effectue la traduction nécessaire sur le trafic pour permettre aux services IPv6 de votre sous-réseau d'accéder aux services IPv4 en dehors de ce sous-réseau.

Vous pouvez activer ou désactiver le DNS64 sur un sous-réseau à l'aide de l'attribut [modify-subnet-à l'aide de la AWS CLI ou de la console VPC en] sélectionnant un sous-réseau et en choisissant Actions > Modifier les paramètres du sous-réseau.

Qu'est-ce que NAT64 ?

NAT64 permet à vos services IPv6 uniquement dans les VPC Amazon de communiquer avec des services IPv4 uniquement au sein du même VPC (dans différents sous-réseaux) ou des VPC connectés, dans vos réseaux sur site ou sur Internet.

NAT64 est automatiquement disponible sur vos passerelles NAT existantes ou sur toutes les nouvelles passerelles NAT que vous créez. Il ne s'agit pas d'une fonction que vous pouvez activer ou désactiver. Le sous-réseau dans lequel se trouve la passerelle NAT n'a pas besoin d'être un sous-réseau à double pile pour que NAT64 fonctionne.

Après avoir activé DNS64, si votre service IPv6 uniquement envoie des paquets réseau à une adresse IPv6 synthétisée via la passerelle NAT, les actions suivantes ont lieu :

- Grâce au préfixe `64:ff9b::/96`, la passerelle NAT reconnaît que la destination d'origine est IPv4 et traduit les paquets IPv6 en IPv4 en remplaçant :
  - l'IPv6 source par sa propre adresse IP privée qui est traduite en adresse IP Elastic par la passerelle Internet ;
  - l'IPv6 de destination par une IPv4 en tronquant le préfixe `64:ff9b::/96`.
- La passerelle NAT envoie les paquets IPv4 traduits vers la destination via la passerelle Internet, la passerelle réseau privé virtuel ou la passerelle de transit et initie une connexion.
- L'hôte IPv4 uniquement renvoie des paquets de réponse IPv4. Une fois la connexion établie, la passerelle NAT accepte les paquets IPv4 de réponse provenant des hôtes externes.

- Les paquets IPv4 de réponse sont destinés à la passerelle NAT, qui reçoit les paquets et annule le protocole NAT en remplaçant son adresse IP (IP de destination) par l'adresse IPv6 de l'hôte et en ajoutant à nouveau le préfixe `64:ff9b::/96` à l'adresse IPv4 source. Le paquet est ensuite acheminé vers l'hôte en suivant l'acheminement local.

De cette façon, la passerelle NAT permet à vos charges de travail IPv6 uniquement dans un sous-réseau de communiquer avec les services IPv4 uniquement en dehors du sous-réseau.

Configuration de DNS64 et NAT64

Suivez les étapes de cette section pour configurer DNS64 et NAT64 afin d'activer la communication avec les services IPv4 uniquement.

Table des matières

Activez la communication avec les services IPv4 uniquement sur Internet avec la CLI AWS

Si vous disposez d'un sous-réseau avec des charges de travail IPv6 uniquement qui doit communiquer avec des services IPv4 uniquement en dehors du sous-réseau, cet exemple montre comment configurer ces services IPv6 uniquement pour leur permettre de communiquer avec les services IPv4 uniquement sur Internet.

Vous devez d'abord configurer une passerelle NAT dans un sous-réseau public (distinct du sous-réseau contenant les charges de travail IPv6 uniquement). Par exemple, le sous-réseau contenant la passerelle NAT doit avoir une `0.0.0.0/0` route pointant vers la passerelle Internet.

Suivez ces étapes pour permettre à ces services IPv6 uniquement de se connecter à des services IPv4 uniquement sur Internet :

1. Ajoutez les trois acheminements suivants à la table de routage du sous-réseau contenant les charges de travail IPv6 uniquement :

   - Acheminement IPv4 (le cas échéant) pointant vers la passerelle NAT.
   - Acheminement `64:ff9b::/96` pointant vers la passerelle NAT. Cela permettra au trafic provenant de vos charges de travail IPv6 uniquement destinées aux services IPv4 uniquement d'être acheminé via la passerelle NAT.

- Acheminement `::/0` IPv6 pointant vers la passerelle Internet de sortie uniquement (ou la passerelle Internet).

  Notez que le fait de pointer `::/0` vers la passerelle Internet permettra aux hôtes IPv6 externes (en dehors du VPC) d'initier une connexion via IPv6.

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-cidr-block
0.0.0.0/0 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
64:ff9b::/96 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
::/0 --egress-only-internet-gateway-id eigw-c0a643a9
```

2. Activez la fonctionnalité DNS64 dans le sous-réseau contenant les charges de travail IPv6 uniquement.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --enable-dns64
```

Désormais, les ressources de votre sous-réseau privé peuvent établir des connexions avec état avec les services IPv4 et IPv6 sur Internet. Configurez votre groupe de sécurité et vos listes ACL réseau de manière appropriée pour autoriser le trafic de sortie et d'entrée vers le trafic `64:ff9b::/96`.

Activez la communication avec les services IPv4 uniquement dans votre environnement sur site

Amazon Route 53 Resolver vous permet de transférer des requêtes DNS depuis votre VPC vers un réseau sur site et vice versa. Pour ce faire, procédez comme suit :

- Créez un point de terminaison Route 53 Resolver sortant dans un VPC et attribuez-lui les adresses IPv4 à partir desquelles vous souhaitez que Route 53 Resolver transfère les requêtes. Pour votre résolveur DNS sur site, ce sont les adresses IP d'où proviennent les requêtes DNS. Par conséquent, ce doit être des adresses IPv4.

- Créez une ou plusieurs règles pour spécifier les noms de domaine des requêtes DNS que vous voulez que Route 53 Resolver transfère vers les résolveurs sur site. Spécifiez également les adresses IPv4 des résolveurs sur site.
- Maintenant que vous avez configuré un point de terminaison Route 53 Resolver sortant, vous devez activer DNS64 sur le sous-réseau contenant vos charges de travail IPv6 uniquement et acheminer toutes les données destinées à votre réseau sur site via une passerelle NAT.

Fonctionnement de DNS64 pour les destinations IPv4 uniquement dans les réseaux sur site :

1. Vous attribuez une adresse IPv4 au point de terminaison Route 53 Resolver sortant dans votre VPC.
2. La requête DNS provenant de votre service IPv6 est transférée à Route 53 Resolver sur IPv6. Route 53 Resolver met la requête en correspondance avec la règle de transfert et obtient une adresse IPv4 pour votre résolveur sur site.
3. Route 53 Resolver convertit le paquet de requête d'IPv6 en IPv4 et le transmet au point de terminaison sortant. Chaque adresse IP du point de terminaison représente une ENI qui transmet la demande à l'adresse IPv4 sur site de votre résolveur DNS.
4. Le résolveur sur site renvoie le paquet de réponse sur IPv4 via le point de terminaison sortant vers Route 53 Resolver.
5. En supposant que la requête ait été effectuée à partir d'un sous-réseau compatible DNS64, Route 53 Resolver effectue deux opérations :

    a. Il vérifie le contenu du paquet de réponses. Si une adresse IPv6 est présente dans l'enregistrement, il conserve le contenu tel quel, mais uniquement s'il ne contient qu'un enregistrement IPv4. Il synthétise également un enregistrement IPv6 en ajoutant le préfixe `64:ff9b::/96` à l'adresse IPv4.

    b. Il recrée un package avec le contenu et l'envoie au service de votre VPC via IPv6.

Surveillez les passerelles NAT avec Amazon CloudWatch

Vous pouvez surveiller votre passerelle NAT en utilisant CloudWatch, qui collecte des informations à partir de votre passerelle NAT et crée des métriques lisibles en temps quasi réel. Vous pouvez utiliser ces informations afin de surveiller et de résoudre les problèmes de votre passerelle NAT. Les données de métriques de la passerelle NAT sont fournies à la fréquence d'1 minute et les statistiques sont enregistrées pendant une période de 15 mois.

Pour plus d'informations sur Amazon CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon. Pour plus d'informations sur les tarifs, consultez Amazon CloudWatch Pricing.

Dimensions et métriques de la passerelle NAT

Les métriques suivantes sont disponibles pour vos passerelles NAT. La colonne de description inclut une description de chaque métrique ainsi que les unités et les statistiques.

Métrique	Description
`ActiveConnectionCount`	Nombre total de connexions TCP actives simultanées via la passerelle NAT. Une valeur équivalant à zéro indique qu'il n'y a aucune connexion active sur la passerelle NAT. Unités : nombre Statistics : la statistique la plus utile est `Max`.
`BytesInFromDestination`	Nombre d'octets reçus par la passerelle NAT en provenance de la destination. Si la valeur de `BytesOutToSource` est inférieure à celle de `BytesInFromDestination`, certaines données risquent d'être perdues lors du traitement de la passerelle NAT, ou le trafic risque d'être bloqué activement par la passerelle NAT. Unités : octets Statistiques : la statistique la plus utile est `Sum`.
`BytesInFromSource`	Nombre d'octets reçus par la passerelle NAT en provenance des clients de votre VPC. Si la valeur de `BytesOutToDestination` est inférieure à celle de `BytesInFromSource`, certaines données risquent d'être

Métrique	Description
	perdues lors du traitement de la passerelle NAT. Unités : octets Statistics : la statistique la plus utile est `Sum`.
`BytesOutToDestination`	Nombre d'octets envoyés à la destination via la passerelle NAT. Une valeur supérieure à zéro indique la présence d'un trafic vers Internet en provenance de clients qui se trouvent derrière la passerelle NAT. Si la valeur de `BytesOutToDestination` est inférieure à celle de `BytesInFromSource`, certaines données risquent d'être perdues lors du traitement de la passerelle NAT. Unité : octets Statistics : la statistique la plus utile est `Sum`.

Métrique	Description
BytesOutToSource	Nombre d'octets envoyés aux clients de votre VPC via la passerelle NAT. Une valeur supérieure à zéro indique la présence d'un trafic en provenance d'Internet vers les clients qui se trouvent derrière la passerelle NAT. Si la valeur de BytesOutToSource est inférieure à celle de BytesInFromDestination, certaines données risquent d'être perdues lors du traitement de la passerelle NAT, ou le trafic risque d'être bloqué activement par la passerelle NAT. Unités : octets Statistics : la statistique la plus utile est Sum.
ConnectionAttemptCount	Nombre de tentatives de connexion effectuées sur la passerelle NAT. Si la valeur de ConnectionEstablishedCount est inférieure à celle de ConnectionAttemptCount, cela indique que des clients se trouvant derrière la passerelle NAT ont tenté d'établir de nouvelles connexions qui n'ont pas abouti. Unité : nombre Statistics : la statistique la plus utile est Sum.

Métrique	Description
`ConnectionEstablishedCount`	Nombre de connexions établies sur la passerelle NAT. Si la valeur de `ConnectionEstablishedCount` est inférieure à celle de `ConnectionAttemptCount`, cela indique que des clients se trouvant derrière la passerelle NAT ont tenté d'établir de nouvelles connexions qui n'ont pas abouti. Unité : nombre Statistics : la statistique la plus utile est `Sum`.
`ErrorPortAllocation`	Nombre de fois où la passerelle NAT n'a pas pu allouer de port source. Une valeur supérieure à zéro indique qu'un trop grand nombre de connexions simultanées sont ouvertes sur la passerelle NAT. Unités : nombre Statistics : la statistique la plus utile est `Sum`.

Métrique	Description
`IdleTimeoutCount`	Nombre de connexions qui sont passées de l'état actif à l'état inactif. Une connexion active passe à l'état inactif si elle a été fermée correctement et si aucune activité n'a eu lieu pendant les dernières 350 secondes. Une valeur supérieure à zéro indique que certaines connexions sont devenues inactives . Si la valeur de `IdleTimeoutCount` augmente, cela peut indiquer que des clients derrière la passerelle NAT réutilisent des connexions obsolètes. Unité : nombre Statistics : la statistique la plus utile est `Sum`.
`PacketsDropCount`	Nombre de paquets abandonnés par la passerelle NAT. Pour calculer le nombre de paquets abandonné s en pourcentage du trafic global de paquets, utilisez cette formule :`PacketsDropCount/ (PacketsInFromSource+Packets InFromDestination)*100` . Si cette valeur dépasse 0,01 % du trafic total sur la passerelle NAT, il se peut qu'il y ait un problème avec le service Amazon VPC. Utilisez le tableau de bord de santé du AWS service pour identifier tout problème lié au service susceptible d'entraîner le rejet de paquets par les passerelles NAT. Unités : nombre Statistiques : la statistique la plus utile est `Sum`.

Métrique	Description
PacketsInFromDestination	Nombre de paquets reçus par la passerelle NAT en provenance de la destination. Si la valeur de PacketsOutToSource est inférieure à celle de PacketsInFromDestination, certaines données risquent d'être perdues lors du traitement de la passerelle NAT, ou le trafic risque d'être bloqué activement par la passerelle NAT. Unité : nombre Statistiques : la statistique la plus utile est Sum.
PacketsInFromSource	Nombre de paquets reçus par la passerelle NAT en provenance des clients de votre VPC. Si la valeur de PacketsOutToDestination est inférieure à celle de PacketsInFromSource, certaines données risquent d'être perdues lors du traitement de la passerelle NAT. Unité : nombre Statistiques : la statistique la plus utile est Sum.

Métrique	Description
PacketsOutToDestination	Nombre de paquets envoyés à la destination via la passerelle NAT. Une valeur supérieure à zéro indique la présence d'un trafic vers Internet en provenance de clients qui se trouvent derrière la passerelle NAT. Si la valeur de PacketsOutToDestination est inférieure à celle de PacketsInFromSource, certaines données risquent d'être perdues lors du traitement de la passerelle NAT. Unité : nombre Statistiques : la statistique la plus utile est Sum.
PacketsOutToSource	Nombre de paquets envoyés aux clients de votre VPC via la passerelle NAT. Une valeur supérieure à zéro indique la présence d'un trafic en provenance d'Internet vers les clients qui se trouvent derrière la passerelle NAT. Si la valeur de PacketsOutToSource est inférieure à celle de PacketsInFromDestination, certaines données risquent d'être perdues lors du traitement de la passerelle NAT, ou le trafic risque d'être bloqué activement par la passerelle NAT. Unité : nombre Statistiques : la statistique la plus utile est Sum.

Métrique	Description
`PeakBytesPerSecond`	Cette métrique indique la moyenne la plus élevée d'octets par seconde sur 10 secondes au cours d'une minute donnée. Unités : nombre Statistiques : la statistique la plus utile est `Maximum`.
`PeakPacketsPerSecond`	Cette métrique calcule le débit de paquets moyen (paquets traités par seconde) toutes les 10 secondes pendant 60 secondes, puis indique le maximum des 6 débits (le débit de paquets moyen le plus élevé). Unités : nombre Statistiques : la statistique la plus utile est `Maximum`.

Pour filtrer les données de métriques, utilisez la dimension suivante.

Dimension	Description
`NatGatewayId`	Permet de filtrer les données en fonction de l'ID de passerelle NAT.

Afficher les CloudWatch métriques de la passerelle NAT

Les métriques de la passerelle NAT sont envoyées à des CloudWatch intervalles d'une minute. Les métriques sont d'abord regroupées par espace de noms de service, puis en fonction des différentes combinaisons de dimensions au sein de chaque espace de noms. Vous pouvez afficher les métriques de vos passerelles NAT en procédant comme suit.

Pour afficher les métriques à l'aide de la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques, Toutes les métriques.
3. Cliquez sur l'espace de noms de la métrique NatGateway.
4. Choisissez la dimension de métrique.

Pour consulter les statistiques à l'aide du AWS CLI

À l'invite de commande, utilisez la commande suivante pour répertorier les métriques disponibles pour le service de passerelle NAT.

```
aws cloudwatch list-metrics --namespace "AWS/NATGateway"
```

Créez des CloudWatch alarmes pour surveiller une passerelle NAT

Vous pouvez créer une CloudWatch alarme qui envoie un message Amazon SNS lorsque l'alarme change d'état. Une alarme surveille une seule métrique pendant la période que vous spécifiez. Elle envoie une notification à une rubrique Amazon SNS en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes.

Par exemple, vous pouvez créer une alarme qui surveille la quantité de trafic entrant dans la passerelle NAT ou sortant de celle-ci. L'alarme suivante surveille la quantité de trafic sortant des clients de votre VPC via la passerelle NAT vers Internet. Elle envoie une notification lorsque le nombre d'octets atteint un seuil de 5 000 000 au cours d'une période de 15 minutes.

Pour créer une alarme pour votre trafic réseau sortant via la passerelle NAT

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, choisissez Alarms (alertes), All alarms (Toutes les alertes).
3. Choisissez Create alarm (Créer une alerte).
4. Choisissez Sélectionner une métrique.
5. Cliquez sur l'espace de noms de la métrique NatGateway, puis choisissez une dimension de métrique. Lorsque vous accédez aux métriques, cochez la case à côté de la BytesOutToDestinationmétrique pour la passerelle NAT, puis choisissez Select metric.
6. Configurez l'alarme comme suit, puis choisissez Next (Suivant) :

   - Pour Statistics (Statistique), choisissez Sum (Somme).

- Pour Période, choisissez 15 minutes.
- Pour Chaque fois, choisissez Supérieur à/Égal à et saisissez `5000000` pour le seuil.

7. Pour Notification, sélectionnez une rubrique SNS existante ou choisissez Create new topic (Créer une rubrique) pour en créer une nouvelle. Choisissez Next (Suivant).
8. Saisissez le nom et la description de l'alarme, puis choisissez Next (Suivant).
9. Lorsque vous avez terminé la configuration de l'alarme, choisissez Créer une alarme.

Vous pouvez créer une alarme qui contrôle les erreurs d'allocation du port et envoie une notification lorsque la valeur est supérieure à zéro (0) pendant trois périodes consécutives de 5 minutes.

Pour créer une alarme pour contrôler les erreurs d'allocation de port

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, choisissez Alarms (alertes), All alarms (Toutes les alertes).
3. Choisissez Create alarm (Créer une alerte).
4. Choisissez Sélectionner une métrique.
5. Cliquez sur l'espace de noms de la métrique NatGateway, puis choisissez une dimension de métrique. Lorsque vous accédez aux métriques, cochez la case à côté de la ErrorPortAllocationmétrique pour la passerelle NAT, puis choisissez Select metric.
6. Configurez l'alarme comme suit, puis choisissez Next (Suivant) :

   - Pour Statistique, choisissez Maximum.
   - Pour Période, choisissez 5 minutes.
   - Pour Chaque fois, choisissez Supérieur à/Égal à et saisissez 0 pour le seuil.
   - Sous Additional configuration (Configuration supplémentaire), saisissez 3 pour les Points de données à signaler.

7. Pour Notification, sélectionnez une rubrique SNS existante ou choisissez Create new topic (Créer une rubrique) pour en créer une nouvelle. Choisissez Next (Suivant).
8. Saisissez le nom et la description de l'alarme, puis choisissez Next (Suivant).
9. Lorsque vous avez terminé de configurer l'alarme, choisissez Create alarm (Créer une alarme).

Pour plus d'informations, consultez la section Utilisation des CloudWatch alarmes Amazon dans le guide de CloudWatch l'utilisateur Amazon.

Résoudre les problèmes des passerelles NAT

Les rubriques suivantes vous aident à résoudre des problèmes courants que vous pouvez rencontrer quand vous créez ou utilisez une passerelle NAT.

Problèmes

Échec de la création d'une passerelle NAT

Problème

Vous créez une passerelle NAT et obtenez le statut `Failed`.

> **Note**
>
> Une passerelle NAT en échec est automatiquement supprimée, généralement en environ une heure.

Cause

Une erreur s'est produite lors de la création de la passerelle NAT. Le message sur le statut fournit la cause de l'erreur.

Solution

Pour afficher le message d'erreur, accédez à la console Amazon VPC, puis choisissez NAT Gateways (Passerelles NAT). Sélectionnez le bouton radio de votre passerelle NAT, puis recherchez Message d'état dans l'onglet Détails.

Le tableau ci-dessous répertorie les causes possibles d'échec, comme mentionné dans la console Amazon VPC. Après avoir appliqué une des étapes correctives indiquées, vous pouvez à nouveau essayer de créer une passerelle NAT.

Erreur affichée	Cause	Solution
Le sous-réseau ne possède pas assez d'adresses libres pour créer cette passerelle NAT	Le sous-réseau que vous avez spécifié ne possède aucune adresse IP privée libre. La passerelle NAT nécessite une interface réseau avec une adresse IP privée allouée à partir de la plage du sous-réseau.	Vérifiez le nombre d'adresses IP disponibles dans votre sous-réseau en accédant à la page Subnets (Sous-réseaux) de la console Amazon VPC. Vous pouvez afficher les Available IPs (Adresses IP disponibles) dans le volet des détails de votre sous-réseau. Pour créer des adresses IP libres dans votre sous-réseau, vous pouvez supprimer des interfaces réseau inutilisées ou mettre fin à des instances dont vous n'avez pas besoin.
Le réseau vpc-xxxxxxxx n'a pas de passerelle Internet attachée	Une passerelle NAT doit être créée dans un VPC avec une passerelle Internet.	Créez et attachez une passerelle Internet à votre VPC. Pour de plus amples informations, veuillez consulter Utiliser des passerelles Internet.
L'adresse IP Elastic eipalloc-xxxxxxxx est déjà associée	L'adresse IP Elastic que vous avez spécifiée est déjà associée à une autre	Vérifiez les ressources associées à l'adresse IP Elastic. Accédez à la page

Erreur affichée	Cause	Solution
	ressource, et ne peut être associée à la passerelle NAT.	Elastic IPs (Adresses IP Elastic) dans la console Amazon VPC et affichez les valeurs spécifiées pour l'ID d'instance ou l'ID d'interface réseau. Si vous n'avez pas besoin de l'adresse IP Elastic pour cette ressource, vous pouvez la dissocier. Sinon, vous pouvez allouer une nouvelle adresse IP Elastic à votre compte. Pour de plus amples informations, veuillez consulter Utiliser des adresses IP Elastic.

Quota de passerelle NAT

Lorsque vous essayez de créer une passerelle NAT, vous obtenez l'erreur suivante.

```
Performing this operation would exceed the limit of 5 NAT gateways
```

Cause

Vous avez atteint le quota de passerelles NAT pour cette zone de disponibilité.

Solution

Si vous avez atteint le quota de cette passerelle NAT pour votre compte, vous pouvez effectuer l'une des actions suivantes :

- Demandez une augmentation du quota de passerelles NAT par zone de disponibilité à l'aide de la console Service Quotas (Quotas de service).
- Vérifiez le statut de votre passerelle NAT. Un statut `Pending`, `Available` ou `Deleting` compte dans votre quota. Si vous avez récemment supprimé une passerelle NAT, attendez quelques

minutes pour que le statut passe de `Deleting` à `Deleted`. Puis essayez de créer une nouvelle passerelle NAT

- Si vous n'avez pas besoin que votre passerelle NAT soit dans une zone de disponibilité spécifique, essayez de créer une passerelle NAT dans une zone de disponibilité dans laquelle vous n'avez pas atteint votre quota.

Pour plus d'informations, consultez Quotas Amazon VPC.

Quota appliqué aux adresses IP Elastic

Problème

Lorsque vous essayez d'allouer une adresse IP Elastic pour votre passerelle NAT, vous obtenez l'erreur suivante.

```
The maximum number of addresses has been reached.
```

Cause

Vous avez atteint le quota d'adresses IP élastiques pour votre compte de cette Région.

Solution

Si vous avez atteint votre quota d'adresses IP Elastic, vous pouvez dissocier une adresse IP Elastic d'une autre ressource. Vous pouvez également demander une augmentation du quota d'adresses IP Elastic à l'aide de la console Service Quotas (Quotas de service).

Zone de disponibilité non prise en charge

Problème

Lorsque vous essayez de créer une passerelle NAT, vous recevez l'erreur suivante : `NotAvailableInZone`.

Cause

Vous essayez peut-être de créer la passerelle NAT dans une zone de disponibilité limitée dans laquelle votre capacité de développement est limitée.

Solution

Nous ne pouvons pas prendre en charge de passerelles NAT dans ces zones de disponibilité. Vous pouvez créer une passerelle NAT dans une zone de disponibilité différente et l'utiliser pour des sous-réseaux privés dans la zone limitée. Vous pouvez également déplacer vos ressources vers une zone de disponibilité non limitée afin que vos ressources et votre passerelle NAT soient dans la même zone.

La passerelle NAT n'apparaît plus

Problème

Vous avez créé une passerelle NAT, mais elle n'est plus visible dans la console Amazon VPC.

Cause

Une erreur peut être survenue lors de la création de votre passerelle NAT et en avoir entraîné l'échec. Une passerelle NAT avec `Failed` comme statut est visible dans la console Amazon VPC pendant un environ une heure. Puis, au bout d'une heure, elle est automatiquement supprimée.

Solution

Consultez les informations dans Échec de la création d'une passerelle NAT, et essayez de créer une nouvelle passerelle NAT.

La passerelle NAT ne répond pas à la commande ping

Problème

Si vous essayez d'effectuer un test ping de l'adresse IP Elastic ou de l'adresse IP privée de la passerelle NAT depuis Internet (par exemple, depuis votre ordinateur familial) ou depuis une instance de votre VPC, vous n'obtenez pas de réponse.

Cause

Une passerelle NAT fait uniquement passer du trafic depuis une instance d'un sous-réseau privé vers Internet.

Solution

Pour tester si votre passerelle NAT fonctionne, consultez Tester la passerelle NAT publique.

Les instances ne peuvent pas accéder à Internet

Problème

Vous avez créé une passerelle NAT publique et suivi les étapes pour la tester, mais la commande `ping` échoue, ou vos instances du sous-réseau privé ne peuvent pas accéder à Internet.

Causes

L'origine du problème peut être l'une des causes suivantes :

- La passerelle NAT n'est pas prête à traiter le trafic.
- Vos tables de routage ne sont pas configurées correctement.
- Vos groupes de sécurité ou listes ACL réseau bloquent le trafic entrant ou sortant.
- Vous utilisez un protocole non pris en charge.

Solution

Vérifiez les informations suivantes :

- Vérifiez que votre passerelle NAT est en état `Available`. Dans la console Amazon VPC, allez sur la page NAT Gateways (Passerelles NAT) et consultez les informations du statut dans le volet des détails. Si la passerelle NAT est en état d'échec, il y a peut-être eu une erreur quand elle a été créée. Pour plus d'informations, consultez Échec de la création d'une passerelle NAT.
- Vérifiez que vous avez correctement configuré vos tables de routage:
  - La passerelle NAT doit être dans un sous-réseau public avec une table de routage qui route le trafic Internet vers une passerelle Internet.
  - Votre instance doit être dans un sous-réseau privé avec une table de routage qui route le trafic Internet vers la passerelle NAT.
  - Vérifiez qu'aucune autre entrée de la table de routage achemine tout ou une partie du trafic Internet vers un autre périphérique au lieu de la passerelle NAT.
- Assurez-vous que les règles du groupe de sécurité pour votre instance privée autorisent le trafic Internet sortant. Afin que la commande `ping` fonctionne, les règles doivent également autoriser le trafic ICMP sortant.

  La passerelle NAT elle-même autorise le trafic sortant et le trafic reçu en réponse à une demande sortante (elle est donc avec état).
- Assurez-vous que les listes ACL réseau qui sont associées au sous-réseau privé et aux sous-réseaux publics n'ont pas de règles qui bloquent le trafic Internet entrant ou sortant. Afin que la commande `ping` fonctionne, les règles doivent également autoriser le trafic ICMP entrant et sortant.

Vous pouvez autoriser les journaux de flux à vous aider à diagnostiquer les connexions abandonnées à cause de la liste ACL réseau ou des règles du groupe de sécurité. Pour plus d'informations, consultez Journalisation du trafic IP à l'aide des journaux de flux VPC.

- Si vous utilisez la commande `ping`, assurez-vous d'avoir effectué un test ping du site Web dont l'ICMP est activé. Si ICMP n'est pas activé, vous ne recevez pas de paquets de réponse. Pour le tester, exécutez la même commande `ping` depuis le terminal de la ligne de commande sur votre propre ordinateur.
- Vérifiez que votre instance peut effectuer un test ping sur d'autres ressources ; par exemple, d'autres instances dans le sous-réseau privé (en supposant que les règles du groupe de sécurité le permettent).
- Assurez-vous que votre connexion utilise uniquement un protocole TCP, UDP ou ICMP.

Échec de la connexion TCP à une destination

Problème

Certaines de vos vos connexions TCP entre des instances d'un sous-réseau privé et une destination spécifique via une passerelle NAT ont réussi, mais d'autres ont échoué ou dépassé le délai.

Causes

L'origine du problème peut être l'une des causes suivantes :

- Le point de terminaison de destination répond avec des paquets TCP fragmentés. Les passerelles NAT ne prennent pas en charge la fragmentation IP pour TCP ou ICMP. Pour plus d'informations, consultez Comparer des passerelles NAT et des instances NAT..
- L'option `tcp_tw_recycle` est activée sur le serveur distant, connu pour provoquer des problèmes en cas de connexions multiples à partir d'un appareil NAT.

Solutions

Vérifiez si le point de terminaison vers lequel vous essayez de vous connecter répond avec des paquets TCP fragmentés en procédant comme suit :

1. Utilisez une instance d'un sous-réseau public avec une adresse IP publique pour déclencher une réponse assez large pour permettre une fragmentation depuis le point de terminaison spécifique.

2. Utiliser l'utilitaire `tcpdump` pour vérifier que le point de terminaison envoie des paquets fragmentés.

   > **Important**
   >
   > Vous devez utiliser une instance d'un sous-réseau public pour effectuer ces contrôles. Vous ne pouvez pas utiliser l'instance à partir de laquelle la connexion initiale échouait ou une instance dans un sous-réseau privé derrière une passerelle NAT ou une instance NAT.

   Les outils de diagnostic qui envoient ou reçoivent des paquets ICMP volumineux signaleront la perte de paquets. Par exemple, la commande `ping -s 10000 example.com` ne fonctionne pas derrière une passerelle NAT.
3. Si le point de terminaison envoie des paquets TCP fragmentés, vous pouvez utiliser une instance NAT au lieu d'une passerelle NAT.

Si vous avez accès au serveur distant, vous pouvez vérifier si l'option `tcp_tw_recycle` est activée en procédant comme suit :

1. Exécutez la commande suivante à partir du serveur.

   ```
   cat /proc/sys/net/ipv4/tcp_tw_recycle
   ```

   Si la sortie est 1, l'option `tcp_tw_recycle` est activée.
2. Si `tcp_tw_recycle` est activé, nous recommandons de le désactiver. Si vous devez réutiliser des connexions, `tcp_tw_reuse` est une option plus sûre.

Si vous n'avez pas accès au serveur distant, vous pouvez tester en désactivant temporairement l'option `tcp_timestamps` sur une instance du sous-réseau privé. Puis connectez-vous à nouveau au serveur distant. Si la connexion aboutit, il est probable que l'échec précédent était dû au fait que `tcp_tw_recycle` était activé sur le serveur distant. Si possible, contactez le propriétaire du serveur distant pour vérifier si l'option est activée et demandez qu'elle soit désactivée.

La sortie traceroute n'affiche pas l'adresse IP privée de la passerelle NAT

Problème

Votre instance peut accéder à Internet, mais quand vous exécutez la commande `traceroute`, la sortie n'affiche pas l'adresse IP privée de la passerelle NAT.

Cause

Dans ce cas, votre instance accède à Internet en utilisant une passerelle différente, comme une passerelle Internet.

Solution

Dans la table de routage du sous-réseau dans lequel se situe votre instance, vérifiez les informations suivantes :

- Assurez-vous qu'une route envoie le trafic Internet vers la passerelle NAT.
- Assurez-vous qu'il n'y a pas de route plus spécifique qui envoie du trafic Internet vers d'autres périphériques, comme une passerelle réseau privé virtuel ou une passerelle Internet.

La connexion Internet est abandonnée après 350 secondes

Problème

Vos instances peuvent accéder à Internet, mais la connexion s'arrête après 350 secondes.

Cause

Si une connexion utilisant une passerelle NAT est inactive pendant 350 secondes ou plus, la connexion expire.

Lorsqu'une connexion expire, une passerelle NAT retourne un paquet RST à toutes les ressources derrière la passerelle NAT qui tentent de poursuivre la connexion (elle n'envoie pas de paquet FIN).

Solution

Pour empêcher que la connexion soit interrompue, vous pouvez initier plus de trafic sur la connexion. Sinon, vous pouvez activer keepalive TCP sur l'instance avec une valeur inférieure à 350 secondes.

La connexion IPsec ne peut pas être établie

Problème

Vous ne pouvez pas établir de connexion IPsec vers une destination.

Cause

Les passerelles NAT ne prennent pas en charge le protocole IPsec pour le moment.

Solution

Vous pouvez utiliser NAT-Traversal (NAT-T) pour encapsuler le trafic IPsec dans UDP, qui est un protocole pris en charge pour les passerelles NAT. Veillez à tester votre configuration NAT-T et IPsec pour vérifier que votre trafic IPsec n'est pas supprimé.

Impossible d'établir de nouvelles connexions

Problème

Vous avez des connexions existantes vers une destination par le biais d'une passerelle NAT, mais vous ne pouvez pas établir de nouvelles connexions.

Cause

Vous avez peut-être atteint la limite de connexions simultanées pour une même passerelle NAT. Pour plus d'informations, consultez Principes de base d'une passerelle NAT. Si vos instances du sous-réseau privé créent un grand nombre de connexions, il se peut que vous ayez atteint cette limite.

Solution

Effectuez l'une des actions suivantes :

- Créez une passerelle NAT par zone de disponibilité et répartissez vos clients sur ces zones.
- Créez des passerelles NAT supplémentaires dans le sous-réseau public et divisez vos clients sur plusieurs sous-réseaux privés, chacun avec une route vers une passerelle NAT différente.
- Limitez le nombre de connexions que vos clients peuvent créer vers la destination.
- Utilisez la métrique `IdleTimeoutCount` dans CloudWatch pour surveiller les augmentations des connexions inactives. Fermez les connexions inactives pour libérer de la capacité.
- Créez une passerelle NAT avec plusieurs adresses IP ou ajoutez des adresses IP secondaires à une passerelle NAT existante. Chaque nouvelle adresse IPv4 peut prendre en charge jusqu'à 55 000 connexions simultanées. Pour plus d'informations, consultez Créer une passerelle NAT ou Modification des associations d'adresses IP secondaires.

Tarification

Lorsque vous provisionnez une passerelle NAT, chaque heure de disponibilité de votre passerelle NAT et chaque gigaoctet de données qu'elle traite vous sont facturés. Pour de plus amples informations, veuillez consulter la Tarification Amazon VPC.

Les stratégies suivantes peuvent vous aider à réduire les frais de transfert de données de votre passerelle NAT :

- Si vos AWS ressources envoient ou reçoivent un volume de trafic important entre les zones de disponibilité, assurez-vous qu'elles se trouvent dans la même zone de disponibilité que la passerelle NAT. Vous pouvez également créer une passerelle NAT dans chaque zone de disponibilité avec des ressources.
- Si la majeure partie du trafic passant par votre passerelle NAT est destinée à AWS des services qui prennent en charge les points de terminaison d'interface ou les points de terminaison de passerelle, envisagez de créer un point de terminaison d'interface ou un point de terminaison de passerelle pour ces services. Pour de plus amples informations sur les économies potentielles, consultez Tarification AWS PrivateLink.

Instances NAT

Une instance NAT fournit la traduction d'adresses réseau (NAT). Vous pouvez utiliser une instance NAT pour permettre aux ressources d'un sous-réseau privé de communiquer avec des destinations situées en dehors du cloud privé virtuel (VPC), telles qu'Internet ou un réseau sur site. Les ressources du sous-réseau privé peuvent initier le trafic IPv4 sortant vers Internet, mais elles ne peuvent pas recevoir de trafic entrant initié sur Internet.

> **Important**
>
> L'AMI NAT est basée sur la dernière version de l'AMI Amazon Linux, 2018.03, qui a atteint la fin du support standard le 31 décembre 2020 et la fin du support de maintenance le 31 décembre 2023. Pour plus d'informations, consultez le billet de blog sur la fin de vie de l'Amazon Linux AMI.
> Si vous utilisez une AMI NAT existante, il est AWS recommandé de migrer vers une passerelle NAT. Les passerelles NAT offrent une meilleure disponibilité, une bande passante plus importante et elles demandent un moindre effort administratif. Pour plus d'informations, consultez Comparer des passerelles NAT et des instances NAT..

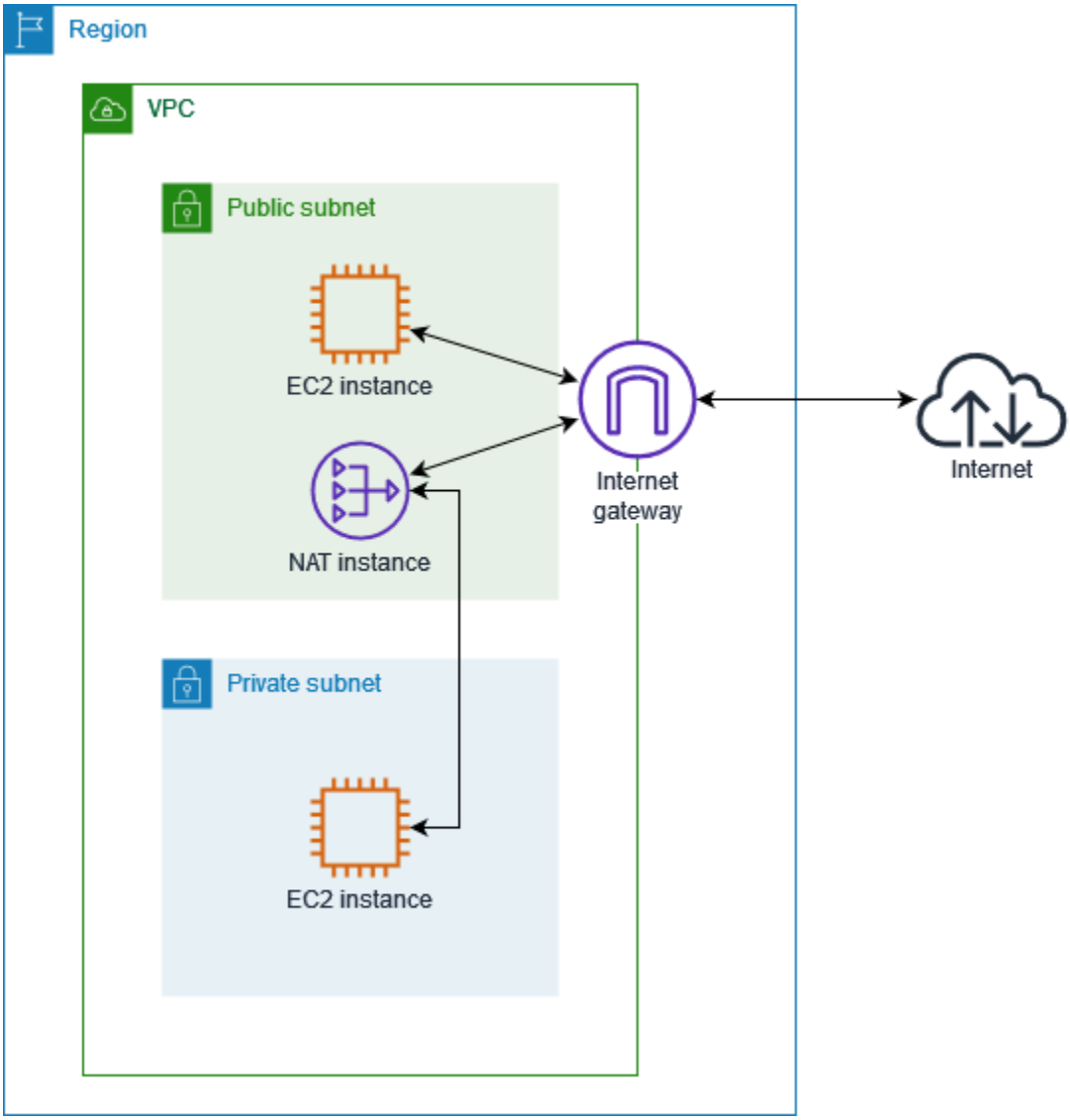
Si les instances NAT correspondent mieux à votre cas d'utilisation que les passerelles NAT, vous pouvez créer votre propre AMI NAT à partir d'une version actuelle d'Amazon Linux, comme décrit dansthe section called "Créer une AMI NAT".

Table des matières

Principes de base d'une instance NAT

Le graphique suivant illustre les principes de base d'une instance NAT. La table de routage associée au sous-réseau privé envoie le trafic Internet depuis les instances du sous-réseau privé vers l'instance NAT dans le sous-réseau public. L'instance NAT envoie ensuite le trafic à la passerelle Internet. Le trafic est attribué à l'adresse IP publique de l'instance NAT. L'instance NAT spécifie un numéro de port élevé pour la réponse ; si une réponse revient, l'instance NAT l'envoie à une instance dans le sous-réseau privé en fonction du numéro de port de la réponse.

L'instance NAT doit avoir un accès à Internet, elle doit donc se trouver dans un sous-réseau public (un sous-réseau qui a une table de routage avec une route vers la passerelle Internet) et disposer d'une adresse IP publique ou d'une adresse IP Elastic.



Pour commencer à utiliser les instances NAT, créez une AMI NAT, créez un groupe de sécurité pour l'instance NAT et lancez l'instance NAT dans votre VPC.

Le quota de votre instance NAT dépend du quota des instances pour la Région. Pour plus d'informations, consultez Quotas du service Amazon EC2 dans le Références générales AWS.

Créer un VPC pour l'instance NAT

Utilisez la procédure suivante pour créer un VPC avec un sous-réseau public et un sous-réseau privé.

Pour créer le VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Sélectionnez Create VPC (Créer un VPC).
3. Sous Resources to create (Ressources à créer), choisissez VPC and more (VPC et autres).
4. Pour Name tag auto-generation (Génération automatique de balises de nom), saisissez un nom pour le VPC.
5. Pour configurer les sous-réseaux, procédez comme suit :
   a. Pour Number of Availability Zones (Nombre de zones de disponibilité), choisissez 1 ou 2, selon vos besoins.
   b. Pour Number of public subnets (Nombre de sous-réseaux publics), assurez-vous de disposer d'un sous-réseau public par zone de disponibilité.
   c. Pour Number of private subnets (Nombre de sous-réseaux privés), assurez-vous de disposer d'un sous-réseau privé par zone de disponibilité.
6. Sélectionnez Create VPC (Créer un VPC).

Créer un groupe de sécurité pour l'instance NAT

Créez un groupe de sécurité avec les règles décrites dans le tableau suivant. Ces règles permettent à votre instance NAT de recevoir du trafic lié à Internet depuis des instances dans le sous-réseau privé, ainsi que du trafic SSH depuis votre réseau. L'instance NAT peut également envoyer le trafic vers Internet pour permettre aux instances du sous-réseau privé de recevoir des mises à jour logicielles.

Les règles recommandées sont décrites ci-dessous.

Entrant

Source	Protocole	Plage de ports	Commentaires
CIDR du sous-réseau privé	TCP	80	Autorisez le trafic HTTP entrant depuis les serveurs dans le sous-réseau privé
CIDR du sous-réseau privé	TCP	443	Autorisez le trafic HTTPS entrant depuis les serveurs dans le sous-réseau privé

Source	Protocole	Plage de ports	Commentaires
Plage d'adresses IP publiques de votre réseau	TCP	22	Autoriser l'accès SSH entrant vers l'instance NAT depuis votre réseau (via la passerelle Internet)

Sortant

Destination	Protocole	Plage de ports	Commentaires
0.0.0.0/0	TCP	80	Autoriser l'accès à Internet du HTTP sortant
0.0.0.0/0	TCP	443	Autoriser l'accès HTTPS sortant à Internet

Pour créer le groupe de sécurité

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez Create security group (Créer un groupe de sécurité).
4. Saisissez un nom et une description pour le groupe de sécurité.
5. Pour VPC, sélectionnez l'ID du VPC pour votre instance NAT.
6. Ajoutez des règles pour le trafic entrant sous Règles entrantes comme suit :
    a. Choisissez Ajouter une règle. Sélectionnez HTTP pour Type et saisissez la plage d'adresses IP de votre sous-réseau privé pour Source.
    b. Choisissez Ajouter une règle. Sélectionnez HTTPS pour Type et saisissez la plage d'adresses IP de votre sous-réseau privé pour Source.
    c. Choisissez Ajouter une règle. Sélectionnez SSH pour Type et saisissez la plage d'adresses IP de votre réseau pour Source.
7. Ajoutez des règles pour le trafic sortant sous Règles sortantes comme suit :

a. Choisissez Ajouter une règle. Choisissez HTTP pour le Type et entrez 0.0.0.0/0 pour Destination.

b. Choisissez Ajouter une règle. Choisissez HTTPS pour le Type et entrez 0.0.0.0/0 pour Destination.

8. Sélectionnez Créer un groupe de sécurité.

Pour plus d'informations, consultez Groupes de sécurité.

Créer une AMI NAT

Une AMI NAT est configurée pour exécuter NAT sur une instance EC2. Vous devez créer une AMI NAT, puis lancer votre instance NAT à l'aide de votre AMI NAT.

Si vous prévoyez d'utiliser un système d'exploitation autre qu'Amazon Linux pour votre AMI NAT, reportez-vous à la documentation de ce système d'exploitation pour savoir comment configurer la NAT. Veillez à enregistrer ces paramètres afin qu'ils soient conservés même après le redémarrage d'une instance.

Pour créer une AMI NAT pour Amazon Linux

1. Lancez une instance EC2 exécutant AL2023 ou Amazon Linux 2. Assurez-vous de spécifier le groupe de sécurité que vous avez créé pour l'instance NAT.
2. Connectez-vous à votre instance et exécutez les commandes suivantes sur l'instance pour activer les iptables.

```
sudo yum install iptables-services -y
sudo systemctl enable iptables
sudo systemctl start iptables
```

3. Procédez comme suit sur l'instance pour activer le transfert d'IP de manière à ce qu'il perdure après le redémarrage :

   a. À l'aide d'un éditeur de texte, tel que nano ou vim, créez le fichier de configuration suivant : `/etc/sysctl.d/custom-ip-forwarding.conf`.

   b. Ajoutez la ligne suivante au fichier de configuration.

```
net.ipv4.ip_forward=1
```

c. Enregistrez le fichier de configuration et quittez l'éditeur de texte.

d. Exécutez la commande suivante pour appliquer le fichier de configuration.

```
sudo sysctl -p /etc/sysctl.d/custom-ip-forwarding.conf
```

4. Exécutez la commande suivante sur l'instance et notez le nom de l'interface réseau principale. Vous aurez besoin de ces informations pour l'étape suivante.

```
netstat -i
```

Dans la sortie de l'exemple suivant, `docker0` est une interface réseau créée par docker, `eth0` est l'interface réseau principale et `lo` est l'interface de bouclage.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0   1500        0      0      0 0             0      0      0      0 BMU
eth0      9001  7276052      0      0 0       5364991      0      0      0 BMRU
lo       65536   538857      0      0 0        538857      0      0      0 LRU
```

Dans la sortie de l'exemple suivant, l'interface réseau principale est `enX0`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enX0      9001     1076      0      0 0          1247      0      0      0 BMRU
lo       65536       24      0      0 0            24      0      0      0 LRU
```

Dans la sortie de l'exemple suivant, l'interface réseau principale est `ens5`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens5      9001    14036      0      0 0          2116      0      0      0 BMRU
lo       65536       12      0      0 0            12      0      0      0 LRU
```

5. Exécutez les commandes suivantes sur l'instance pour configurer le NAT. Si l'interface réseau principale n'est pas `eth0`, remplacez *`eth0`* par l'interface réseau principale que vous avez notée à l'étape précédente.

```
sudo /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo /sbin/iptables -F FORWARD
sudo service iptables save
```

6. Créez une AMI NAT à partir de l'instance EC2. Pour plus d'informations, consultez la section Création d'une AMI Linux à partir d'une instance dans le guide de l'utilisateur Amazon EC2.

Lancer une instance NAT

Utilisez la procédure suivante pour lancer une instance NAT à l'aide du VPC, du groupe de sécurité et de l'AMI NAT que vous avez créés.

Pour lancer une instance NAT

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Sur le tableau de bord, choisissez Lancer une instance.
3. Pour Nom, saisissez un nom pour votre instance NAT.
4. Pour Images d'application et de système d'exploitation, sélectionnez votre AMI NAT (choisissez Parcourir plus d'AMI, Mes AMI).
5. Dans Type d'instance, choisissez un type d'instance fournissant les ressources de calcul, de mémoire et de stockage dont votre instance NAT a besoin.
6. Pour Paire de clés, sélectionnez une paire de clés existante ou choisissez Créer une paire de clés.
7. Sous Network settings (Paramètres réseau), effectuez les opérations suivantes :
   a. Choisissez Modifier.
   b. Pour VPC, choisissez le VPC que vous avez créé.
   c. Pour Sous-réseau, choisissez le sous-réseau public que vous avez créé.
   d. Pour Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer). Vous pouvez également, après avoir lancé l'instance NAT, allouer une adresse IP Elastic et l'attribuer à l'instance NAT.
   e. Pour Pre-feu, choisissez Sélectionner un groupe de sécurité existant, puis choisissez le groupe de sécurité que vous avez créé.
8. Choisissez Launch instance (Lancer une instance). Sélectionnez l'ID de l'instance pour ouvrir la page des détails de l'instance. Attendez que l'état de l'instance passe à En cours d'exécution et que les vérifications de l'état réussissent.
9. Désactiver les vérifications de la source/destination pour l'instance NAT (voir Désactiver des contrôles de source/destination).

10. Mettez à jour la table de routage pour envoyer du trafic vers l'instance NAT (voir Mise à jour de la table de routage).

Désactiver des contrôles de source/destination

Chaque instance EC2 effectue des source/destination checks par défaut. Cela signifie que l'instance doit être la source ou la destination de tout trafic qu'elle envoie ou qu'elle reçoit. Cependant, une instance NAT doit pouvoir envoyer et recevoir du trafic quand elle n'est pas la source ni la destination. Par conséquent, vous devez désactiver les source/destination checks sur l'instance NAT.

Pour désactiver la vérification de la source/destination

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance NAT.
4. Sélectionnez Actions, Mise en réseau, Modifier la vérification de la source/destination.
5. Pour Vérifier la source/destination, sélectionnez Arrêter.
6. Choisissez Enregistrer.
7. Si l'instance NAT possède une interface réseau secondaire, sélectionnez-la depuis Interfaces réseau sous l'onglet Networking (Mise en réseau). Sélectionnez l'ID d'interface pour accéder à la page Network interfaces (Interfaces réseau). Sélectionnez Actions, Change source/dest. check (Changer la vérification de source/destionation), désélectionnez Enable (Activer), puis sélectionnez Save (Enregistrer).

Mise à jour de la table de routage

La table de routage du sous-réseau privé doit contenir une route qui envoie le trafic Internet vers l'instance NAT.

Pour mettre à jour la table de routage

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Route tables (Tables de routage).
3. Sélectionnez la table de routage pour le sous-réseau privé.
4. Sous l'onglet Routes, choisissez Modifier les routes, puis Ajouter une route.
5. Saisissez 0.0.0.0/0 pour Destination et l'ID d'instance de l'instance NAT pour Cible.

6. Sélectionnez Enregistrer les modifications.

Pour plus d'informations, consultez Configuration des tables de routage.

Tester votre instance NAT

Après avoir lancé une instance NAT et effectué les étapes de configuration ci-dessus, vous pouvez tester si une instance de votre sous-réseau privé peut accéder à Internet par l'intermédiaire de l'instance NAT en utilisant l'instance NAT comme serveur bastion.

Tâches

- Étape 1 : mettez à jour le groupe de sécurité de l'instance NAT
- Étape 2 : lancez une instance de test dans le sous-réseau privé
- Étape 3 : envoi d'un ping à un site Web compatible ICMP
- Étape 4 : Nettoyer

Étape 1 : mettez à jour le groupe de sécurité de l'instance NAT

Pour autoriser les instances de votre sous-réseau privé à envoyer du trafic ping à l'instance NAT, ajoutez une règle autorisant le trafic ICMP entrant et sortant. Pour permettre à l'instance NAT de servir de serveur bastion, ajoutez une règle autorisant le trafic SSH sortant vers le sous-réseau privé.

Pour mettre à jour le groupe de sécurité de votre instance NAT

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Cochez la case du groupe de sécurité associé à votre instance NAT.
4. Sous l'onglet Inbound Rules (Règles entrantes), sélectionnez Edit inbound rules (Modifier les règles entrantes).
5. Choisissez Add rule. Sélectionnez Tout ICMP - IPv4 pour Type. Choisissez Personnalisé pour Source et saisissez la plage d'adresses IP de votre sous-réseau privé. Sélectionnez Enregistrer les règles.
6. Sélectionnez Outbound rules (Modifier les règles sortantes) sous l'onglet Outbound rules (Règles sortantes).
7. Choisissez Add rule. Sélectionnez SSH pour Type. Sélectionnez Personnalisé pour Destination et saisissez la plage d'adresses IP de votre sous-réseau privé.

8. Choisissez Add rule. Sélectionnez Tout ICMP - IPv4 pour Type. Choisissez Anywhere - IPv4 (N'importe où - IPv4) pour Destination. Sélectionnez Enregistrer les règles.

Étape 2 : lancez une instance de test dans le sous-réseau privé

Lancez une instance dans votre sous-réseau privé. Vous devez autoriser l'accès SSH depuis l'instance NAT et utiliser la même paire de clés que celle que vous avez utilisée pour l'instance NAT.

Pour lancer une instance de test dans le sous-réseau privé

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Sur le tableau de bord, choisissez Lancer une instance.
3. Sélectionnez votre sous-réseau privé.
4. N'assignez pas d'adresse IP publique à cette instance.
5. Assurez-vous que le groupe de sécurité de cette instance autorise l'accès SSH entrant depuis votre instance NAT ou depuis la plage d'adresses IP de votre sous-réseau public, ainsi que le trafic ICMP sortant.
6. Sélectionnez la même paire de clés que celle que vous avez utilisée pour l'instance NAT.

Étape 3 : envoi d'un ping à un site Web compatible ICMP

Pour vérifier que l'instance de test de votre sous-réseau privé peut utiliser votre instance NAT pour communiquer avec Internet, exécutez la commande ping.

Pour tester la connexion Internet à partir de votre instance privée

1. À partir de votre ordinateur local, configurez le transfert de l'agent SSH afin de pouvoir utiliser l'instance NAT comme serveur bastion.

   Linux and macOS

   ```
   ssh-add key.pem
   ```

   Windows

   Téléchargez et installez Pageant, s'il n'est pas déjà installé.

   Convertissez votre clé privée au format .ppk avec PuTTYgen.

Démarrez Pageant, cliquez avec le bouton droit sur l'icône Pageant de la barre des tâches (il peut être masqué) et choisissez Ajouter une clé. Sélectionnez le fichier .ppk que vous avez créé, saisissez le mot de passe si nécessaire et choisissez Ouvrir.

2. À partir de votre ordinateur local, connectez-vous à votre instance NAT.

   Linux and macOS

   ```
   ssh -A ec2-user@nat-instance-public-ip-address
   ```

   Windows

   Connectez-vous à votre instance NAT à l'aide de PuTTY. Pour Authentification, vous devez sélectionner Autoriser le transfert des agents et laisser Fichier de clé privée pour l'authentification vide.

3. À partir de l'instance NAT, exécutez la commande ping et spécifiez un site Web compatible avec ICMP.

   ```
   [ec2-user@ip-10-0-4-184]$ ping ietf.org
   ```

   Pour vérifier que votre instance NAT dispose d'un accès à Internet, vérifiez que vous avez reçu une sortie telle que la suivante, puis appuyez sur Ctrl+C pour annuler la commande ping. Dans le cas contraire, vérifiez que l'instance NAT se trouve dans un sous-réseau public (sa table de routage contient une route vers une passerelle Internet).

   ```
   PING ietf.org (104.16.45.99) 56(84) bytes of data.
   64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=7.88 ms
   64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.09 ms
   64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=7.97 ms
   ...
   ```

4. Depuis votre instance NAT, connectez-vous à votre instance dans votre sous-réseau privé en utilisant son adresse IP privée.

   ```
   [ec2-user@ip-10-0-4-184]$ ssh ec2-user@private-server-private-ip-address
   ```

5. Depuis votre instance privée, vérifiez que vous pouvez vous connecter à Internet en exécutant la commande ping.

```
[ec2-user@ip-10-0-135-25]$ ping ietf.org
```

Pour vérifier que votre instance privée dispose d'un accès à Internet via l'instance NAT, vérifiez que vous avez reçu une sortie telle que la suivante, puis appuyez sur Ctrl+C pour annuler la commande ping.

```
PING ietf.org (104.16.45.99) 56(84) bytes of data.
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=8.76 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.26 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=8.27 ms
...
```

Résolution des problèmes

Si la commande ping échoue à partir du serveur du sous-réseau privé, procédez comme suit pour résoudre le problème :

- Vérifiez que vous avez effectué un test ping du site Web dont l'ICMP est activé. Dans le cas contraire, votre serveur ne pourra pas recevoir de paquets de réponse. Pour le tester, exécutez la même commande ping depuis un terminal de ligne de commande sur votre propre ordinateur.
- Vérifiez que le groupe de sécurité de votre instance NAT autorise le trafic ICMP entrant provenant de votre sous-réseau privé. Si ce n'est pas le cas, votre instance NAT ne peut pas recevoir la commande ping depuis votre instance privée.
- Vérifiez que vous avez désactivé la vérification source/destination pour votre instance NAT. Pour plus d'informations, consultez Désactiver des contrôles de source/destination.
- Vérifiez que vous avez correctement configuré vos tables de routage. Pour plus d'informations, consultez Mise à jour de la table de routage.

Étape 4 : Nettoyer

Si vous n'avez plus besoin du serveur de test dans le sous-réseau privé, résiliez l'instance afin qu'elle ne vous soit plus facturée. Pour de plus amples informations, veuillez consulter Résilier une instance dans le Guide de l'utilisateur Amazon EC2.

Si vous n'avez plus besoin de l'instance NAT, vous pouvez l'arrêter ou la résilier afin qu'elle ne vous soit plus facturée. Si vous avez créé une AMI NAT, vous pouvez créer une nouvelle instance NAT chaque fois que vous en avez besoin.

Comparer des passerelles NAT et des instances NAT.

Vous trouverez ci-dessous un résumé de haut niveau des différences entre les instances NAT et les passerelles NAT. Nous vous recommandons d'utiliser des passerelles NAT car elles offrent une disponibilité et une bande passante supérieures, et nécessitent moins d'efforts d'administration de votre part.

Attribut	Passerelle NAT	Instance NAT
Disponibilité	Hautement disponible. Les passerelles NAT dans chaque zone de disponibilité sont implémentées de manière redondante. Créez une passerelle NAT dans chaque zone de disponibilité pour assurer une architecture de zone indépendante.	Utilisez un script pour gérer le failover entre les instances.
Bande passante	Augmentez l'échelle à 100 Gbit/s.	Dépend de la bande passante du type d'instance.
Maintenance	Géré par AWS. Vous n'avez aucune maintenance à réaliser.	Gérée par vous, par exemple, en installant des mises à jour logicielles ou des correctifs de système d'exploitation sur l'instance.
Performances	Le logiciel est optimisé pour gérer le trafic NAT.	Une AMI générique configurée pour exécuter NAT.
Coût	Facturé en fonction du nombre de passerelles NAT que vous utilisez, de la durée de leur utilisation et de la quantité de données que vous envoyez via les passerelles NAT.	Facturé en fonction du nombre d'instances NAT que vous utilisez, de la durée de leur utilisation et du type d'instance ainsi que leur taille.

Attribut	Passerelle NAT	Instance NAT
Type et taille	Offre homogène ; vous n'avez pas besoin de décider du type ou de la taille.	Choisissez un type et une taille d'instance adaptés à la charge de travail que vous prévoyez.
Adresses publiques	Choisissez l'adresse IP Elastic à associer à une passerelle NAT publique lors de sa création.	Utilisez une adresse IP Elastic ou une adresse IP publique avec une instance NAT. Vous pouvez modifier l'adresse IP publique à tout moment en associant une nouvelle adresse IP Elastic à l'instance.
Adresses privées	Automatiquement sélectionnées dans la plage d'adresses IP du sous-réseau quand vous créez la passerelle.	Assignation d'une adresse IP privée spécifique depuis la plage d'adresses IP du sous-réseau quand vous lancez l'instance.
Groupes de sécurité	Vous ne pouvez pas associer de groupes de sécurité à des passerelles NAT. Vous pouvez en associer aux ressources derrière la passerelle NAT pour contrôler le trafic entrant et sortant.	Associés à votre instance NAT et aux ressources derrière l'instance NAT pour contrôler le trafic entrant et sortant.
Listes ACL réseau	Utilisez une liste ACL réseau pour contrôler le trafic à destination et en provenance du sous-réseau dans lequel votre passerelle NAT réside.	Utilisez une liste ACL réseau pour contrôler le trafic à destination et en provenance du sous-réseau dans lequel votre instance NAT réside.
Journaux de flux	Utilisez des journaux de flux pour capturer le trafic.	Utilisez des journaux de flux pour capturer le trafic.
Réacheminement de port	Non pris en charge.	Personnalisez manuellement la configuration pour prendre en charge le réacheminement de port.
Serveurs bastion	Non pris en charge.	Utilisés comme un serveur bastion.

Attribut	Passerelle NAT	Instance NAT
Métriques du trafic	Affichez les métriques CloudWatch pour la passerelle NAT.	Affichez CloudWatch les métriques de l'instance.
Comportement en cas d'expiration	Lorsqu'une connexion expire, une passerelle NAT retourne un paquet RST à toutes les ressources derrière la passerelle NAT qui tentent de poursuivre la connexion (elle n'envoie pas de paquet FIN).	Lorsqu'une connexion expire, une instance NAT envoie un paquet FIN aux ressources derrière l'instance NAT afin de fermer la connexion.
Fragmentation IP	Prend en charge la transmission de paquets fragmentés IP pour le protocole UDP. Ne prend pas en charge la fragmentation pour les protocoles TCP et ICMP. Les paquets fragmentés pour ces protocoles seront supprimés.	Prend en charge la reconstitution des paquets fragmentés IP pour les protocoles TCP, UDP et ICMP.

Migration d'une instance NAT vers une passerelle NAT

Si vous utilisez déjà une instance NAT, nous vous recommandons de la remplacer par une passerelle NAT. Vous pouvez créer une passerelle NAT dans le même sous-réseau que votre instance NAT, puis remplacer l'acheminement existant dans votre table de routage qui pointe vers l'instance NAT par un acheminement qui pointe vers la passerelle NAT. Pour utiliser la même adresse IP Elastic pour la passerelle NAT que celle que vous utilisez actuellement pour votre instance NAT, vous devez d'abord dissocier l'adresse IP élastique de votre instance NAT, puis l'associer à votre passerelle NAT au moment de créer la passerelle.

Si vous modifiez votre routage d'une instance NAT à une passerelle NAT, ou si vous dissociez l'adresse IP Elastic de votre instance NAT, toutes les connexions en cours sont abandonnées et doivent être rétablies. Assurez-vous de ne pas avoir de tâches importantes (ou toute autre tâche qui fonctionne via l'instance NAT) en cours d'exécution.

Associer des adresses IP Elastic à des ressources dans votre VPC

Une adresse IP Elastic est une adresse IPv4 publique statique conçue pour le cloud computing dynamique. Vous pouvez associer une adresse IP Elastic à n'importe quelle instance ou interface réseau pour n'importe quel VPC de votre compte. Avec une adresse IP Elastic, vous pouvez contourner un problème de défaillance d'une instance en remappant rapidement l'adresse vers une autre instance de votre VPC.

Concepts et règles d'adresse IP Elastic

Pour utiliser une adresse IP Elastic, vous devez d'abord l'allouer pour l'utiliser dans votre compte. Ensuite, vous pouvez l'associer à une instance ou une interface réseau de votre VPC. Votre adresse IP Elastic reste attribuée à votre AWS compte jusqu'à ce que vous la divulguiez explicitement.

Une adresse IP Elastic est une propriété d'une interface réseau. Vous pouvez associer une adresse IP Elastic à une instance en mettant à jour l'interface réseau attachée à l'instance. Veuillez noter que l'avantage d'associer une adresse IP Elastic à l'interface réseau au lieu de l'associer directement à l'instance est que vous pouvez déplacer tous les attributs de l'interface réseau d'une instance vers une autre en une seule étape. Pour plus d'informations, consultez la section Elastic network interfaces dans le guide de l'utilisateur Amazon EC2.

Les règles suivantes s'appliquent :

- Une adresse IP Elastic peut être associée à une seule instance ou interface réseau à la fois.
- Vous pouvez déplacer une adresse IP Elastic d'une instance ou d'une interface réseau vers une autre.
- Si vous associez une adresse IP Elastic à l'interface réseau eth0 de votre instance, son adresse IPv4 publique actuelle (si elle en avait une) est libérée vers le groupe d'adresses IP publiques EC2-VPC. Si vous dissociez l'adresse IP Elastic, l'interface réseau eth0 est automatiquement assignée à une nouvelle adresse IPv4 publique en quelques minutes. Cette règle ne s'applique pas si vous avez attaché une seconde interface réseau à votre instance.
- Vous êtes limité à cinq adresses IP Elastic. Pour les conserver, vous pouvez utiliser un périphérique NAT. Pour plus d'informations, consultez Connectez-vous à Internet ou à d'autres réseaux à l'aide de périphériques NAT.
- Les adresses IP Elastic pour IPv6 ne sont pas prises en charge.

- Vous pouvez baliser une adresse IP Elastic allouée pour être utilisée dans un VPC, mais les balises d'allocation des coûts ne sont pas prises en charge. Si vous récupérez une adresse IP Elastic, les balises ne sont pas récupérées.
- Vous pouvez accéder à une adresse IP Elastic à partir d'Internet lorsque le groupe de sécurité et la liste ACL réseau autorisent le trafic à partir de l'adresse IP source. Le trafic de réponse depuis le VPC vers Internet nécessite une passerelle Internet. Pour de plus amples informations, veuillez consulter Groupes de sécurité et Listes ACL réseau.
- Vous pouvez utiliser l'une des options suivantes pour les adresses IP Elastic :
  - Demander à Amazon de fournir les adresses IP Elastic. Lorsque vous sélectionnez cette option, vous pouvez associer les adresses IP Elastic à un groupe de bordure réseau. C'est l'endroit à partir duquel nous publions le bloc d'adresse CIDR. La définition du groupe de bordure réseau limite le bloc d'adresse CIDR à ce groupe.
  - Utilisez vos propres adresses IP Pour plus d'informations sur l'apport de vos propres adresses IP, consultez la section Bring your own IP addresses (BYOIP) dans le guide de l'utilisateur Amazon EC2.

Les adresses IP Elastic sont régionales. Pour en savoir plus sur l'utilisation de Global Accelerator pour provisionner des adresses IP globales, consultez Utilisation d'adresses IP statiques mondiales au lieu d'adresses IP statiques régionales dans le Guide du développeur AWS Global Accelerator .

Utiliser des adresses IP Elastic

Les sections suivantes expliquent comment utiliser les adresses IP Elastic.

Tâches

- allouer une adresse IP Elastic ;
- Associer une adresse IP Elastic
- Afficher vos adresses IP Elastic
- Baliser une adresse IP Elastic
- Dissocier une adresse IP Elastic
- Transfert d'adresses IP Elastic
- Libérer une adresse IP Elastic
- Récupérer une adresse IP Elastic
- Présentation des API et des commandes

allouer une adresse IP Elastic ;

Avant d'utiliser une adresse IP Elastic, vous devez en allouer une pour une utilisation dans votre VPC.

Pour allouer une adresse IP Elastic

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Elastic IPs.
3. Choisissez Allocate Elastic IP address (Allouer l'adresse IP Elastic).
4. (Facultatif) Lorsque vous allouez une adresse IP Elastc (EIP), vous choisissez le Groupe de bordures réseau dans lequel vous souhaitez allouer l'EIP. Un groupe frontalier réseau est un ensemble de zones de disponibilité (AZ), de zones Locales ou de zones de longueur d'onde à partir AWS duquel est annoncée une adresse IP publique. Les zones Locales et les Zones de longueur d'onde peuvent avoir des groupes de frontières de réseau différents de ceux des zones de disponibilité d'une région afin de garantir une latence minimale ou une distance physique minimale entre le AWS réseau et les clients accédant aux ressources de ces zones.

   > **Important**
   >
   > Vous devez allouer un EIP dans le même groupe frontalier du réseau que la AWS ressource qui sera associée à l'EIP. Une EIP appartenant à un groupe de bordures réseau ne peut être annoncée que dans les zones de ce groupe de bordures réseau et dans aucune autre zone représentée par d'autres groupes de bordures réseau.

   Si vous avez des zones locales ou des zones Wavelength qui sont activées (pour plus d'informations, consultez Enable a Local Zone ou Enable Wavelength Zones), vous pouvez choisir un groupe de bordures réseau pour les zones de disponibilité, les zones locales ou les zones Wavelength. Choisissez le groupe de bordure du réseau avec soin, car l'EIP et la AWS ressource à laquelle il est associé doivent résider dans le même groupe de bordure du réseau. Vous pouvez utiliser la console EC2 pour afficher le groupe de bordures réseau dans lequel se trouvent vos zones de disponibilité, vos zones locales ou vos zones Wavelength (voir Local Zones). En général, toutes les zones de disponibilité d'une région appartiennent au même groupe de bordures réseau, tandis que les zones locales ou les zones Wavelength appartiennent à leurs propres groupes de bordures réseau distincts.

Si vous n'avez pas de zones locales ou de zones Wavelength activées, lorsque vous allouez une EIP, le groupe de bordures réseau qui représente toutes les zones de disponibilité de la région (par exemple, `us-west-2`) est prédéfini pour vous et vous ne pouvez pas le modifier. Cela signifie que l'EIP que vous allouez à ce groupe de bordures réseau sera annoncée dans toutes les zones de disponibilité de la région dans laquelle vous vous trouvez.

5. Pour Public IPv4 address pool (Groupe d'adresses IPv4 publiques), choisissez l'une des options suivantes :

   - Amazon's pool of IP addresses (Groupes d'adresses IP d'Amazon) : À utiliser si vous souhaitez qu'une adresse IPv4 soit allouée à partir du groupe d'adresses IP d'Amazon.
   - Mon pool d'adresses IPv4 publiques : si vous souhaitez allouer une adresse IPv4 à partir d'un pool d'adresses IP que vous avez intégré à votre compte. AWS Cette option est désactivée si vous ne disposez pas de groupes d'adresses IP.
   - Customer owned pool of IPv4 addresses (Groupe d'adresses IPv4 appartenant au client) : si vous souhaitez allouer une adresse IPv4 depuis un groupe créé à partir de votre réseau sur site pour une utilisation avec un Outpost. Cette option n'est disponible que si vous disposez d'un Outpost.

6. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une balise] Choisissez Ajouter une nouvelle balise et procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Value (Valeur), saisissez la valeur de clé.

   [Supprimer une balise] Choisissez Supprimer à la droite de la clé et de la valeur de la balise.

7. Choisissez Allocate.

Associer une adresse IP Elastic

Vous pouvez associer une adresse IP Elastic à une instance en cours d'exécution ou une interface réseau dans votre VPC.

Après avoir associé l'adresse IP Elastic à votre instance, celle-ci reçoit un nom d'hôte DNS si les noms d'hôte DNS sont activés. Pour plus d'informations, consultez Attributs DNS pour votre VPC.

Associer une adresse IP Elastic à une instance ou une interface réseau

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Adresses IP Elastic.
3. Sélectionnez une adresse IP Elastic qui est allouée pour être utilisée avec un VPC (la colonne Scope (Étendue) a la valeur `vpc`), choisissez Actions, puis Associate address (Associer une adresse).
4. Choisissez Instance ou Network interface, puis sélectionnez l'ID d'instance ou d'interface réseau. Sélectionnez l'adresse IP privée à laquelle associer l'adresse IP Elastic. Choisissez Associate.

Afficher vos adresses IP Elastic

Vous pouvez afficher les adresses IP Elastic qui sont allouées à votre compte.

Voir vos adresses IP Elastic

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Adresses IP Elastic.
3. Pour filtrer la liste affichée, commencez à taper une partie de l'adresse IP Elastic ou l'un de ses attributs dans la zone de recherche.

Baliser une adresse IP Elastic

Vous pouvez appliquer des balises à votre adresse IP Elastic afin de l'identifier ou de la classer en fonction des besoins de votre organisation.

Pour baliser une adresse IP Elastic

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Adresses IP Elastic.
3. Sélectionnez l'adresse IP Elastic et choisissez Tags.
4. Sélectionnez Manage tags (Gérer les balises), entrez les clés et valeurs de balises requises, puis choisissez Save (Enregistrer).

Dissocier une adresse IP Elastic

Pour modifier la ressource à laquelle l'adresse IP Elastic est associée, vous devez d'abord la dissocier de la ressource actuellement associée.

Dissocier une adresse IP Elastic

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Adresses IP Elastic.
3. Sélectionnez l'adresse IP Elastic, puis choisissez Actions, Disassociate Elastic IP address (Dissocier l'adresse IP Elastic).
4. A l'invite, choisissez Disassociate (Dissocier).

Transfert d'adresses IP Elastic

Cette section décrit comment transférer des adresses IP Elastic d'un compte Compte AWS à un autre. Le transfert d'adresses IP Elastic peut être utile dans les situations suivantes :

- Restructuration organisationnelle : utilisez les transferts d'adresses IP élastiques pour déplacer rapidement les charges de travail de l'une Compte AWS à l'autre. Vous n'avez pas besoin d'attendre que les nouvelles adresses IP Elastic soient autorisées dans vos groupes de sécurité et vos NACL.
- Administration centralisée de la sécurité : utilisez un compte AWS de sécurité centralisé pour suivre et transférer les adresses IP élastiques dont la conformité en matière de sécurité a été vérifiée.
- Reprise après sinistre : utilisez les transferts d'adresses IP Elastic pour remapper rapidement les adresses IP des charges de travail Internet accessibles au public dans les situations d'urgence.

Le transfert d'adresses IP Elastic est gratuit.

Tâches

- Activation du transfert d'adresses IP Elastic
- Désactivation du transfert d'adresses IP Elastic
- Acceptation d'une adresse IP Elastic transférée

Activation du transfert d'adresses IP Elastic

Cette section décrit comment accepter une adresse IP Elastic transférée. Notez les limitations suivantes en ce qui concerne l'activation des adresses IP Elastic pour le transfert :

- Vous pouvez transférer les adresses IP Elastic de n'importe quel Compte AWS (compte source) vers n'importe quel autre AWS compte de la même AWS région (compte de transfert).
- Lorsque vous transférez une adresse IP Elastic, il existe une liaison en deux étapes entre les Comptes AWS. Lorsque le compte source lance le transfert, les comptes de transfert ont sept jours pour accepter le transfert de l'adresse IP Elastic. Pendant ces sept jours, le compte source peut consulter le transfert en attente (par exemple dans la AWS console ou à l'aide de la commande AWS CLI describe-address-transfers). Au bout de sept jours, le transfert expire et la propriété de l'adresse IP Elastic revient au compte source.
- Les transferts acceptés sont visibles sur le compte source (par exemple dans la AWS console ou à l'aide de la AWS CLI commande describe-address-transfers) pendant trois jours après leur acceptation.
- AWS n'informe pas les comptes de transfert des demandes de transfert d'adresse IP Elastic en attente. Le propriétaire du compte source doit informer le propriétaire du compte de transfert qu'il doit accepter une demande de transfert d'adresse IP Elastic.
- Toutes les balises associées à une adresse IP Elastic en cours de transfert sont réinitialisées lorsque le transfert est terminé.
- Vous ne pouvez pas transférer les adresses IP élastiques allouées à partir de pools d'adresses IPv4 publics que vous apportez à votre Compte AWS compte, communément appelés pools d'adresses BYOIP (Bring Your Own IP).
- Si vous tentez de transférer une adresse IP Elastic à laquelle est associé un enregistrement DNS inversé, vous pouvez lancer le processus de transfert, mais le compte de transfert ne sera pas en mesure de l'accepter tant que l'enregistrement DNS associé n'aura pas été supprimé.
- Si vous avez activé et configuré AWS Outposts, vous avez peut-être alloué des adresses IP élastiques à partir d'un pool d'adresses IP (CoIP) appartenant au client. Vous ne pouvez pas transférer des adresses IP Elastic attribuées à partir d'un groupe CoIP. Cependant, vous pouvez l'utiliser AWS RAM pour partager une CoIP avec un autre compte. Pour plus d'informations, voir Adresses IP appartenant au client dans le Guide de l'utilisateur AWS Outposts .
- Vous pouvez utiliser Amazon VPC IPAM pour suivre le transfert d'adresses IP Elastic vers les comptes d'une organisation depuis AWS Organizations. Pour plus d'informations, voir Afficher l'historique des adresses IP. Cependant, si une adresse IP Elastic est transférée vers un compte

Compte AWS en dehors de l'organisation, l'historique d'audit IPAM de l'adresse IP Elastic sera perdu.

Cette procédure doit être suivie par le compte source.

Pour activer le transfert d'adresses IP Elastic

1. Assurez-vous d'utiliser le AWS compte source.
2. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
3. Dans le panneau de navigation, choisissez Adresses IP Elastic.
4. Sélectionnez une ou plusieurs adresses IP Elastic à activer pour le transfert, puis choisissez Actions, Enable transfer (Activer le transfert).
5. Si vous transférez plusieurs adresses IP Elastic, l'option Transfer type (Type de transfert) s'affiche. Choisissez l'une des options suivantes :
   - Choisissez Compte unique si vous transférez les adresses IP élastiques vers un seul AWS compte.
   - Choisissez Plusieurs comptes si vous transférez les adresses IP élastiques vers plusieurs AWS comptes.
6. Dans Transfer account ID (ID de compte de transfert), saisissez les ID des comptes AWS vers lesquels vous souhaitez transférer les adresses IP Elastic.
7. Confirmez le transfert en saisissant **`enable`** dans la zone de texte.
8. Sélectionnez Envoyer.
9. Pour accepter le transfert, voir Acceptation d'une adresse IP Elastic transférée. Pour désactiver le transfert, voir Désactivation du transfert d'adresses IP Elastic.

Désactivation du transfert d'adresses IP Elastic

Cette section décrit comment désactiver un transfert d'adresses IP Elastic après que le transfert ait été activé.

Ces étapes doivent être effectuées par le compte source qui a activé le transfert.

Pour désactiver un transfert d'adresse IP Elastic

1. Assurez-vous d'utiliser le AWS compte source.

2. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
3. Dans le panneau de navigation, choisissez Adresses IP Elastic.
4. Dans la liste des ressources des adresses IP Elastic, assurez-vous que la propriété qui affiche la colonne Transfer status (État du transfert) est activée.
5. Sélectionnez une ou plusieurs adresses IP Elastic dont Transfer status (État du transfert) est Pending (En attente), puis choisissez Actions, Disable transfer (Désactiver le transfert).
6. Confirmez en saisissant **`disable`** dans la zone de texte.
7. Sélectionnez Envoyer.

Acceptation d'une adresse IP Elastic transférée

Cette section décrit comment accepter une adresse IP Elastic transférée.

Lorsque vous transférez une adresse IP Elastic, il existe une liaison en deux étapes entre les Comptes AWS. Lorsque le compte source lance le transfert, les comptes de transfert ont sept jours pour accepter le transfert de l'adresse IP Elastic. Pendant ces sept jours, le compte source peut consulter le transfert en attente (par exemple dans la AWS console ou à l'aide de la commande AWS CLI describe-address-transfers). Au bout de sept jours, le transfert expire et la propriété de l'adresse IP Elastic revient au compte source.

Lorsque vous acceptez des transferts, notez les exceptions suivantes qui peuvent se produire et comment les résoudre :

- AddressLimitDépassé : si votre compte de transfert a dépassé le quota d'adresses IP Elastic, le compte source peut activer le transfert d'adresses IP Elastic, mais cette exception se produit lorsque le compte de transfert essaie d'accepter le transfert. Par défaut, tous les AWS comptes sont limités à 5 adresses IP élastiques par région. Consultez la section Limite d'adresse IP élastique dans le guide de l'utilisateur Amazon EC2 pour obtenir des instructions sur l'augmentation de cette limite.
- InvalidTransfer. AddressCustomPtrSet: Si vous ou un membre de votre organisation avez configuré l'adresse IP élastique que vous essayez de transférer pour utiliser la recherche DNS inversée, le compte source peut activer le transfert pour l'adresse IP élastique, mais cette exception se produit lorsque le compte de transfert essaie d'accepter le transfert. Pour résoudre ce problème, le compte source doit supprimer l'enregistrement DNS de l'adresse IP Elastic. Pour plus d'informations, consultez Supprimer un enregistrement DNS inversé dans le guide de l'utilisateur Amazon EC2.

- InvalidTransfer. AddressAssociated: Si une adresse IP élastique est associée à une instance ENI ou EC2, le compte source peut activer le transfert pour l'adresse IP élastique, mais cette exception se produit lorsque le compte de transfert essaie d'accepter le transfert. Pour résoudre ce problème, le compte source doit dissocier l'adresse IP Elastic. Pour plus d'informations, consultez Dissocier une adresse IP élastique dans le guide de l'utilisateur Amazon EC2.

Pour toute autre exception, contactez AWS Support.

Cette procédure doit être suivie par le compte de transfert.

Pour accepter un transfert d'adresse IP Elastic

1. Assurez-vous d'utiliser le compte de transfert.
2. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
3. Dans le panneau de navigation, choisissez Adresses IP Elastic.
4. Choisissez Actions, puis Accept transfer (Accepter le transfert).
5. Aucune balise associée à l'adresse IP Elastic transférée n'est transférée avec l'adresse IP Elastic lorsque vous acceptez le transfert. Si vous souhaitez définir une balise Name (Nom) pour l'adresse IP Elastic que vous acceptez, sélectionnez Create a tag with a key of 'Name' and a value that you specify (Créer une balise avec la clé « Nom » et une valeur que vous spécifiez).
6. Saisissez l'adresse IP Elastic que vous voulez transférer.
7. Si vous acceptez plusieurs adresses IP Elastic transférées, choisissez Add address (Ajouter une adresse) pour saisir une adresse IP Elastic supplémentaire.
8. Sélectionnez Envoyer.

Libérer une adresse IP Elastic

Si vous n'avez plus besoin d'une adresse IP Elastic, nous vous recommandons de la libérer. Toute adresse IP Elastic allouée pour être utilisée avec un VPC mais qui n'est pas associée à une instance vous est facturée. L'adresse IP Elastic ne doit pas être associée à une instance ou à une interface réseau.

Libérer une adresse IP Elastic

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Adresses IP Elastic.

3. Sélectionnez l'adresse IP Elastic à libérer, puis choisissez Actions, Release Elastic IP addresses (Libérer des adresses IP Elastic).
4. Lorsque vous y êtes invité, choisissez Libérer.

Récupérer une adresse IP Elastic

Si vous avez libéré une adresse IP Elastic mais vous changez d'avis, vous pouvez essayer de la récupérer. Vous ne pouvez pas récupérer l'adresse IP Elastic si elle a été attribuée à un autre AWS compte ou si sa récupération entraîne un dépassement de votre quota d'adresses IP Elastic.

Vous pouvez récupérer une adresse IP Elastic à l'aide de l'API Amazon EC2 ou d'un outil de ligne de commande.

Pour récupérer une adresse IP élastique à l'aide du AWS CLI

Utilisez la commande allocate-address et précisez l'adresse IP à l'aide du paramètre `--address`.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

Présentation des API et des commandes

Vous pouvez exécuter les tâches décrites sur cette section à l'aide de la ligne de commande ou d'une API. Pour plus d'informations sur les interfaces de ligne de commande et la liste des actions liées aux API disponibles, consultez Utilisation d'Amazon VPC.

Accepter le transfert d'une adresse IP Elastic

- accept-address-transfer (AWS CLI)
- Approve-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Allouer une adresse IP Elastic

- allocate-address (AWS CLI)
- New-EC2Address (AWS Tools for Windows PowerShell)

Associer une adresse IP Elastic à une instance ou une interface réseau

- associate-address (AWS CLI)

- Register-EC2Address (AWS Tools for Windows PowerShell)

Décrire des transferts d'adresses IP Elastic

- describe-address-transfers (AWS CLI)
- Get-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Désactivation du transfert d'adresses IP Elastic

- disable-address-transfer (AWS CLI)
- Disable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Dissocier une adresse IP Elastic

- disassociate-address (AWS CLI)
- Unregister-EC2Address (AWS Tools for Windows PowerShell)

Activation du transfert d'adresses IP Elastic

- enable-address-transfer (AWS CLI)
- Enable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Libérer une adresse IP Elastic

- release-address (AWS CLI)
- Remove-EC2Address (AWS Tools for Windows PowerShell)

Baliser une adresse IP Elastic

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Afficher vos adresses IP Elastic

- describe-addresses (AWS CLI)

- Get-EC2Address (AWS Tools for Windows PowerShell)

Tarification

Pour garantir une utilisation efficace des adresses IP Elastic, nous imposons une petite redevance horaire. Pour plus d'informations, consultez Adresse IPv4 publique dans Tarification d'Amazon VPC.

Connectez votre VPC à d'autres VPC et réseaux à l'aide d'une passerelle de transit

Vous pouvez connecter vos clouds privés virtuels (VPC) et les réseaux sur site à l'aide d'une passerelle de transit, qui agit comme un hub central, acheminant le trafic entre les VPC, les connexions VPN et les connexions AWS Direct Connect. Pour plus d'informations, consultez AWS Transit Gateway.

Le tableau suivant décrit certains cas d'utilisation courants pour les passerelles de transit et fournit des liens vers des informations supplémentaires dans le Amazon VPC Transit Gateways (Passerelles de transit Amazon VPC).

Exemple	Utilisation
Routeur centralisé	Configurez votre passerelle Transit Gateway en tant que routeur centralisé qui connecte tous vos VPC, AWS Direct Connect et les connexions AWS Site-to-Site VPN. Pour de plus amples informations, veuillez consulter la section Exemple : routeur centralisé.
VPC isolés	Configurez votre passerelle Transit Gateway en tant que routeurs isolés multiples. Cela revient à utiliser plusieurs passerelles de transit, tout en offrant une plus grande flexibilité dans les cas où les routes et les attachements peuvent changer. Pour de plus amples informations, veuillez consulter la section Exemple : VPC isolés.
VPC isolés avec services partagés	Configurez votre passerelle Transit Gateway en tant que routeurs isolés multiples qui utilisent un service partagé. Cela revient à utiliser plusieurs passerelles de transit, tout en offrant

Exemple	Utilisation
	une plus grande flexibilité dans les cas où les routes et les attachements peuvent changer. Pour plus d'informations, veuillez consulter la section Exemple : VPC isolés avec services partagés.

Connexion de votre VPC à des réseaux distants utilisant AWS Virtual Private Network

Vous pouvez connecter votre VPC à des réseaux et utilisateurs distants en utilisant les options de connectivité VPN suivantes.

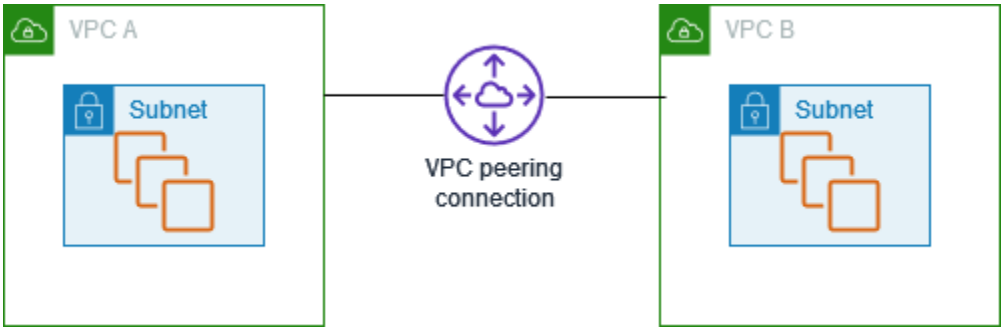
Option de connectivité VPN	Description
AWS Site-to-Site VPN	Vous pouvez créer une connexion VPN IPsec entre votre VPC et votre réseau distant. Du côté AWS de la connexion Site-to-Site VPN, une passerelle réseau privé virtuel ou une passerelle de transit fournit deux points de terminaison VPN (tunnels) pour un basculement automatique. Vous configurez votre appareil de passerelle client du côté distant de la connexion Site-to-Site VPN. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS Site-to-Site VPN.
AWS Client VPN	AWS Client VPN est un service VPN géré basé sur le client qui vous permet d'accéder de façon sécurisée à vos ressources AWS ou à votre réseau sur site. Avec AWS Client VPN, vous configurez un point de terminaison auquel vos utilisateurs peuvent se connecter pour établir une session VPN TLS sécurisée. Cela permet aux clients d'accéder à des ressources dans AWS ou sur site à partir de n'importe quel endroit en utilisant un client VPN basé sur OpenVPN. Pour plus d'informations, consultez le Guide d'administration AWS Client VPN.
AWS VPN CloudHub	Si vous avez plus d'un réseau distant (par exemple, plusieurs succursales), vous pouvez créer plusieurs connexions AWS Site-to-Site VPN via votre passerelle réseau privé virtuel pour permettre la communication

Option de connectivité VPN	Description
	entre ces réseaux. Pour de plus amples informations, veuillez consulter Fourniture d'une communication sécurisée entre les sites à l'aide du VPN CloudHub dans le Guide de l'utilisateur AWS Site-to-Site VPN.
Appliance VPN logicielle tierce	Vous pouvez créer une connexion VPN vers votre réseau distant en utilisant une instance Amazon EC2 dans votre VPC qui exécute une appliance VPN logicielle tierce. AWS ne fournit ni ne gère aucune appliance VPN logicielle tierce ; cependant, vous pouvez choisir parmi une large gamme de produits proposés par nos partenaires et les communautés open source. Vous trouverez des appliances VPN logiciell es tierces sur le AWS Marketplace.

Vous pouvez aussi utiliser AWS Direct Connect pour établir une connexion privée dédiée depuis un réseau distant vers votre VPC. Vous pouvez combiner cette connexion à un AWS Site-to-Site VPN pour créer une connexion à chiffrement IPsec. Pour plus d'informations, consultez Présentation de AWS Direct Connect dans le Guide de l'utilisateur AWS Direct Connect.

Connexion de VPC avec l'appairage de VPC

Une connexion d'appairage de VPC est une connexion de mise en réseau entre deux VPC qui permet de router le trafic entre ces derniers de manière privée. Les ressources des VPC appairés peuvent communiquer entre elles comme si elles se trouvaient dans le même réseau. Vous pouvez créer une connexion d'appairage de VPC entre vos propres VPC, avec un VPC situé dans un autre Compte AWS ou avec un VPC au sein d'une autre Région AWS. Le trafic entre des VPC appairés ne traverse pas l'Internet public.



AWS utilise l'infrastructure existante d'un VPC pour créer la connexion d'appairage de VPC. Une connexion d'appairage de VPC n'est ni une passerelle, ni une connexion AWS Site-to-Site VPN et elle ne repose pas sur un élément matériel physique distinct. Il n'y a donc pas de point unique de défaillance pour la communication, ni de goulet d'étranglement en termes de bande passante.

Pour plus d'informations, consultez le Guide de l'appairage de VPC Amazon.

Surveillance de votre VPC

Vous pouvez utiliser les outils suivants pour surveiller le trafic ou l'accès au réseau dans votre cloud privé virtuel (VPC).

Journaux de flux VPC

Vous pouvez utiliser les journaux de flux VPC pour capturer des informations détaillées sur le trafic entrant et sortant des interfaces réseau dans vos VPC.

Amazon VPC IP Address Manager (IPAM)

Vous pouvez utiliser l'IPAM pour planifier, suivre et surveiller les adresses IP pour vos charges de travail. Pour plus d'informations, consultez la section concernant IP Address Manager(Gestionnaire des adresses IP).

Mise en miroir du trafic

Vous pouvez utiliser cette fonction pour copier le trafic réseau depuis une interface réseau d'une instance EC2 d'Amazon, puis l'envoyer à des appareils de surveillance et de sécurité hors bande en vue d'une inspection approfondie des paquets. Vous pouvez détecter les anomalies du réseau et de la sécurité, obtenir des informations opérationnelles, mettre en œuvre des contrôles de conformité et de sécurité et résoudre les problèmes. Pour en savoir plus, consultez la section Traffic Mirroring (Mise en miroir du trafic).

Reachability Analyzer

Vous pouvez utiliser cet outil pour analyser et déboguer l'accessibilité réseau entre deux ressources dans votre VPC. Une fois que vous avez spécifié les ressources sources et de destination, « Reachability Analyzer » produit des détails saut par saut du chemin virtuel entre elles lorsqu'elles sont accessibles, et identifie le composant bloquant lorsqu'ils sont inaccessibles. Pour de plus amples renseignements, consultez la section Reachability Analyzer.

Network Access Analyzer

Vous pouvez utiliser « Network Access Analyzer » pour comprendre l'accès réseau de vos ressources. Cet outil permet d'identifier les améliorations apportées à la posture de sécurité de votre réseau et à démontrer que votre réseau répond à des exigences de conformité spécifiques. Pour de plus amples informations, consultez la section Network Access Analyzer.

Journaux CloudTrail

Vous pouvez utiliser AWS CloudTrail pour capturer des informations détaillées sur les appels effectués vers l'API Amazon VPC. Vous pouvez utiliser ces journaux CloudTrail générés afin de déterminer les appels qui ont été effectués, l'adresse IP source d'où provient les appels, qui les a effectués, quand ils ont été effectués, ainsi de suite. Pour en savoir plus, consultez la section Logging Amazon EC2 Amazon EBS, and Amazon VPC API calls using AWS CloudTrail (Journalisation des appels d'API Amazon EC2 Amazon EBS et Amazon VPC API avec CloudTrail) dans la Référence d'API Amazon EC2.

Journalisation du trafic IP à l'aide des journaux de flux VPC

La fonctionnalité de journaux de flux VPC vous permet de capturer des informations sur le trafic IP circulant vers et depuis les interfaces réseau dans votre VPC. Les données du journal de flux peuvent être publiées aux emplacements suivants : Amazon CloudWatch Logs, Amazon S3 ou Amazon Data Firehose. Après avoir créé un journal de flux, vous pouvez récupérer et consulter les enregistrements du journal de flux dans le groupe de journaux, le compartiment ou le flux de diffusion que vous avez configuré.

Les journaux de flux peuvent vous aider pour de nombreuses tâches, par exemple :

- Diagnostiquer les règles de groupe de sécurité trop restrictives
- Surveiller le trafic qui accède à votre instance
- Déterminer la direction du trafic vers et depuis les interfaces réseau

Les données du journal de flux sont collectées en dehors du chemin d'accès de votre trafic réseau et n'affectent donc pas le débit réseau ou la latence. Vous pouvez créer ou supprimer des journaux de flux sans risque d'impact sur les performances du réseau.

> **Note**
>
> Cette section ne traite que des journaux de flux pour les VPC. Pour plus d'informations sur les journaux de flux pour les passerelles de transit introduits dans la version 6, consultez la section Enregistrement du trafic réseau à l'aide des journaux de flux de transit de Transit Gateway dans le guide de l'utilisateur d'Amazon VPC Transit Gateways.

Table des matières

Principes de base des journaux de flux

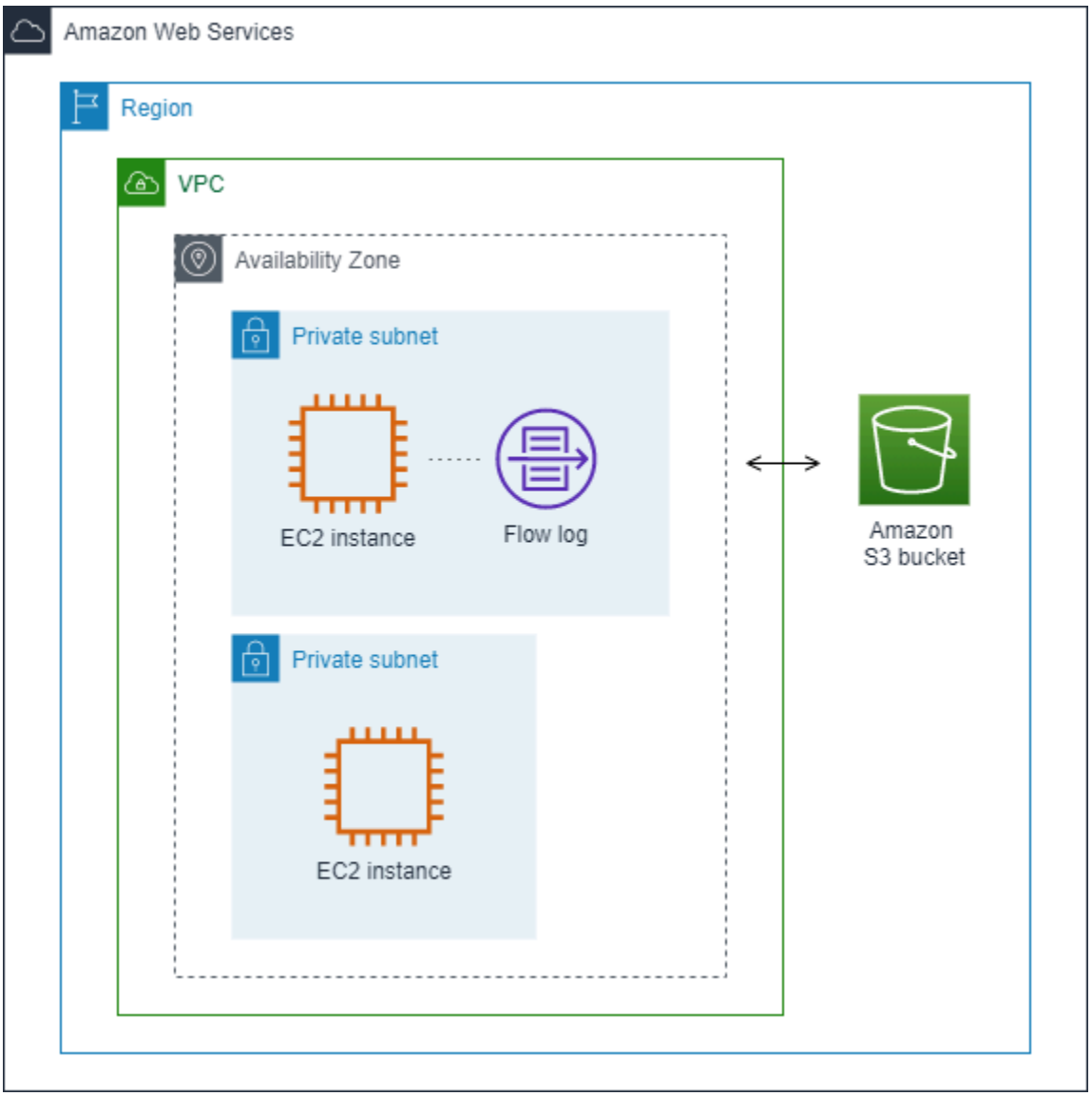
Vous pouvez créer un journal de flux pour un VPC, un sous-réseau ou une interface réseau. Si vous créez un journal de flux pour un sous-réseau ou VPC, chaque interface réseau du sous-réseau ou du VPC est surveillée.

Les données des journaux de flux pour une interface réseau surveillée sont enregistrées sous forme d'enregistrements de journaux de flux. Il s'agit d'événements de journaux, composés de champs qui décrivent le flux de trafic. Pour plus d'informations, consultez Enregistrements de journaux de flux.

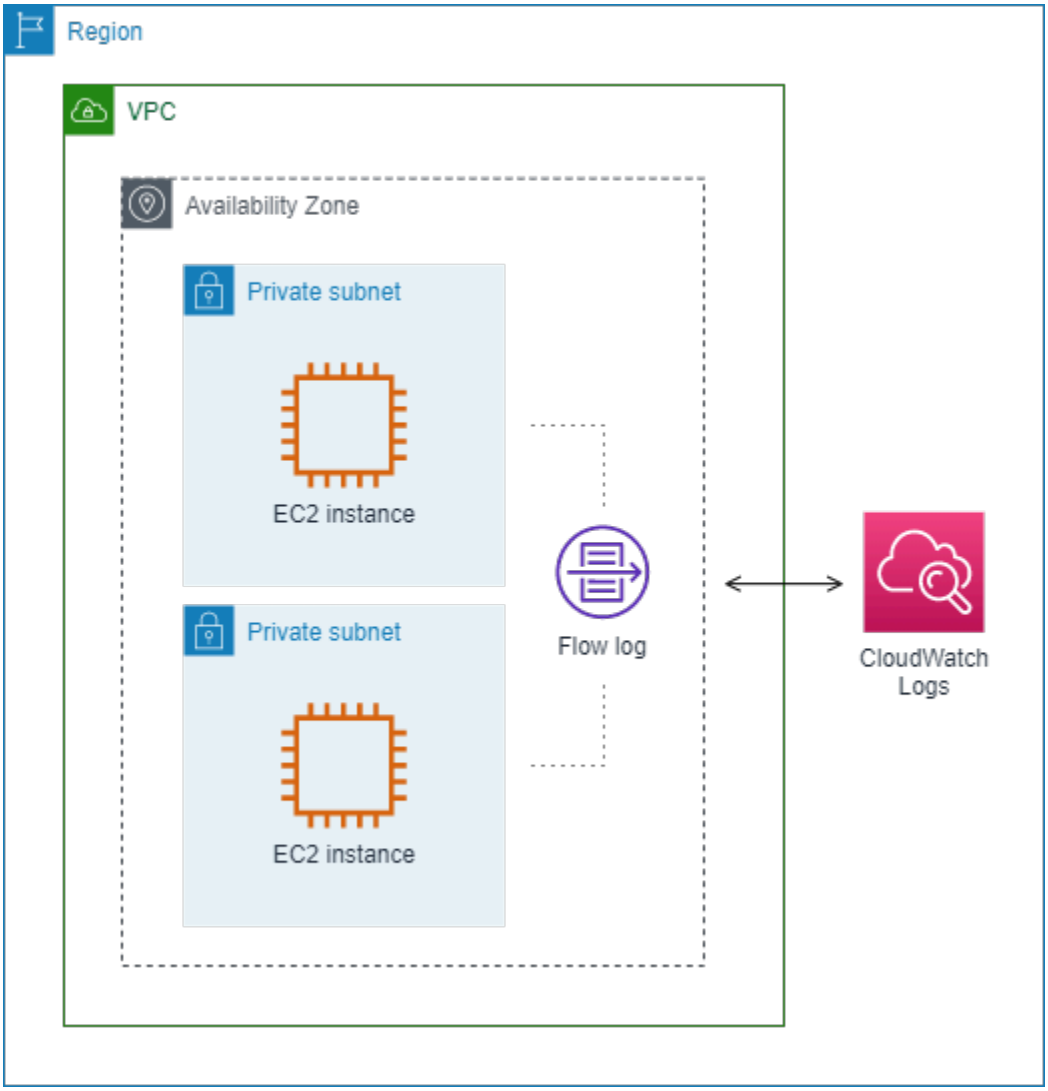
Pour créer un journal de flux, vous spécifiez :

- La ressource pour laquelle vous souhaitez créer le journal de flux.
- Le type de trafic à capturer (le trafic accepté, le trafic rejeté ou tout le trafic)
- Les destinations où publier les données du journal de flux.

Dans l'exemple suivant, vous créez un journal de flux qui capture le trafic accepté pour l'interface réseau de l'une des instances EC2 dans un sous-réseau privé et publie les enregistrements du journal de flux dans un compartiment Amazon S3.



Dans l'exemple suivant, un journal de flux capture tout le trafic d'un sous-réseau et publie les enregistrements du journal de flux sur Amazon CloudWatch Logs. Le journal de flux capture le trafic pour toutes les interfaces réseau du sous-réseau.



Une fois que vous avez créé un journal de flux, plusieurs minutes peuvent s'écouler avant qu'il ne commence à collecter et à publier des données dans les destinations choisies. Les journaux de flux ne capturent pas de flux de journaux en temps réel pour vos interfaces réseau. Pour plus d'informations, consultez Créer un journal de flux.

Si vous lancez une instance dans votre sous-réseau après avoir créé un journal de flux pour votre sous-réseau ou VPC, nous créons un flux de journal (pour les CloudWatch journaux) ou un objet de fichier journal (pour Amazon S3) pour la nouvelle interface réseau dès qu'il y a du trafic réseau pour l'interface réseau.

Vous pouvez générer des journaux de flux pour les interfaces réseau créées par d'autres services AWS , par exemple :

- Elastic Load Balancing

- Amazon RDS
- Amazon ElastiCache
- Amazon Redshift
- Amazon WorkSpaces
- Passerelles NAT
- Passerelles de transit

Quel que soit le type d'interface réseau, vous devez utiliser la console Amazon EC2 ou l'API Amazon EC2 afin de créer un journal de flux pour une interface réseau.

Vous pouvez appliquer des balises à vos journaux de flux. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez. Les balises peuvent vous aider à organiser vos journaux de flux, par exemple par objectif ou par propriétaire.

Si vous n'avez plus besoin d'un journal de flux, vous pouvez le supprimer. Dans ce cas, vous désactivez le service de journaux de flux pour la ressource, de sorte qu'aucun autre enregistrement de journal de flux n'est créé ou publié. La suppression d'un journal de flux ne supprime aucune donnée existante du journal de flux. Après avoir supprimé un journal de flux, vous pouvez supprimer les données du journal de flux directement de la destination lorsque vous en avez terminé. Pour plus d'informations, consultez Supprimer un journal de flux.

Enregistrements de journaux de flux

Un enregistrement de journal de flux représente un flux de réseau dans votre VPC. Par défaut, chaque enregistrement capture un flux de trafic IP réseau (caractérisé par un 5-tuple par interface réseau) qui se produit dans un intervalle d'agrégation, également appelé fenêtre de capture.

Chaque enregistrement est une chaîne de caractères avec des champs séparés par des espaces. Un enregistrement inclut des valeurs pour les différents composants du flux IP, par exemple la source, la destination et le protocole.

Lorsque vous créez un journal de flux, vous pouvez utiliser le format par défaut pour l'enregistrement de journal de flux ou spécifier un format personnalisé.

Table des matières

Intervalle d'agrégation

L'intervalle d'agrégation est la période pendant laquelle un flux particulier est capturé et agrégé dans un enregistrement de journal de flux. Par défaut, l'intervalle d'agrégation maximal est de 10 minutes. Lorsque vous créez un journal de flux, vous pouvez spécifier un intervalle d'agrégation maximal d'une minute. Les journaux de flux avec un intervalle d'agrégation maximal d'une minute produisent un volume d'enregistrements de journaux de flux plus élevé que ceux avec un intervalle d'agrégation maximal de 10 minutes.

Lorsqu'une interface réseau est associée à une instance basée sur Nitro, l'intervalle d'agrégation est toujours d'une minute maximum, quel que soit celui qui a été spécifié.

Une fois les données capturées dans un intervalle d'agrégation, le traitement et la publication des données sur CloudWatch Logs ou Amazon S3 prennent plus de temps. Le service de journalisation des flux fournit généralement CloudWatch les journaux à Logs en 5 minutes environ et à Amazon S3 en 10 minutes environ. La fourniture des journaux est effectuée au mieux des possibilités disponibles. Il est donc possible que vos journaux soient retardés au-delà du délai de remise habituel.

Format par défaut

Avec le format par défaut, les enregistrements de journaux de flux incluent les champs version 2, dans l'ordre indiqué dans le tableau Champs disponibles. Vous ne pouvez pas personnaliser ou modifier le format par défaut. Pour capturer les champs supplémentaires ou un sous-ensemble de champs différent, spécifiez plutôt un format personnalisé.

Format personnalisé

Avec un format personnalisé, vous spécifiez quels champs sont inclus dans les enregistrements de journaux de flux et dans quel ordre. Cela vous permet de créer des journaux de flux qui correspondent spécifiquement à vos besoins et d'ignorer les champs qui ne sont pas pertinents. L'utilisation d'un format personnalisé peut également réduire la nécessité de faire appel à des processus distincts pour extraire des informations spécifiques des journaux de flux publiés. Vous pouvez spécifier n'importe quel nombre de champs de journal de flux disponibles, mais vous devez indiquer au moins un champ.

Champs disponibles

Le tableau suivant décrit tous les champs disponibles pour un enregistrement de journal de flux. La colonne Version indique la version des journaux de flux VPC dans laquelle le champ a été introduit. Le format par défaut inclut tous les champs version 2, dans même ordre que dans le tableau.

Lorsque vous publiez des données du journal de flux sur Amazon S3, le type de données des champs dépend du format du journal de flux. Si le format est en texte brut, tous les champs sont de type STRING. Si le format est Parquet, consultez le tableau des types de données de champ.

Si un champ ne s'applique pas à un enregistrement spécifique ou pourrait ne pas être calculé pour celui-ci, ce dernier affiche le symbole « - » pour cette entrée. Les champs de métadonnées qui ne proviennent pas directement de l'en-tête des paquets sont des approximations optimales, et leurs valeurs peuvent être manquantes ou inexactes.

Champ	Description	Version
version	Version des journaux de flux VPC Si vous utilisez le format par défaut, la version est 2. Si vous utilisez un format personnalisé, la version est la version la plus élevée parmi les champs spécifiés. Par exemple, si vous spécifiez uniquement des champs issus de la version 2, la version est 2. Si vous spécifiez un mélange de champs des versions 2, 3 et 4, la version est 4. Type de données Parquet : INT_32	2
account-id	ID de AWS compte du propriétaire de l'interface réseau source pour laquelle le trafic est enregistré. Si l'interface réseau est créée par un AWS service, par exemple lors de la création d'un point de terminaison VPC ou d'un Network Load Balancer, l'enregistrement peut s'unknownafficher pour ce champ. Type de données Parquet : CHAÎNE	2
interface-id	ID de l'interface réseau pour laquelle le trafic est enregistré. Type de données Parquet : CHAÎNE	2
srcaddr	Adresse source pour le trafic entrant, ou adresse IPv4 ou IPv6 de l'interface réseau pour le trafic sortant sur l'interface réseau.	2

Champ	Description	Version
	L'adresse IPv4 de l'interface réseau correspond toujours à son adresse IPv4 privée. Voir aussi pkt-srcaddr. Type de données Parquet : CHAÎNE	
dstaddr	Adresse de destination pour le trafic sortant, ou adresse IPv4 ou IPv6 de l'interface réseau pour le trafic entrant sur l'interface réseau. L'adresse IPv4 de l'interface réseau correspond toujours à son adresse IPv4 privée. Voir aussi pkt-dstaddr. Type de données Parquet : CHAÎNE	2
srcport	Port source du trafic Type de données Parquet : INT_32	2
dstport	Port de destination du trafic Type de données Parquet : INT_32	2
protocol	Numéro de protocole IANA du trafic (pour plus d'informations, consultez la page Assigned Internet Protocol Numbers). Type de données Parquet : INT_32	2
packets	Nombre de paquets transférés pendant le flux. Type de données Parquet : INT_64	2
bytes	Nombre d'octets transférés pendant le flux. Type de données Parquet : INT_64	2
start	Heure, en secondes Unix, à laquelle le premier paquet du flux a été reçu dans l'intervalle d'agrégation. Jusqu'à 60 secondes peuvent s'écouler après la transmission ou la réception du paquet sur l'interface réseau. Type de données Parquet : INT_64	2

Champ	Description	Version
end	Heure, en secondes Unix, à laquelle le dernier paquet du flux a été reçu dans l'intervalle d'agrégation. Jusqu'à 60 secondes peuvent s'écouler après la transmission ou la réception du paquet sur l'interface réseau. Type de données Parquet : INT_64	2
action	Action associée au trafic : • ACCEPT — Le trafic a été accepté. • REJECT — Le trafic a été rejeté. Par exemple, le trafic n'a pas été autorisé par les groupes de sécurité ou les ACL réseau, ou des paquets sont arrivés après la fermeture de la connexion. Type de données Parquet : CHAÎNE	2
log-status	Statut de journalisation du journal de flux : • OK : les données sont consignées normalement dans les destinations choisies. • NODATA : il n'y a eu aucun trafic réseau depuis ou vers l'interfa ce réseau pendant l'intervalle d'agrégation. • SKIPDATA : certains enregistrements de journaux de flux ont été ignorés pendant l'intervalle d'agrégation. Cela peut être dû à une contrainte de capacité interne ou à une erreur interne. Type de données Parquet : CHAÎNE	2
vpc-id	ID du VPC qui contient l'interface réseau pour laquelle le trafic est enregistré. Type de données Parquet : CHAÎNE	3

Champ	Description	Version
subnet-id	ID du sous-réseau qui contient l'interface réseau pour laquelle le trafic est enregistré. Type de données Parquet : CHAÎNE	3
instance-id	ID de l'instance associée à l'interface réseau pour laquelle le trafic est enregistré, si vous êtes propriétaire de l'instance. Renvoie un symbole « - » pour une interface réseau gérée par demandeur, par exemple, l'interface réseau pour une passerelle NAT. Type de données Parquet : CHAÎNE	3

Champ	Description	Version
tcp-flags	Valeur de masque de bits pour les indicateurs TCP suivants : • FIN : 1 • SYN : 2 • RST : 4 • SYN-ACK : 18 Si aucun indicateur pris en charge n'est enregistré, la valeur de l'indicateur TCP est 0. Par exemple, étant donné que les indicateurs tcp ne prennent pas en charge la journalisation des indicateurs ACK ou PSH, les enregistrements du trafic avec ces indicateurs non pris en charge donneront aux indicateurs tcp la valeur 0. Si, toutefois , un indicateur non pris en charge est accompagné d'un indicateu r pris en charge, nous indiquerons la valeur de l'indicateur pris en charge. Par exemple, si ACK fait partie de SYN-ACK, il en indique 18. Et s'il existe un enregistrement tel que SYN+ECE, étant donné que SYN est un indicateur pris en charge alors que ECE ne l'est pas, la valeur de l'indicateur TCP est 2. Si, pour une raison ou une autre, la combinaison d'indicateurs n'est pas valide et que la valeur ne peut pas être calculée, la valeur est « - ». Si aucun indicateur n'est envoyé, la valeur de l'indicateur TCP est 0. Les indicateurs TCP peuvent être interrogés pendant l'intervalle d'agrégation. Pour les connexions courtes, les indicateurs peuvent être définis sur la même ligne dans l'enregistrement de journal de flux, par exemple, 19 pour SYN-ACK et FIN, et 3 pour SYN et FIN. Pour obtenir un exemple, consultez Séquence d'indicateur TCP. Pour des informations générales sur les indicateurs TCP (comme la signification des indicateurs tels que FIN, SYN et ACK), consultez Structure d'un segment TCP sur Wikipédia. Type de données Parquet : INT_32	3

Champ	Description	Version
type	Type de trafic. Les valeurs possibles sont les suivantes : IPv4 | IPv6 | EFA. Pour plus d'informations, consultez Elastic Fabric Adapter (EFA). Type de données Parquet : CHAÎNE	3
pkt-srcaddr	Adresse IP source (d'origine) du trafic au niveau du paquet. Utilisez ce champ avec le champ srcaddr pour faire la distinction entre l'adresse IP d'une couche intermédiaire via laquelle les flux transitent et l'adresse IP source d'origine du trafic. Par exemple, lorsque le trafic transite par le biais d'une interface réseau pour une passerelle NAT ou lorsque l'adresse IP d'un pod dans Amazon EKS est différente de celle de l'interface réseau du nœud d'instance sur lequel le pod s'exécute (pour la communication dans un VPC). Type de données Parquet : CHAÎNE	3
pkt-dstaddr	Adresse IP de destination (d'origine) du trafic au niveau du paquet. Utilisez ce champ avec le champ dstaddr pour faire la distinction entre l'adresse IP d'une couche intermédiaire via laquelle le trafic transite et l'adresse IP de destination finale du trafic. Par exemple, lorsque le trafic transite par le biais d'une interface réseau pour une passerelle NAT ou lorsque l'adresse IP d'un pod dans Amazon EKS est différente de celle de l'interface réseau du nœud d'instance sur lequel le pod s'exécute (pour la communication dans un VPC). Type de données Parquet : CHAÎNE	3
region	Région contenant l'interface réseau pour laquelle le trafic est enregistré. Type de données Parquet : CHAÎNE	4

Champ	Description	Version
az-id	ID de la zone de disponibilité qui contient l'interface réseau pour laquelle le trafic est enregistré. Si le trafic provient d'un sous-empl acement, l'enregistrement affiche un symbole « - » pour ce champ. Type de données Parquet : CHAÎNE	4
sublocation-type	Type de sous-emplacement renvoyé dans le champ sublocation-id. Les valeurs possibles sont les suivantes : wavelength | outpost | localzone. Si le trafic ne provient pas d'un sous-emplacement, l'enregistrement affiche un symbole « - » pour ce champ. Type de données Parquet : CHAÎNE	4
sublocation-id	ID du sous-emplacement qui contient l'interface réseau pour laquelle le trafic est enregistré. Si le trafic ne provient pas d'un sous-emplacement, l'enregistrement affiche un symbole « - » pour ce champ. Type de données Parquet : CHAÎNE	4
pkt-src-aws-service	Le nom du sous-ensemble de plages d'adresses IP pour le pkt-srcaddr champ, si l'adresse IP source est celle d'un AWS service. Si le pkt-srcaddr appartient à une plage superposée, il n'affiche ra qu'un seul des pkt-src-aws-service codes de service. AWS Les valeurs possibles sont les suivantes : AMAZON | AMAZON_AP PFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEE TINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRON T | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTA NCE_CONNECT | GLOBALACCELERATOR | KINESIS_V IDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_R ESOLVER | S3 | WORKSPACES_GATEWAYS. Type de données Parquet : CHAÎNE	5

Champ	Description	Version
pkt-dst-aws-service	Le nom du sous-ensemble de plages d'adresses IP pour le pkt-dstaddr champ, si l'adresse IP de destination est celle d'un AWS service. Pour obtenir une liste des valeurs possibles, consultez le champ pkt-src-aws-service. Type de données Parquet : CHAÎNE	5
flow-direction	La direction du flux par rapport à l'interface où le trafic est capturé. Les valeurs possibles sont les suivantes : ingress | egress. Type de données Parquet : CHAÎNE	5
traffic-path	Chemin emprunté par le trafic de sortie vers la destination. Pour déterminer si le trafic est un trafic de sortie, cochez la case du champ flow-direction. Les valeurs possibles sont les suivantes. Si aucune des valeurs ne s'applique, le champ est défini sur « - ». • 1 — Via une autre ressource dans le même VPC, y compris les ressources qui créent une interface réseau dans le VPC • 2 — Via une passerelle Internet ou un point de terminaison de VPC de passerelle • 3 — Via une passerelle réseau privé virtuel • 4 — Via une connexion d'appairage de VPC intra-région • 5 — Via une connexion d'appairage de VPC entre régions • 6 — Via une passerelle locale • 7 — Via un point de terminaison de VPC de passerelle (instances basées sur Nitro uniquement) • 8 — Via une passerelle Internet (instances basées sur Nitro uniquement) Type de données Parquet : INT_32	5

Champ	Description	Version
ecs-cluster-arn	AWS Nom de ressource (ARN) du cluster ECS si le trafic provient d'une tâche ECS en cours d'exécution. Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs :ListClusters. Type de données Parquet : CHAÎNE	7
nom-cluster ecs	Nom du cluster ECS si le trafic provient d'une tâche ECS en cours d'exécution. Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs :ListClusters. Type de données Parquet : CHAÎNE	7
ecs-container-instance-arn	ARN de l'instance de conteneur ECS si le trafic provient d'une tâche ECS en cours d'exécution sur une instance EC2. Si le fournisseur de capacité l'est AWS Fargate, ce champ sera « - ». Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs : ListClusters et ecs : ListContainer Instances. Type de données Parquet : CHAÎNE	7
identifiant d'instance du conteneur ecs	ID de l'instance de conteneur ECS si le trafic provient d'une tâche ECS en cours d'exécution sur une instance EC2. Si le fournisseur de capacité l'est AWS Fargate, ce champ sera « - ». Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs : ListClusters et ecs : ListContainer Instances. Type de données Parquet : CHAÎNE	7
identifiant du conteneur ECS	ID d'exécution Docker du conteneur si le trafic provient d'une tâche ECS en cours d'exécution. S'il existe un ou plusieurs conteneurs dans la tâche ECS, il s'agira de l'ID d'exécution docker du premier conteneur. Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs :ListClusters. Type de données Parquet : CHAÎNE	7

Champ	Description	Version
ecs-second-container-id	ID d'exécution Docker du conteneur si le trafic provient d'une tâche ECS en cours d'exécution. S'il existe plusieurs conteneurs dans la tâche ECS, il s'agira de l'ID d'exécution Docker du second conteneur. Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs :ListClusters. Type de données Parquet : CHAÎNE	7
nom-service ECS	Nom du service ECS si le trafic provient d'une tâche ECS en cours d'exécution et que la tâche ECS est démarrée par un service ECS. Si la tâche ECS n'est pas démarrée par un service ECS, ce champ sera « - ». Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs : ListClusters et ecs :ListServices. Type de données Parquet : CHAÎNE	7
ecs-task-definition-arn	ARN de la définition de tâche ECS si le trafic provient d'une tâche ECS en cours d'exécution. Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs : ListClusters et ecs : ListTaskDefinitions Type de données Parquet : CHAÎNE	7
ecs-task-arn	ARN de la tâche ECS si le trafic provient d'une tâche ECS en cours d'exécution. Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs : ListClusters et ecs :ListTasks. Type de données Parquet : CHAÎNE	7
identifiant de tâche ecs	ID de la tâche ECS si le trafic provient d'une tâche ECS en cours d'exécution. Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs : ListClusters et ecs :ListTasks. Type de données Parquet : CHAÎNE	7

Exemples d'enregistrements de journaux de flux

Vous trouverez ci-après des exemples d'enregistrements de flux de journal qui capturent des flux de trafic spécifiques.

Pour de plus amples informations sur le format des enregistrements de journal de flux, veuillez consulter Enregistrements de journaux de flux. Pour de plus amples informations sur la création de journaux de flux, consultez Utiliser des journaux de flux.

Table des matières

Trafic accepté et rejeté

Voici des exemples d'enregistrement de journal de flux par défaut.

Dans cet exemple, le trafic SSH (port de destination 22, protocole TCP) entre l'adresse IP 172.31.16.139 et l'interface réseau avec adresse IP privée est 172.31.16.21 et l'ID eni-1235b8ca123456789 a été autorisé dans le compte 123456789010.

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249
 1418530010 1418530070 ACCEPT OK
```

Dans cet exemple, le trafic RDP (port de destination 3389, protocole TCP) vers l'interface réseau eni-1235b8ca123456789 du compte 123456789010 a été rejeté.

```
2 123456789010 eni-1235b8ca123456789 172.31.9.69 172.31.9.12 49761 3389 6 20 4249
 1418530010 1418530070 REJECT OK
```

Aucune donnée et enregistrements ignorés

Voici des exemples d'enregistrement de journal de flux par défaut.

Dans cet exemple, aucune donnée n'a été enregistrée pendant l'intervalle d'agrégation.

```
2 123456789010 eni-1235b8ca123456789 - - - - - - - 1431280876 1431280934 - NODATA
```

Dans cet exemple, les enregistrements ont été ignorés pendant l'intervalle d'agrégation. La fonctionnalité de journaux de flux VPC ignore les enregistrements lorsqu'elle ne peut pas capturer les données d'un journal de flux pendant un intervalle d'agrégation, car il dépasse la capacité interne. Un enregistrement ignoré peut représenter plusieurs flux qui n'ont pas été capturés pour l'interface réseau pendant l'intervalle d'agrégation.

```
2 123456789010 eni-11111111aaaaaaaaa - - - - - - - 1431280876 1431280934 - SKIPDATA
```

Règles de groupe de sécurité et de liste ACL réseau

Si vous utilisez des journaux de flux pour diagnostiquer des règles de groupe de sécurité ou de liste ACL réseau trop restrictives ou permissives, déterminez si ces ressources sont avec ou sans état. Les groupes de sécurité sont avec état : cela signifie que les réponses au trafic autorisé sont également autorisées, même si les règles de votre groupe de sécurité ne l'autorise pas. Inversement, les listes ACL réseau sont sans état. Par conséquent, les réponses au trafic autorisé sont soumises aux règles des listes ACL réseau.

Imaginons, par exemple, que vous utilisiez la commande ping depuis votre ordinateur personnel (dont l'adresse IP est 203.0.113.12) vers votre instance (l'adresse IP privée de l'interface réseau est 172.31.16.139). Les règles de trafic entrant de votre groupe de sécurité autorisent le trafic ICMP, mais les règles sortantes n'autorisent pas ce trafic. Comme les groupes de sécurité sont avec état, le ping de réponse provenant de votre instance est autorisé. Votre liste ACL réseau autorise le trafic ICMP entrant, mais pas le trafic ICMP sortant. Les listes ACL réseau étant « sans état », le ping de réponse est abandonné et n'atteint pas votre ordinateur personnel. Dans un journal de flux par défaut, cette information est affichée sous la forme de deux enregistrements de journaux de flux :

- Un enregistrement ACCEPT pour le ping d'origine qui était autorisé par l'ACL réseau et le groupe de sécurité, et donc autorisé à atteindre votre instance.
- Un enregistrement REJECT pour le ping de réponse qui l'ACL réseau a refusé.

```
2 123456789010 eni-1235b8ca123456789 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027
 1432917142 ACCEPT OK
```

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094
 1432917142 REJECT OK
```

Si votre ACL réseau autorise le trafic ICMP sortant, le journal de flux affiche deux enregistrements ACCEPT (un pour le ping d'origine et un pour le ping de réponse). Si votre groupe de sécurité refuse le trafic ICMP entrant, le journal de flux affiche un seul enregistrement REJECT, car le trafic n'était pas autorisé à atteindre votre instance.

Trafic IPv6

Voici un exemple d'enregistrement de journal de flux par défaut. Dans cet exemple, le trafic SSH (port 22) de l'adresse IPv6 2001:db8:1234:a100:8d6e:3477:df66:f105 vers l'interface réseau eni-1235b8ca123456789 du compte 123456789010 a été autorisé.

```
2 123456789010 eni-1235b8ca123456789 2001:db8:1234:a100:8d6e:3477:df66:f105
 2001:db8:1234:a102:3304:8879:34cf:4071 34892 22 6 54 8855 1477913708 1477913820 ACCEPT
 OK
```

Séquence d'indicateur TCP

Cette section contient des exemples de journaux de flux personnalisés qui capturent les champs suivants dans l'ordre suivant.

```
version vpc-id subnet-id instance-id interface-id account-id type srcaddr dstaddr
 srcport dstport pkt-srcaddr pkt-dstaddr protocol bytes packets start end action tcp-
flags log-status
```

Dans les exemples de cette section, le tcp-flags champ est représenté par la second-to-last valeur du journal de flux. Les indicateurs TCP peuvent vous aider à identifier la direction du trafic, par exemple, quel serveur a initié la connexion.

> **Note**
>
> Pour plus d'informations sur l'option tcp-flags et une explication de chacun des indicateurs TCP, consultez Champs disponibles.

Dans les enregistrements suivants (à partir de 7:47:55 PM et jusqu'à 7:48:53 PM), deux connexions ont été démarrées par un client vers un serveur s'exécutant sur le port 5001. Deux indicateurs SYN

(2) ont été reçues par le serveur à partir du client depuis des ports source différents sur le client (43416 et 43418). Pour chaque indicateur SYN, un SYN-ACK a été envoyé depuis le serveur vers le client (18) sur le port correspondant.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43416 5001
 52.213.180.42 10.0.0.62 6 568 8 1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43416 10.0.0.62
 52.213.180.42 6 376 7 1566848875 1566848933 ACCEPT 18 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 100701 70 1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 632 12 1566848875 1566848933 ACCEPT 18 OK
```

Dans le deuxième intervalle d'agrégation, l'une des connexions qui a été établie pendant le flux précédent est désormais fermée. Le client a envoyé un indicateur FIN (1) au serveur pour la connexion sur le port 43418. Le serveur a envoyé un indicateur au client sur le port 43418.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 63388 1219 1566848933 1566849113 ACCEPT 1 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 23294588 15774 1566848933 1566849113 ACCEPT 1 OK
```

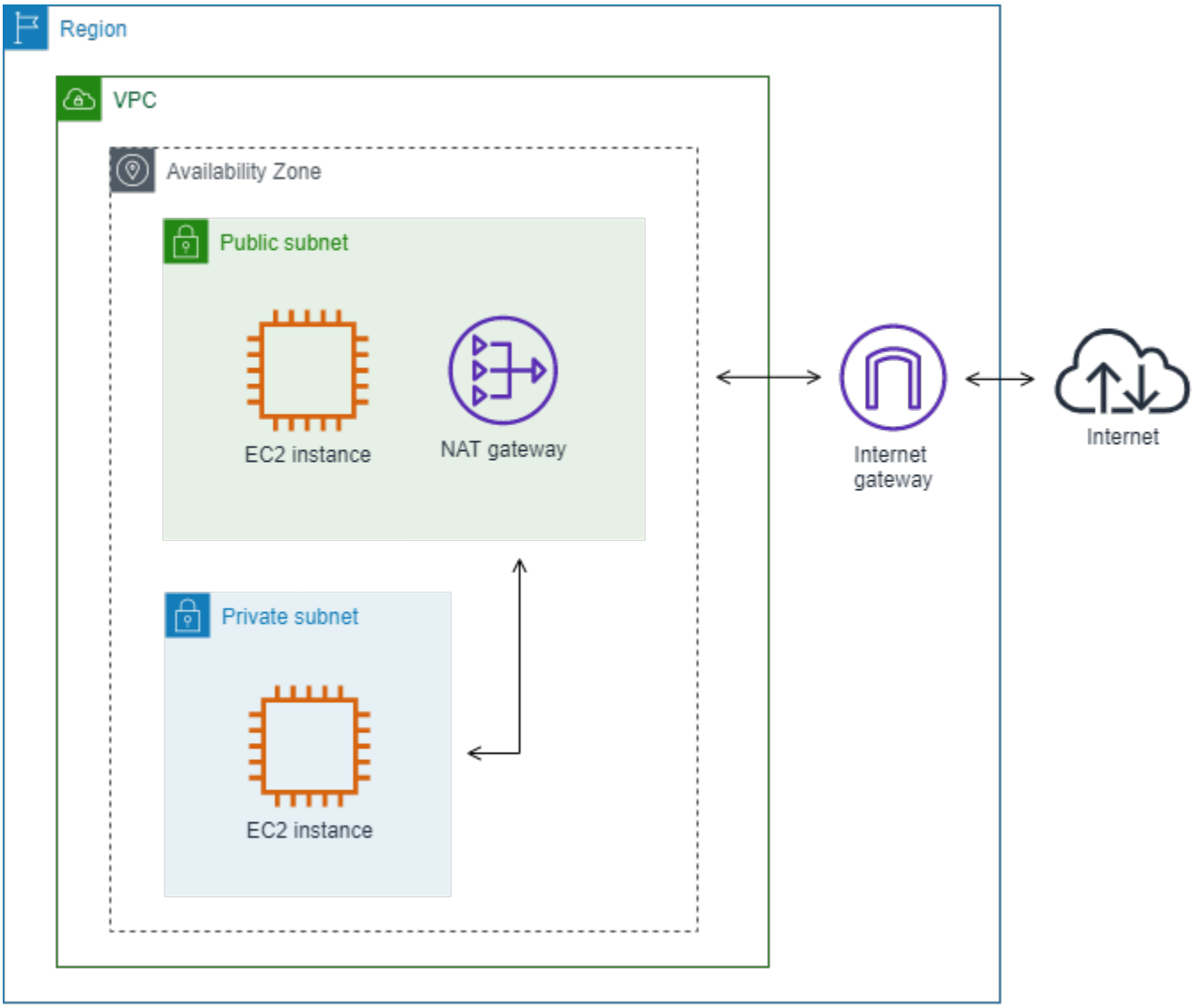
Pour des connexions courtes (par exemple, de quelques secondes) qui sont ouvertes et fermées au cours d'un seul intervalle d'agrégation, les indicateurs peuvent être définis sur la même ligne dans l'enregistrement de flux de journal pour le flux de trafic dans la même direction. Dans l'exemple suivant, la connexion est établie et fermée au cours du même intervalle d'agrégation. Dans la première ligne, la valeur de l'indicateur TCP est 3, ce qui indique qu'un SYN et un message FIN ont été envoyés depuis le client vers le serveur. Dans la deuxième ligne, la valeur de l'indicateur TCP est 19, ce qui indique qu'un SYN-ACK et un message FIN ont été envoyés depuis le serveur vers le client.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43638 5001
 52.213.180.42 10.0.0.62 6 1260 17 1566933133 1566933193 ACCEPT 3 OK
```

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43638  10.0.0.62
 52.213.180.42 6 967 14 1566933133 1566933193 ACCEPT 19 OK
```

Trafic via une passerelle NAT

Dans cet exemple, une instance dans un sous-réseau privé accède à Internet via une passerelle NAT située dans un sous-réseau public.



Le journal de flux personnalisé suivant pour l'interface réseau de la passerelle NAT capture les champs ci-après dans l'ordre suivant.

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

Le journal de flux montre le flux de trafic depuis l'adresse IP de l'instance (10.0.1.5) via l'interface réseau de la passerelle NAT vers un hôte sur Internet (203.0.113.5). L'interface réseau de la passerelle NAT est une interface réseau gérée par demandeur. L'enregistrement de journal de flux affiche donc un symbole « - » pour le champ instance-id. La ligne suivante montre le trafic depuis l'instance source vers l'interface réseau de la passerelle NAT. Les valeurs pour les champs dstaddr et pkt-dstaddr sont différentes. Le champ dstaddr affiche l'adresse IP privée de l'interface réseau de la passerelle NAT, et le champ pkt-dstaddr affiche l'adresse IP de destination finale de l'hôte sur Internet.

```
- eni-1235b8ca123456789 10.0.1.5 10.0.0.220 10.0.1.5 203.0.113.5
```

Les deux lignes suivantes montrent le trafic depuis l'interface réseau de la passerelle NAT vers l'hôte cible sur Internet et le trafic de la réponse de l'hôte à l'interface réseau de la passerelle NAT.

```
- eni-1235b8ca123456789 10.0.0.220 203.0.113.5 10.0.0.220 203.0.113.5
- eni-1235b8ca123456789 203.0.113.5 10.0.0.220 203.0.113.5 10.0.0.220
```

La ligne suivante montre le trafic depuis l'interface réseau de la passerelle NAT vers l'instance source. Les valeurs pour les champs srcaddr et pkt-srcaddr sont différentes. Le champ srcaddr affiche l'adresse IP privée de l'interface réseau de la passerelle NAT, et le champ pkt-srcaddr affiche l'adresse IP de l'hôte sur Internet.

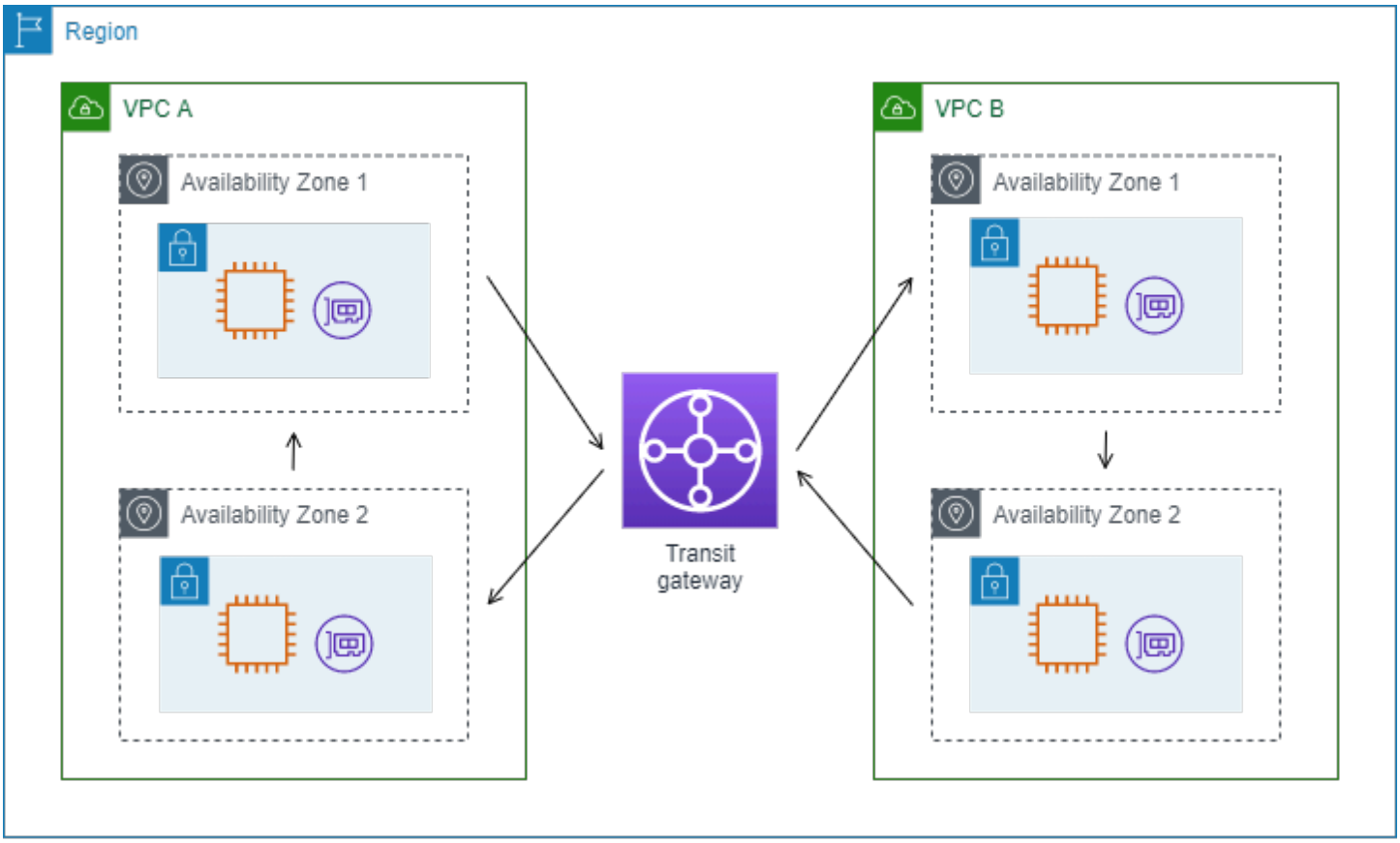
```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

Vous créez un autre journal de flux personnalisé à l'aide du même ensemble de champs que ci-dessus. Vous créez le journal de flux pour l'interface réseau de l'instance dans le sous-réseau privé. Dans ce cas, le champ instance-id renvoie l'ID de l'instance qui est associée à l'interface réseau, et il n'y a pas de différence entre les champs dstaddr et pkt-dstaddr, et les champs srcaddr et pkt-srcaddr. Contrairement à l'interface réseau pour la passerelle NAT, cette interface réseau n'est pas une interface réseau intermédiaire pour le trafic.

```
i-01234567890123456 eni-1111aaaa2222bbbb3 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
 #Traffic from the source instance to host on the internet
i-01234567890123456 eni-1111aaaa2222bbbb3 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
 #Response traffic from host on the internet to the source instance
```

Trafic via une passerelle de transit

Dans cet exemple, un client dans le VPC A se connecte à un serveur web dans le VPC B par le biais d'une passerelle de transit. Le client et le serveur sont dans des zones de disponibilité différentes. Le trafic arrive au serveur dans le VPC B en utilisant un ID d'interface réseau élastique (dans cet exemple, supposons que l'ID est eni-11111111111111111) et quitte le VPC B en utilisant un autre (par exemple eni-22222222222222222).



Vous créez un journal de flux personnalisé pour le VPC B avec le format suivant.

```
version interface-id account-id vpc-id subnet-id instance-id srcaddr dstaddr srcport
 dstport protocol tcp-flags type pkt-srcaddr pkt-dstaddr action log-status
```

Les lignes suivantes des enregistrements de journal de flux illustrent le flux de trafic sur l'interface réseau pour le serveur web. La première ligne est le trafic de la demande du client et la dernière ligne est le trafic de la réponse du serveur web.

```
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.20.33.164 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164
 10.40.2.236 ACCEPT OK
```

```
...
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.40.2.236 10.20.33.164 80 39812 6 19 IPv4 10.40.2.236
 10.20.33.164 ACCEPT OK
```

La ligne suivante est le trafic de la demande sur eni-11111111111111111, une interface réseau gérée par demandeur pour la passerelle de transit dans le sous-réseau subnet-11111111aaaaaaaaa. L'enregistrement de journal de flux affiche donc un symbole « - » pour le champ instance-id. Le champ srcaddr affiche l'adresse IP privée de l'interface réseau de la passerelle de transit et le champ pkt-srcaddr affiche l'adresse IP source du client dans le VPC A.

```
3 eni-11111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaaa -
 10.40.1.175 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164 10.40.2.236 ACCEPT OK
```

La ligne suivante est le trafic de la réponse sur eni-22222222222222222, une interface réseau gérée par demandeur pour la passerelle de transit dans le sous-réseau subnet-22222222bbbbbbbbb. Le champ dstaddr affiche l'adresse IP privée de l'interface réseau de la passerelle de transit et le champ pkt-dstaddr affiche l'adresse IP du client dans le VPC A.

```
3 eni-22222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb -
 10.40.2.236 10.40.2.31 80 39812 6 19 IPv4 10.40.2.236 10.20.33.164 ACCEPT OK
```

Nom du service, chemin du trafic et direction du flux

Voici un exemple de champs pour un enregistrement de journal de flux personnalisé.

```
version srcaddr dstaddr srcport dstport protocol start end type packets bytes account-
id vpc-id subnet-id instance-id interface-id region az-id sublocation-type sublocation-
id action tcp-flags pkt-srcaddr pkt-dstaddr pkt-src-aws-service pkt-dst-aws-service
 traffic-path flow-direction log-status
```

Dans l'exemple suivant, la version est 5 car les enregistrements incluent des champs version 5. Une instance EC2 appelle le service Amazon S3. Les journaux de flux sont capturés sur l'interface réseau pour l'instance. Le premier enregistrement a une direction de flux de ingress et le second enregistrement a une direction de flux de egress. Pour l'enregistrement egress, traffic-path est 8, indiquant que le trafic passe par une passerelle Internet. Le champ traffic-path n'est pas pris en charge pour le trafic ingress. Lorsque pkt-srcaddr ou pkt-dstaddr est une adresse IP publique, le nom du service s'affiche.

```
5 52.95.128.179 10.0.0.71 80 34210 6 1616729292 1616729349 IPv4 14 15044
 123456789012 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b
 eni-1235b8ca123456789 ap-southeast-2 apse2-az3 - - ACCEPT 19 52.95.128.179 10.0.0.71
 S3 - - ingress OK
5 10.0.0.71 52.95.128.179 34210 80 6 1616729292 1616729349 IPv4 7 471 123456789012 vpc-
abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b eni-1235b8ca123456789
 ap-southeast-2 apse2-az3 - - ACCEPT 3 10.0.0.71 52.95.128.179 - S3 8 egress OK
```

Limitations des journaux de flux

Lorsque vous utilisez des journaux de flux, vous devez tenir compte des limitations suivantes :

- Vous ne pouvez pas activer les journaux de flux pour les VPC qui sont appairés à votre VPC, sauf si le VPC pair est inclus dans votre compte.
- Une fois que vous avez créé un journal de flux, vous ne pouvez pas modifier sa configuration ou le format d'enregistrement du journal de flux. Par exemple, vous ne pouvez pas associer un rôle IAM différent au journal de flux ou ajouter/supprimer des champs dans l'enregistrement de journal de flux. En revanche, vous pouvez supprimer le journal de flux et en créer un autre avec la configuration requise.
- Si votre interface réseau comporte plusieurs adresses IPv4 et que le trafic est envoyé vers une adresse IPv4 privée secondaire, le journal de flux affiche l'adresse IPv4 privée principale dans le champ `dstaddr`. Pour capturer l'adresse IP de destination d'origine, créez un journal de flux avec le champ `pkt-dstaddr`.
- Si le trafic est envoyé à une interface réseau et que la destination n'est pas l'une des adresses IP de l'interface réseau, le journal de flux affiche l'adresse IPv4 privée principale dans le champ `dstaddr`. Pour capturer l'adresse IP de destination d'origine, créez un journal de flux avec le champ `pkt-dstaddr`.
- Si le trafic est envoyé depuis une interface réseau et que la source n'est pas l'une des adresses IP de l'interface réseau, le journal de flux affiche l'adresse IPv4 privée principale dans le champ `srcaddr`. Pour capturer l'adresse IP source d'origine, créez un journal de flux avec le champ `pkt-srcaddr`.
- Si le trafic est envoyé depuis ou vers une interface réseau, les champs `srcaddr` et `dstaddr` du journal de flux affichent toujours l'adresse IPv4 privée principale, quelle que soit la source ou la destination du paquet. Pour capturer la source ou la destination du paquet, créez un journal de flux avec les champs `pkt-srcaddr` et `pkt-dstaddr`.

- Lorsque votre interface réseau est attachée à une instance basée sur Nitro, l'intervalle d'agrégation est toujours d'une minute maximum, quel que soit l'intervalle d'agrégation maximal spécifié.

Les journaux de flux ne capturent pas tout le trafic IP. Les types de trafic suivants ne sont pas consignés :

- Le trafic généré par des instances lorsqu'elles contactent le serveur DNS Amazon. Si vous utilisez votre propre serveur DNS, tout le trafic vers ce dernier est consigné.
- Le trafic généré par une instance Windows pour l'activation de la licence Windows d'Amazon.
- Le trafic depuis et vers `169.254.169.254` pour les métadonnées de l'instance.
- Le trafic depuis et vers `169.254.169.123` pour Amazon Time Sync Service.
- Le trafic DHCP.
- Trafic en miroir.
- Le trafic vers l'adresse IP réservée pour le routeur VPC par défaut.
- Trafic entre une interface réseau de point de terminaison et une interface réseau de Network Load Balancer.

Limitations spécifiques aux champs ECS disponibles dans la version 7 :

- Pour créer des abonnements aux journaux de flux avec des champs ECS, votre compte doit contenir au moins un cluster ECS.
- Les champs ECS ne sont pas calculés si les tâches ECS sous-jacentes ne sont pas détenues par le propriétaire de l'abonnement au journal de flux. Par exemple, si vous partagez un sous-réseau (`SubnetA`) avec un autre compte (`AccountB`), puis que vous créez un abonnement au journal de flux pour`SubnetA`, si vous `AccountB` lancez des tâches ECS dans le sous-réseau partagé, votre abonnement recevra les journaux de trafic des tâches ECS lancées par, `AccountB` mais les champs ECS de ces journaux ne seront pas calculés pour des raisons de sécurité.
- Si vous créez des abonnements aux journaux de flux avec des champs ECS au niveau des ressources du VPC/sous-réseau, tout trafic généré pour les interfaces réseau autres qu'ECS sera également fourni pour vos abonnements. Les valeurs des champs ECS seront « - » pour le trafic IP non ECS. Par exemple, vous avez un sous-réseau (`subnet-000000`) et vous créez un abonnement au journal de flux pour ce sous-réseau avec des champs ECS ()`fl-00000000`. Dans`subnet-000000`, vous lancez une instance EC2 (`i-0000000`) connectée à Internet et générant activement du trafic IP. Vous lancez également une tâche ECS en cours d'exécution (`ECS-Task-1`) dans le même sous-réseau. Étant donné que `i-0000000` `ECS-Task-1` les deux

entités génèrent du trafic IP, votre abonnement aux journaux de flux `fl-00000000` fournira des journaux de trafic pour les deux entités. Toutefois, seules les métadonnées ECS réelles `ECS-Task-1` seront disponibles pour les champs ECS que vous avez inclus dans votre LogFormat. Pour le trafic `i-0000000` associé, ces champs auront la valeur « - ».

- `ecs-container-id`et `ecs-second-container-id` sont classés au fur et à mesure que le service VPC Flow Logs les reçoit du flux d'événements ECS. Il n'est pas garanti qu'ils soient dans le même ordre que celui dans lequel vous les voyez sur la console ECS ou dans l'appel DescribeTask d'API. Si un conteneur passe à l'état STOPPÉ alors que la tâche est toujours en cours d'exécution, il peut continuer à apparaître dans votre journal.
- Les métadonnées ECS et les journaux de trafic IP proviennent de deux sources différentes. Nous commençons à calculer votre trafic ECS dès que nous obtenons toutes les informations requises auprès des dépendances en amont. Une fois que vous avez démarré une nouvelle tâche, nous commençons à calculer vos champs ECS 1) lorsque nous recevons du trafic IP pour l'interface réseau sous-jacente et 2) lorsque nous recevons l'événement ECS qui contient les métadonnées de votre tâche ECS indiquant que la tâche est en cours d'exécution. Lorsque vous arrêtez une tâche, nous arrêtons de calculer vos champs ECS 1) lorsque nous ne recevons plus de trafic IP pour l'interface réseau sous-jacente ou lorsque nous recevons du trafic IP retardé de plus d'une journée et 2) lorsque nous recevons l'événement ECS contenant les métadonnées de votre tâche ECS indiquant que votre tâche n'est plus en cours d'exécution.
- Seules les tâches ECS lancées en mode `awsvpc` réseau sont prises en charge.

Tarification

Les frais d'ingestion et d'archivage de données pour les journaux payants s'appliquent lorsque vous publiez des journaux de flux. Pour plus d'informations sur la tarification lors de la publication de journaux vendus, ouvrez Amazon CloudWatch Pricing, sélectionnez Logs et recherchez Vended Logs.

Pour suivre les frais de publication des journaux de flux, vous pouvez appliquer des balises d'allocation des coûts à votre ressource de destination. Par la suite, votre rapport de répartition des AWS coûts inclut l'utilisation et les coûts agrégés par ces balises. Vous pouvez appliquer des balises associées à des catégories métier (telles que les centres de coûts, les noms d'applications ou les propriétaires) pour organiser les coûts relatifs à divers services. Pour plus d'informations, consultez les ressources suivantes :

- Utilisation des balises de répartition des coûts dans le Guide de l'utilisateur AWS Billing .

- Étiquetez les groupes de CloudWatch journaux dans Amazon Logs dans le guide de l'utilisateur Amazon CloudWatch Logs
- Utilisation des balises de répartition des coûts pour les compartiments S3dans le Guide de l'utilisateur Amazon Simple Storage
- Marquer vos flux de diffusion dans le guide du développeur Amazon Data Firehose

Utiliser des journaux de flux

Vous pouvez utiliser les journaux de flux à l'aide des consoles Amazon EC2 et Amazon VPC.

Tâches

- Contrôler l'utilisation des journaux de flux
- Créer un journal de flux
- Afficher un journal de flux
- Marquer un journal de flux
- Supprimer un journal de flux
- Présentation des API et de l'interface de ligne de commande (CLI)

Contrôler l'utilisation des journaux de flux

Par défaut, les utilisateurs ne sont pas autorisés à utiliser des journaux de flux. Vous pouvez créer un rôle IAM avec une politique attachée qui autorise les utilisateurs à créer, décrire et supprimer des journaux de flux.

Voici un exemple de politique qui accorde aux utilisateurs les autorisations complètes pour créer, décrire et supprimer des journaux de flux.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
```

```
      ],
      "Resource": "*"
    }
  ]
}
```

Pour plus d'informations, consultez the section called "Fonctionnement d'Amazon VPC avec IAM".

Créer un journal de flux

Vous pouvez créer des journaux de flux pour vos VPC, sous-réseaux ou interfaces réseau. Lorsque vous créez un journal de flux, vous devez spécifier sa destination. Pour plus d'informations, consultez les ressources suivantes :

- the section called "Créez un journal de flux qui publie dans CloudWatch Logs"
- the section called "Créer un journal de flux qui publie vers Amazon S3"
- the section called "Créez un journal de flux qui sera publié sur Amazon Data Firehose"

Afficher un journal de flux

Vous pouvez consulter des informations sur les journaux de flux d'une ressource, telle qu'une interface réseau. Les informations affichées incluent l'ID du journal de flux, sa configuration et des informations sur son statut.

Pour consulter des informations sur les journaux de flux

1. Effectuez l'une des actions suivantes :
   - Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/. Dans le volet de navigation, choisissez Network Interfaces. Cochez la case correspondant à l'interface réseau.
   - Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, sélectionnez Vos VPC. Cochez la case correspondant au VPC.
   - Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux). Cochez la case correspondant au sous-réseau.
2. Choisissez Flow Logs (Journaux de flux).
3. (Facultatif) Pour afficher les données du journal de flux, ouvrez la destination du journal.

Marquer un journal de flux

Vous pouvez ajouter ou supprimer des balises pour un journal de flux à tout moment.

Pour gérer les balises d'un journal de flux

1. Effectuez l'une des actions suivantes :
   - Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/. Dans le volet de navigation, choisissez Network Interfaces. Cochez la case correspondant à l'interface réseau.
   - Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, sélectionnez Vos VPC. Cochez la case correspondant au VPC.
   - Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux). Cochez la case correspondant au sous-réseau.
2. Choisissez Flow Logs (Journaux de flux).
3. Choisissez Actions, Manage tags (Gérer les balises).
4. Pour ajouter une nouvelle étiquette, choisissez Add new tag (Ajouter une nouvelle étiquette), puis entrez la clé et la valeur de l'étiquette. Pour supprimer une identification, choisissez Supprimer.
5. Lorsque vous avez terminé d'ajouter ou de supprimer des balises, choisissez Save (Enregistrer).

Supprimer un journal de flux

Vous pouvez supprimer un journal de flux à tout moment. Une fois que vous supprimez un journal de flux, plusieurs minutes peuvent s'écouler avant qu'il ne cesse de collecter des données.

La suppression d'un journal de flux ne supprime pas les données de journal de la destination et ne modifie pas la ressource de destination. Vous devez supprimer les données du journal de flux existant directement depuis la destination et nettoyer la ressource de destination à l'aide de la console du service de destination.

Pour supprimer un journal de flux

1. Effectuez l'une des actions suivantes :

- Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/. Dans le volet de navigation, choisissez Network Interfaces. Cochez la case correspondant à l'interface réseau.
- Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, sélectionnez Vos VPC. Cochez la case correspondant au VPC.
- Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux). Cochez la case correspondant au sous-réseau.

2. Choisissez Flow Logs (Journaux de flux).
3. Choisissez Actions, Delete flow logs (Supprimer les journaux de flux).
4. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

Présentation des API et de l'interface de ligne de commande (CLI)

Vous pouvez exécuter les tâches décrites sur cette page à l'aide de la ligne de commande ou de l'API. Pour plus d'informations sur les interfaces de ligne de commande et la liste des actions liées aux API disponibles, consultez Utilisation d'Amazon VPC.

Créer un journal de flux

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)
- CreateFlowJournaux (API de requête Amazon EC2)

Décrire un journal de flux

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)
- DescribeFlowJournaux (API de requête Amazon EC2)

Baliser un journal de flux

- create-tags et delete-tags (AWS CLI)
- New-EC2Taget Remove-EC2Tag(AWS Tools for Windows PowerShell)
- CreateTagset DeleteTags(API de requête Amazon EC2)

Supprimer un journal de flux

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlowJournaux (API de requête Amazon EC2)

Publier les journaux de flux dans CloudWatch Logs

Les journaux de flux peuvent publier les données des journaux de flux directement sur Amazon CloudWatch.

Lors de la publication dans CloudWatch Logs, les données du journal de flux sont publiées dans un groupe de journaux, et chaque interface réseau possède un flux de journal unique dans le groupe de journaux. Les flux de journaux contiennent des enregistrements de journaux de flux. Vous pouvez créer plusieurs journaux de flux qui publient des données dans le même groupe de journaux. Si la même interface réseau est présente dans un ou plusieurs journaux de flux d'un même groupe de journaux, elle dispose d'un flux de journaux combiné. Si vous avez indiqué qu'un journal de flux doit capturer le trafic refusé et que l'autre journal de flux doit capturer le trafic accepté, le flux de journaux combiné capture l'ensemble du trafic.

Dans CloudWatch Logs, le champ d'horodatage correspond à l'heure de début enregistrée dans l'enregistrement du journal de flux. Le champ IngestionTime indique la date et l'heure auxquelles l'enregistrement du journal de flux a été reçu par Logs. CloudWatch Cet horodatage est ultérieur à l'heure de fin capturée dans l'enregistrement du journal de flux.

Pour plus d'informations sur CloudWatch les journaux, consultez la section Journaux envoyés à CloudWatch Logs dans le guide de l'utilisateur Amazon CloudWatch Logs.

Tarification

Les frais d'ingestion de données et d'archivage pour les journaux vendus s'appliquent lorsque vous publiez des journaux de flux dans Logs. CloudWatch Pour plus d'informations, ouvrez Amazon CloudWatch Pricing, sélectionnez Logs et recherchez Vended Logs.

Table des matières

- Créez un journal de flux qui publie dans CloudWatch Logs
- Afficher les enregistrements de journaux de flux
- Rechercher des enregistrements de journaux de flux
- Enregistrements du flux de processus dans CloudWatch Logs

Rôle IAM pour la publication des journaux de flux dans Logs CloudWatch

Le rôle IAM associé à votre journal de flux doit disposer d'autorisations suffisantes pour publier des journaux de flux dans le groupe de journaux spécifié dans CloudWatch Logs. Le rôle IAM doit appartenir à votre AWS compte.

La stratégie IAM associée à votre rôle IAM; doit au moins inclure les autorisations suivantes :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

Assurez-vous que votre rôle possède la politique de confiance suivante, qui permet au service de journaux de flux d'assumer le rôle.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
```

```
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Nous vous recommandons d'utiliser les clés de condition `aws:SourceAccount` et `aws:SourceArn` pour vous protéger contre le problème du député confus. Par exemple, vous pouvez ajouter le bloc de condition suivant à la stratégie d'approbation précédente. Le compte source est le propriétaire du journal de flux et l'ARN source est l'ARN du journal de flux. Si vous ne connaissez pas l'ID du journal de flux, vous pouvez remplacer cette partie de l'ARN par un caractère générique (*), puis mettre à jour la stratégie après avoir créé le journal de flux.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

Créer un rôle IAM pour les journaux de flux

Vous pouvez mettre à jour un rôle existant comme décrit ci-dessus. Vous pouvez également utiliser la procédure suivante pour créer un nouveau rôle à utiliser avec les journaux de flux. Vous allez spécifier ce rôle lors de la création du journal de flux.

Création d'un rôle IAM pour les journaux de flux

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Policies (Politiques).
3. Sélectionnez Create policy (Créer une politique).
4. Sur la page Create policy (Créer une stratégie), procédez comme suit :
    a. Choisissez JSON.
    b. Remplacez le contenu de cette fenêtre par la politique d'autorisations au début de cette section.
    c. Choisissez Suivant.

d. Entrez un nom pour votre politique ainsi qu'une description et des balises facultatives, puis choisissez Créer une politique.

5. Dans le panneau de navigation, choisissez Roles (Rôles).
6. Sélectionnez Create role (Créer un rôle).
7. Pour Trusted entity type (Type d'entité de confiance), choisissez Custom trust policy (Politique de confiance personnalisée). Pour Custom trust policy (Politique de confiance personnalisée), remplacez `"Principal": {},` par ce qui suit, puis choisissez Next (Suivant).

```
"Principal": {
   "Service": "vpc-flow-logs.amazonaws.com"
},
```

8. Sur la page Add permissions (Ajouter des autorisations), cochez la case correspondant à la politique que vous avez créée plus tôt dans cette procédure, puis choisissez Next (Suivant).
9. Entrez un nom pour votre rôle et fournissez une description, le cas échéant.
10. Sélectionnez Créer un rôle.

Autorisations pour les responsables IAM qui publient des journaux de flux dans Logs CloudWatch

Vérifiez que le principal IAM que vous utilisez pour effectuer la demande est autorisé à lancer l'`iam:PassRole`action.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

Créez un journal de flux qui publie dans CloudWatch Logs

Vous pouvez créer des journaux de flux pour vos VPC, sous-réseaux ou interfaces réseau. Si vous effectuez ces étapes en tant qu'utilisateur utilisant un rôle IAM particulier, assurez-vous que ce rôle

dispose des autorisations nécessaires pour utiliser l'action `iam:PassRole`. Pour plus d'informations, consultez Autorisations pour les responsables IAM qui publient des journaux de flux dans Logs CloudWatch .

Prérequis

- Créez un rôle IAM, comme décrit dans the section called "Rôle IAM pour la publication des journaux de flux dans Logs CloudWatch ".

Pour créer un journal de flux à l'aide de la console

1. Effectuez l'une des actions suivantes :
   - Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/. Dans le volet de navigation, choisissez Network Interfaces. Cochez la case correspondant à l'interface réseau.
   - Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, sélectionnez Vos VPC. Cochez la case correspondant au VPC.
   - Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux). Cochez la case correspondant au sous-réseau.
2. Choisissez Actions, Create flow log (Créer le journal de flux).
3. Pour Filter (Filtre), spécifiez le type de trafic à journaliser. Sélectionnez All (Tout) pour journaliser le trafic accepté et refusé, Reject (Rejeter) pour enregistrer uniquement le trafic refusé ou Accept (Accepter) pour enregistrer uniquement le trafic accepté.
4. Pour Maximum aggregation interval (Intervalle d'agrégation maximal), choisissez la période maximale pendant laquelle un flux est capturé et agrégé dans un enregistrement de journal de flux.
5. Pour Destination, choisissez Envoyer vers CloudWatch les journaux.
6. Dans Groupe de journaux de destination, sélectionnez le nom d'un groupe de journaux existant ou entrez le nom d'un nouveau groupe de journaux qui sera créé lors de la création de ce journal de flux.
7. Pour le rôle IAM, spécifiez le nom du rôle autorisé à publier des journaux dans CloudWatch Logs.
8. Pour Log record format (Format d'enregistrement du journal), sélectionnez le format de l'enregistrement du journal de flux.

- Pour utiliser le format par défaut, choisissez AWS default format (Format par défaut).
- Pour utiliser un format personnalisé, choisissez Custom format (Format personnalisé), puis sélectionnez des champs dans Log format (Format du journal).

9. Pour Métadonnées supplémentaires, indiquez si vous souhaitez inclure les métadonnées d'Amazon ECS dans le format du journal.
10. (Facultatif) Sélectionnez Add new tag (Ajouter une nouvelle balise) pour appliquer des identifications au journal de flux.
11. Choisissez Créer le journal de flux.

Pour créer un journal de flux à l'aide de la ligne de commande

Utilisez l'une des commandes suivantes.

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)

L' AWS CLI exemple suivant crée un journal de flux qui capture tout le trafic accepté pour le sous-réseau spécifié. Les journaux de flux sont transmis au groupe de journaux spécifié. Le `--deliver-logs-permission-arn` paramètre spécifie le rôle IAM requis pour publier dans CloudWatch Logs.

```
aws ec2 create-flow-logs --resource-type Subnet --resource-ids subnet-1a2b3c4d --
traffic-type ACCEPT --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

Afficher les enregistrements de journaux de flux

Vous pouvez consulter les enregistrements de vos journaux de flux à l'aide de la console CloudWatch Logs. Après la création de votre journal de flux, quelques minutes peuvent s'écouler avant qu'il ne soit visible dans la console.

Pour consulter les enregistrements du journal de flux publiés dans CloudWatch Logs à l'aide de la console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation de gauche, choisissez Logs (Journaux), Log groups (Groupes de journaux).

3. Sélectionnez le nom du groupe de journaux contenant vos journaux de flux pour ouvrir la page de détails correspondante.
4. Sélectionnez le nom du flux de journaux contenant les enregistrements du journal de flux. Pour plus d'informations, consultez Enregistrements de journaux de flux.

Pour afficher les enregistrements du journal de flux publiés dans CloudWatch Logs à l'aide de la ligne de commande

- get-log-events (AWS CLI)
- Obtenez un appel () LogEventAWS Tools for Windows PowerShell

Rechercher des enregistrements de journaux de flux

Vous pouvez rechercher les enregistrements de vos journaux de flux publiés dans CloudWatch Logs à l'aide de la console CloudWatch Logs. Vous pouvez utiliser des filtres de métrique pour filtrer les enregistrements de journal de flux. Les enregistrements de journaux de flux sont délimités par un espace.

Pour rechercher des enregistrements de journaux de flux à l'aide de la console CloudWatch Logs

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation de gauche, choisissez Logs (Journaux), Log groups (Groupes de journaux).
3. Sélectionnez le groupe de journaux qui contient votre journal de flux, puis sélectionnez le flux de journaux si vous connaissez l'interface réseau que vous recherchez. Sinon, choisissez Search log group (Rechercher dans le groupe de journaux). Cela peut prendre un certain temps s'il existe de nombreuses interfaces réseau dans votre groupe de journaux, ou en fonction de la plage de temps que vous sélectionnez.
4. Sous Filtrer les événements, entrez la chaîne ci-dessous. Cela suppose que l'enregistrement de journaux de flux utilise le format par défaut.

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport, protocol,
 packets, bytes, start, end, action, logstatus]
```

5. Modifiez le filtre selon vos besoins en spécifiant des valeurs pour les champs. Dans les exemples suivants, le filtrage a lieu en fonction d'adresses IP source spécifiques.

```
[version, accountid, interfaceid, srcaddr = 10.0.0.1, dstaddr, srcport, dstport,
 protocol, packets, bytes, start, end, action, logstatus]
[version, accountid, interfaceid, srcaddr = 10.0.2.*, dstaddr, srcport, dstport,
 protocol, packets, bytes, start, end, action, logstatus]
```

Les exemples suivants sont filtrés par port de destination, le nombre d'octets et le rejet éventuel du trafic.

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
 dstport = 8080, protocol, packets, bytes, start, end, action, logstatus]
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
 dstport = 8080, protocol, packets, bytes >= 400, start, end, action = REJECT,
 logstatus]
```

Enregistrements du flux de processus dans CloudWatch Logs

Vous pouvez utiliser les enregistrements des journaux de flux comme vous le feriez avec tout autre événement de journal collecté par CloudWatch Logs. Pour plus d'informations sur la surveillance des données de journal et les filtres métriques, consultez la section Recherche et filtrage des données de journal dans le guide de CloudWatch l'utilisateur Amazon.

Exemple : création d'un filtre CloudWatch métrique et d'une alarme pour un journal de flux

Dans cet exemple, vous avez un journal de flux pour `eni-1a2b3c4d`. Vous souhaitez créer une alarme qui vous alerte si au moins 10 tentatives de connexion à votre instance via le port TCP 22 (SSH) sont refusées dans un laps de temps d'une heure. Tout d'abord, vous devez créer un filtre de métrique qui correspond au modèle de trafic pour lequel créer l'alarme. Vous pouvez ensuite créer une alarme pour le filtre de métrique.

Pour créer un filtre de métrique pour le trafic SSH refusé et une alarme pour ce filtre :

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation de gauche, choisissez Logs (Journaux), Log groups (Groupes de journaux).
3. Cochez la case en regard du groupe de journaux, puis choisissez Actions, Create metric filter (Créer un filtre de métrique).
4. Pour Filter pattern (Modèle de filtre), entrez la chaîne suivante.

```
[version, account, eni, source, destination, srcport, destport="22", protocol="6",
 packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]
```

5. Pour Select log data to test (Sélectionner les données de journal à tester), sélectionnez le flux de journal de votre interface réseau. (Facultatif) Pour afficher les lignes de données de journal qui correspondent au modèle de filtre, choisissez Test pattern (Tester le modèle).
6. Lorsque vous avez terminé, choisissez Next (Suivant).
7. Entrez un nom de filtre, un espace de noms de mesure et un nom de métrique. Définissez la valeur de métrique sur 1. Lorsque vous avez terminé, choisissez Next (Suivant), puis Create metric filter (Créer un filtre de métrique).
8. Dans le panneau de navigation, choisissez Alarms (Alarmes), All alarms (Toutes les alarmes).
9. Choisissez Create alarm (Créer une alerte).
10. Sélectionnez le nom de la métrique que vous avez créée, puis sélectionnez Sélectionner une métrique.
11. Configurez l'alarme comme suit, puis choisissez Next (Suivant) :
    - Pour Statistics (Statistique), choisissez Sum (Somme). Ainsi, vous capturez le nombre total de points de données pour la période spécifiée.
    - Pour Period (Période), choisissez 1 hour (1 heure).
    - Pour chaque fois que TimeSinceLastActive c'est... , choisissez Greater/Equal et entrez 10 comme seuil.
    - Sous Additional configuration (Configuration supplémentaire), conservez la valeur 1 pour Datapoints to alarm (Points de données à signaler).
12. Choisissez Suivant.
13. Pour Notification, sélectionnez une rubrique SNS existante ou choisissez Create new topic (Créer une rubrique) pour en créer une nouvelle. Choisissez Next (Suivant).
14. Saisissez le nom et la description de l'alarme, puis choisissez Next (Suivant).
15. Lorsque vous avez fini de prévisualiser l'alarme, choisissez Créer une alarme.

Publier des journaux vers flux sur Amazon S3

Les journaux de flux peuvent publier des données de journal de flux vers Amazon S3.

Lors de la publication vers Amazon S3, les données de journal de flux sont publiées dans un compartiment Amazon S3 existant que vous indiquez. Les enregistrements de journaux de flux pour toutes les interfaces réseau surveillées sont publiés dans une série d'objets de fichier journal qui sont stockés dans le compartiment. Si le journal de flux capture des données pour un VPC, il publie les enregistrements de journaux de flux pour toutes les interfaces réseau dans le VPC sélectionné.

Pour créer un compartiment Amazon S3 à utiliser avec les journaux de flux, reportez-vous à Créer un compartiment dans le Guide de l'utilisateur Amazon Simple Storage Service.

Pour plus d'informations sur la journalisation de plusieurs comptes, veuillez consulter Journalisation centrale dans la bibliothèque de solutions AWS .

Pour plus d'informations sur CloudWatch les journaux, consultez la section Journaux envoyés à Amazon S3 dans le guide de l'utilisateur Amazon CloudWatch Logs.

Tarification

Les frais d'ingestion et d'archivage de données pour les journaux mis à payants s'appliquent lorsque vous publiez des journaux de flux vers Amazon S3. Pour plus d'informations, ouvrez Amazon CloudWatch Pricing, sélectionnez Logs et recherchez Vended Logs.

Table des matières

Fichiers journaux de flux

VPC Flow Logs collecte des données sur le trafic IP entrant et sortant de votre VPC dans des enregistrements de journal, agrège ces enregistrements dans des fichiers journaux, puis publie les fichiers journaux dans le compartiment Amazon S3 à intervalles de 5 minutes. Plusieurs

fichiers peuvent être publiés et chaque fichier journal peut contenir une partie ou la totalité des enregistrements du journal de flux pour le trafic IP enregistré au cours des 5 minutes précédentes.

Dans Amazon S3, le champ Last modified (Dernière modification) du fichier de journal de flux indique la date et l'heure du téléchargement du fichier dans le compartiment Amazon S3. Cette date est postérieure à l'horodatage du nom du fichier et diffère par le temps nécessaire pour charger le fichier vers le compartiment Amazon S3.

Format de fichier journal

Vous pouvez spécifier l'un des formats suivants pour les fichiers journaux. Chaque fichier est compressé dans un seul fichier Gzip.

- Text : texte brut. Il s'agit du format par défaut.
- Parquet : Apache Parquet est un format de données en colonnes. Les requêtes sur les données au format Parquet sont 10 à 100 fois plus rapides que les requêtes sur des données en texte brut. Les données au format Parquet avec compression Gzip occupent 20 % moins d'espace de stockage que le texte brut avec compression Gzip.

> **Note**
>
> Si les données en format Parquet avec compression Gzip sont inférieures à 100 Ko par période d'agrégation, le stockage des données en format Parquet peut prendre plus de place que le texte brut avec compression Gzip en raison des exigences de mémoire de fichiers Parquet.

Options de fichier journal

Le cas échéant, vous pouvez spécifier les options suivantes :

- Hive-compatible S3 prefixes (Préfixes S3 compatibles Hive) : activez les préfixes compatibles Hive au lieu d'importer des partitions dans vos outils compatibles Hive. Avant d'exécuter des requêtes, utilisez la commande MSCK REPAIR TABLE.
- Hourly partitions (Partitions horaires) : si vous disposez d'un grand volume de journaux et que vous ciblez généralement les requêtes à une heure spécifique, vous pouvez obtenir des résultats plus rapidement et économiser sur les coûts des requêtes en partitionnant les journaux toutes les heures.

Structure du compartiment S3 du fichier journal

Les fichiers journaux sont enregistrés dans le compartiment Amazon S3 indiqué à l'aide d'une structure de dossiers qui est déterminée par l'ID du journal de flux, sa région, sa date de création et ses options de destination.

Par défaut, les fichiers sont distribués vers l'emplacement suivant.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Si vous activez les préfixes S3 compatibles Hive, les fichiers sont envoyés à l'emplacement suivant.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/
```

Si vous activez les partitions horaires, les fichiers sont envoyés à l'emplacement suivant.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

Si vous activez les partitions compatibles Hive et que vous partitionnez le journal de flux par heure, les fichiers sont envoyés à l'emplacement suivant.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/hour=hour/
```

Noms des fichiers journaux

Le nom de fichier d'un fichier journal est basé sur l'ID du journal de flux, la région et la date et l'heure de création. Les noms de fichier utilisent le format suivant.

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

Voici un exemple de fichier journal pour un flux de journal créé par le compte AWS 123456789012, pour une ressource dans la région us-east-1, le June 20, 2018 à 16:20 UTC. Le fichier contient les enregistrements de journaux de flux avec une heure de fin comprise entre 16:20:00 et 16:24:59.

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

Autorisations pour les principaux IAM qui publient des journaux de flux vers Amazon S3

Le principal IAM qui crée le journal de flux doit utiliser un rôle IAM qui dispose des autorisations suivantes, nécessaires pour publier les journaux de flux dans le compartiment Amazon S3 de destination.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource": "*"
    }
  ]
}
```

Autorisations du compartiment Amazon S3 pour les journaux de flux

Par défaut, les compartiments Amazon S3 et les objets qu'ils contiennent sont privés. Seul le propriétaire du compartiment peut accéder au compartiment et aux objets qui y sont stockés. Cependant, le propriétaire du compartiment peut accorder l'accès à d'autres ressources et à d'autres utilisateurs en créant une politique d'accès.

Si l'utilisateur qui crée le journal de flux est le propriétaire du compartiment et dispose des autorisations `PutBucketPolicy` et `GetBucketPolicy` pour le compartiment, nous attachons automatiquement la stratégie suivante au compartiment. Cette politique remplace toute politique existante attachée au compartiment.

Sinon, le propriétaire du compartiment doit ajouter cette stratégie au compartiment en spécifiant l'ID du compte AWS du créateur du journal de flux. Sinon, la création du journal de flux échoue. Pour plus d'informations, consultez Utilisation de stratégies de compartiment dans le Guide de l'utilisateur Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "my-s3-arn/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id,
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketAcl",
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        }
    ]
}
```

L'ARN que vous spécifiez pour *my-s3-arn* varie selon que vous utilisez des préfixes S3 compatibles avec Hive.

- Préfixes par défaut

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- Préfixes S3 compatibles avec Hive

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

Il est recommandé d'accorder ces autorisations au principal du service de livraison des journaux plutôt qu'à des Compte AWS ARN individuels. Une autre bonne pratique consiste également à utiliser les clés de condition `aws:SourceAccount` et `aws:SourceArn` afin de vous protéger contre le problème du député confus. Le compte source est le propriétaire du journal de flux et l'ARN source est l'ARN à caractère générique (*) du service de journaux.

Politique de clé obligatoire à utiliser avec SSE-KMS

Vous pouvez protéger les données de votre compartiment Amazon S3 en activant le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) ou le chiffrement côté serveur avec des clés KMS (SSE-KMS) sur votre compartiment S3. Pour plus d'informations, consultez la section Protection des données à l'aide d'un chiffrement côté serveur dans le Guide de l'utilisateur d'Amazon S3.

Si vous choisissez l'option SSE-S3, aucune configuration supplémentaire n'est requise. Amazon S3 gère la clé de chiffrement.

Si vous choisissez l'option SSE-KMS, vous devez utiliser un ARN de clé gérée par le client. Si vous utilisez un identifiant de clé, vous pouvez rencontrer une erreur LogDestination non livrable lors de la création d'un journal de flux. De même, vous devez mettre à jour la stratégie de clé gérée par le client afin que le compte de diffusion des journaux puisse écrire des données dans votre compartiment S3. Pour plus d'informations sur la politique de clé requise pour une utilisation avec SSE-KMS, consultez le chiffrement côté serveur du compartiment Amazon S3 dans le guide de l'utilisateur Amazon CloudWatch Logs.

Autorisations pour les fichiers journaux Amazon S3

Outre les stratégies de compartiment obligatoires, Amazon S3 utilise des listes de contrôle d'accès (ACL) afin de gérer l'accès aux fichiers journaux créés par un journal de flux. Par défaut, le propriétaire du compartiment dispose d'autorisations `FULL_CONTROL` sur chaque fichier journal. Si le propriétaire de la diffusion des journaux n'est pas le propriétaire du compartiment, il ne dispose

d'aucune autorisation. Le compte de diffusion des journaux possède les autorisations `READ` et `WRITE`. Pour de plus amples informations, veuillez consulter Présentation des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Créer un journal de flux qui publie vers Amazon S3

Après avoir créé et configuré votre compartiment Amazon S3, vous pouvez créer des journaux de flux pour vos interfaces réseaux, sous-réseaux ou et VPC.

Pour créer un journal de flux à l'aide de la console

1. Effectuez l'une des actions suivantes :
   - Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/. Dans le volet de navigation, choisissez Network Interfaces. Cochez la case correspondant à l'interface réseau.
   - Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, sélectionnez Vos VPC. Cochez la case correspondant au VPC.
   - Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux). Cochez la case correspondant au sous-réseau.
2. Choisissez Actions, Create flow log (Créer le journal de flux).
3. Pour Filter (Filtrer), spécifiez le type de données de trafic IP à journaliser.
   - Accepter — Consigne uniquement le trafic accepté.
   - Rejeter — Consigne uniquement le trafic rejeté.
   - All (Tout) : journalise le trafic accepté et rejeté.
4. Pour Maximum aggregation interval ((Intervalle d'agrégation maximal), choisissez la période maximale pendant laquelle un flux est capturé et agrégé dans un enregistrement de journal de flux.
5. Pour Destination, choisissez (Send to an Amazon S3 bucket)Envoyer vers un compartiment Amazon S3.
6. Pour S3 bucket ARN (ARN de compartiment S3)), indiquez l'Amazon Resource Name (ARN) d'un compartiment Amazon S3 existant. Vous pouvez éventuellement inclure un sous-dossier. Par exemple, pour spécifier le sous-dossier `my-logs` dans me compartiment `my-bucket`, utilisez l'ARN suivant :

   ```
   arn:aws:s3:::my-bucket/my-logs/
   ```

Le compartiment ne peut pas utiliser `AWSLogs` comme nom de sous-dossier, car il s'agit d'un terme réservé.

Si vous êtes le propriétaire du compartiment, nous créons automatiquement une politique de ressource et l'attachons au compartiment. Pour de plus amples informations, veuillez consulter Autorisations du compartiment Amazon S3 pour les journaux de flux.

7. Pour Log record format (Format d'enregistrement du journal), sélectionnez le format de l'enregistrement du journal de flux.
   - Pour utiliser le format de registre de journal de flux par défaut, sélectionnez AWS default format (Format par défaut).
   - Pour créer un format personnalisé, choisissez Custom format (Format personnalisé). Pour Log format (Format de journal), choisissez les champs à inclure dans l'enregistrement de journal de flux.
8. Pour Métadonnées supplémentaires, indiquez si vous souhaitez inclure les métadonnées d'Amazon ECS dans le format du journal.
9. Pour Format du fichier journal, spécifiez le format du fichier journal.
   - Text : texte brut. Il s'agit du format par défaut.
   - Parquet : Apache Parquet est un format de données en colonnes. Les requêtes sur les données au format Parquet sont 10 à 100 fois plus rapides que les requêtes sur des données en texte brut. Les données au format Parquet avec compression Gzip occupent 20 % moins d'espace de stockage que le texte brut avec compression Gzip.
10. (Facultatif) Pour utiliser des préfixes S3 compatibles avec Hive, choisissez Hive-compatible S3 prefix (Préfixe S3 compatible HIVE), Enable. (Activer).
11. (Facultatif) Pour partitionner vos journaux de flux par heure, choisissez Every 1 hour (60 mins) (Toutes les 1 heure (60 minutes)).
12. (Facultatif) Pour ajouter une identification au journal de flux, choisissez Add new tag (Ajouter une nouvelle identification) et spécifiez la clé et la valeur de l'identification.
13. Choisissez Create flow log. (Créer le journal de flux).

Pour créer un journal de flux qui publie vers Amazon S3 à l'aide de l'outil de ligne de commande

Utilisez l'une des commandes suivantes :

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)

L' AWS CLI exemple suivant crée un journal de flux qui capture tout le trafic pour le VPC spécifié et fournit les journaux de flux au compartiment Amazon S3 spécifié. Le paramètre `--log-format` spécifie un format personnalisé pour les enregistrements de journal de flux.

```
aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-00112233344556677 --
traffic-type ALL --log-destination-type s3 --log-destination arn:aws:s3:::flow-log-
bucket/custom-flow-logs/ --log-format '${version} ${vpc-id} ${subnet-id} ${instance-
id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${tcp-flags} ${type} ${pkt-
srcaddr} ${pkt-dstaddr}'
```

Afficher les enregistrements de journaux de flux

Vous pouvez consulter vos enregistrements de journal de flux à l'aide de la console Amazon S3. Après la création de votre journal de flux, quelques minutes peuvent s'écouler avant qu'il ne soit visible dans la console.

Pour afficher des enregistrements de journal de flux publiés dans Amazon S3

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Sélectionnez le nom du compartiment pour ouvrir sa page de détails.
3. Accédez au dossier contenant les fichiers journaux. *Par exemple, préfixe/AWSLogs/account_id /vpcflowlogs/ region/year/month/day /.*
4. Cochez la case à côté du nom de fichier, puis choisissez Download (Télécharger).

Traiter des enregistrements de journal de flux dans Amazon S3

Les fichiers journaux sont compressés. Si vous ouvrez les fichiers journaux à l'aide de la console Amazon S3, ils sont décompressés et les enregistrements de journal de flux s'affichent. Si vous téléchargez les fichiers, vous devez les décompresser pour afficher les enregistrements de journaux de flux.

Vous pouvez également interroger les enregistrements de journal de flux dans les fichiers journaux à l'aide d'Amazon Athena. Amazon Athena est un service de requête interactif qui facilite l'analyse des données dans Amazon S3 à l'aide du langage SQL standard. Pour de plus amples d'informations,

veuillez consulter Interrogation des journaux de flux Amazon VPC dans le Guide de l'utilisateur Amazon Athena.

Publier des journaux de flux sur Amazon Data Firehose

Les journaux de flux peuvent publier les données des journaux de flux directement sur Amazon Data Firehose.

Lors de la publication sur Amazon Data Firehose, les données du journal de flux sont publiées dans un flux de diffusion Amazon Data Firehose, au format texte brut.

Tarification

Des frais d'ingestion et de diffusion standard s'appliquent. Pour plus d'informations, ouvrez Amazon CloudWatch Pricing, sélectionnez Logs et recherchez Vended Logs.

Table des matières

Rôles IAM pour la diffusion entre comptes

Lorsque vous publiez sur Amazon Data Firehose, vous pouvez choisir un flux de diffusion enregistré sur le même compte que la ressource à surveiller (le compte source) ou sur un autre compte (le compte de destination). Pour permettre la transmission de journaux de flux entre comptes à Amazon Data Firehose, vous devez créer un rôle IAM dans le compte source et un rôle IAM dans le compte de destination.

Rôles

Rôle du compte source

Dans le compte source, créez un rôle qui accorde les autorisations suivantes. Dans cet exemple, le rôle a pour nom `mySourceRole`, mais vous pouvez choisir un nom différent. La dernière instruction

permet au rôle dans le compte de destination d'assumer ce rôle. Les instructions de condition garantissent que ce rôle est transmis uniquement au service de diffusion de journaux, et uniquement lors de la surveillance de la ressource spécifiée. Lorsque vous créez votre politique, spécifiez les VPC, les interfaces réseau ou les sous-réseaux que vous surveillez à l'aide de la clé de condition `iam:AssociatedResourceARN`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
          "StringEquals": {
              "iam:PassedToService": "delivery.logs.amazonaws.com"
          },
          "StringLike": {
              "iam:AssociatedResourceARN": [
                  "arn:aws:ec2:region:source-account:vpc/vpc-00112233344556677"
              ]
          }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
          "logs:CreateLogDelivery",
          "logs:DeleteLogDelivery",
          "logs:ListLogDeliveries",
          "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}
```

Assurez-vous que ce rôle possède la politique de confiance suivante, qui permet au service de diffusion de journaux d'assumer ce rôle.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

À partir du compte source, observez la procédure suivante afin de créer le rôle.

Pour créer le rôle du compte source

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Policies (Politiques).
3. Sélectionnez Create policy (Créer une politique).
4. Sur la page Create policy (Créer une stratégie), procédez comme suit :
   a. Choisissez JSON.
   b. Remplacez le contenu de cette fenêtre par la politique d'autorisations au début de cette section.
   c. Choisissez Suivant.
   d. Entrez un nom pour votre politique ainsi qu'une description et des balises facultatives, puis choisissez Créer une politique.
5. Dans le panneau de navigation, choisissez Roles (Rôles).
6. Sélectionnez Create role (Créer un rôle).
7. Pour Trusted entity type (Type d'entité de confiance), choisissez Custom trust policy (Politique de confiance personnalisée). Pour Custom trust policy (Politique de confiance personnalisée), remplacez `"Principal": {},` par ce qui suit, qui spécifie le service de diffusion de journaux. Choisissez Suivant.

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. Sur la page Add permissions (Ajouter des autorisations), cochez la case correspondant à la politique que vous avez créée plus tôt dans cette procédure, puis choisissez Next (Suivant).
9. Entrez un nom pour votre rôle et fournissez une description, le cas échéant.
10. Sélectionnez Créer un rôle.

Rôle du compte de destination

Dans le compte de destination, créez un rôle dont le nom commence par AWSLogDeliveryFirehoseCrossAccountRole. Ce rôle doit accorder les autorisations suivantes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

Assurez-vous que ce rôle possède la politique de confiance suivante, qui permet au rôle que vous avez créé dans le compte source d'assumer ce rôle.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

À partir du compte de destination, appliquez la procédure suivante afin de créer le rôle.

Pour créer le rôle du compte de destination

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Policies (Politiques).
3. Sélectionnez Create policy (Créer une politique).
4. Sur la page Create policy (Créer une stratégie), procédez comme suit :
   a. Choisissez JSON.
   b. Remplacez le contenu de cette fenêtre par la politique d'autorisations au début de cette section.
   c. Choisissez Suivant.
   d. Entrez un nom pour votre politique commençant par AWSLogDeliveryFirehoseCrossAccountRole, puis choisissez Créer une politique.
5. Dans le panneau de navigation, choisissez Roles (Rôles).
6. Sélectionnez Create role (Créer un rôle).
7. Pour Trusted entity type (Type d'entité de confiance), choisissez Custom trust policy (Politique de confiance personnalisée). Pour Custom trust policy (Politique de confiance personnalisée), remplacez `"Principal": {},` par ce qui suit, qui spécifie le rôle de compte source. Choisissez Suivant.

   ```
   "Principal": {
      "AWS": "arn:aws:iam::source-account:role/mySourceRole"
   },
   ```

8. Sur la page Add permissions (Ajouter des autorisations), cochez la case correspondant à la politique que vous avez créée plus tôt dans cette procédure, puis choisissez Next (Suivant).
9. Entrez un nom pour votre rôle et fournissez une description, le cas échéant.
10. Sélectionnez Créer un rôle.

Créez un journal de flux qui sera publié sur Amazon Data Firehose

Vous pouvez créer des journaux de flux pour vos VPC, sous-réseaux ou interfaces réseau.

Prérequis

- Créez le flux de livraison Amazon Data Firehose de destination. Utilisez Direct Put en tant que source. Pour plus d'informations, consultez Création d'un flux de diffusion Amazon Data Firehose.
- Si vous publiez des journaux de flux sur un autre compte, créez les rôles IAM requis, comme décrit dans the section called "Rôles IAM pour la diffusion entre comptes".

Pour créer un journal de flux publié sur Amazon Data Firehose

1. Effectuez l'une des actions suivantes :
   - Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/. Dans le volet de navigation, choisissez Network Interfaces. Cochez la case correspondant à l'interface réseau.
   - Ouvrez la console VPC d'Amazon sur https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, sélectionnez Vos VPC. Cochez la case correspondant au VPC.
   - Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux). Cochez la case correspondant au sous-réseau.
2. Choisissez Actions, Create flow log (Créer le journal de flux).
3. Pour Filter (Filtre), spécifiez le type de trafic à journaliser.
   - Accept (Accepter) : journalise uniquement le trafic accepté
   - Reject (Rejeter) : journalise uniquement le trafic rejeté
   - All (Tout) : journalise le trafic accepté et rejeté
4. Pour Maximum aggregation interval (Intervalle d'agrégation maximal), choisissez la période maximale pendant laquelle un flux est capturé et agrégé dans un enregistrement de journal de flux.
5. Pour Destination, choisissez l'une ou l'autre des options suivantes :
   - Envoyer à Amazon Data Firehose via le même compte : le flux de diffusion et la ressource à surveiller se trouvent dans le même compte.

- Envoyer à Amazon Data Firehose via un autre compte : le flux de diffusion et la ressource à surveiller se trouvent dans des comptes différents.

6. Pour le nom du flux Amazon Data Firehose, choisissez le flux de diffusion que vous avez créé.
7. [Diffusion entre comptes uniquement] Pour IAM roles (Rôles IAM), spécifiez les rôles requis (voir the section called "Rôles IAM pour la diffusion entre comptes").
8. Pour Log record format (Format d'enregistrement du journal), sélectionnez le format de l'enregistrement du journal de flux.

   - Pour utiliser le format de registre de journal de flux par défaut, sélectionnez AWS default format (Format par défaut).
   - Pour créer un format personnalisé, choisissez Custom format (Format personnalisé). Pour Log format (Format de journal), choisissez les champs à inclure dans l'enregistrement de journal de flux.

9. Pour Métadonnées supplémentaires, indiquez si vous souhaitez inclure les métadonnées d'Amazon ECS dans le format du journal.
10. (Facultatif) Choisissez Ajouter une balise pour appliquer des balises au journal de flux.
11. Choisissez Create flow log (Créer le journal de flux).

Pour créer un journal de flux publié sur Amazon Data Firehose à l'aide d'un outil de ligne de commande

Utilisez l'une des commandes suivantes :

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)

L' AWS CLI exemple suivant crée un journal de flux qui capture tout le trafic pour le VPC spécifié et fournit les journaux de flux au flux de diffusion Amazon Data Firehose spécifié dans le même compte.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream
```

L' AWS CLI exemple suivant crée un journal de flux qui capture tout le trafic pour le VPC spécifié et fournit les journaux de flux au flux de diffusion Amazon Data Firehose spécifié dans un autre compte.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

Enregistrements du journal des flux de processus dans Amazon Data Firehose

Vous pouvez obtenir les données du journal de flux depuis la destination que vous avez configurée pour le flux de diffusion.

Interroger des journaux de flux à l'aide d'Amazon Athena

Amazon Athena est un service de requête interactif vous permet d'analyser des données dans Amazon S3, telles que vos journaux de flux, à l'aide du langage SQL standard. Vous pouvez utiliser Athena avec les journaux de flux VPC pour obtenir rapidement des informations exploitables concernant le trafic qui passe par votre VPC. Par exemple, vous pouvez identifier les ressources de vos Virtual Private Clouds (VPC) qui sont les principaux interlocuteurs ou identifier les adresses IP avec les connexions TCP les plus rejetées.

Options

- Vous pouvez rationaliser et automatiser l'intégration de vos journaux de flux VPC à Athena en générant un CloudFormation modèle qui crée les AWS ressources requises et des requêtes prédéfinies que vous pouvez exécuter pour obtenir des informations sur le trafic circulant dans votre VPC.
- Vous pouvez créer vos propres requêtes à l'aide d'Athena. Pour de plus amples d'informations, veuillez consulter Interroger des journaux de flux à l'aide d'Amazon Athena dans le Guide de l'utilisateur Amazon Athena.

Tarification

Vous encourez des frais Amazon Athena standard pour l'exécution des requêtes. Vous encourez des frais AWS Lambda standard pour la fonction Lambda qui charge de nouvelles partitions selon un calendrier récurrent (lorsque vous spécifiez une fréquence de chargement de partition et que vous ne spécifiez pas de dates de début et de fin).

Pour utiliser les requêtes prédéfinies

- Générer le CloudFormation modèle à l'aide de la console
- Générez le CloudFormation modèle à l'aide du AWS CLI
- Exécuter une requête prédéfinie

Générer le CloudFormation modèle à l'aide de la console

Une fois les premiers journaux de flux envoyés dans votre compartiment S3, vous pouvez les intégrer à Athena en générant un CloudFormation modèle et en utilisant le modèle pour créer une pile.

Prérequis

- La région sélectionnée doit prendre en charge AWS Lambda Amazon Athena.
- Les compartiments Amazon S3 doivent se trouver dans la région sélectionnée.
- Le format d'enregistrement du journal de flux doit inclure les champs utilisés par les requêtes prédéfinies spécifiques que vous souhaitez exécuter.

Pour générer le modèle à l'aide de la console

1. Effectuez l'une des actions suivantes :
   - Ouvrez la console Amazon VPC. Dans le panneau de navigation, sélectionnez Your VPCs (Vos VPC) et sélectionnez votre VPC.
   - Ouvrez la console Amazon VPC. Dans le panneau de navigation, sélectionnez Subnets (Sous-réseaux), puis sélectionnez votre sous-réseau.
   - Ouvrez la console Amazon EC2. Dans le volet de navigation, sélectionnez Network Interfaces (Interfaces réseau), puis sélectionnez votre interface réseau.
2. Dans l'onglet Flow logs (Journaux de flux), sélectionnez un journal de flux qui publie dans Amazon S3, puis choisissez Actions, Generate Athena integration (Générer l'intégration Athena).
3. Spécifiez la fréquence de chargement de la partition. Si vous choisissez None (Aucun), vous devez spécifier les dates de début et de fin de partition, en utilisant des dates dans le passé. Si

vous choisissez Daily (Tous les journaux), Weekly (Toutes les semaines) ou Monthly (Tous les mois), les dates de début et de fin de la partition sont facultatives. Si vous ne spécifiez aucune date de début et de fin, le CloudFormation modèle crée une fonction Lambda qui charge de nouvelles partitions selon un calendrier récurrent.

4. Sélectionnez ou créez un compartiment S3 pour le modèle généré et un compartiment S3 pour les résultats de la requête.
5. Choisissez Generate Athena integration (Générer l'intégration Athena).
6. (Facultatif) Dans le message de réussite, cliquez sur le lien pour accéder au compartiment que vous avez spécifié pour le CloudFormation modèle et personnalisez le modèle.
7. Dans le message de réussite, choisissez Create CloudFormation stack pour ouvrir l'assistant Create Stack dans la AWS CloudFormation console. L'URL du CloudFormation modèle généré est spécifiée dans la section Modèle. Exécutez l'assistant pour créer les ressources spécifiées dans le modèle.

Ressources créées par le CloudFormation modèle

- Une base de données Athena. Le nom de la base de données est vpcflowlogsathenadatabase<flow-logs-subscription-id>.
- Un groupe de travail Athéna. Le nom du groupe de travail est <flow-log-subscription-id><partition-load-frequency><start-date><end-date>workgroup
- Un tableau Athena partitionné qui correspond à vos enregistrements de journaux de flux. Le nom du tableau est <flow-log-subscription-id><partition-load-frequency><start-date><end-date>.
- Un ensemble de requêtes nommées Athena. Pour plus d'informations, consultez Requêtes prédéfinies.
- Une fonction Lambda qui charge de nouvelles partitions dans le tableau conformément à la fréquence spécifiée (quotidienne, hebdomadaire ou mensuelle).
- Un rôle IAM qui accorde l'autorisation d'exécuter les fonctions Lambda.

Générez le CloudFormation modèle à l'aide du AWS CLI

Une fois les premiers journaux de flux envoyés dans votre compartiment S3, vous pouvez générer et utiliser un CloudFormation modèle à intégrer à Athena.

Utilisez la commande get-flow-logs-integration-template suivante pour générer le modèle. CloudFormation

```
aws ec2 get-flow-logs-integration-template --cli-input-json file://config.json
```

Voici un exemple du fichier `config.json`.

```
{
    "FlowLogId": "fl-12345678901234567",
    "ConfigDeliveryS3DestinationArn": "arn:aws:s3:::my-flow-logs-athena-integration/
templates/",
    "IntegrateServices": {
        "AthenaIntegrations": [
            {
                "IntegrationResultS3DestinationArn": "arn:aws:s3:::my-flow-logs-
analysis/athena-query-results/",
                "PartitionLoadFrequency": "monthly",
                "PartitionStartDate": "2021-01-01T00:00:00",
                "PartitionEndDate": "2021-12-31T00:00:00"
            }
        ]
    }
}
```

Utilisez la commande create-stack suivante pour créer une pile à l'aide du modèle généré CloudFormation .

```
aws cloudformation create-stack --stack-name my-vpc-flow-logs --template-body file://
my-cloudformation-template.json
```

Exécuter une requête prédéfinie

Le CloudFormation modèle généré fournit un ensemble de requêtes prédéfinies que vous pouvez exécuter pour obtenir rapidement des informations pertinentes sur le trafic de votre AWS réseau. Après avoir créé la pile et vérifié que toutes les ressources ont été créées correctement, vous pouvez exécuter l'une des requêtes prédéfinies.

Pour exécuter une requête prédéfinie à l'aide de la console

1. Ouvrez la console Athena.
2. Dans le panneau de navigation de gauche, choisissez Query Editor (Éditeur de requête). Sous Groupe de travail, sélectionnez le groupe de travail créé par le CloudFormation modèle.

3. Sélectionnez Saved queries (Requêtes enregistrées), sélectionnez une requête, modifiez les paramètres selon vos besoins, puis exécutez la requête. Pour obtenir la liste des requêtes prédéfinies disponibles, consultez la section Requêtes prédéfinies.
4. Sous Query results (Résultats de requête), consultez les résultats de la requête.

Requêtes prédéfinies

Vous trouverez ci-dessous la liste complète des requêtes nommées Athena. Les requêtes prédéfinies fournies lorsque vous générez le modèle varient en fonction des champs qui font partie du format d'enregistrement du journal de flux. Par conséquent, le modèle peut ne pas contenir toutes ces requêtes prédéfinies.

- VpcFlowLogsAcceptedTrafic : connexions TCP autorisées en fonction de vos groupes de sécurité et de vos ACL réseau.
- VpcFlowLogsAdminPortTraffic— Les 10 adresses IP les plus fréquentées, telles qu'elles sont enregistrées par les applications qui répondent aux demandes sur les ports administratifs.
- VpcFlowLogsIPv4Traffic — Nombre total d'octets de trafic IPv4 enregistrés.
- VpcFlowLogsIPv6Traffic — Nombre total d'octets du trafic IPv6 enregistrés.
- VpcFlowLogsRejectedTCPTraffic : connexions TCP rejetées en fonction de vos groupes de sécurité ou de vos ACL réseau.
- VpcFlowLogsRejectedTrafic : trafic rejeté en fonction de vos groupes de sécurité ou de vos ACL réseau.
- VpcFlowLogsSshRdpTraffic— Le trafic SSH et RDP.
- VpcFlowLogsTopTalkers — Les 50 adresses IP ayant enregistré le plus de trafic.
- VpcFlowLogsTopTalkersPacketNiveau — Les 50 adresses IP au niveau des paquets ayant enregistré le plus de trafic.
- VpcFlowLogsTopTalkingInstances— Les identifiants des 50 instances ayant enregistré le plus de trafic.
- VpcFlowLogsTopTalkingSubnets— Les identifiants des 50 sous-réseaux ayant enregistré le plus de trafic.
- VpcFlowLogsTopTCPTraffic — Tout le trafic TCP enregistré pour une adresse IP source.
- VpcFlowLogsTotalBytesTransferred— Les 50 paires d'adresses IP source et de destination avec le plus grand nombre d'octets enregistrés.

- VpcFlowLogsTotalBytesTransferredPacketLevel— Les 50 paires d'adresses IP source et de destination au niveau des paquets avec le plus grand nombre d'octets enregistrés.
- VpcFlowLogsTrafficFrmSrcAddr — Le trafic enregistré pour une adresse IP source spécifique.
- VpcFlowLogsTrafficToDstAddr — Le trafic enregistré pour une adresse IP de destination spécifique.

Résoudre les problèmes liés aux journaux de flux de VPC

Voici des problèmes que vous pourriez rencontrer lors de l'utilisation des journaux de flux.

Problèmes

- Enregistrements de journaux de flux incomplets
- Le journal de flux est actif, mais il n'existe aucun enregistrement de journal de flux ni groupe de journaux
- Erreur « LogDestination NotFound Exception » ou « Accès refusé pour » LogDestination
- Dépassement de la limite de politique de compartiment Amazon S3
- LogDestination non livrable

Enregistrements de journaux de flux incomplets

Problème

Vos enregistrements de journaux de flux sont incomplets ou ne sont plus publiés.

Cause

Il se peut qu'un problème se produise lors de la transmission des journaux de flux au groupe de CloudWatch journaux Logs.

Solution

Dans la console Amazon EC2 ou Amazon VPC, sélectionnez l'onglet Flow Logs (Journaux de flux) de la ressource concernée. Pour plus d'informations, consultez Afficher un journal de flux. Le tableau des journaux de flux affiche les erreurs dans la colonne Status (Status). Vous pouvez aussi utiliser la commande describe-flow-logs et vérifier la valeur qui s'affiche dans le champ `DeliverLogsErrorMessage`. L'une des erreurs suivantes peut s'afficher :

- `Rate limited`: Cette erreur peut se produire si la limitation CloudWatch des journaux a été appliquée, c'est-à-dire lorsque le nombre d'enregistrements du journal de flux pour une interface réseau est supérieur au nombre maximum d'enregistrements pouvant être publiés dans un délai donné. Cette erreur peut également se produire si vous avez atteint le quota du nombre de groupes de CloudWatch journaux que vous pouvez créer. Pour plus d'informations, consultez la section CloudWatchService Quotas dans le guide de CloudWatch l'utilisateur Amazon.
- `Access error` : cette erreur se produit dans les conditions suivantes :
  - Le rôle IAM de votre journal de flux ne dispose pas des autorisations suffisantes pour publier les enregistrements du journal de flux dans le groupe de CloudWatch journaux.
  - Le rôle IAM n'a pas de relation d'approbation avec le service des journaux de flux.
  - La relation d'approbation ne spécifie pas le service des journaux de flux comme principal

  Pour plus d'informations, consultez Rôle IAM pour la publication des journaux de flux dans Logs CloudWatch .
- `Unknown error` : une erreur interne s'est produite dans le service de journaux de flux.

Le journal de flux est actif, mais il n'existe aucun enregistrement de journal de flux ni groupe de journaux

Problème

Vous avez créé un journal de flux et la console Amazon VPC ou Amazon EC2 l'affiche comme étant `Active`. Cependant, vous ne pouvez voir aucun flux de journal dans CloudWatch les journaux ni dans les fichiers journaux de votre compartiment Amazon S3.

Causes possibles :

- Le journal de flux est toujours en cours de création. Dans certains cas, la création du groupe de journaux et l'affichage des données peuvent prendre plus de dix minutes après la création du journal de flux.
- Aucun trafic n'a encore été enregistré pour vos interfaces réseau. Le groupe de CloudWatch journaux dans Logs n'est créé que lorsque le trafic est enregistré.

Solution

Attendez quelques minutes que le groupe de journaux soit créé ou que le trafic soit enregistré.

Erreur « LogDestination NotFound Exception » ou « Accès refusé pour » LogDestination

Problème

Vous obtenez une erreur `Access Denied for LogDestination` ou une erreur `LogDestinationNotFoundException` lorsque vous créez un journal de flux.

Causes possibles :

- Lorsque vous créez un journal de flux qui publie des données dans un compartiment Amazon S3, cette erreur indique que le compartiment S3 spécifié est introuvable ou que la politique de compartiment n'autorise pas la publication des journaux dans le compartiment.
- Lorsque vous créez un journal de flux qui publie des données sur Amazon CloudWatch Logs, cette erreur indique que le rôle IAM n'autorise pas la remise de journaux au groupe de journaux.

Solution

- Lors de la publication dans Amazon S3, assurez-vous d'avoir spécifié l'ARN d'un compartiment S3 existant et que son format est correct. Si vous ne possédez pas le compartiment S3, vérifiez que la politique de compartiment possède les autorisations requises et utilise l'ID de compte et le nom de compartiment corrects dans l'ARN.
- Lors de la publication dans CloudWatch Logs, vérifiez que le rôle IAM dispose des autorisations requises.

Dépassement de la limite de politique de compartiment Amazon S3

Problème

Vous recevez le message d'erreur suivant lorsque vous essayez de créer un journal de flux : `LogDestinationPermissionIssueException`.

Causes possibles :

La taille des politiques de compartiment Amazon S3 est limitée à 20 Ko.

Chaque fois que vous créez un journal de flux publié dans un compartiment Amazon S3, nous ajoutons automatiquement l'ARN de compartiment spécifié, qui inclut le chemin du dossier, à l'élément `Resource` dans la politique de compartiment.

Si vous créez plusieurs journaux de flux publiés dans le même compartiment, vous risquez de dépasser la limite de la politique de compartiment.

Solution

- Nettoyez la politique de compartiment en supprimant les entrées de journal de flux qui ne sont plus nécessaires.
- Accordez des autorisations au compartiment complet en remplaçant les entrées de journal de flux individuelles par ce qui suit.

  ```
  arn:aws:s3:::bucket_name/*
  ```

  Si vous accordez des autorisations au compartiment complet, les nouveaux abonnements de journal de flux n'ajoutent pas de nouvelles autorisations à la politique de compartiment.

LogDestination non livrable

Problème

Vous recevez le message d'erreur suivant lorsque vous essayez de créer un journal de flux : `LogDestination <bucket name> is undeliverable`.

Causes possibles :

Le compartiment Amazon S3 cible est chiffré à l'aide du chiffrement côté serveur avec AWS KMS (SSE-KMS) et le chiffrement par défaut du compartiment est un ID de clé KMS.

Solution

La valeur doit être un ARN de clé KMS. Modifiez le type de chiffrement S3 par défaut d'un ID de clé KMS en ARN de la clé KMS. Pour plus d'informations, consultez Configuration du chiffrement par défaut dans le Guide de l'utilisateur Amazon Simple Storage Service.

Métriques CloudWatch pour vos VPC

Amazon VPC publie des données concernant vos VPC sur Amazon CloudWatch. Vous pouvez récupérer des statistiques sur vos VPC sous la forme de données de séries temporelles, appelées métriques. Considérez une métrique comme une variable à surveiller, et les données comme la valeur de cette variable au fil du temps. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon CloudWatch.

Table des matières

Métriques et dimensions de NAU

Utilisation des adresses réseau (NAU) est une métrique appliquée aux ressources de votre réseau virtuel pour vous permettre de planifier et de surveiller la taille de votre VPC. La surveillance de la NAU est gratuite. La surveillance de la NAU est utile, car si vous épuisez la NAU ou les quotas NAU appairés pour votre VPC, vous ne pouvez pas lancer de nouvelles instances EC2 ou provisionner de nouvelles ressources, telles que des points de terminaison de VPC Network Load Balancer, des fonctions Lambda, des attachements de la passerelle de transit et des passerelles NAT.

Si vous avez activé la surveillance de l'utilisation des adresses réseau pour un VPC, Amazon VPC envoie des métriques relatives à la NAU à Amazon CloudWatch. La taille d'un VPC est mesurée par le nombre d'unités d'utilisation des adresses réseau (NAU) que contient le VPC.

Ces mesures permettent de comprendre le taux de croissance de votre VPC, prévoir quand votre VPC atteindra sa taille limite ou créer des alarmes lorsque les seuils de taille sont dépassés.

L'espace de noms `AWS/EC2` inclut les métriques suivantes pour la surveillance de la NAU.

Métrique	Description
`NetworkAddressUsage`	Décompte NAU par VPC. Critères de notification • Toutes les 24 heures. Dimensions • Nom : `Per-VPC Metrics`, Valeur : ID du VPC.
`NetworkAddressUsagePeered`	Décompte NAU pour le VPC et tous les VPC auxquels il est appairé.

Métrique	Description
	Critères de notification • Toutes les 24 heures. Dimensions • Nom : `Per-VPC Metrics`, valeur : ID du VPC.

L'espace de noms `AWS/Usage` inclut les métriques suivantes pour la surveillance de la NAU.

Métrique	Description
`ResourceCount`	Décompte NAU par VPC. Critères de notification • Toutes les 24 heures. Dimensions • Nom : `Service`, valeur : `EC2` • Nom : `Type`, valeur : `Resource` • Nom : `Resource`, valeur : ID du VPC. • Nom : `Class`, valeur : `NetworkAddressUsage`
`ResourceCount`	Décompte NAU pour le VPC et tous les VPC auxquels il est appairé. Critères de notification • Toutes les 24 heures. Dimensions

Métrique	Description
	• Nom : `Service`, valeur : `EC2` • Nom : `Type`, valeur : `Resource` • Nom : `Resource`, valeur : ID du VPC. • Nom : `Class`, valeur : `NetworkAddressUsagePeered`
`ResourceCount`	Vue combinée de l'utilisation de la NAU sur les VPC. Critères de notification • Toutes les 24 heures. Dimensions • Nom : `Service`, valeur : `EC2` • Nom : `Type`, valeur : `Resource` • Nom : `Resource`, valeur : `VPC` • Nom : `Class`, valeur : `NetworkAddressUsage`

Métrique	Description
`ResourceCount`	Vue combinée de l'utilisation de la NAU sur les VPC appairés. Critères de notification • Toutes les 24 heures. Dimensions • Nom : `Service`, valeur : `EC2` • Nom : `Type`, valeur : `Resource` • Nom : `Resource`, valeur : `VPC` • Nom : `Class`, valeur : `NetworkAddressUsagePeered`

Activer ou désactiver la surveillance de la NAU

Pour consulter les métriques NAU dans CloudWatch, vous devez d'abord activer la surveillance sur chaque VPC à surveiller.

Pour activer ou désactiver la surveillance de la NAU

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Your VPCs (Vos VPC).
3. Cochez la case correspondant au VPC.
4. Sélectionnez Actions, Edit VPC settings (Modifier les paramètres du VPC).
5. Effectuez l'une des actions suivantes :

   - Pour activer la surveillance, sélectionnez Network mapping units metrics settings (Paramètres des métriques des unités de mappage réseau), Enable network address usage metrics (Activer les métriques d'utilisation des adresses réseau).
   - Pour désactiver la surveillance, désélectionnez Network mapping units metrics settings (Paramètres des métriques des unités de mappage réseau), Enable network address usage metrics (Activer les métriques d'utilisation des adresses réseau).

Pour activer ou désactiver la surveillance à l'aide de la ligne de commande

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Exemple de l'alarme NAU CloudWatch

Vous pouvez utiliser la commande AWS CLI suivante et l'exemple `.json` pour créer une alarme Amazon CloudWatch et une notification SNS qui suit l'utilisation de NAU du VPC avec 50 000 NAU comme seuil. Dans cet exemple, vous devez d'abord créer une rubrique Amazon SNS. Pour plus d'informations, consultez Prise en main d'Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

```
aws cloudwatch put-metric-alarm --cli-input-json file://nau-alarm.json
```

Voici un exemple de `nau-alarm.json`.

```
{
    "Namespace": "AWS/EC2",
    "MetricName": "NetworkAddressUsage",
    "Dimensions": [{
        "Name": "Per-VPC Metrics",
        "Value": "vpc-0123456798"
    }],
    "AlarmActions": ["arn:aws:sns:us-west-1:123456789012:my_sns_topic"],
    "ComparisonOperator": "GreaterThanThreshold",
    "Period": 86400,
    "EvaluationPeriods": 1,
    "Threshold": 50000,
    "AlarmDescription": "Tracks NAU utilization of the VPC with 50k NAUs as the
 threshold",
    "AlarmName": "VPC NAU Utilization",
    "Statistic": "Maximum"
}
```

Sécurité dans Amazon Virtual Private Cloud

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Virtual Private Cloud, consultez la section AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lorsque vous utilisez Amazon VPC. Les rubriques suivantes expliquent comment configurer Amazon VPC pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Amazon VPC.

Table des matières

Protection des données dans Amazon Virtual Private Cloud

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Virtual Private Cloud. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Amazon VPC ou une autre entreprise à Services AWS l'aide de la console, de l'API ou AWS des AWS CLI SDK. Toutes les données

que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Confidentialité du trafic inter-réseau dans Amazon VPC

Amazon Virtual Private Cloud propose trois fonctionnalités que vous pouvez utiliser pour accroître et surveiller la sécurité de votre Virtual Private Cloud (VPC) :

- Groupes de sécurité : les groupes de sécurité autorisent un trafic entrant et sortant spécifique au niveau des ressources (comme une instance EC2). Lorsque vous lancez une instance, vous pouviez l'associer à un ou plusieurs groupes de sécurité. Chaque instance de votre VPC pourrait appartenir à un ensemble de groupes de sécurité différent. Si vous ne spécifiez pas de groupe de sécurité lorsque vous lancez une instance, celle-ci est automatiquement associée au groupe de sécurité par défaut pour sont VPC. Pour plus d'informations, consultez Groupes de sécurité.
- Listes de contrôle d'accès (ACL) réseau : les ACL réseau autorisent ou refusent un trafic entrant et sortant spécifique au niveau du sous-réseau. Pour plus d'informations, consultez Contrôle du trafic vers les sous-réseaux avec des listes ACL réseau.
- Journaux de flux : les journaux de flux capturent les informations sur le trafic IP circulant vers et depuis les interfaces réseau de votre VPC. Vous pouvez créer un journal de flux pour un VPC, un sous-réseau ou une interface réseau. Les données des CloudWatch journaux de flux sont publiées sur Logs ou Amazon S3, et elles peuvent vous aider à diagnostiquer les règles ACL trop restrictives ou trop permissives des groupes de sécurité et des réseaux. Pour plus d'informations, consultez Journalisation du trafic IP à l'aide des journaux de flux VPC.
- Mise en miroir du trafic : vous pouvez copier le trafic réseau à partir d'une interface réseau Elastic d'une instance Amazon EC2. Vous pouvez ensuite envoyer le trafic vers les dispositifs out-of-band de sécurité et de surveillance. Pour de plus amples informations, veuillez consulter le Guide de mise en miroir du trafic.

Identity and Access Management pour Amazon VPC

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Des administrateurs IAM contrôlent les personnes qui peuvent être authentifiées (connectées) et autorisées (disposant

d'autorisations) pour utiliser des ressources Amazon VPC. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Table des matières

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Amazon VPC.

Utilisateur du service : Si vous utilisez le service Amazon VPC pour effectuer vos tâches, votre administrateur vous fournira les informations d'identification et les autorisations nécessaires. Vous pourrez avoir besoin d'autorisations supplémentaires si vous utilisez davantage de fonctionnalités Amazon VPC. Comprendre la gestion des accès peut vous aider à demander à votre administrateur les autorisations appropriées. Si vous ne pouvez pas accéder à une fonctionnalité dans Amazon VPC, veuillez consulter Résoudre les problèmes d'identité et d'accès Amazon VPC.

Administrateur du service : Si vous êtes le responsable des ressources Amazon VPC de votre entreprise, vous bénéficiez probablement d'un accès total à ce service. C'est à vous de déterminer les fonctionnalités et les ressources Amazon VPC auxquelles vos employés pourront accéder. Vous envoyez les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs du service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour découvrir la façon dont votre entreprise peut utiliser IAM avec Amazon VPC, veuillez consulter Fonctionnement d'Amazon VPC avec IAM.

Administrateur IAM : Si vous êtes un administrateur IAM, vous souhaiterez peut-être obtenir des informations sur la façon dont vous pouvez écrire des stratégies pour gérer l'accès à Amazon VPC. Pour afficher des exemples de stratégies, veuillez consulter Exemples de stratégie Amazon VPC.

S'authentifier avec des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et

le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir

d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, veuillez consulter Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gérer l'accès à l'aide de stratégies

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un

administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques

basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Fonctionnement d'Amazon VPC avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon VPC, vous devez comprendre quelles sont les fonctionnalités IAM qui peuvent être utilisées dans cette situation. Pour obtenir une vue d'ensemble de la manière dont Amazon VPC et les autres AWS services fonctionnent avec IAM, consultez la section AWS Services compatibles avec IAM dans le guide de l'utilisateur d'IAM.

Table des matières

Vous pouvez préciser les actions autorisées ou refusées grâce aux stratégies basées sur les identités IAM. Pour certaines actions, vous pouvez indiquer les ressources et les conditions dans lesquelles les actions sont autorisées ou refusées. Amazon VPC est compatible avec des actions, des ressources et des clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Actions

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Amazon VPC partage son espace de nom d'API avec Amazon EC2. Les actions de stratégie dans Amazon VPC utilisent le préfixe suivant avant l'action : `ec2:`. Par exemple, pour accorder à un utilisateur l'autorisation de créer un VPC à l'aide de l'opération d'API `CreateVpc`, vous accordez l'accès à l'action `ec2:CreateVpc`. Les déclarations de stratégie doivent inclure un élément `Action` ou `NotAction`.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme l'indique l'exemple suivant.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

Vous pouvez aussi préciser plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante.

```
"Action": "ec2:Describe*"
```

Pour afficher la liste des actions Amazon VPC, consultez Actions définies par Amazon EC2 dans Référence de l'autorisation de service.

Ressources

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

L'ARN de la ressource VPC est décrit dans l'exemple suivant.

```
arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}
```

Par exemple, pour indiquer le VPC `vpc-1234567890abcdef0` dans votre déclaration, utilisez l'ARN décrit dans l'exemple suivant.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-1234567890abcdef0"
```

Pour indiquer tous les VPC d'une région spécifique appartenant à un compte précis, utilisez le caractère générique (*).

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
```

Certaines actions Amazon VPC, telles que celles destinées à la création de ressources, ne peuvent pas être exécutées sur une ressource spécifique. Dans ce cas, vous devez utiliser le caractère générique (*).

```
"Resource": "*"
```

De nombreuses actions d'API Amazon EC2 nécessitent plusieurs ressources. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Pour afficher la liste des types de ressources et de leurs ARN, consultez Types de ressources définies par Amazon EC2 dans Référence de l'autorisation de service.

Clés de condition

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Toutes les actions Amazon EC2 prennent en charge les clés de condition `aws:RequestedRegion` et `ec2:Region`. Pour de plus amples informations, veuillez consulter Exemple : Restreindre l'accès à une région spécifique.

Amazon VPC définit son propre ensemble de clés de condition et est également compatible avec l'utilisation de certaines clés de condition globales. Pour afficher la liste des clés de condition Amazon VPC, consultez Clés de condition pour Amazon EC2 dans Référence de l'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, veuillez consulter Actions définies par Amazon EC2.

Politiques basées sur les ressources Amazon VPC

Les stratégies basées sur les ressources sont des documents de stratégie JSON précisant les actions qu'un principal spécifié peut effectuer sur la ressource Amazon VPC et dans quelles conditions.

Pour permettre un accès comptes multiples , vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une stratégie basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource se trouvent dans des AWS comptes différents, vous devez également accorder à l'entité principale l'autorisation d'accéder à la ressource. Accordez l'autorisation en attachant une stratégie basée sur les identités à l'entité. Toutefois, si une stratégie basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre stratégie basée sur l'identité n'est requise. Pour plus d'informations, consultez Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

Autorisation basée sur les balises

Vous pouvez attacher des balises aux ressources Amazon VPC ou transmettre des balises dans une demande. Pour le contrôle d'accès basé sur des balises, vous devez fournir les informations des balises dans l'élément de condition d'une politique utilisant des clés de condition. Pour de plus amples informations, consultez les sections Baliser des ressources lors de la création et Contrôler l'accès aux ressources EC2 à l'aide de balises de ressources dans le Guide de l'utilisateur Amazon EC2.

Pour afficher un exemple de stratégie basée sur l'identité permettant de limiter l'accès à une ressource basée sur les balises de cette ressource, veuillez consulter Lancer des instances dans un VPC précis.

Rôles IAM

Un rôle IAM est une entité au sein de vous Compte AWS qui possède des autorisations spécifiques.

Utiliser des informations d'identification temporaires

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à l'aide de la fédération, endosser un rôle IAM ou encore pour endosser un rôle entre comptes. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRoleou GetFederationToken.

Amazon VPC est compatible avec l'utilisation des informations d'identification temporaires.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Les passerelles de transit sont compatibles avec les rôles liés au service.

Rôles de service

Cette fonction permet à un service d'endosser une fonction du service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les rôles de service s'affichent dans votre compte IAM et sont la propriété du compte. Cela signifie qu'un administrateur IAM peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

Amazon VPC est compatible avec les rôles de service pour les journaux de flux. Lorsque vous créez un journal de flux, vous devez choisir un rôle qui autorise le service de journaux de flux à accéder aux CloudWatch journaux. Pour plus d'informations, consultez the section called "Rôle IAM pour la publication des journaux de flux dans Logs CloudWatch ".

Exemples de stratégie Amazon VPC

Les rôles IAM ne sont pas autorisés, par défaut, à créer ou modifier des ressources VPC. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. Un administrateur IAM doit créer des politiques IAM autorisant les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. L'administrateur doit ensuite attacher ces politiques aux rôles IAM qui ont besoin de ces autorisations.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Table des matières

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Amazon VPC dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utiliser la console Amazon VPC

Pour accéder à la console Amazon VPC, vous devez disposer d'un ensemble minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Amazon VPC de votre AWS compte. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (rôles IAM) tributaires de cette politique.

La stratégie suivante autorise les utilisateurs à répertorier les ressources dans la console VPC, mais pas à les créer, à les mettre à jour ou à les supprimer.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeMovingAddresses",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeStaleSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTrafficMirrorFilters",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
```

```
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetManagedPrefixListAssociations",
                "ec2:GetManagedPrefixListEntries"
            ],
            "Resource": "*"
        }
    ]
}
```

Il n'est pas nécessaire d'accorder des autorisations de console minimales pour les rôles qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès uniquement aux actions qui correspondent à l'opération d'API que le rôle doit effectuer.

Créer un VPC avec un sous-réseau public

L'exemple suivant donne la possibilité aux utilisateurs de créer des VPC, des sous-réseaux, des tables de routage et des passerelles Internet. Les rôles peuvent également attacher une passerelle Internet à un VPC et créer des routes dans les tables de routage. L'action `ec2:ModifyVpcAttribute` permet aux rôles d'activer les noms d'hôte DNS pour le VPC, de sorte que chaque instance lancée dans un VPC reçoit un nom d'hôte DNS.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateInternetGateway",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource": "*"
    }
   ]
}
```

La politique précédente permet également aux rôles de créer un VPC dans la console Amazon VPC.

Modifier et supprimer les ressources VPC

Vous avez la possibilité de contrôler les ressources VPC que les rôles peuvent modifier ou supprimer. Par exemple, la stratégie suivante permet aux rôles de travailler avec les tables de routage et de supprimer celles comportant la balise `Purpose=Test`. La stratégie précise également que les rôles peuvent uniquement supprimer les passerelles Internet qui possèdent la balise `Purpose=Test`. Les rôles ne peuvent pas utiliser les tables de routage ou les passerelles Internet qui ne possèdent pas cette balise.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteInternetGateway",
            "Resource": "arn:aws:ec2:*:*:internet-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRouteTable",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:route-table/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        }
    ]
}
```

Gérer les groupes de sécurité

La politique suivante permet aux rôles de gérer les groupes de sécurité. La première instruction permet aux rôles de supprimer tout groupe de sécurité comportant la balise `Stack=test` et de gérer les règles entrantes et sortantes de tout groupe de sécurité avec la balise `Stack=test`. La deuxième instruction exige des rôles qu'ils marquent tous les groupes de sécurité qu'ils créent avec la balise `Stack=Test`. La troisième instruction permet aux rôles de créer des identifications lors de la création d'un groupe de sécurité. La quatrième instruction permet aux rôles d'afficher tout groupe de sécurité et toute règle de groupe de sécurité. La cinquième instruction permet aux rôles de créer un groupe de sécurité dans un VPC.

> **Note**
>
> Cette politique ne peut pas être utilisée par le AWS CloudFormation service pour créer un groupe de sécurité avec les balises requises. Si vous supprimez la condition de l'action `ec2:CreateSecurityGroup` qui nécessite la balise, la politique fonctionnera.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:ModifySecurityGroupRules",
                "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Stack": "test"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Stack": "test"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "Stack"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeVpcs",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        }
    ]
}
```

Pour permettre aux rôles de modifier le groupe de sécurité associé à une instance, ajoutez l'action `ec2:ModifyInstanceAttribute` à votre stratégie.

Ajoutez l'action `ec2:ModifyNetworkInterfaceAttribute` à votre stratégie pour permettre aux rôles de modifier les groupes de sécurité d'une interface réseau.

Gérer les règles de groupe de sécurité

La stratégie suivante accorde aux rôles l'autorisation d'afficher tous les groupes de sécurité et toutes les règles de groupe de sécurité, d'ajouter et de supprimer des règles entrantes et sortantes pour les groupes de sécurité d'un VPC spécifique et de modifier des descriptions de règles pour le VPC spécifié. La première instruction utilise la clé de condition `ec2:Vpc` pour limiter les autorisations à un VPC spécifique.

La deuxième instruction autorise les rôles à décrire tout l'ensemble des groupes de sécurité, règles de groupe de sécurité et balises. Cela permet aux rôles d'afficher les règles du groupe de sécurité pour les modifier.

```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupEgress",
       "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
       "ec2:ModifySecurityGroupRules"
    ],
     "Resource": "arn:aws:ec2:region:account-id:security-group/*",
      "Condition": {
        "ArnEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:DescribeSecurityGroups",
          "ec2:DescribeSecurityGroupRules",
          "ec2:DescribeTags"
      ],
```

```
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:ModifySecurityGroupRules"
      ],
      "Resource": "arn:aws:ec2:region:account-id:security-group-rule/*"
    }
  ]
}
```

Lancer des instances dans un sous-réseau précis

La stratégie suivante autorise les rôles à lancer des instances dans un sous-réseau spécifique et à utiliser un groupe de sécurité spécifique dans la demande. La stratégie l'effectue en spécifiant l'ARN pour le sous-réseau et l'ARN pour le groupe de sécurité. Si les rôles tentent de lancer une instance dans un sous-réseau différent ou d'utiliser un groupe de sécurité différent, la demande échoue (à moins qu'une autre stratégie ou instruction n'autorise les rôles à le faire).

La stratégie autorise également l'utilisation des ressources de l'interface réseau. Une fois lancée dans un sous-réseau, la demande `RunInstances` crée une interface réseau principale par défaut, afin que le rôle ait besoin d'être autorisé à créer cette ressource lors du lancement de l'instance.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-*",
        "arn:aws:ec2:region:account:instance/*",
        "arn:aws:ec2:region:account:subnet/subnet-id",
        "arn:aws:ec2:region:account:network-interface/*",
        "arn:aws:ec2:region:account:volume/*",
        "arn:aws:ec2:region:account:key-pair/*",
        "arn:aws:ec2:region:account:security-group/sg-id"
      ]
    }
   ]
}
```

Lancer des instances dans un VPC précis

La stratégie suivante autorise les rôles à lancer des instances dans n'importe quel sous-réseau au sein d'un VPC spécifique. La stratégie l'effectue en appliquant une clé de condition (`ec2:Vpc`) à la ressource du sous-réseau.

La stratégie autorise également les rôles à lancer des instances en n'utilisant que les AMI ayant la balise « `department=dev` ».

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account-id:subnet/*",
        "Condition": {
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region::image/ami-*",
      "Condition": {
         "StringEquals": {
            "ec2:ResourceTag/department": "dev"
            }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account:instance/*",
         "arn:aws:ec2:region:account:volume/*",
         "arn:aws:ec2:region:account:network-interface/*",
         "arn:aws:ec2:region:account:key-pair/*",
         "arn:aws:ec2:region:account:security-group/*"
         ]
      }
   ]
```

```
}
```

Exemples supplémentaires de stratégie Amazon VPC

Vous trouverez d'autres exemples de stratégies IAM liées à Amazon VPC dans la documentation suivante :

- Listes de préfixes gérées
- Mise en miroir du trafic
- Passerelles de transit
- Points de terminaison VPC et services de points de terminaison VPC
- Stratégies de point de terminaison d'un VPC
- Appairage de VPC
- AWS Wavelength

Résoudre les problèmes d'identité et d'accès Amazon VPC

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon VPC et IAM.

Problèmes

- Action à effectuer dans Amazon VPC refusée
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes ressources Amazon VPC

Action à effectuer dans Amazon VPC refusée

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations concernant un sous-réseau mais qu'il appartient à un rôle IAM qui ne détient pas les autorisations `ec2:DescribeSubnets`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeSubnets on resource: subnet-id
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour la politique pour lui permettre d'accéder au sous-réseau.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Amazon VPC.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Amazon VPC. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes ressources Amazon VPC

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Amazon VPC est compatible avec ces fonctionnalités, veuillez consulter Fonctionnement d'Amazon VPC avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

AWS politiques gérées pour Amazon Virtual Private Cloud

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonVPC FullAccess

Vous pouvez attacher la stratégie `AmazonVPCFullAccess` à vos identités IAM. Cette stratégie accorde des autorisations qui permettent un accès complet à Amazon VPC.

Pour consulter les autorisations associées à cette politique, consultez AmazonVPC FullAccess dans le manuel AWS Managed Policy Reference.

AWS politique gérée : AmazonVPC Access ReadOnly

Vous pouvez attacher la stratégie `AmazonVPCReadOnlyAccess` à vos identités IAM. Cette stratégie accorde des autorisations qui permettent d'accéder en lecture seule à Amazon VPC.

Pour consulter les autorisations associées à cette politique, consultez AmazonVPC ReadOnly Access dans le manuel AWS Managed Policy Reference.

AWS politique gérée : Opérations AmazonVPC CrossAccount NetworkInterface

Vous pouvez associer la politique `AmazonVPCCrossAccountNetworkInterfaceOperations` à vos identités IAM. Cette politique accorde des autorisations qui permettent à l'identité de créer des interfaces réseau et de les attacher à des ressources entre comptes.

Pour consulter les autorisations associées à cette politique, consultez la section CrossAccountNetworkInterfaceOpérations d'AmazonVPC dans le manuel AWS Managed Policy Reference.

Mises à jour des politiques gérées par Amazon VPC AWS

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon VPC depuis que ce service a commencé à suivre ces modifications en mars 2021.

Modification	Description	Date
the section called “Amazon VPC FullAccess” – Mise à jour d'une stratégie existante	Ajout de l'GetSecurityGroup sForVpcaction, qui vous permet d'obtenir des groupes de sécurité utilisables dans votre VPC.	8 février 2024

Modification	Description	Date
the section called "Accès à Amazon VPC ReadOnly" – Mise à jour d'une politique existante	Ajout de l'GetSecurityGroupsForVpcaction, qui vous permet d'obtenir des groupes de sécurité utilisables dans votre VPC.	8 février 2024
the section called "Opérations Amazon VPC CrossAccount NetworkInterface" – Mise à jour d'une politique existante	Ajout des actions AssignIpv6Addresses et UnassignIpv6Addresses, qui vous permettent de gérer les adresses IPv6 associées aux interfaces réseau.	25 septembre 2023
the section called "Accès à Amazon VPC ReadOnly" – Mise à jour d'une politique existante	Ajout de l'action DescribeSecurityGroupRules, qui vous permet d'afficher les règles des groupes de sécurité.	2 août 2021
the section called "Amazon VPC FullAccess" – Mise à jour d'une politique existante	Ajout des actions DescribeSecurityGroupRules et ModifySecurityGroupRules, qui vous permettent d'afficher et de modifier les règles des groupes de sécurité.	2 août 2021
the section called "Amazon VPC FullAccess" – Mise à jour d'une politique existante	Ajout d'actions pour des passerelles d'opérateur, des groupes IPv6, des passerelles locales et des tables de routage de passerelle locale.	23 Juin 2021
the section called "Accès à Amazon VPC ReadOnly" – Mise à jour d'une politique existante	Ajout d'actions pour des passerelles d'opérateur, des groupes IPv6, des passerelles locales et des tables de routage de passerelle locale.	23 Juin 2021

Sécurité de l'infrastructure dans Amazon VPC

En tant que service géré, Amazon Virtual Private Cloud est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Amazon VPC via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Isolement de réseau

Un cloud privé virtuel (VPC) est un réseau virtuel situé dans votre propre zone logiquement isolée dans le cloud. AWS Utilisez des VPC distincts pour isoler l'infrastructure par charge de travail ou entité organisationnelle.

Un sous-réseau est une plage d'adresses IP dans un VPC. Lorsque vous lancez une instance, vous la lancez dans un sous-réseau de votre VPC. Utilisez des sous-réseaux pour isoler les niveaux de votre application (par exemple, web, application et base de données) dans un VPC unique. Utilisez des sous-réseaux privés pour vos instances si elles ne doivent pas être accessibles directement à partir d'Internet.

Vous pouvez l'utiliser AWS PrivateLinkpour permettre aux ressources de votre VPC de se connecter à Services AWS l'aide d'adresses IP privées, comme si ces services étaient hébergés directement dans votre VPC. Par conséquent, il n'est pas nécessaire d'utiliser une passerelle Internet ou un périphérique NAT pour y accéder Services AWS.

Contrôler le trafic réseau

Vous devez prendre en compte les éléments suivants pour le contrôle du trafic réseau vers les ressources de votre VPC, comme les instances EC2 :

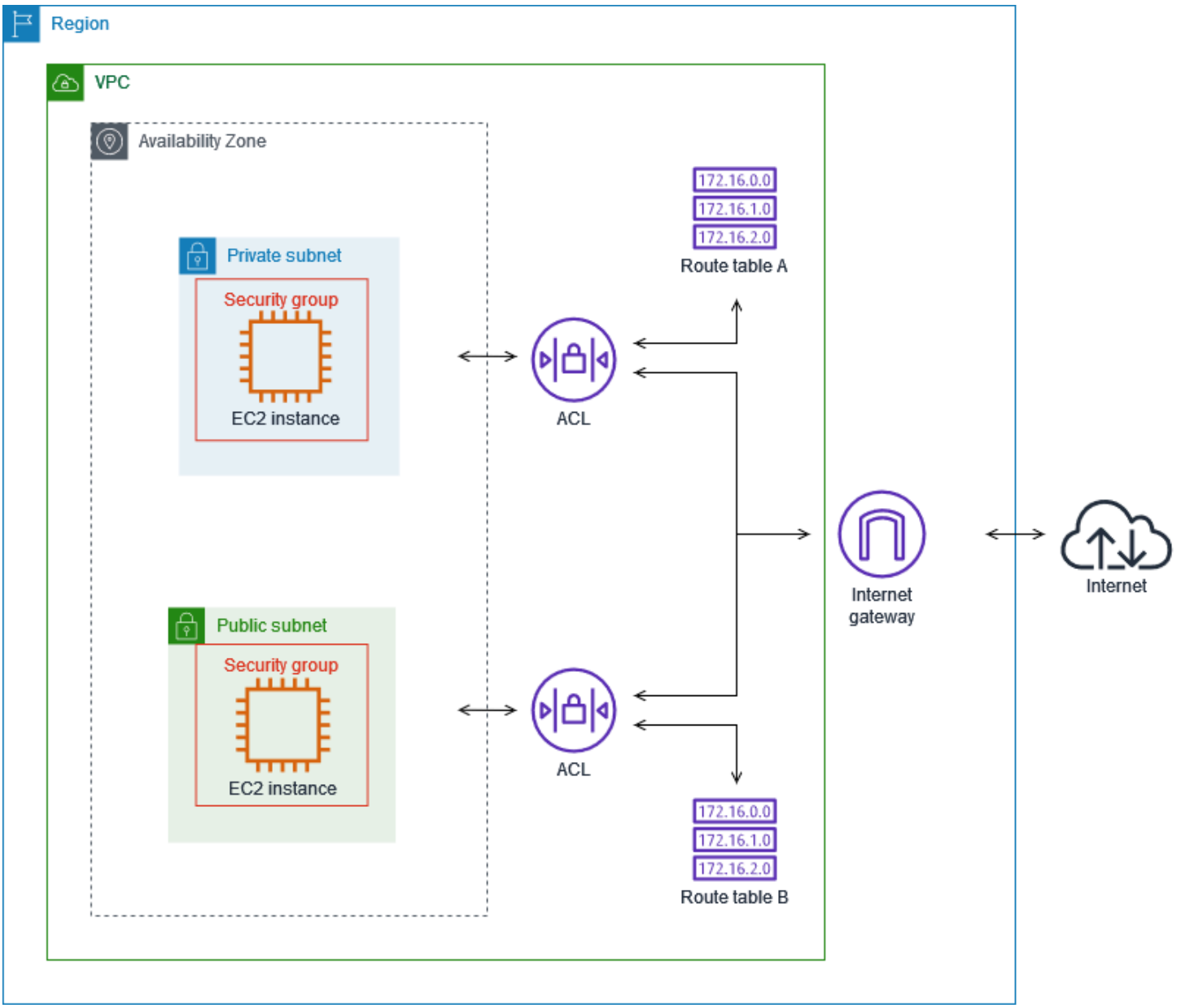
- Utilisez les groupes de sécurité comme mécanisme principal pour contrôler l'accès réseau à vos VPC. Si nécessaire, utilisez les listes ACL réseau pour fournir un contrôle de réseau sans état et à grain grossier. Les groupes de sécurité sont plus polyvalents que les listes ACL réseau en raison de leur capacité à effectuer un filtrage des paquets avec état et à créer des règles qui référencent d'autres groupes de sécurité. Les listes ACL réseau peuvent être efficaces en tant que contrôle secondaire (par exemple, pour refuser un sous-ensemble spécifique de trafic) ou garde-fous de sous-réseau de haut niveau. De plus, comme les ACL réseau s'appliquent à l'ensemble d'un sous-réseau, elles peuvent être utilisées comme defense-in-depth si une instance était lancée sans le groupe de sécurité approprié.
- Utilisez des sous-réseaux privés pour vos instances si elles ne doivent pas être accessibles directement à partir d'Internet. Utilisez un hôte bastion ou une passerelle NAT pour l'accès Internet à partir d'instances de sous-réseaux privés.
- Configurez des tables de routage de sous-réseau avec les routes réseau minimales pour répondre à vos exigences de connectivité.
- Envisagez l'utilisation de groupes de sécurité supplémentaires ou d'interfaces réseau pour contrôler et vérifier le trafic de gestion d'instance Amazon EC2 séparément du trafic d'application régulier. Ainsi, vous pouvez mettre en œuvre des politiques IAM spéciales pour le contrôle des modifications, ce qui facilite l'audit des modifications apportées aux règles de groupe de sécurité ou aux scripts automatisés de vérification des règles. Plusieurs interfaces réseau procurent également des options supplémentaires pour contrôler le trafic réseau, notamment la possibilité de créer des stratégies de routage basées sur l'hôte ou de tirer parti de différentes règles de routage de sous-réseau d'un VPC basées sur des interfaces réseau affectées à un sous-réseau.
- Utilisez AWS Virtual Private Network ou AWS Direct Connect pour établir des connexions privées entre vos réseaux distants et vos VPC. Pour plus d'informations, consultez Network-to-Amazon VPC connectivity options.
- Utilisez des journaux de flux VPC pour surveiller la trafic atteignant vos instances.
- Utilisez AWS Security Hub pour rechercher les accès réseau non intentionnels à partir de vos instances.
- Utilisez AWS Network Firewall pour protéger les sous-réseaux de votre VPC contre les menaces réseau courantes.

Comparer les groupes de sécurité et les listes ACL réseau

Le tableau ci-après récapitule les différences de base entre les groupes de sécurité et les listes ACL réseau.

Groupe de sécurité	ACL réseau
Fonctionne au niveau de l'instance	Fonctionne au niveau du sous-réseau
S'applique à une instance uniquement si elle est associée à l'instance	S'applique à toutes les instances déployées dans le sous-réseau associé (forme une couche de défense supplémentaire si les règles du groupe de sécurité sont trop permissives)
Prend en charge les règles d'autorisation uniquement	Prend en charge les règles d'autorisation et les règles de refus
Evalue toutes les règles avant de décider si le trafic doit être autorisé	Les règles sont évaluées dans l'ordre, en commençant par la règle numérotée la plus basse, lorsque nous décidons d'autoriser le trafic
Est avec état : le trafic de retour est autorisé quelles que soient les règles	Sans état : le trafic de retour doit être explicite ment autorisé par des règles

Le schéma ci-après illustre les couches de sécurité fournies par les groupes de sécurité et les listes ACL réseau. Par exemple, le trafic d'une passerelle Internet est routé vers le sous-réseau approprié à l'aide de routes dans la table de routage. Les règles de la liste ACL réseau associée au sous-réseau contrôlent le trafic autorisé dans le sous-réseau. Les règles du groupe de sécurité associé à une instance contrôlent le trafic autorisé dans l'instance.



Vous pouvez sécuriser vos instances en utilisant uniquement des groupes de sécurité. Toutefois, vous pouvez ajouter des ACL réseau en tant que couche supplémentaire de défense. Pour plus d'informations, consultez Exemple : contrôler l'accès aux instances dans un sous-réseau.

Contrôlez le trafic vers vos AWS ressources à l'aide de groupes de sécurité

Un groupe de sécurité contrôle le trafic autorisé à atteindre et à quitter les ressources auxquelles il est associé. Par exemple, après avoir associé un groupe de sécurité à une instance EC2, il contrôle le trafic entrant et sortant pour l'instance.

Lorsque vous créez un VPC, celui-ci est fourni avec un groupe de sécurité par défaut. Vous pouvez créer des groupes de sécurité supplémentaires pour un VPC, chacun avec ses propres règles entrantes et sortantes. Vous pouvez spécifier la source, la plage de ports et le protocole pour chaque règle entrante. Vous pouvez spécifier la destination, la plage de ports et le protocole pour chaque règle sortante.

Le schéma suivant illustre un VPC avec un sous-réseau, une passerelle Internet et un groupe de sécurité. Le sous-réseau contient une instance EC2. Le groupe de sécurité est attribué à l'instance. Le groupe de sécurité fonctionne comme un pare-feu virtuel. Le seul trafic qui atteint l'instance est le trafic autorisé par les règles du groupe de sécurité. Par exemple, si le groupe de sécurité contient une règle qui autorise le trafic ICMP vers l'instance depuis votre réseau, vous pouvez envoyer une commande ping à l'instance depuis votre ordinateur. Si le groupe de sécurité ne contient pas de règle autorisant le trafic SSH, vous ne pourrez pas vous connecter à votre instance via SSH.

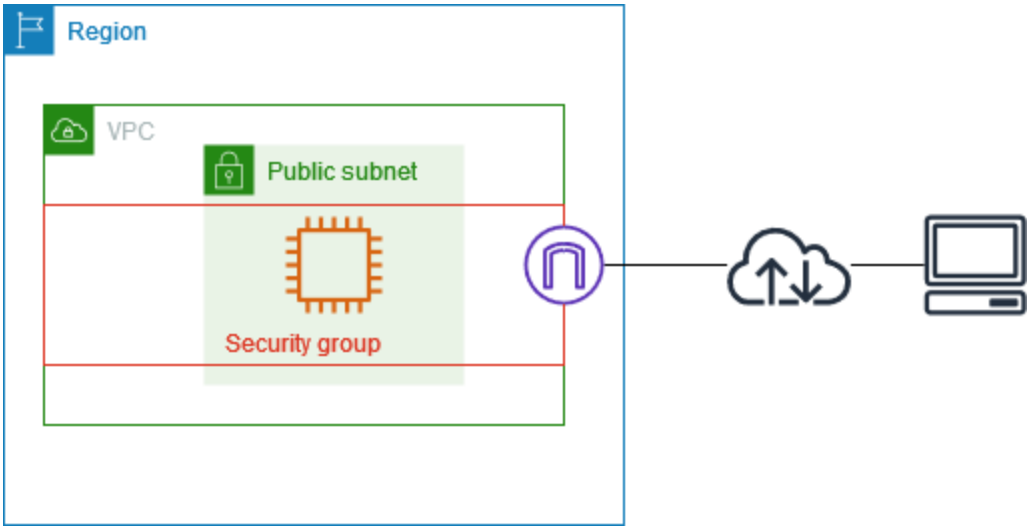


Table des matières

Tarification

L'utilisation de groupes de sécurité n'entraîne aucuns frais supplémentaires.

Principes de base des groupes de sécurité

- Vous pouvez attribuer un groupe de sécurité uniquement aux ressources créées dans le même VPC que le groupe de sécurité. Vous pouvez attribuer plusieurs groupes de sécurité à une ressource.
- Quand vous créez un groupe de sécurité, vous devez lui attribuer un nom et une description. Les règles suivantes s'appliquent :
  - Un nom de groupe de sécurité doit être unique dans le VPC.
  - Les noms et les descriptions peuvent inclure jusqu'à 255 caractères.
  - Les noms et les descriptions peuvent comporter uniquement les caractères suivants : a à z, A à Z, 0 à 9, les espaces et ._-:/()#,@[]+=&;{}!$*.
  - Lorsque le nom contient des espaces de fin, nous supprimons l'espace situé à la fin du nom. Par exemple, si vous entrez « Test Security Group » pour le nom, nous le stockons comme « Test Security Group ».
  - Un nom de groupe de sécurité ne peut pas commencer par `sg-`.
- Les groupes de sécurité sont avec état. Par exemple, si vous envoyez une demande à partir d'une instance, le trafic de réponse pour cette demande est autorisé à atteindre l'instance, quelles que soient les règles du groupe de sécurité entrant. Les réponses au trafic entrant autorisé sont autorisées à quitter l'instance, quelles que soient les règles de trafic sortant.
- Les groupes de sécurité ne filtrent pas le trafic vers et depuis les services suivants :
  - Amazon Domain Name Services (DNS)
  - Amazon Dynamic Host Configuration Protocol (DHCP)
  - Métadonnées d'instance Amazon EC2.
  - Points de terminaison des métadonnées de tâches Amazon ECS
  - Activation de licence pour les instances Windows
  - Service de synchronisation temporelle d'Amazon
  - Adresses IP réservées utilisées par le routeur VPC par défaut
- Des quotas s'appliquent au nombre de groupes de sécurité que vous pouvez créer par VPC, au nombre de règles que vous pouvez ajouter à chaque groupe de sécurité, et au nombre de groupes de sécurité que vous pouvez associer à une interface réseau. Pour plus d'informations, consultez Quotas Amazon VPC.

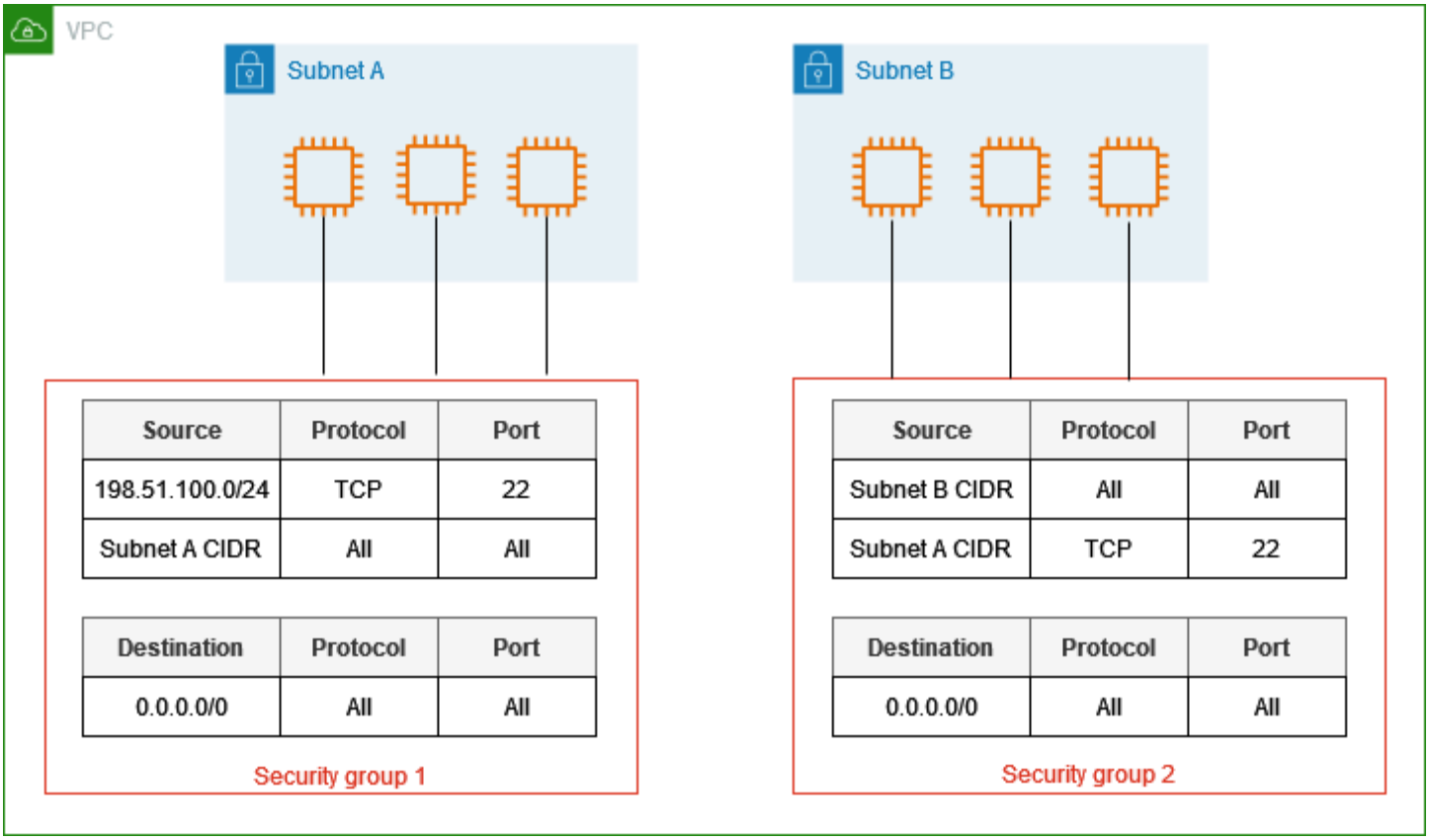
Bonnes pratiques

- Autorisez uniquement certains principaux IAM à créer et à modifier les groupes de sécurité.
- Créez le nombre minimum de groupes de sécurité dont vous avez besoin afin de réduire le risque d'erreur. Utilisez chaque groupe de sécurité pour gérer l'accès aux ressources possédant des fonctions et des exigences de sécurité similaires.
- Lorsque vous ajoutez des règles entrantes pour les ports 22 (SSH) ou 3389 (RDP) afin de pouvoir accéder à vos instances EC2, autorisez uniquement les plages d'adresses IP spécifiques. Si vous spécifiez 0.0.0.0/0 (IPv4) et ::/ (IPv6), cela permet à n'importe qui d'accéder à vos instances à partir de n'importe quelle adresse IP qui utilise le protocole spécifié.
- N'ouvrez pas des plages de ports trop vastes. Assurez-vous que l'accès via chaque port est limité aux sources ou aux destinations qui en ont besoin.
- Envisagez de créer des listes ACL réseau avec des règles similaires à celles de vos groupes de sécurité, afin d'ajouter une couche de sécurité supplémentaire à votre VPC. Pour en savoir plus sur les différences entre les groupes de sécurité et les listes ACL réseau, consultez la section Comparer les groupes de sécurité et les listes ACL réseau.

Exemple de groupe de sécurité

Le schéma suivant illustre un VPC avec deux groupes de sécurité et deux sous-réseaux. Les instances du sous-réseau A ont les mêmes exigences de connectivité et sont donc associées au groupe de sécurité 1. Les instances du sous-réseau B ont les mêmes exigences de connectivité et sont donc associées au groupe de sécurité 2. Les règles du groupe de sécurité autorisent le trafic comme suit :

- La première règle entrante du groupe de sécurité 1 autorise le trafic SSH vers les instances du sous-réseau A à partir de la plage d'adresses spécifiée (par exemple, une plage de votre propre réseau).
- La deuxième règle entrante du groupe de sécurité 1 permet aux instances du sous-réseau A de communiquer entre elles en utilisant n'importe quel protocole et port.
- La première règle entrante du groupe de sécurité 2 permet aux instances du sous-réseau B de communiquer entre elles en utilisant n'importe quel protocole et port.
- La deuxième règle entrante du groupe de sécurité 2 permet aux instances du sous-réseau A de communiquer avec les instances du sous-réseau B à l'aide du protocole SSH.
- Les deux groupes de sécurité utilisent la règle sortante par défaut, qui autorise tout le trafic.



Règles des groupes de sécurité

Les règles d'un groupe de sécurité contrôlent le trafic entrant autorisé à atteindre les ressources associées au groupe de sécurité. Les règles contrôlent également le trafic sortant autorisé à les quitter.

Vous pouvez ajouter ou retirer des règles pour un groupe de sécurité (ou encore autoriser ou révoquer un accès entrant ou sortant). Une règle s'applique au trafic entrant (ingress) ou sortant (egress). Vous pouvez accorder l'accès à une source ou une destination spécifique.

Table des matières

- Exemple de règles
- Résoudre les problèmes d'accessibilité

Règles de base de groupe de sécurité

- Vous pouvez indiquer des règles d'autorisation, mais pas des règles d'interdiction.
- Lorsque vous créez un groupe de sécurité pour la première fois, il n'existe pas de règles entrantes. Par conséquent, aucun trafic entrant n'est autorisé tant que vous n'avez pas ajouté de règles entrantes au groupe de sécurité.
- Lorsque vous créez un groupe de sécurité pour la première fois, il possède une règle sortante qui autorise tout le trafic sortant de la ressource. Vous pouvez retirer la règle et ajouter des règles sortantes qui autorisent un trafic sortant spécifique uniquement. Si votre groupe de sécurité n'a pas de règles sortantes, aucun trafic sortant n'est autorisé.
- Lorsque vous associez plusieurs groupes de sécurité à une ressource, les règles de chaque groupe de sécurité sont regroupées pour former un ensemble unique de règles utilisées pour déterminer s'il faut autoriser l'accès.
- Lorsque vous ajoutez, mettez à jour ou supprimez des règles, vos modifications sont automatiquement appliquées à toutes les ressources associées au groupe de sécurité. L'effet de certaines modifications de règle peut dépendre de la manière dont le trafic est suivi. Pour plus d'informations, consultez la section Suivi des connexions dans le guide de l'utilisateur Amazon EC2.
- Lorsque vous créez une règle de groupe de sécurité, AWS attribuez un identifiant unique à la règle. Vous pouvez utiliser l'ID d'une règle lorsque vous utilisez l'API ou la CLI pour modifier ou supprimer la règle.

Limitation

Les groupes de sécurité ne peuvent pas bloquer les requêtes DNS à destination ou en provenance du résolveur Route 53, parfois appelé « adresse IP VPC+2 » (voir le guide Amazon Route 53 Resolverdu développeur Amazon Route 53) ou DNS. AmazonProvided Afin de filtrer les demandes DNS via Route 53 Resolver, utilisez Route 53 Resolver DNS Firewall.

Composants d'une règle de groupe de sécurité

- Protocole : le protocole à autoriser. Les protocoles les plus courants sont 6 (TCP) 17 (UDP) et 1 (ICMP).

- Port range (Plage de ports) : pour TCP, UDP ou un protocole personnalisé : la plage de ports autorisée. Vous pouvez spécifier un seul numéro de port (par exemple, `22`), ou une plage de numéros de port (par exemple, `7000-8000`).
- ICMP type and code (Type et code ICMP) : pour ICMP, le code et le type ICMP. Par exemple, utilisez le type 8 pour la requête ICMP Echo ou 128 pour la requête ICMPv6 Echo.
- Source or destination (Source ou destination) : la source (règles entrantes) ou la destination (règles sortantes) pour le trafic à autoriser. Spécifiez l'un des éléments suivants :
  - Adresse IPv4 unique. Vous devez utiliser la longueur de préfixe `/32`. Par exemple, `203.0.113.1/32`.
  - Adresse IPv6 unique. Vous devez utiliser la longueur de préfixe `/128`. Par exemple, `2001:db8:1234:1a00::123/128`.
  - Plage d'adresses IPv4, en notation de bloc d'adresses CIDR. Par exemple, `203.0.113.0/24`.
  - Plage d'adresses IPv6, en notation de bloc d'adresses CIDR. Par exemple, `2001:db8:1234:1a00::/64`.
  - ID d'une liste des préfixes. Par exemple, `pl-1234abc1234abc123`. Pour plus d'informations, consultez the section called "Listes de préfixes gérées".
  - ID d'un groupe de sécurité. Par exemple, `sg-1234567890abcdef0`. Pour plus d'informations, consultez the section called "Référencement des groupes de sécurité".
- (Facultatif) Description : vous pouvez ajouter une description pour la règle, par exemple, pour vous aider à l'identifier ultérieurement. Une description peut inclure jusqu'à 255 caractères. Les caractères autorisés sont : a-z, A-Z, 0-9, espaces et ._-:/()#,@[]+=;{}!$*.

Référencement des groupes de sécurité

Lorsque vous spécifiez un groupe de sécurité comme source ou destination d'une règle, cette règle affecte toutes les instances associées aux groupes de sécurité. Les instances peuvent communiquer dans la direction spécifiée, en utilisant les adresses IP privées des instances, via le protocole et le port spécifiés.

Par exemple, ce qui suit présente une règle entrante pour un groupe de sécurité référençant le groupe de sécurité sg-0abcdef1234567890. Cette règle autorise le trafic SSH entrant depuis les instances associées à sg-0abcdef1234567890.

Source	Protocole	Plage de ports
sg-0abcdef1234567890	TCP	22

Lorsque vous référencez un groupe de sécurité dans une règle de groupe de sécurité, tenez compte des points suivants :

- Les groupes de sécurité doivent appartenir au même VPC ou VPC appairé.
- Aucune règle du groupe de sécurité référencé n'est ajoutée au groupe de sécurité le référençant.
- Pour les règles entrantes, les instances EC2 associées au groupe de sécurité peuvent recevoir le trafic entrant des adresses IP privées des instances EC2 associées au groupe de sécurité.
- Pour les règles sortantes, les instances EC2 associées au groupe de sécurité peuvent envoyer le trafic sortant aux adresses IP privées des instances EC2 associées au groupe de sécurité.

Limitation

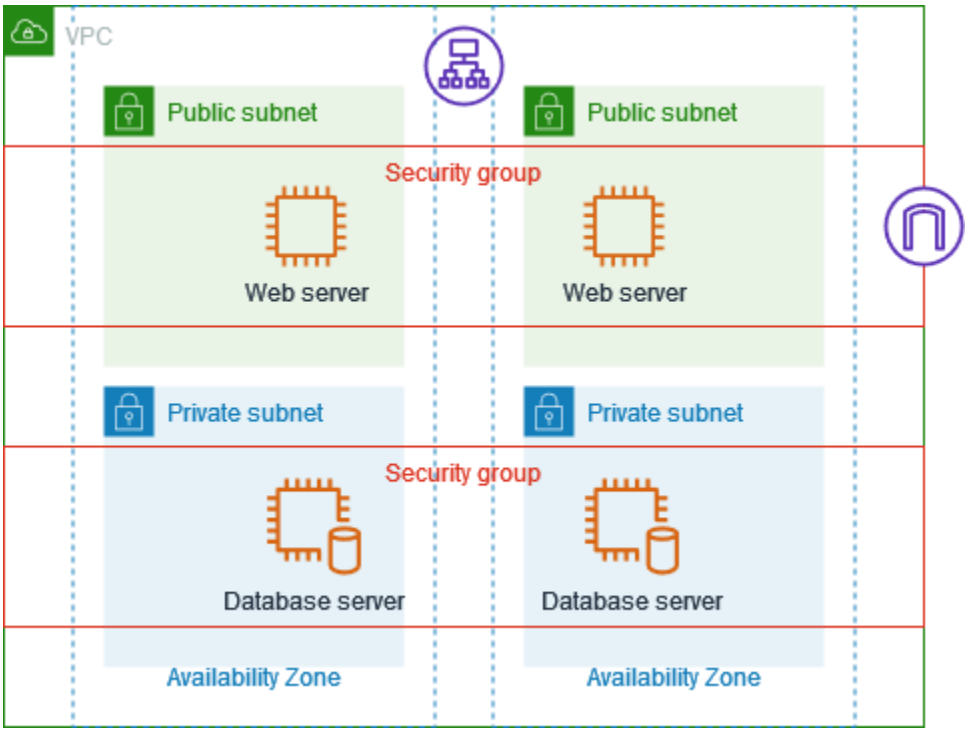
Si vous configurez des acheminements pour transférer le trafic entre deux instances de sous-réseaux différents via une appliance middlebox, vous devez vous assurer que les groupes de sécurité des deux instances autorisent le trafic à transiter entre les instances. Le groupe de sécurité de chaque instance doit référencer l'adresse IP privée de l'autre instance ou la plage d'adresses CIDR du sous-réseau qui contient l'autre instance en tant que source. Si vous référencez le groupe de sécurité de l'autre instance en tant que source, cela n'autorise pas le trafic à transiter entre les instances.

Exemple

Le schéma suivant montre un VPC avec des sous-réseaux dans deux zones de disponibilité, une passerelle Internet et un Application Load Balancer. Chaque zone de disponibilité possède un sous-réseau public pour les serveurs Web et un sous-réseau privé pour les serveurs de base de données. Il existe des groupes de sécurité distincts pour l'équilibreur de charge, les serveurs Web et les serveurs de base de données. Créez les règles du groupe de sécurité suivantes pour autoriser le trafic.

- Ajoutez des règles au groupe de sécurité de l'équilibreur de charge pour autoriser le trafic HTTP et HTTPS en provenance d'Internet. La source est 0.0.0.0/0.

- Ajoutez des règles au groupe de sécurité pour les serveurs Web afin d'autoriser le trafic HTTP et HTTPS uniquement en provenance de l'équilibreur de charge. La source est le groupe de sécurité pour l'équilibreur de charge.
- Ajoutez des règles au groupe de sécurité pour les serveurs de base de données afin d'autoriser les demandes de base de données provenant des serveurs Web. La source est le groupe de sécurité pour les serveurs Web.



Taille de groupe de sécurité

Le type de source ou de destination détermine la façon dont chaque règle est prise en compte dans le nombre maximum de règles que vous pouvez avoir par groupe de sécurité.

- Une règle référençant un bloc CIDR compte comme une seule règle.
- Une règle référençant un autre groupe de sécurité compte comme une seule règle, quelle que soit la taille du groupe de sécurité référencé.
- Une règle référençant une liste de préfixes gérée par le client compte comme la taille maximale de la liste de préfixes. Par exemple, si la taille maximale de votre liste de préfixes est égale à 20, une règle la référençant compte comme 20 règles.
- Une règle qui fait référence à une liste de préfixes AWS gérée compte comme le poids de la liste de préfixes. Par exemple, si le poids de la liste de préfixes est égale à 10, une règle la référençant

compte comme 10 règles. Pour plus d'informations, consultez the section called "Listes AWS de préfixes gérées disponibles".

Règles du groupe de sécurité obsolètes

Si votre VPC est connecté à un autre VPC par appairage de VPC ou s'il utilise un VPC partagé par un autre compte, une règle de groupe de sécurité peut référencer un groupe de sécurité dans le VPC pair ou le VPC partagé. Cela permet aux ressources associées au groupe de sécurité référencé et à celles associées au groupe de sécurité de référencement de communiquer entre elles.

Si le groupe de sécurité du VPC partagé est supprimé ou si la connexion d'appairage de VPC est supprimée, la règle de groupe de sécurité est marquée comme étant obsolète. Vous pouvez supprimer des règles de groupe de sécurité obsolètes comme vous le feriez pour toute autre règle de groupe de sécurité. Pour plus d'informations, consultez la section Travailler avec des règles de groupe de sécurité obsolètes dans le guide Amazon VPC Peering.

Utiliser des règles de groupe de sécurité

Les tâches suivantes vous montrent comment utiliser les règles de groupe de sécurité.

Autorisations nécessaires

- Gérer les règles de groupe de sécurité

Tâches

- Ajouter des règles à un groupe de sécurité
- Mettre à jour les règles du groupe de sécurité
- Étiqueter des règles de groupe de sécurité
- Supprimer des règles de groupe de sécurité

Ajouter des règles à un groupe de sécurité

Lorsque vous ajoutez une règle à un groupe de sécurité, la nouvelle règle est automatiquement appliquée à toutes les ressources associées au groupe de sécurité.

Si vous disposez d'une connexion d'appairage VPC, vous pouvez référencer des groupes de sécurité à partir du VPC pair comme source ou destination des règles d'entrée et de sortie dans les règles de votre groupe de sécurité. Pour de plus amples informations, veuillez consulter Mise à jour de

vos groupes de sécurité pour référencer des groupes de sécurité de VPC appairé dans le Guide d'appairage Amazon VPC.

Pour plus d'informations sur les autorisations requises pour gérer des règles de groupe de sécurité, veuillez consulter Gérer les règles de groupe de sécurité.

> **Warning**
>
> Si vous choisissez Anywhere-IPv4, vous autorisez le trafic provenant de toutes les adresses IPv4. Si vous choisissez Anywhere-IPv6, vous autorisez le trafic provenant de toutes les adresses IPv6. Lorsque vous ajoutez des règles pour les ports 22 (SSH) ou 3389 (RDP), autorisez uniquement une plage d'adresses IP spécifique à accéder à vos instances.

Pour ajouter une règle à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité.
4. Choisissez Actions, Edit inbound rules (Modifier les règles entrantes) or Actions, Edit outbound rules (Modifier les règles sortantes).
5. Pour chaque règle, choisissez Add rule (Ajouter une règle), puis procédez comme suit :

   a. Pour Type, choisissez le type de protocole à autoriser.

      - Pour TCP ou UDP, vous devez saisir la plage de ports à autoriser.
      - Pour un protocole ICMP personnalisé, vous devez choisir le nom du type d'ICMP dans Protocole et, le cas échéant, le nom de code dans Plage de ports.
      - Pour un autre type, le protocole et la plage de ports sont configurés automatiquement.

   b. Pour Source type (Type de source) (règles entrantes) ou Destination type (Type de destination) (règles sortantes), effectuez l'une des opérations suivantes pour autoriser le trafic :

      - Choisissez Personnalisé, puis entrez une adresse IP en notation CIDR, un bloc d'adresse CIDR, un autre groupe de sécurité ou une liste de préfixes.
      - Choisissez Anywhere-IPv4 (Partout-IPv4) pour autoriser le trafic de toute adresse IPv4 (règles entrantes) ou permettre au trafic d'atteindre toutes les adresses IPv4 (règles

sortantes). Cela ajoute automatiquement une règle pour le bloc d'adresses CIDR IPv4 0.0.0.0/0.

- Choisissez Anywhere-IPv6 (Partout-IPv6) pour autoriser le trafic de toute adresse IPv6 (règles entrantes) ou permettre au trafic d'atteindre toutes les adresses IPv6 (règles sortantes). Cela ajoute automatiquement une règle pour le bloc d'adresse CIDR IPv6 ::/0.
- Choisissez My IP (Mon adresse IP) pour autoriser uniquement le trafic provenant de (règles entrantes) ou à destination de (règles sortantes) l'adresse IPv4 publique de votre ordinateur local.

c. (Facultatif) Pour Description, saisissez une brève description de la règle.

6. Sélectionnez Enregistrer les règles.

Pour ajouter une règle à un groupe de sécurité à l'aide du AWS CLI

Utilisez les commandes authorize-security-group-ingress et authorize-security-group-egress.

Mettre à jour les règles du groupe de sécurité

Lorsque vous mettez à jour une règle, la règle mise à jour est automatiquement appliquée à toutes les ressources associées au groupe de sécurité.

Pour en savoir plus sur les autorisations requises pour gérer des règles de groupe de sécurité, consultez Gérer les règles de groupe de sécurité.

Pour mettre à jour une règle à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité.
4. Choisissez Actions, Edit inbound rules (Modifier les règles entrantes) or Actions, Edit outbound rules (Modifier les règles sortantes).
5. Mettez à jour la règle comme requis.
6. Sélectionnez Enregistrer les règles.

Pour mettre à jour une règle de groupe de sécurité à l'aide du AWS CLI

Utilisez les commandes modify-security-group-rules, update-security-group-rule-descriptions-ingress et update-security-group-rule-descriptions-egress.

Étiqueter des règles de groupe de sécurité

Ajoutez des étiquettes à vos ressources pour les organiser et les identifier, par exemple selon leur but, leur propriétaire ou leur environnement. Vous pouvez ajouter des étiquettes aux règles de groupe de sécurité. Les clés d'étiquette doivent être uniques pour chaque règle de groupe de sécurité. Si vous ajoutez une étiquette avec une clé qui est déjà associée à la règle de groupe de sécurité, cela a pour effet de mettre à jour la valeur de cette étiquette.

Pour étiqueter une règle à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité.
4. Sous l'onglet Règles entrantes ou Règles sortantes, sélectionnez la case à cocher de la règle, puis choisissez Gérer les étiquettes.
5. La page Gérer les étiquettes affiche toutes les étiquettes affectées à la règle. Pour ajouter une étiquette, choisissez Ajouter une étiquette, puis entrez la clé et la valeur de l'étiquette. Pour supprimer une balise, choisissez Remove (Supprimer) en regard de la balise à supprimer.
6. Sélectionnez Save changes (Enregistrer les modifications).

Pour baliser une règle à l'aide du AWS CLI

Utilisez la commande create-tags.

Supprimer des règles de groupe de sécurité

Lorsque vous supprimez une règle d'un groupe de sécurité, la modification est automatiquement appliquée à toutes les instances qui sont associées au groupe de sécurité.

Pour supprimer une règle de groupe de sécurité à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité.
4. Choisissez Actions, puis Edit inbound rules (Modifier les règles entrantes) pour supprimer une règle entrante ou Edit outbound rules (Modifier les règles sortantes) pour supprimer une règle sortante.
5. Cliquez sur le bouton Delete (Supprimer) à côté de la règle à supprimer.

6. Sélectionnez Enregistrer les règles. Vous pouvez également choisir Prévisualiser les modifications, vérifier vos modifications, puis cliquer sur Confirmer.

Pour supprimer une règle de groupe de sécurité à l'aide du AWS CLI

Utilisez les commandes revoke-security-group-ingress et revoke-security-group-egress.

Exemple de règles

Serveurs Web

Voici des exemples de règles pour un groupe de sécurité pour vos serveurs web. Les serveurs web peuvent recevoir du trafic HTTP et HTTPS de toutes les adresses IPv4 et IPv6 et envoyer du trafic SQL ou MySQL à vos serveurs de base de données.

> **Warning**
>
> Lorsque vous ajoutez des règles pour les ports 22 (SSH) ou 3389 (RDP) afin de pouvoir accéder à vos instances EC2, nous vous recommandons de n'autoriser que des plages d'adresses IP spécifique. Si vous spécifiez 0.0.0.0/0 (IPv4) et ::/ (IPv6), cela permet à n'importe qui d'accéder à vos instances à partir de n'importe quelle adresse IP qui utilise le protocole spécifié.

Entrant

Source	Protocole	Plage de ports	Description
0.0.0.0/0	TCP	80	Autorise l'accès HTTP entrant depuis l'ensemble des adresses IPv4
::/0	TCP	80	Autorise l'accès HTTP entrant depuis l'ensemble des adresses IPv6
0.0.0.0/0	TCP	443	

Source	Protocole	Plage de ports	Description
			Autorise l'accès HTTPS entrant depuis l'ensemble des adresses IPv4
::/0	TCP	443	Autorise l'accès HTTPS entrant depuis l'ensemble des adresses IPv6
Plage d'adresses IPv4 publiques de votre réseau	TCP	22	(Facultatif) Autorise l'accès SSH entrant à partir des adresses IP IPv4 de votre réseau
Plage d'adresses IPv6 de votre réseau	TCP	22	(Facultatif) Autorise l'accès SSH entrant à partir des adresses IP IPv6 de votre réseau
Plage d'adresses IPv4 publiques de votre réseau	TCP	3389	(Facultatif) Autorise l'accès RDP entrant à partir des adresses IP IPv4 de votre réseau
Plage d'adresses IPv6 de votre réseau	TCP	3389	(Facultatif) Autorise l'accès RDP entrant à partir des adresses IP IPv6 de votre réseau
ID de ce groupe de sécurité	Tous	Tous	(Facultatif) Autorise le trafic entrant à partir des autres serveurs associés à ce groupe de sécurité

Sortant

Destination	Protocole	Plage de ports	Description
ID du groupe de sécurité pour les instances exécutant Microsoft SQL Server	TCP	1433	Autorise l'accès sortant à Microsoft SQL Server
ID du groupe de sécurité pour les instances exécutant MySQL	TCP	3306	Autorise l'accès sortant à MySQL

Serveurs de base de données

Les serveurs de base de données nécessitent des règles qui autorisent des protocoles spécifiques entrants, tels que MySQL ou Microsoft SQL Server. Pour obtenir des exemples, consultez Règles de serveur de base de données dans le Guide de l'utilisateur Amazon EC2. Pour de plus amples informations sur les groupes de sécurité pour les instances DB Amazon RDS, veuillez consulter Contrôle d'accès par groupes de sécurité dans le Guide de l'utilisateur Amazon RDS.

Résoudre les problèmes d'accessibilité

Reachability Analyzer est un outil d'analyse de configuration statique. Utilisez Reachability Analyzer pour analyser et déboguer l'accessibilité réseau entre deux ressources de votre VPC. Reachability Analyzer hop-by-hop fournit des détails sur le chemin virtuel entre ces ressources lorsqu'elles sont accessibles, et identifie le composant bloquant dans le cas contraire. Par exemple, il peut identifier les règles de groupe de sécurité manquantes ou mal configurées.

Pour plus d'informations, reportez-vous au Guide de l'Analyseur d'accessibilité.

Groupes de sécurité par défaut pour vos VPC

Vos VPC par défaut et tous les VPC que vous créez sont fournis avec un groupe de sécurité par défaut. Le nom du groupe de sécurité par défaut est « default ».

Nous vous recommandons de créer des groupes de sécurité pour des ressources ou des groupes de ressources spécifiques plutôt que d'utiliser le groupe de sécurité par défaut. Cependant, si vous

n'associez pas de groupe de sécurité à certaines ressources au moment de la création, nous les associons au groupe de sécurité par défaut. Par exemple, si vous ne spécifiez pas de groupe de sécurité lorsque vous lancez une instance EC2, nous associons l'instance au groupe de sécurité par défaut de son VPC.

Principes de base des groupes de sécurité par défaut

- Vous pouvez modifier les règles du groupe de sécurité par défaut.
- Vous ne pouvez pas supprimer un groupe de sécurité par défaut. Si vous essayez de supprimer un groupe de sécurité par défaut, nous renvoyons le code d'erreur suivante : `Client.CannotDelete`.

Règles par défaut

Les tableaux ci-après décrivent les règles par défaut pour un groupe de sécurité par défaut.

Entrant

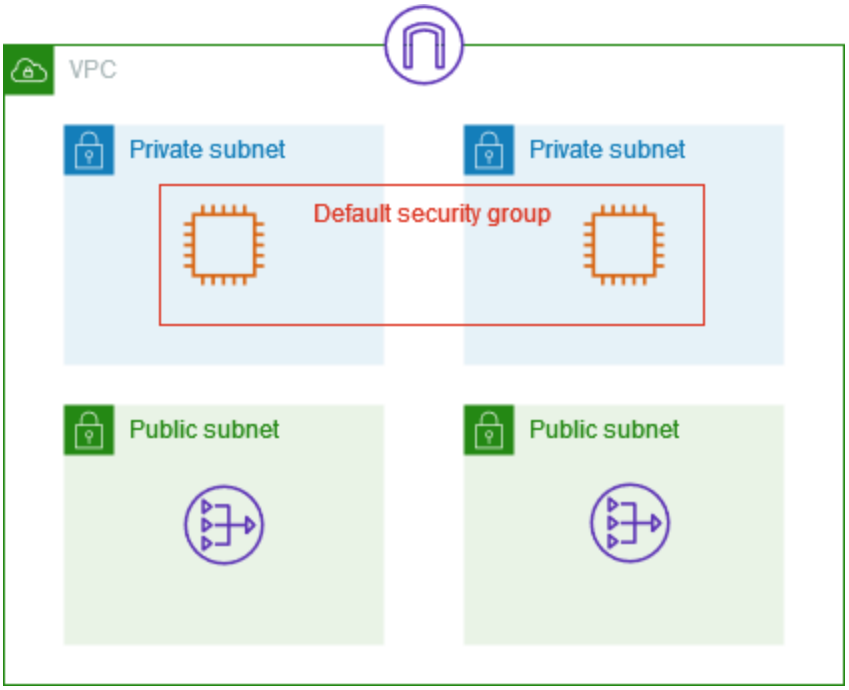
Source	Protocole	Plage de ports	Description
sg-1234567890abcdef0	Tous	Tous	Autorise le trafic entrant à partir de toutes les ressources attribuées à ce groupe de sécurité. La source est l'ID de ce groupe de sécurité.

Sortant

Destination	Protocole	Plage de ports	Description
0.0.0.0/0	Tous	Tous	Autorise tout le trafic IPv4 sortant.
::/0	Tous	Tous	Autorise tout le trafic IPv6 sortant. Cette règle est ajoutée uniquement si votre VPC dispose d'un bloc d'adresse CIDR IPv6 associé.

Exemple

Le schéma suivant montre un VPC avec un groupe de sécurité, une passerelle Internet et une passerelle NAT par défaut. La sécurité par défaut contient uniquement ses règles par défaut et elle est associée à deux instances EC2 exécutées dans le VPC. Dans ce scénario, chaque instance peut recevoir du trafic entrant en provenance de l'autre instance sur tous les ports et protocoles. Les règles par défaut ne permettent pas aux instances de recevoir de trafic depuis la passerelle Internet ou la passerelle NAT. Si vos instances doivent recevoir de trafic supplémentaire, nous vous recommandons de créer un groupe de sécurité avec les règles requises et d'associer le nouveau groupe de sécurité aux instances au lieu du groupe de sécurité par défaut.



Utiliser des groupes de sécurité

Les tâches suivantes vous montrent comment utiliser les groupes de sécurité.

Tâches

- Création d'un groupe de sécurité
- Afficher vos groupes de sécurité
- Étiqueter vos groupes de sécurité
- Supprimer un groupe de sécurité
- Gérer les groupes de sécurité à l'aide de Firewall Manager

Autorisations nécessaires

Avant de commencer, vérifiez que vous disposez des autorisations requises.

- Gérer les groupes de sécurité
- Gérer les règles de groupe de sécurité

Les règles d'un groupe de sécurité contrôlent le trafic entrant autorisé à atteindre les ressources associées au groupe de sécurité. Pour plus d'informations sur les règles de groupe de sécurité, consultez Règles des groupes de sécurité.

Création d'un groupe de sécurité

Par défaut, les nouveaux groupes de sécurité commencent avec seulement une règle de trafic sortant, qui permet à la totalité du trafic de quitter la ressource. Vous devez ajouter des règles pour activer un trafic entrant ou limiter le trafic sortant.

Pour créer un groupe de sécurité à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez Create security group (Créer un groupe de sécurité).
4. Saisissez un nom et une description pour le groupe de sécurité. Vous ne pouvez pas modifier le nom et la description d'un groupe de sécurité créé.
5. Dans VPC, choisissez un VPC. Le groupe de sécurité ne peut être utilisé que dans le VPC dans lequel il est créé.
6. Vous pouvez ajouter des règles de groupe de sécurité maintenant ou plus tard. Pour plus d'informations, consultez Ajouter des règles à un groupe de sécurité.
7. Vous pouvez ajouter des étiquettes maintenant ou ultérieurement. Pour ajouter une étiquette, choisissez Ajouter une nouvelle étiquette), puis entrez la clé et la valeur de l'étiquette.
8. Sélectionnez Créer un groupe de sécurité.

Une fois que le groupe de sécurité est créé, vous pouvez effectuer l'une des actions suivantes :

- Attribuez le groupe de sécurité à une instance EC2 lorsque vous lancez l'instance ou modifiez le groupe de sécurité actuellement affecté à une instance. Pour plus d'informations, consultez Lancer une instance ou Modifier les groupes de sécurité dans le guide de l'utilisateur Amazon EC2.

- Ajoutez des règles de groupe de sécurité. Les règles d'un groupe de sécurité contrôlent le trafic entrant autorisé à atteindre les ressources associées au groupe de sécurité. Pour plus d'informations sur les règles de groupe de sécurité, consultez Utiliser des règles de groupe de sécurité.

Pour créer un groupe de sécurité à l'aide du AWS CLI

Utilisez la commande create-security-group.

Afficher vos groupes de sécurité

Vous pouvez afficher des informations sur vos groupes de sécurité comme suit.

Pour afficher vos groupes de sécurité à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Vos groupes de sécurité sont répertoriés. Pour afficher les détails d'un groupe de sécurité spécifique, y compris ses règles entrantes et sortantes, sélectionnez le groupe de sécurité. Pour plus d'informations sur la mise à jour des règles de groupe de sécurité, consultez Mettre à jour les règles du groupe de sécurité.

Pour afficher tous vos groupes de sécurité relevant des différentes régions

Ouvrez la console Amazon EC2 Global View à l'adresse https://console.aws.amazon.com/ec2globalview/home. Pour plus d'informations, consultez Répertorier et filtrer les ressources à l'aide d'Amazon EC2 Global View dans le guide de l'utilisateur Amazon EC2.

Pour afficher vos groupes de sécurité à l'aide du AWS CLI

Utilisez les commandes describe-security-groups et describe-security-group-rules.

Étiqueter vos groupes de sécurité

Ajoutez des étiquettes à vos ressources pour les organiser et les identifier, par exemple selon leur but, leur propriétaire ou leur environnement. Vous pouvez ajouter des balises à vos groupes de sécurité. Les clés de balise doivent être uniques pour chaque règle de groupe de sécurité. Si vous ajoutez une balise avec une clé qui est déjà associée à la règle, cela met à jour la valeur de cette balise.

Pour étiqueter un groupe de sécurité à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Activez la case à cocher en regard du groupe de sécurité.
4. Choisissez Actions, Gérer les balises. La page Gérer les étiquettes affiche toutes les étiquettes affectées au groupe de sécurité.
5. Pour ajouter une étiquette, choisissez Ajouter une nouvelle balise, puis entrez la clé et la valeur de la balise. Pour supprimer une étiquette, choisissez Remove (Retirer) en regard de l'étiquette à supprimer.
6. Sélectionnez Enregistrer les modifications.

Pour étiqueter un groupe de sécurité à l'aide du AWS CLI

Utilisez la commande create-tags.

Supprimer un groupe de sécurité

Vous pouvez supprimer un groupe de sécurité uniquement s'il n'est associé à aucune ressource. Vous ne pouvez pas supprimer un groupe de sécurité par défaut.

Si vous utilisez la console, vous pouvez supprimer plusieurs groupes de sécurité simultanément. Si vous utilisez la ligne de commande ou l'API, vous ne pouvez supprimer qu'un seul groupe de sécurité à la fois.

Pour supprimer un groupe de sécurité à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité, puis choisissez Actions, Supprimer les groupes de sécurité.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour supprimer un groupe de sécurité à l'aide du AWS CLI

Utilisez la commande delete-security-group.

Gérer les groupes de sécurité à l'aide de Firewall Manager

AWS Firewall Manager simplifie les tâches d'administration et de maintenance de vos groupes de sécurité sur plusieurs comptes et ressources. Avec Firewall Manager, vous pouvez configurer et auditer les groupes de sécurité pour votre organisation à partir d'un seul compte d'administrateur central. Firewall Manager applique automatiquement les règles et les protections sur l'ensemble de vos comptes et de vos ressources, même celles qui sont ajoutées ultérieurement. Firewall Manager est particulièrement utile lorsque vous souhaitez protéger l'ensemble de votre organisation ou si vous ajoutez fréquemment de nouvelles ressources que vous souhaitez protéger à partir d'un compte d'administrateur central.

Vous pouvez utiliser Firewall Manager pour gérer de manière centralisée les groupes de sécurité de la manière suivante :

- Configurer des groupes de sécurité de base communs dans votre organisation : vous pouvez utiliser une stratégie de groupe de sécurité commune pour fournir une association centralisée de groupes de sécurité aux comptes et aux ressources de votre organisation. Vous spécifiez où et comment appliquer la stratégie dans votre organisation.
- Audit des groupes de sécurité existants dans votre organisation : vous pouvez utiliser une stratégie de groupe de sécurité d'audit pour vérifier les règles existantes utilisées dans les groupes de sécurité de votre organisation. Vous pouvez étendre la stratégie pour auditer tous les comptes, des comptes spécifiques ou des ressources balisées au sein de votre organisation. Firewall Manager détecte automatiquement les nouveaux comptes et ressources pour les auditer. Vous pouvez créer des règles d'audit pour définir les règles de groupe de sécurité à autoriser ou à interdire au sein de votre organisation, et pour rechercher les groupes de sécurité non utilisés ou redondants.
- Obtenir des rapports sur les ressources non conformes et les corriger : vous pouvez obtenir des rapports et des alertes sur les ressources non conformes pour vos stratégies de référence et d'audit. Vous pouvez également définir des flux de travail de correction automatique afin de corriger les ressources non conformes détectées par Firewall Manager.

Pour en savoir plus sur l'utilisation de Firewall Manager pour gérer vos groupes de sécurité, consultez les ressources suivantes dans le guide du AWS Firewall Manager développeur :

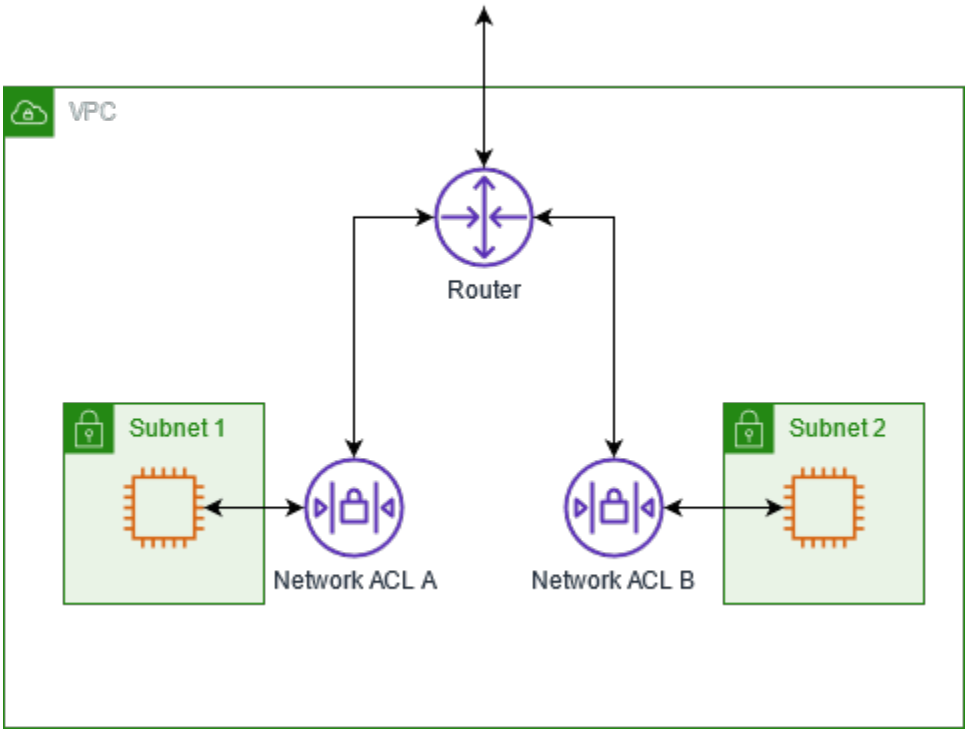
- AWS Firewall Manager prérequis
- Commencer à utiliser les AWS Firewall Manager politiques des groupes de sécurité Amazon VPC
- Comment fonctionnent les politiques de groupe de sécurité dans AWS Firewall Manager
- Cas d'utilisation des stratégies de groupe de sécurité

Contrôle du trafic vers les sous-réseaux avec des listes ACL réseau

Une liste de contrôle d'accès (ACL) réseau autorise ou refuse un trafic entrant ou sortant spécifique au niveau du sous-réseau. Vous pouvez utiliser l'ACL réseau par défaut pour votre VPC ou vous pouvez en créer une personnalisée pour votre VPC à l'aide de règles similaires aux règles de vos groupes de sécurité afin d'ajouter une couche de sécurité supplémentaire à votre VPC.

L'utilisation d'ACL réseau n'implique aucun coût supplémentaire.

Le diagramme suivant illustre un VPC avec deux sous-réseaux. Chaque sous-réseau possède une ACL réseau. Lorsque du trafic entre dans le VPC (par exemple, à partir d'un VPC appairé, d'une connexion VPN ou d'Internet), le routeur envoie le trafic vers sa destination. L'ACL réseau A détermine quel trafic destiné au sous-réseau 1 est autorisé à entrer dans le sous-réseau 1 et quel trafic destiné à un emplacement en dehors du sous-réseau 1 est autorisé à quitter le sous-réseau 1. De même, l'ACL B du réseau détermine quel trafic est autorisé à entrer et à sortir du sous-réseau 2.



Pour en savoir plus sur les différences entre les groupes de sécurité et les listes ACL réseau, consultez Comparer les groupes de sécurité et les listes ACL réseau.

Table des matières

Principes de base des listes ACL réseau

Vous trouverez ci-dessous les principes de base à connaître concernant les listes ACL réseau :

- Votre VPC est automatiquement associé à une liste ACL réseau par défaut, que vous pouvez modifier. Par défaut, il autorise tout le trafic IPv4 entrant et sortant, ainsi que le trafic IPv6, le cas échéant.
- Vous pouvez créer une ACL réseau personnalisée et l'associer à un sous-réseau pour autoriser ou refuser un trafic entrant ou sortant spécifique au niveau du sous-réseau.
- Chaque sous-réseau de votre VPC doit être associé à une liste ACL réseau. Si vous n'associez pas explicitement un sous-réseau à une liste ACL réseau, le sous-réseau est automatiquement associé à la liste ACL réseau par défaut.
- Vous pouvez associer une liste ACL réseau à plusieurs sous-réseaux. Cependant, un sous-réseau ne peut être associé qu'à une seule liste ACL réseau à la fois. Lorsque vous associez une liste ACL réseau à un sous-réseau, l'association antérieure est supprimée.
- Une ACL réseau possède des règles entrantes et des règles sortantes. Chaque règle peut autoriser ou refuser le trafic. Chaque règle possède un numéro compris entre 1 et 32 766. Nous évaluons les règles dans l'ordre, en commençant par la règle ayant le numéro le plus bas, lorsque nous décidons d'autoriser ou de refuser le trafic. Si le trafic correspond à une règle, celle-ci est appliquée et nous n'évaluons aucune règle supplémentaire. Lorsque vous créez des règles, nous vous recommandons de commencer par des incréments (par exemple, des incréments de 10 ou 100), de façon à pouvoir insérer de nouvelles règles par la suite si nécessaire.
- Nous évaluons les règles ACL du réseau lorsque le trafic entre et sort du sous-réseau, et non lorsqu'il est acheminé au sein d'un sous-réseau.

- Les NACL sont sans état, ce qui signifie que les informations sur le trafic précédemment envoyé ou reçu ne sont pas sauvegardées. Si, par exemple, vous créez une règle NACL pour autoriser un trafic entrant spécifique vers un sous-réseau, les réponses à ce trafic ne sont pas automatiquement autorisées. Cela contraste avec le fonctionnement des groupes de sécurité. Les groupes de sécurité sont avec état, ce qui signifie que les informations sur le trafic précédemment envoyé ou reçu sont enregistrées. Si, par exemple, un groupe de sécurité autorise le trafic entrant vers une instance EC2, les réponses sont automatiquement autorisées, quelles que soient les règles du groupe de sécurité pour le trafic sortant.
- Les ACL réseau ne peuvent pas bloquer les requêtes DNS à destination ou en provenance du résolveur Route 53 (également connu sous le nom d'adresse IP VPC+2 ou DNS). AmazonProvided Pour filtrer les demandes DNS via Route 53 Resolver, vous pouvez activer Route 53 Resolver DNS Firewall (voir le Guide du développeur Amazon Route 53).
- Les listes ACL réseau ne peuvent pas bloquer le trafic vers le service de métadonnées d'instance (IMDS). Pour gérer l'accès à IMDS, consultez la section Configurer les options de métadonnées d'instance dans le Guide de l'utilisateur Amazon EC2.
- Les listes ACL réseau ne filtrent pas le trafic vers et depuis les services suivants :
  - Amazon Domain Name Services (DNS)
  - Amazon Dynamic Host Configuration Protocol (DHCP)
  - Métadonnées d'instance Amazon EC2.
  - Points de terminaison des métadonnées de tâches Amazon ECS
  - Activation de licence pour les instances Windows
  - Service de synchronisation temporelle d'Amazon
  - Adresses IP réservées utilisées par le routeur VPC par défaut
- Il existe des quotas (également appelés limites) pour le nombre de listes ACL réseau par VPC et le nombre de règles par liste ACL réseau. Pour plus d'informations, consultez Quotas Amazon VPC.

Règles des listes ACL réseau

Vous pouvez ajouter des règles à la liste ACL réseau par défaut ou en supprimer. Vous pouvez également créer des listes ACL réseau supplémentaires pour votre VPC. Lorsque vous ajoutez une règle à une liste ACL réseau ou en supprimez, les modifications s'appliquent automatiquement aux sous-réseaux auxquels elle est associée.

Une règle d'une liste ACL réseau est composée des éléments suivants :

- Numéro de règle. les règles sont évaluées en commençant par la règle comportant le numéro le plus bas. Lorsqu'une règle correspond au trafic, elle s'applique même si une règle avec un numéro plus élevé la contredit.
- Type. Type de trafic ; par exemple, SSH. Vous pouvez également spécifier tout le trafic ou une plage personnalisée.
- Protocole. Vous pouvez spécifier n'importe quel protocole associé à un numéro de protocole standard. Pour plus d'informations, consultez la page Protocol Numbers. Si vous indiquez ICMP comme protocole, vous pouvez indiquer tout ou partie des types et codes ICMP.
- Plage de ports. Port d'écoute ou plage de ports pour le trafic. Par exemple, 80 pour le trafic HTTP.
- Source. [Règles entrantes uniquement] Source du trafic (plage CIDR).
- Destination. [Règles sortantes uniquement] Destination du trafic (plage CIDR).
- Autoriser/Refuser. Indique s'il faut autoriser ou refuser le trafic spécifié.

Si vous ajoutez une règle à l'aide d'un outil de ligne de commande ou de l'API Amazon EC2, la plage CIDR est automatiquement remise à sa forme canonique. Par exemple, si vous spécifiez `100.68.0.18/18` pour la plage CIDR, nous créons une règle avec une plage CIDR `100.68.0.0/18`.

Liste ACL réseau par défaut

La liste ACL réseau par défaut est configurée pour autoriser l'ensemble du trafic à entrer et sortir des sous-réseaux auxquels elle est associée. Chaque liste ACL réseau inclut également une règle par défaut dont le numéro est un astérisque (*). Cette règle permet de s'assurer qu'un paquet sera refusé s'il ne correspond à aucune des autres règles numérotées. Vous ne pouvez pas modifier ni supprimer cette règle.

Voici un exemple de liste ACL réseau par défaut pour un VPC qui prend en charge IPv4 uniquement.

Entrant

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser
100	Tout le trafic IPv4	Tous	Tous	0.0.0.0/0	AUTORISER

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser
*	Tout le trafic IPv4	Tous	Tous	0.0.0.0/0	REFUSER

Sortant

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/ Refuser
100	Tout le trafic IPv4	Tous	Tous	0.0.0.0/0	AUTORISER
*	Tout le trafic IPv4	Tous	Tous	0.0.0.0/0	REJETER

Si vous créez un VPC avec un bloc d'adresse CIDR IPv6, ou si vous associez un bloc d'adresse CIDR IPv6 à votre VPC existant, nous ajoutons automatiquement des règles qui autorisent tout le trafic IPv6 à entrer et sortir de votre sous-réseau. Nous ajoutons également des règles dont les numéros sont des astérisques, ce qui garantit qu'un paquet est refusé s'il ne correspond à aucune des autres règles numérotées. Vous ne pouvez pas modifier ou supprimer ces règles. Voici un exemple de liste ACL réseau par défaut pour un VPC qui prend en charge IPv4 et IPv6.

> **Note**
>
> Si vous avez modifié les règles entrantes de votre liste ACL réseau par défaut, nous n'ajoutons pas automatiquement de règle `ALLOW` pour le trafic IPv6 entrant lorsque vous associez un bloc IPv6 à votre VPC. De même, si vous avez modifié les règles sortantes, nous n'ajoutons pas automatiquement de règle `ALLOW` pour le trafic IPv6 sortant.

Entrant

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser
100	Tout le trafic IPv4	Tous	Tous	0.0.0.0/0	AUTORISER
101	Tout le trafic IPv6	Tous	Tous	::/0	AUTORISER
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REJETER
*	Tout le trafic IPv6	Tous	Tous	::/0	REFUSER

Sortant

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/ Refuser
100	Tout le trafic	Tous	Tous	0.0.0.0/0	AUTORISER
101	Tout le trafic IPv6	Tous	Tous	::/0	AUTORISER
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REJETER
*	Tout le trafic IPv6	Tous	Tous	::/0	REFUSER

Liste ACL réseau personnalisée

L'exemple suivant illustre une liste ACL réseau personnalisée pour un VPC qui prend en charge IPv4 uniquement. Il inclut des règles entrantes autorisant le trafic HTTP et HTTPS entrant (100 et 110). Une règle sortante correspondante autorise les réponses à ce trafic entrant (140), qui couvre les ports éphémères 32768-65535. Pour savoir comment sélectionner la plage de ports éphémères appropriée, consultez la section Ports éphémères.

La liste ACL réseau inclut également des règles entrantes qui autorisent le trafic SSH et RDP dans le sous-réseau. La règle sortante 120 autorise les réponses à sortir du sous-réseau.

La liste ACL réseau inclut des règles sortantes (100 et 110) qui autorisent le trafic HTTP et HTTPS sortant du sous-réseau. Une règle entrante correspondante autorise les réponses à ce trafic sortant (140), qui couvre les ports éphémères 32768-65535.

Chaque liste ACL réseau inclut une règle par défaut dont le numéro est un astérisque. Cette règle permet de s'assurer qu'un paquet sera refusé s'il ne correspond à aucune des autres règles. Vous ne pouvez pas modifier ni supprimer cette règle.

Entrant

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser	Commentaires
100	HTTP	TCP	80	0.0.0.0/0	AUTORISE	Autorise le trafic HTTP entrant depuis n'importe quelle adresse IPv4.
110	HTTPS	TCP	443	0.0.0.0/0	AUTORISE	Autorise le trafic HTTPS entrant depuis n'importe quelle adresse IPv4.
120	SSH	TCP	22	192.0.2.0/24	AUTORISE	Autorise le trafic SSH entrant depuis la plage d'adresses IPv4 publiques de votre réseau domestique (via la passerelle Internet).
130	RDP	TCP	3389	192.0.2.0/24	AUTORISE	Autorise le trafic RDP entrant vers les serveurs web depuis la plage d'adresses IPv4 publiques

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser	Commentaires
						de votre réseau domestique (via la passerelle Internet).
140	TCP personnalisé	TCP	32768/65535	0.0.0.0/0	AUTORISE	Autorise le trafic IPv4 de retour entrant depuis Internet (pour les demandes qui proviennent du sous-réseau). Cette plage est uniquement à titre d'exemple.
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REJETER	Refuse l'ensemble du trafic IPv4 entrant qui n'est pas déjà géré par une règle précédente (non modifiable).

Sortant

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/ Refuser	Commentaires
100	HTTP	TCP	80	0.0.0.0/0	AUTORISE	Autorise le trafic HTTP IPv4 sortant du sous-réseau vers Internet.
110	HTTPS	TCP	443	0.0.0.0/0	AUTORISE	Autorise le trafic HTTPS IPv4 sortant

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/Refuser	Commentaires
						du sous-réseau vers Internet.
120	SSH	TCP	1024-65535	192.0.2.0/24	AUTORISE	Autorise le retour du trafic SSH sortant vers la plage d'adresses IPv4 publique de votre réseau domestique (via la passerelle Internet).
140	TCP personnalisé	TCP	32768/65535	0.0.0.0/0	AUTORISE	Autorise les réponses IPv4 sortantes aux clients sur Internet (par exemple, la diffusion de pages web auprès des visiteurs des serveurs web dans le sous-réseau). Cette plage est uniquement à titre d'exemple.
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REJETER	Refuse l'ensemble du trafic IPv4 sortant qui n'est pas déjà géré par une règle précédente (non modifiable).

Lorsqu'un paquet arrive dans le sous-réseau, nous l'évaluons par rapport aux règles de trafic entrant de la liste ACL à laquelle le sous-réseau est associé (en commençant par le haut de la liste des règles, puis en descendant). Voici comment se produit l'évaluation si le paquet est destiné au port HTTPS (443). Le paquet ne correspond pas à la première règle évaluée (règle 100). Il correspond à la deuxième (110), qui autorise le paquet dans le sous-réseau. Si le paquet avait été destiné au port 139 (NetBIOS), il ne correspond à aucune des règles et la règle * finit par refuser le paquet.

Vous pouvez ajouter une règle deny lorsque vous considérez que vous avez légitimement besoin d'ouvrir une grande plage de ports, mais que vous souhaitez refuser certains ports de cette plage. Dans le tableau, assurez-vous simplement de placer la règle deny avant celle qui autorise le trafic de la grande plage de ports.

Vous ajoutez des règles allow en fonction de votre cas d'utilisation. Par exemple, vous pouvez ajouter une règle qui autorise l'accès TCP et UDP sortant sur le port 53 pour la résolution DNS. Pour chaque règle que vous ajoutez, assurez-vous qu'il existe une règle entrante ou sortante correspondante qui autorise le trafic de réponse.

L'exemple suivant illustre une liste ACL réseau personnalisée pour un VPC auquel est associé un bloc d'adresse CIDR IPv6. Cette liste ACL réseau inclut des règles pour l'ensemble du trafic HTTP et HTTPS IPv6. Dans ce cas, de nouvelles règles ont été insérées entre les règles existantes pour le trafic IPv4. Vous pouvez également ajouter les règles en tant que règles de nombre supérieur après les règles IPv4. Le trafic IPv4 est distinct du trafic IPv6 et, par conséquent, aucune des règles définies pour le trafic IPv4 ne s'applique au trafic IPv6.

Entrant

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser	Commentaires
100	HTTP	TCP	80	0.0.0.0/0	AUTORISE	Autorise le trafic HTTP entrant depuis n'importe quelle adresse IPv4.
105	HTTP	TCP	80	::/0	AUTORISE	Autorise le trafic HTTP entrant depuis n'importe quelle adresse IPv6.

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser	Commentaires
110	HTTPS	TCP	443	0.0.0.0/0	AUTORISE	Autorise le trafic HTTPS entrant depuis n'importe quelle adresse IPv4.
115	HTTPS	TCP	443	::/0	AUTORISE	Autorise le trafic HTTPS entrant depuis n'importe quelle adresse IPv6.
120	SSH	TCP	22	192.0.2.0/24	AUTORISE	Autorise le trafic SSH entrant depuis la plage d'adresses IPv4 publiques de votre réseau domestique (via la passerelle Internet).
130	RDP	TCP	3389	192.0.2.0/24	AUTORISE	Autorise le trafic RDP entrant vers les serveurs web depuis la plage d'adresses IPv4 publiques de votre réseau domestique (via la passerelle Internet).

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser	Commentaires
140	TCP personnalisé	TCP	32768/65535	0.0.0.0/0	AUTORISE	Autorise le trafic IPv4 de retour entrant depuis Internet (pour les demandes qui proviennent du sous-réseau). Cette plage est uniquement à titre d'exemple.
145	TCP personnalisé	TCP	32768-65535	::/0	AUTORISE	Autorise le trafic IPv6 de retour entrant depuis Internet (pour les demandes qui proviennent du sous-réseau). Cette plage est uniquement à titre d'exemple.
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REJETER	Refuse l'ensemble du trafic IPv4 entrant qui n'est pas déjà géré par une règle précédente (non modifiable).
*	Tout le trafic	Tous	Tous	::/0	REFUSER	Refuse l'ensemble du trafic IPv6 entrant qui n'est pas déjà géré par une règle précédente (non modifiable).

Sortant

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/ Refuser	Commentaires
100	HTTP	TCP	80	0.0.0.0/0	AUTORISE	Autorise le trafic HTTP IPv4 sortant du sous-réseau vers Internet.
105	HTTP	TCP	80	::/0	AUTORISE	Autorise le trafic HTTP IPv6 sortant du sous-réseau vers Internet.
110	HTTPS	TCP	443	0.0.0.0/0	AUTORISE	Autorise le trafic HTTPS IPv4 sortant du sous-réseau vers Internet.
115	HTTPS	TCP	443	::/0	AUTORISE	Autorise le trafic HTTPS IPv6 sortant du sous-réseau vers Internet.
140	TCP personnalisé	TCP	32768/65535	0.0.0.0/0	AUTORISE	Autorise les réponses IPv4 sortantes aux clients sur Internet (par exemple, la diffusion de pages web auprès des visiteurs des serveurs web dans le sous-réseau). Cette plage est uniquement à titre d'exemple.

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/Refuser	Commentaires
145	TCP personnalisé	TCP	32768-65535	::/0	AUTORISE	Autorise les réponses IPv6 sortantes aux clients sur Internet (par exemple, la diffusion de pages web auprès des visiteurs des serveurs web du sous-réseau). Cette plage est uniquement à titre d'exemple.
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REJETER	Refuse l'ensemble du trafic IPv4 sortant qui n'est pas déjà géré par une règle précédente (non modifiable).
*	Tout le trafic	Tous	Tous	::/0	REFUSER	Refuse l'ensemble du trafic IPv6 sortant qui n'est pas déjà géré par une règle précédente (non modifiable).

ACL réseau personnalisés et autres services AWS

Si vous créez une ACL réseau personnalisée, soyez conscient de l'impact que cela peut avoir sur les ressources que vous créez à l'aide d'autres AWS services.

Avec Elastic Load Balancing, si le sous-réseau de vos instances backend comporte une liste de contrôle d'accès réseau à laquelle vous avez ajouté une règle refuser pour tout le trafic dont la source est `0.0.0.0/0` ou le CIDR du sous-réseau, votre équilibreur de charge ne peut pas effectuer de vérifications d'état sur les instances. Pour de plus amples informations sur les règles des listes de contrôle d'accès réseau recommandées pour vos équilibreurs de charge et vos instances backend, veuillez consulter Listes de contrôle d'accès réseau pour équilibreurs de charge dans un VPC dans le Guide de l'utilisateur pour Classic Load Balancers.

Ports éphémères

L'exemple de liste ACL réseau fourni dans la section précédente utilise la plage de ports éphémères 32768-65535. Toutefois, vous pouvez choisir une plage différente pour vos listes ACL réseau, en fonction du type de client que vous utilisez ou avec lequel vous communiquez.

Le client qui initie la demande choisit la plage de ports éphémères, qui varie en fonction de son système d'exploitation.

- De nombreux noyaux Linux (y compris le noyau Amazon Linux) utilisent les ports 32768-61000.
- Les demandes provenant d'Elastic Load Balancing utilisent les ports 1024-65535.
- Les systèmes d'exploitation Windows exécutant Windows Server 2003 utilisent les ports 1025-5000.
- Windows Server 2008 et les versions ultérieures utilisent les ports 49152-65535.
- Une passerelle NAT utilise les ports 1024-65535.
- AWS Lambda les fonctions utilisent les ports 1024-65535.

Par exemple, si une demande arrive sur un serveur Web dans votre VPC en provenance d'un client Windows 10 sur Internet, votre liste ACL réseau doit comporter une règle sortante pour autoriser le trafic destiné aux ports 49152-65535.

Si une instance de votre VPC correspond au client initiant la demande, votre liste de contrôle d'accès réseau doit comporter une règle entrante pour autoriser le trafic destiné aux ports éphémères propres à ce type d'instance (Amazon Linux, Windows Server 2008, etc.).

En pratique, pour couvrir les différents types de clients susceptibles d'initier du trafic vers des instances destinées au public dans votre VPC, vous pouvez ouvrir les ports éphémères 1024-65535. Toutefois, vous pouvez également ajouter des règles à la liste ACL afin de refuser le trafic sur tous

les ports malveillants inclus dans cette plage. Assurez-vous de placer les règles deny avant les règles allow qui ouvrent la grande plage de ports éphémères.

Détection de la MTU du chemin

La détection de la MTU du chemin permet de déterminer la MTU du chemin entre deux appareils. La MTU du chemin correspond à la taille maximum du paquet prise en charge sur le chemin entre l'hôte de départ et l'hôte de destination.

Pour IPv4, si un hôte envoie un paquet dont la taille est plus importante que la MTU définie pour l'hôte destinataire ou que celle d'un appareil se trouvant sur le chemin, l'hôte ou l'appareil destinataire supprime le paquet et retourne le message ICMP suivant : `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Type 3, Code 4). Cela indique à l'hôte émetteur de diviser la charge utile en plusieurs paquets plus petits, puis de les retransmettre.

Le protocole IPv6 ne prend pas en charge la fragmentation dans le réseau. Si un hôte envoie un paquet dont la taille est plus importante que la MTU définie pour l'hôte destinataire ou que celle d'un appareil se trouvant sur le chemin, l'hôte ou l'appareil destinataire supprime le paquet et retourne le message ICMP suivant : `ICMPv6 Packet Too Big (PTB)` (Type 2). Cela indique à l'hôte émetteur de diviser la charge utile en plusieurs paquets plus petits, puis de les retransmettre.

Si l'unité de transmission maximale (MTU) entre les hôtes de vos sous-réseaux est différente, ou si vos instances communiquent avec d'autres instances via Internet, vous devez ajouter la règle de liste ACL réseau suivante, à la fois entrante et sortante. Cela garantit que Path MTU Discovery peut fonctionner correctement et empêcher la perte de paquets. Sélectionnez Custom ICMP Rule (Règle ICMP personnalisée) pour le type et Destination Unreachable (Destination inaccessible), fragmentation required, and DF flag set (fragmentation requise et indicateur DF défini) pour la plage de ports (type 3, code 4). Si vous utilisez la détermination d'itinéraire (traceroute), ajoutez également la règle suivante : sélectionnez Custom ICMP Rule (Règle ICMP personnalisée) pour le type, et Time Exceeded (Temps dépassé), TTL expired transit (Transit TTL expiré) pour la plage de ports (type 11, code 0). Pour plus d'informations, consultez la section Unité de transmission maximale (MTU) du réseau pour votre instance EC2 dans le guide de l'utilisateur Amazon EC2.

Utiliser les ACL réseau

Les tâches suivantes vous montrent comment utiliser les ACL réseau à l'aide de la console Amazon VPC.

Tâches

Déterminer les associations de listes ACL réseau

La console Amazon VPC vous permet d'identifier l'ACL réseau associée à un sous-réseau. Les listes ACL réseau peuvent être associées à plusieurs sous-réseaux. Par conséquent, vous pouvez également identifier les sous-réseaux associés à une liste ACL réseau.

Pour identifier la liste ACL réseau associée à un sous-réseau :

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Subnets, puis sélectionnez le sous-réseau.

   La liste ACL réseau associée au sous-réseau est incluse dans l'onglet Network ACL, avec les règles de la liste ACL réseau.

Pour identifier les sous-réseaux associés à une liste ACL réseau :

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Network ACLs. La colonne Associated With indique le nombre de sous-réseaux associés à chaque liste ACL réseau.
3. Sélectionnez une liste ACL réseau.
4. Dans le volet des détails, choisissez Subnet Associations (Associations de sous-réseau) afin d'afficher les sous-réseaux associés à la liste ACL réseau.

Créer une ACL réseau

Vous pouvez créer une liste ACL réseau personnalisée pour votre VPC. Par défaut, une liste ACL réseau que vous créez bloque l'ensemble du trafic entrant et sortant jusqu'à l'ajout de règles. De plus, elle n'est associée à aucun sous-réseau tant que vous n'avez pas explicitement effectué cette opération.

Pour créer une liste ACL réseau

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Network ACLs.
3. Sélectionnez Create Network ACL.
4. Dans la boîte de dialogue Create Network ACL (Créer une liste ACL réseau), vous pouvez, le cas échéant, nommer votre liste ACL réseau et sélectionner l'ID de votre VPC à partir de la liste VPC. Choisissez Yes, Create (Oui, Créer).

Ajouter et supprimer des règles

Lorsque vous ajoutez une règle ou en supprimez une d'une liste ACL, tous les sous-réseaux qui y sont associés sont concernés par la modification. Vous n'avez pas besoin de terminer et de relancer les instances du sous-réseau. Les modifications entrent en vigueur après une courte période.

> **Important**
>
> Soyez très prudent si vous ajoutez et supprimez des règles en même temps. Les règles d'ACL réseau définissent les types de trafic réseau qui peuvent entrer ou quitter vos VPC. Si vous supprimez des règles entrantes ou sortantes, puis ajoutez plus de nouvelles entrées que celles autorisées dans Quotas Amazon VPC, les entrées sélectionnées pour suppression seront supprimées, et les nouvelles entrées ne seront pas ajoutées. Cela peut occasionner des problèmes de connectivité inattendus et empêcher involontairement l'accès à vos VPC et à partir de ceux-ci.

Si vous utilisez l'API Amazon EC2 ou un outil de ligne de commande, vous ne pouvez pas modifier les règles. Vous ne pouvez ajouter et supprimer que des règles. Si vous utilisez la console Amazon VPC, vous pouvez modifier les entrées des règles existantes. La console supprime la règle existante et ajoute une nouvelle règle pour vous. Si vous souhaitez modifier la position d'une règle

dans la liste ACL, vous devez en ajouter une nouvelle avec le numéro de votre choix, puis supprimer la règle d'origine.

Pour ajouter des règles à une liste ACL réseau :

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Network ACLs.
3. Dans le volet des détails, choisissez l'onglet Inbound Rules ou Outbound Rules, en fonction du type de règle que vous souhaitez ajouter, puis choisissez Edit.
4. Dans Rule #, saisissez un numéro de règle (par exemple, 100). Ce numéro ne doit pas être déjà utilisé dans la liste ACL réseau. Nous traitons les règles dans l'ordre, en commençant par le numéro le plus bas.

   Nous vous recommandons de laisser un intervalle entre les numéros de règles (par exemple, 100, 200, 300), plutôt que d'utiliser des numéros séquentiels (comme 101, 102, 103). Cela vous permettra d'ajouter plus facilement une nouvelle règle, sans procéder à une nouvelle numérotation des règles existantes.
5. Sélectionnez une règle dans la liste Type. Par exemple, pour ajouter une règle pour HTTP, choisissez HTTP. Pour ajouter une règle autorisant l'ensemble du trafic TCP, sélectionnez All TCP. Pour certaines de ces options (par exemple, HTTP), nous indiquons le port à votre place. Pour utiliser un protocole non répertorié, choisissez Custom Protocol Rule.
6. (Facultatif) Si vous créez une règle d'un protocole personnalisé, sélectionnez le numéro et le nom du protocole dans la liste Protocol. Pour plus d'informations, consultez la liste des numéros de protocole fournie par l'IANA.
7. (Facultatif) Si le protocole que vous avez sélectionné nécessite un numéro de port, saisissez ce dernier ou la plage de ports (en les séparant par un tiret, par exemple 49152-65535).
8. Dans le champ Source ou Destination (selon qu'il s'agit d'une règle entrante ou sortante), saisissez la plage d'adresses CIDR à laquelle la règle s'applique.
9. Dans la liste Allow/Deny, sélectionnez ALLOW pour autoriser le trafic spécifié ou DENY pour le refuser.
10. (Facultatif) Pour ajouter une autre règle, choisissez Add another rule et répétez les étapes 4 à 9 si nécessaire.
11. Lorsque vous avez terminé, choisissez Save.

Pour supprimer une règle d'une liste ACL réseau :

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Network ACLs, puis sélectionnez la liste ACL réseau.
3. Dans le volet des détails, sélectionnez l'onglet Inbound Rules ou Outbound Rules, puis choisissez Edit. Choisissez Remove pour la règle à supprimer, puis Save.

Associer un sous-réseau à une liste ACL réseau :

Pour appliquer les règles d'une liste ACL réseau à un sous-réseau spécifique, vous devez associer ce dernier à la liste ACL réseau. Vous pouvez associer une liste ACL réseau à plusieurs sous-réseaux. Cependant, un sous-réseau ne peut être associé qu'à une seule liste ACL réseau. Tout sous-réseau qui n'est pas spécifiquement associé à une liste ACL spécifique est associé à la liste ACL réseau par défaut.

Pour associer un sous-réseau à une liste ACL réseau :

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Network ACLs, puis sélectionnez la liste ACL réseau.
3. Dans le volet des détails, sous l'onglet Subnet Associations, choisissez Edit. Cochez la case Associate pour le sous-réseau à associer à la liste ACL réseau, puis sélectionnez Save.

Dissocier une liste ACL réseau d'un sous-réseau

Vous pouvez dissocier une liste ACL réseau personnalisée d'un sous-réseau. Lorsque le sous-réseau a été dissocié de la liste ACL réseau personnalisée, il est alors automatiquement associé à la liste ACL réseau par défaut.

Pour dissocier un sous-réseau d'une liste ACL réseau :

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Network ACLs, puis sélectionnez la liste ACL réseau.
3. Dans le volet des détails, choisissez l'onglet Subnet Associations.
4. Sélectionnez Edit, puis décochez la case Associate correspondant au sous-réseau. Choisissez Enregistrer.

Modifier l'ACL réseau d'un sous-réseau

Vous pouvez modifier la liste ACL réseau associée à un sous-réseau. Par exemple, lorsque vous créez un sous-réseau, il est initialement associé à la liste ACL réseau par défaut. Vous pouvez choisir de l'associer à une liste ACL réseau personnalisée que vous avez créée.

Après avoir modifié la liste ACL réseau d'un sous-réseau, vous n'avez pas à interrompre et relancer les instances du sous-réseau. Les modifications entrent en vigueur après une courte période.

Pour modifier l'association d'une liste ACL réseau à un sous-réseau :

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Subnets, puis sélectionnez le sous-réseau.
3. Sélectionnez l'onglet Network ACL, puis Edit.
4. Dans la liste Change to (Remplacer par), sélectionnez la liste ACL réseau à associer au sous-réseau, puis choisissez Save (Enregistrer).

Supprimer une liste ACL réseau

Vous ne pouvez supprimer une liste ACL réseau que si elle n'est associée à aucun sous-réseau. Vous ne pouvez pas supprimer la liste ACL réseau par défaut.

Pour supprimer une liste ACL réseau :

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Network ACLs.
3. Sélectionnez la liste ACL réseau, puis choisissez Delete.
4. Dans la boîte de dialogue de confirmation, choisissez Yes, Delete (Oui, supprimer).

Présentation des API et des commandes

Vous pouvez exécuter les tâches décrites sur cette page à l'aide de la ligne de commande ou d'un API. Pour plus d'informations sur les interfaces de ligne de commande et la liste des API disponibles, consultez Utilisation d'Amazon VPC.

Créer une liste ACL réseau pour votre VPC

- create-network-acl (AWS CLI)

- New-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Décrire une ou plusieurs de vos listes ACL réseau

- describe-network-acls (AWS CLI)
- Get-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Ajouter une règle à une liste ACL réseau

- create-network-acl-entry (AWS CLI)
- New-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Supprimer une règle d'une liste ACL réseau

- delete-network-acl-entry (AWS CLI)
- Remove-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Remplacer une règle existante dans une liste ACL réseau

- replace-network-acl-entry (AWS CLI)
- Set-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Remplacer une association de liste ACL réseau

- replace-network-acl-association (AWS CLI)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Supprimer une liste ACL réseau

- delete-network-acl (AWS CLI)
- Remove-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Gérez les ACL du réseau à l'aide de Firewall Manager

AWS Firewall Manager simplifie les tâches d'administration et de maintenance de votre réseau ACL sur plusieurs comptes et sous-réseaux. Vous pouvez utiliser Firewall Manager pour surveiller les comptes et les sous-réseaux de votre organisation et pour appliquer automatiquement les configurations ACL réseau que vous avez définies. Firewall Manager est particulièrement utile lorsque vous souhaitez protéger l'ensemble de votre organisation ou si vous ajoutez fréquemment de nouveaux sous-réseaux que vous souhaitez protéger automatiquement à partir d'un compte d'administrateur central.

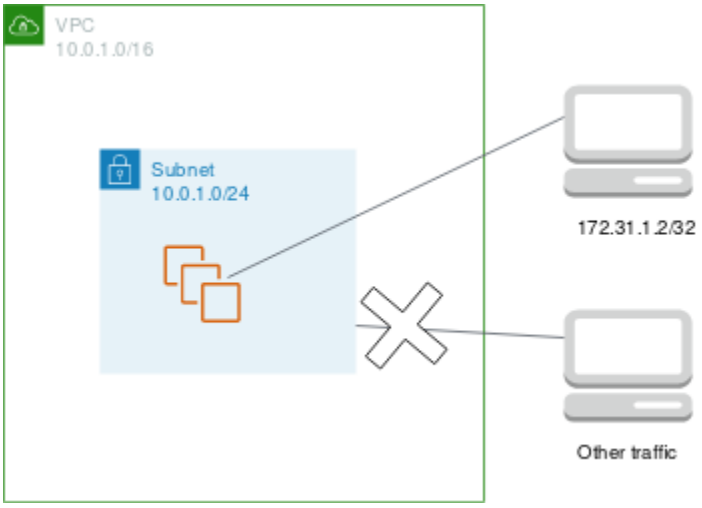
Avec une politique d'ACL réseau Firewall Manager, à l'aide d'un seul compte administrateur, vous pouvez configurer, surveiller et gérer les ensembles de règles minimaux que vous souhaitez définir dans les ACL réseau que vous utilisez au sein de votre organisation. Vous spécifiez les comptes et les sous-réseaux de votre organisation qui sont concernés par la politique de Firewall Manager. Firewall Manager indique l'état de conformité des ACL réseau pour les sous-réseaux concernés, et vous pouvez configurer Firewall Manager pour corriger automatiquement les ACL réseau non conformes, afin de les mettre en conformité.

Pour en savoir plus sur l'utilisation de Firewall Manager pour gérer les ACL de votre réseau, consultez les ressources suivantes dans le guide du AWS Firewall Manager développeur :

- AWS Firewall Manager prérequis
- Commencer à utiliser les AWS Firewall Manager politiques ACL du réseau Amazon VPC
- Politiques relatives à la liste de contrôle d'accès au réseau (ACL) Amazon Virtual Private Cloud

Exemple : contrôler l'accès aux instances dans un sous-réseau

Dans cet exemple, les instances de votre sous-réseau peuvent communiquer entre elles et sont accessibles depuis un ordinateur distant fiable. L'ordinateur distant peut être un ordinateur de votre réseau local ou une instance d'un autre sous-réseau ou VPC. Vous l'utilisez pour vous connecter à vos instances afin d'effectuer des tâches administratives. Vos règles de groupe de sécurité et de liste ACL réseau autorisent l'accès à partir de l'adresse IP de votre ordinateur distant (172.31.1.2/32). Le reste du trafic provenant d'Internet ou d'autres réseaux est refusé. Ce scénario vous offre la possibilité de modifier les groupes de sécurité ou les règles de groupe de sécurité pour vos instances, et de définir la liste ACL réseau comme la couche de défense des sauvegardes.



Voici un exemple de groupe de sécurité à associer aux instances. Les groupes de sécurité sont avec état. Par conséquent, vous n'avez pas besoin d'une règle qui autorise les réponses pour le trafic entrant.

Entrant

Type de protocole	Protocole	Plage de ports	Source	Commentaires
Tout le trafic	Tous	Tous les comptes	sg-123456 7890abcdef0	Toutes les instances associées à ce groupe de sécurité peuvent communiquer entre elles.
SSH	TCP	22	172.31.1.2/32	Autorise l'accès SSH entrant depuis l'ordinat eur distant.

Sortant

Type de protocole	Protocole	Plage de ports	Destination	Commentaires
Tout le trafic	Tous	Tous les comptes	sg-1234567890abcdef0	Toutes les instances associées à ce groupe de sécurité peuvent communiquer entre elles.

Voici un exemple d'ACL réseau à associer aux sous-réseaux pour les instances. Les règles ACL réseau s'appliquent à toutes les instances du sous-réseau. Les listes ACL réseau sont sans état. Par conséquent, vous avez besoin d'une règle qui autorise les réponses pour le trafic entrant.

Entrant

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser	Commentaires
100	SSH	TCP	22	172.31.1.2/32	AUTORISER	Autorise le trafic entrant depuis l'ordinateur distant.
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REFUSER	Refuse tout autre trafic entrant.

Sortant

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/ Refuser	Commentaires
100	TCP personnalisé	TCP	1024-65535	172.31.1.2/32	AUTORISER	Autorise les réponses sortantes vers l'ordinateur distant.
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REFUSER	Refuse tout autre trafic sortant.

Si vous rendez accidentellement vos règles de groupe de sécurité trop permissives, l'ACL réseau de cet exemple continue d'autoriser l'accès uniquement à partir de l'adresse IP spécifiée. Par exemple, le groupe de sécurité suivant contient une règle qui autorise l'accès SSH entrant à partir de n'importe quelle adresse IP. Toutefois, si vous associez ce groupe de sécurité à une instance d'un sous-réseau qui utilise l'ACL réseau, seules les autres instances du sous-réseau et de votre ordinateur distant peuvent accéder à l'instance, car les règles ACL réseau refusent tout autre trafic entrant vers le sous-réseau.

Entrant

Type	Protocole	Plage de ports	Source	Commentaires
Tout le trafic	Tous	Tous les comptes	sg-1234567890abcdef0	Toutes les instances associées à ce groupe de sécurité peuvent communiquer entre elles.

Type	Protocole	Plage de ports	Source	Commentaires
SSH	TCP	22	0.0.0.0/0	Autorise l'accès SSH depuis n'importe quelle adresse IP.

Sortant

Type	Protocole	Plage de ports	Destination	Commentaires
Tout le trafic	Tous	Tous	0.0.0.0/0	Autorise tout le trafic sortant.

Résoudre les problèmes d'accessibilité

Reachability Analyzer est un outil d'analyse de configuration statique. Utilisez Reachability Analyzer pour analyser et déboguer l'accessibilité réseau entre deux ressources de votre VPC. Reachability Analyzer hop-by-hop fournit des détails sur le chemin virtuel entre ces ressources lorsqu'elles sont accessibles, et identifie le composant bloquant dans le cas contraire. Par exemple, il peut identifier les règles ACL du réseau manquantes ou mal configurées.

Pour plus d'informations, reportez-vous au Guide de l'Analyseur d'accessibilité.

Résilience dans Amazon Virtual Private Cloud

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées à l'aide d'un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Vous pouvez configurer vos VPC pour répondre aux exigences de résilience de vos charges de travail. Pour plus d'informations, consultez les ressources suivantes :

- Comprendre les modèles de résilience et les compromis (blog d'AWS architecture)
- Planifiez la topologie de votre réseau (AWS Well-Architected Framework)
- Options de connectivité Amazon Virtual Private Cloud (AWS livres blancs)

Validation de conformité pour cloud privé virtuel d'Amazon

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière

de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).

- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Bonnes pratiques de sécurité pour votre VPC

Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

- Lorsque vous ajoutez des sous-réseaux à votre VPC pour héberger votre application, créez-les dans plusieurs zones de disponibilité. Une zone de disponibilité est un ou plusieurs centres de données distincts dotés d'une alimentation, d'un réseau et d'une connectivité redondants dans une AWS région. L'utilisation de plusieurs zones de disponibilité rend vos applications de production hautement disponibles, tolérantes aux pannes et évolutives. Pour en savoir plus, consultez Amazon VPC sur AWS.

- Utilisez des groupes de sécurité pour contrôler le trafic vers les instances EC2 dans vos sous-réseaux. Pour plus d'informations, consultez Groupes de sécurité.
- Utilisez les ACL réseau pour contrôler le trafic entrant et sortant au niveau du sous-réseau. Pour plus d'informations, consultez Contrôle du trafic vers les sous-réseaux avec des listes ACL réseau.
- Gérez l'accès aux AWS ressources de votre VPC à l'aide de la fédération d'identité AWS Identity and Access Management (IAM), des utilisateurs et des rôles. Pour plus d'informations, consultez Identity and Access Management pour Amazon VPC.
- Utilisez les journaux de flux de VPC pour surveiller le trafic IP entrant et sortant du VPC, du sous-réseau, ou de l'interface réseau. Pour plus d'informations, consultez Journaux de flux VPC.
- L'analyseur d'accès réseau identifie les accès réseau non intentionnels à vos ressources sur nos VPC. Pour plus d'informations, consultez le Guide de l'utilisateur de l'analyseur d'accès réseau.
- AWS Network Firewall Utilisez-le pour surveiller et protéger votre VPC en filtrant le trafic entrant et sortant. Pour plus d'informations, consultez le Guide de l'utilisateur AWS Network Firewall.
- Utilisez Amazon GuardDuty pour détecter les menaces potentielles qui pèsent sur vos comptes, vos conteneurs, vos charges de travail et vos données au sein de votre AWS environnement. La détection des menaces de base inclut la surveillance des journaux de flux VPC associés à vos instances Amazon EC2. Pour plus d'informations, consultez la section VPC Flow Logs dans le guide de GuardDuty l'utilisateur Amazon.

Pour obtenir des réponses aux questions fréquentes liées à la sécurité du VPC, consultez Sécurité et filtrage dans les Questions fréquentes (FAQ) d'Amazon VPC.

Utilisez Amazon VPC avec d'autres Services AWS

Vous pouvez utiliser Amazon VPC avec d'autres solutions Services AWS pour créer des solutions qui répondent à vos besoins.

Table des matières

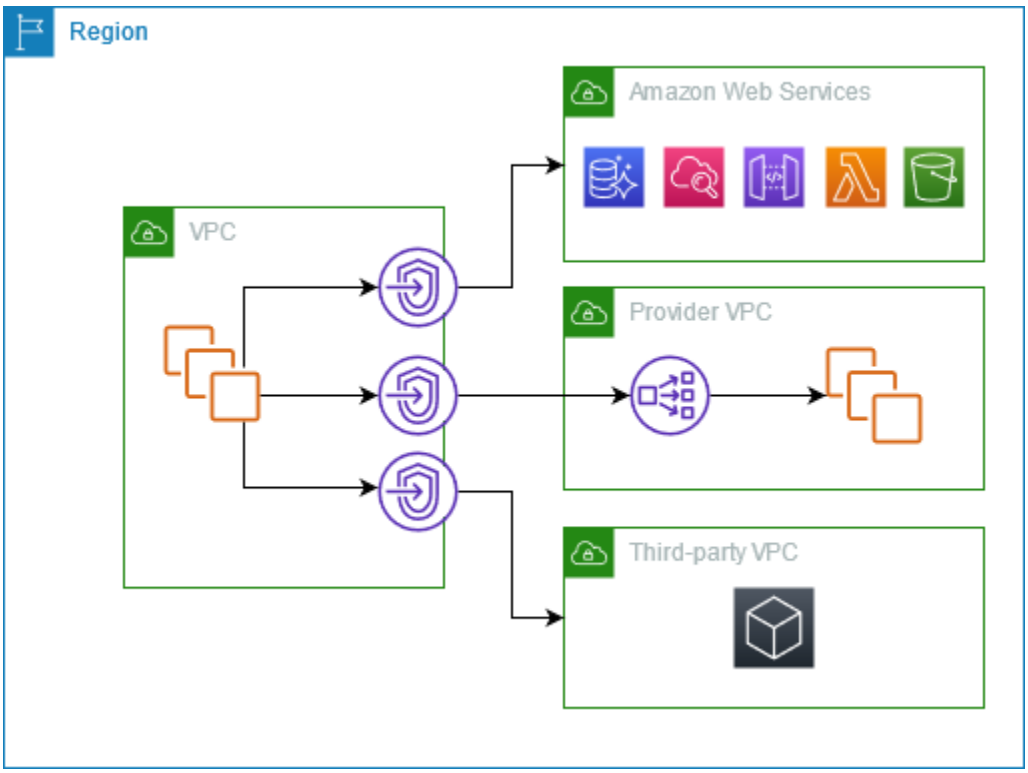
Connexion de votre VPC à des services avec AWS PrivateLink

AWS PrivateLink établit la connectivité privée entre les VPC et les Services AWS pris en charge, les services hébergés par d'autres Comptes AWS et les services AWS Marketplace pris en charge. Pour communiquer avec le service, vous n'avez pas besoin de passerelle Internet, de périphérique NAT, d'adresse IP publique, AWS Direct Connect de connexion AWS Site-to-Site VPN ou de connexion.

Pour utiliser AWS PrivateLink, créez un point de terminaison de votre VPC, en spécifiant le nom du service et un sous-réseau. Une interface réseau Elastic est ainsi créée dans le sous-réseau qui sert de point d'entrée au trafic destiné au service.

Vous pouvez créer votre propre service de point de terminaison de VPC, optimisé par la technologie AWS PrivateLink, et permettre à d'autres clients AWS d'accéder à votre service.

Le diagramme suivant illustre les cas d'utilisation courants pour AWS PrivateLink. Le VPC de gauche possède plusieurs instances EC2 dans un sous-réseau privé et trois points de terminaison VPC d'interface. Le point de terminaison du VPC du haut se connecte à un Service AWS. Le point de terminaison d'un VPC du milieu se connecte à un service hébergé par un autre Compte AWS (service de point de terminaison d'un VPC). Le point de terminaison d'un VPC du bas se connecte à un service partenaire AWS Marketplace.



Pour de plus amples informations, veuillez consulter AWS PrivateLink.

Filtrage du trafic réseau avec AWS Network Firewall

Vous pouvez filtrer le trafic réseau au niveau du périmètre de votre VPC à l'aide de AWS Network Firewall. Network Firewall est un pare-feu réseau dynamique, géré et un service de détection et de prévention des intrusions. Pour plus d'informations, consultez le Guide du développeur AWS Network Firewall.

Configurez Network Firewall avec les ressources AWS suivantes.

Ressource Network Firewall	Description
Pare-feu	Un pare-feu connecte le comportement de filtrage du trafic réseau d'une politique de pare-feu au VPC que vous souhaitez protéger. La configuration du pare-feu inclut des spécifications pour les zones de disponibilité et les sous-réseaux où les points de terminaison du pare-feu sont placés. Elle définit également des paramètres généraux, notamment

Ressource Network Firewall	Description
	la configuration de la journalisation du pare-feu et le balisage sur la ressource de pare-feu AWS. Pour plus d'informations, consultez Pare-feux dans AWS Network Firewall.
Stratégie de pare-feu	Une stratégie de pare-feu définit le comportement de surveillance et de protection d'un pare-feu. Les détails du comportement sont définis dans les groupes de règles que vous ajoutez à votre politique et dans certains paramètres de politique par défaut. Pour utiliser une politique de pare-feu, associez-la à un ou plusieurs pare-feux. Pour de plus amples informations, veuillez consulter Politiques de pare-feu dans AWS Network Firewall.
Groupe de règles	Un groupe de règles est un ensemble réutilisable de critères pour l'inspection et la gestion du trafic réseau. Ajoutez un ou plusieurs groupes de règles à une stratégie de pare-feu dans le cadre de votre configuration de stratégie. Vous pouvez définir des groupes de règles sans état afin d'inspecter chaque paquet réseau de manière isolée. Les groupes de règles sans état présentent un comportement et une utilisation similaires aux listes de contrôle d'accès réseau (ACL) d'Amazon VPC. Vous pouvez également définir des groupes de règles dynamiques pour inspecter des paquets dans le contexte de leur flux de trafic. Les groupes de règles dynamiques sont similaires en termes de comportement et d'utilisation à ceux des groupes de sécurité Amazon VPC. Pour de plus amples informations, veuillez consulter Groupes de règles dans AWS Network Firewall.

Vous pouvez également utiliser AWS Firewall Manager pour configurer et gérer de manière centralisée les ressources Network Firewall sur vos comptes et applications dans AWS Organizations. Vous pouvez gérer des pare-feux pour plusieurs comptes à l'aide d'un seul compte dans Firewall Manager. Pour plus d'informations, consultez AWS Firewall Manager dans AWS WAF, AWS Firewall Manager et le AWS Shield AdvancedGuide du développeur.

Filtrage du trafic DNS utilisant Route 53 Resolver DNS pare-feu

Avec le pare-feu DNS, vous définissez des règles de filtrage des noms de domaine dans les groupes de règles que vous associez à vos VPC. Vous pouvez spécifier des listes de noms de domaine à autoriser ou à bloquer, et personnaliser les réponses pour les requêtes DNS que vous bloquez. Pour plus d'informations, consultez la documentation de Route 53 Resolver DNS Firewall.

Vous implémentez le pare-feu DNS avec les ressources AWS suivantes.

Ressource de pare-feu DNS	Description
Créer un groupe de règles de pare-feu DNS	Un groupe de règles de pare-feu DNS est un ensemble nommé et réutilisable de règles de pare-feu DNS pour filtrer les requêtes DNS. Vous remplissez le groupe de règles avec les règles de filtrage, puis associez le groupe à un ou plusieurs VPC d'Amazon VPC. Lorsque vous associez un groupe de règles à un VPC, vous activez le filtrage du pare-feu DNS pour le VPC. Ensuite, lorsque le résolveur reçoit une requête DNS pour un VPC auquel un groupe de règles est associé, le résolveur transmet la requête au pare-feu DNS pour filtrage. Chaque règle du groupe de règles spécifie une liste de domaines et une action à effectuer sur les requêtes DNS dont les domaines correspon dent aux spécifications de domaine de la liste. Vous pouvez autoriser , bloquer ou alerter en cas de requêtes correspondantes. Vous pouvez également définir des réponses personnalisées pour les requêtes bloquées. Pour plus d'informations, consultez Groupes de règles et règles dans Route 53 Resolver DNS Firewall.
Domain list (Liste des domaines)	Une liste de domaines est un ensemble réutilisable de spécifications de domaine que vous utilisez dans une règle de pare-feu DNS, à l'intérieur d'un groupe de règles. Pour plus d'informations, consultez la Listes de domaines dans Route 53 Resolver DNS Firewall.

Vous pouvez également utiliser AWS Firewall Manager pour configurer et gérer de manière centralisée les ressources de pare-feu DNS sur vos comptes et organisations dans AWS Organizations. Vous pouvez gérer des pare-feux pour plusieurs comptes à l'aide d'un seul compte dans Firewall Manager. Pour plus d'informations, consultez AWS Firewall Manager dans AWS WAF, AWS Firewall Manager et le AWS Shield AdvancedGuide du développeur.

Résoudre les problèmes d'accessibilité à l'aide de Reachability Analyzer

Reachability Analyzer est un outil d'analyse de configuration statique. Utilisez Reachability Analyzer pour analyser et déboguer l'accessibilité réseau entre deux ressources de votre VPC. Reachability Analyzer hop-by-hop fournit des détails sur le chemin virtuel entre ces ressources lorsqu'elles sont accessibles, et identifie le composant bloquant dans le cas contraire.

Vous pouvez utiliser Reachability Analyzer pour analyser l'accessibilité entre les ressources suivantes :

- instances
- Passerelles Internet
- Interfaces réseau
- Passerelles de transit
- Attachements de passerelle de transit
- Services de points de terminaison d'un VPC
- Points de terminaison d'un VPC
- Connexions d'appairage de VPC
- Passerelles VPN

Pour plus d'informations, reportez-vous au Guide de l'Analyseur d'accessibilité.

Exemples de VPC

Voici des exemples de configuration pour vos clouds privés virtuels (VPC).

Exemples

- Exemple : VPC pour un environnement de test
- Exemple : VPC pour serveurs web et de base de données
- Exemple : VPC avec des serveurs dans des sous-réseaux privés et NAT

Exemples associés

- Pour connecter vos VPC les uns aux autres, consultez Configurations d'appairage de VPC dans le Guide d'appairage d'Amazon VPC.
- Pour connecter vos VPC à votre propre réseau, consultez Architectures Site-to-Site VPN dans le Guide de l'utilisateur AWS Site-to-Site VPN.
- Pour connecter vos VPC entre eux et à votre propre réseau, consultez les exemples de passerelles de transit dans les Passerelles de transit Amazon VPC.

Ressources supplémentaires

- Comprendre les modèles de résilience et les compromis (Blog d'architecture AWS)
- Planifier la topologie de votre réseau (cadre AWS Well-Architected)
- Amazon Virtual Private Cloud Connectivity Options (livres blancs AWS)

Exemple : VPC pour un environnement de test

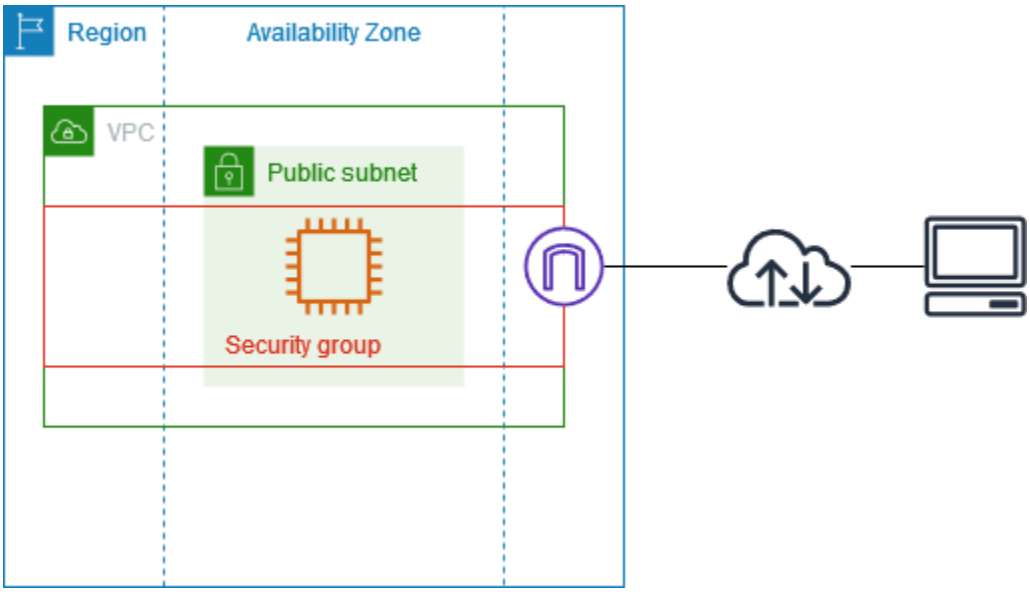
Cet exemple montre comment créer un VPC que vous pouvez utiliser comme environnement de développement ou de test. Ce VPC n'étant pas destiné à être utilisé en production, il n'est pas nécessaire de déployer vos serveurs dans plusieurs zones de disponibilité. Pour réduire les coûts et la complexité, vous pouvez déployer vos serveurs dans une seule zone de disponibilité.

Table des matières

- Déploiement de votre application
- Tester votre configuration
- Nettoyage

Présentation

Le schéma suivant fournit un aperçu des ressources incluses dans l'exemple. Le VPC possède un sous-réseau public dans une seule zone de disponibilité et une passerelle Internet. Le serveur est une instance EC2 qui s'exécute dans le sous-réseau public. Le groupe de sécurité de l'instance autorise le trafic SSH depuis votre propre ordinateur, ainsi que tout autre trafic spécifiquement requis pour vos activités de développement ou de test.



Routage

Lorsque vous créez ce VPC en utilisant la console Amazon VPC, nous créons une table de routage pour le sous-réseau public avec des routes locales et des routes vers la passerelle Internet. Voici un exemple de table de routage avec des routes pour IPv4 et IPv6. Si vous créez un sous-réseau IPv4 uniquement au lieu d'un sous-réseau double pile, votre table de routage inclut uniquement les routes IPv4.

Destination	Cible
10.0.0.0/16	locale

Destination	Cible
2001:db8:1234:1a00::/56	locale
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Sécurité

Pour cet exemple de configuration, vous devez créer un groupe de sécurité pour votre instance, qui autorise le trafic dont votre application a besoin. Par exemple, vous pourriez avoir besoin d'ajouter une règle qui autorise le trafic SSH depuis votre ordinateur ou le trafic HTTP depuis votre réseau.

Vous trouverez ci-dessous des exemples de règles entrantes pour un groupe de sécurité, avec des règles pour IPv4 et IPv6. Si vous créez des sous-réseaux IPv4 uniquement au lieu de sous-réseaux double pile, vous n'avez besoin que des règles pour IPv4.

Entrant

Source	Protocole	Plage de ports	Description
0.0.0.0/0	TCP	80	Autorise l'accès HTTP entrant depuis l'ensemble des adresses IPv4
::/0	TCP	80	Autorise l'accès HTTP entrant depuis l'ensemble des adresses IPv6
0.0.0.0/0	TCP	443	Autorise l'accès HTTPS entrant depuis l'ensemble des adresses IPv4
::/0	TCP	443	Autorise l'accès HTTPS entrant depuis l'ensemble des adresses IPv6

Source	Protocole	Plage de ports	Description
Plage d'adresses IPv4 publiques de votre réseau	TCP	22	(Facultatif) Autorise l'accès SSH entrant à partir des adresses IP IPv4 de votre réseau
Plage d'adresses IPv6 de votre réseau	TCP	22	(Facultatif) Autorise l'accès SSH entrant à partir des adresses IP IPv6 de votre réseau
Plage d'adresses IPv4 publiques de votre réseau	TCP	3389	(Facultatif) Autorise l'accès RDP entrant à partir des adresses IP IPv4 de votre réseau
Plage d'adresses IPv6 de votre réseau	TCP	3389	(Facultatif) Autorise l'accès RDP entrant à partir des adresses IP IPv6 de votre réseau

Créer le VPC

Utilisez la procédure suivante pour créer un VPC avec un sous-réseau public dans une seule zone de disponibilité. Cette configuration est adaptée à un environnement de développement ou de test.

Pour créer le VPC

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Sur le tableau de bord, choisissez Créer un VPC.
3. Sous Ressources à créer, choisissez VPC et plus encore.
4. Configurer le VPC

    a. Pour Name tag auto-generation (Génération automatique de balises de nom), saisissez un nom pour le VPC.

    b. Pour Bloc d'adresse CIDR IPv4, vous pouvez conserver la suggestion par défaut ou saisir le bloc d'adresse CIDR requis par votre application ou votre réseau. Pour de plus amples informations, veuillez consulter the section called “Blocs CIDR VPC”.

    c. (Facultatif) Si votre application communique à l'aide d'adresses IPv6, choisissez Bloc d'adresse CIDR IPv6, Bloc d'adresse CIDR IPv6 fourni par Amazon.

5. Configurer les sous-réseaux

    a. Pour Nombre de zones de disponibilité (AZ), choisissez 1. Vous pouvez conserver la zone de disponibilité par défaut ou développer Personnalisez les zones de disponibilité et sélectionner une zone de disponibilité.

    b. Pour Number of public subnets (Nombre de sous-réseaux publics), choisissez 1.

    c. Pour Number of private subnets (Nombre de sous-réseaux privés), choisissez 0.

    d. Vous pouvez conserver le bloc d'adresse CIDR par défaut pour le sous-réseau public ou développer Personnaliser les blocs d'adresse CIDR du sous-réseau et saisir un bloc d'adresse CIDR. Pour de plus amples informations, veuillez consulter the section called "Blocs d'adresse CIDR de sous-réseau".

6. Pour Passerelles NAT, conservez la valeur par défaut, Aucune.

7. Pour VPC endpoints (Points de terminaison d'un VPC), choisissez None (Aucun). Un point de terminaison d'un VPC de passerelle pour S3 est utilisé uniquement pour accéder à Amazon S3 à partir de sous-réseaux privés.

8. Pour Options DNS, conservez les deux options sélectionnées. Votre instance recevra un nom d'hôte DNS public qui correspond à ses adresses IP publiques.

9. Sélectionnez Create VPC (Créer un VPC).

Déploiement de votre application

Il existe plusieurs façons de déployer des instances EC2. Par exemple :

- Assistant de lancement d'instance Amazon EC2
- Amazon EC2 Auto Scaling
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Après avoir déployé une instance EC2, vous pouvez vous connecter à l'instance, installer le logiciel dont vous avez besoin pour votre application, puis créer une image pour une utilisation future. Pour plus d'informations, découvrez comment créer une AMI Linux ou une AMI Windows dans la documentation Amazon EC2. Vous pouvez également utiliser EC2 Image Builder pour créer et gérer votre Amazon Machine Image (AMI).

Tester votre configuration

Après avoir terminé le déploiement de votre application, vous pouvez la tester. Si vous ne parvenez pas à vous connecter à votre instance EC2, ou si votre application ne parvient pas à envoyer ou à recevoir le trafic que vous attendez, vous pouvez utiliser Reachability Analyzer pour résoudre les problèmes. Par exemple, Reachability Analyzer peut identifier les problèmes de configuration liés à vos tables de routage ou à vos groupes de sécurité. Pour plus d'informations, reportez-vous au Guide de l'Analyseur d'accessibilité.

Nettoyage

Lorsque vous avez terminé avec cette configuration, vous pouvez le supprimer. Avant de supprimer le VPC, vous devez résilier votre instance. Pour de plus amples informations, veuillez consulter the section called “Supprimer votre VPC”.

Exemple : VPC pour serveurs web et de base de données

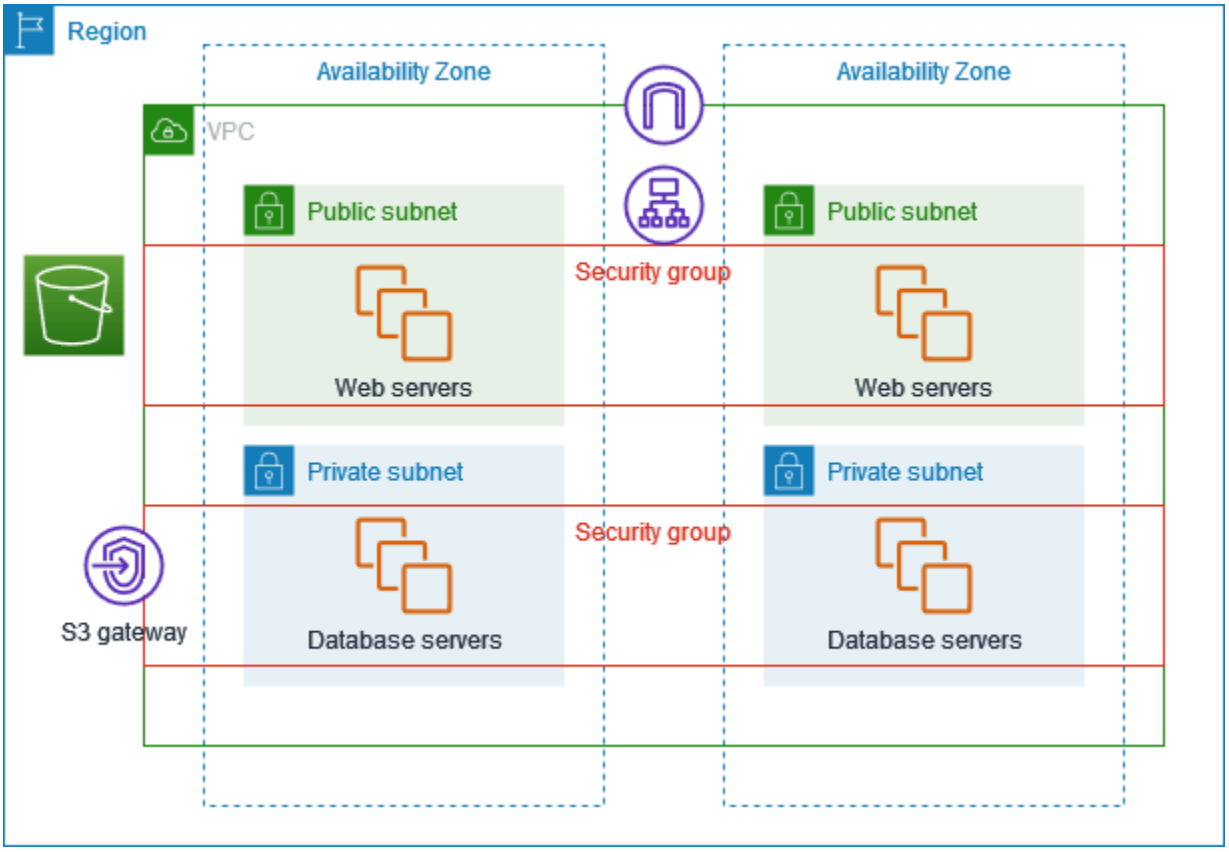
Cet exemple montre comment créer un VPC que vous pouvez utiliser pour une architecture à deux niveaux dans un environnement de production. Pour améliorer la résilience, vous déployez les serveurs dans deux zones de disponibilité.

Table des matières

Présentation

Le schéma suivant fournit un aperçu des ressources incluses dans l'exemple. Le VPC contient des sous-réseaux privés et des sous-réseaux publics dans deux zones de disponibilité. Les serveurs web s'exécutent dans les sous-réseaux publics et reçoivent le trafic des clients via un équilibreur de charge. Le groupe de sécurité pour les serveurs web autorise le trafic en provenance de l'équilibreur de charge. Les serveurs de base de données s'exécutent dans les sous-réseaux privés et reçoivent

du trafic en provenance des serveurs web. Le groupe de sécurité pour les serveurs de base de données autorise le trafic en provenance des serveurs web. Les serveurs de base de données peuvent se connecter à Amazon S3 via un point de terminaison d'un VPC de passerelle.



Routage

Lorsque vous créez ce VPC à l'aide de la console Amazon VPC, nous créons une table de routage pour les sous-réseaux publics avec des routes locales et des routes vers la passerelle Internet, ainsi qu'une table de routage pour chaque sous-réseau privé avec des routes locales et une route vers le point de terminaison d'un VPC de la passerelle.

Voici un exemple de table de routage pour les sous-réseaux publics, avec des routes pour IPv4 et IPv6. Si vous créez des sous-réseaux IPv4 uniquement au lieu de sous-réseaux double pile, votre table de routage inclut uniquement les routes IPv4.

Destination	Cible
10,0.0.0/16	locale
2001:db8:1234:1a00::/56	locale

Destination	Cible
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Voici un exemple de table de routage pour les sous-réseaux privés, avec des routes locales pour IPv4 et IPv6. Si vous avez créé des sous-réseaux IPv4 uniquement, votre table de routage inclut uniquement la route IPv4. La dernière route envoie le trafic destiné à Amazon S3 vers le point de terminaison d'un VPC de la passerelle.

Destination	Cible
10,0.0.0/16	locale
2001:db8:1234:1a00::/56	local
s3-prefix-list-id	*s3-gateway-id*

Sécurité

Pour cet exemple de configuration, vous créez un groupe de sécurité pour l'équilibreur de charge, un groupe de sécurité pour les serveurs Web et un groupe de sécurité pour les serveurs de base de données.

Équilibreur de charge

Le groupe de sécurité de votre Application Load Balancer ou Network Load Balancer doit autoriser le trafic entrant provenant des clients sur le port d'écoute de l'équilibreur de charge. Pour accepter du trafic en provenance de n'importe quel endroit sur Internet, spécifiez 0.0.0.0/0 en tant que source. Le groupe de sécurité de l'équilibreur de charge doit également autoriser le trafic sortant de l'équilibreur de charge vers les instances cibles sur le port d'écoute de l'instance et sur le port de surveillance de l'état.

Serveurs Web

Les règles de groupe de sécurité suivantes permettent aux serveurs Web de recevoir le trafic HTTP et HTTPS en provenance de l'équilibreur de charge. Vous pouvez éventuellement autoriser les

serveurs web à recevoir du trafic SSH ou RDP en provenance de votre réseau. Les serveurs Web peuvent envoyer du trafic SQL ou MySQL à vos serveurs de base de données.

Entrant

Source	Protocole	Plage de ports	Description
ID du groupe de sécurité pour l'équilibreur de charge	TCP	80	Autorise l'accès HTTP entrant depuis l'équilibreur de charge
ID du groupe de sécurité pour l'équilibreur de charge	TCP	443	Autorise l'accès HTTPS entrant depuis l'équilibreur de charge
Plage d'adresses IPv4 publiques de votre réseau	TCP	22	(Facultatif) Autorise l'accès SSH entrant à partir des adresses IP IPv4 de votre réseau
Plage d'adresses IPv6 de votre réseau	TCP	22	(Facultatif) Autorise l'accès SSH entrant à partir des adresses IP IPv6 de votre réseau
Plage d'adresses IPv4 publiques de votre réseau	TCP	3389	(Facultatif) Autorise l'accès RDP entrant à partir des adresses IP IPv4 de votre réseau
Plage d'adresses IPv6 de votre réseau	TCP	3389	(Facultatif) Autorise l'accès RDP entrant à partir des adresses IP IPv6 de votre réseau

Sortant

Destination	Protocole	Plage de ports	Description
ID du groupe de sécurité pour les instances exécutant Microsoft SQL Server	TCP	1433	Autorise l'accès Microsoft SQL Server sortant aux serveurs de base de données
ID du groupe de sécurité pour les instances exécutant MySQL	TCP	3306	Autorise l'accès MySQL sortant aux serveurs de base de données

Serveurs de base de données

Les règles de groupe de sécurité suivantes autorisent les serveurs de base de données à recevoir des demandes de lecture et écriture depuis les serveurs web.

Entrant

Source	Protocole	Plage de ports	Commentaires
ID du groupe de sécurité du serveur web	TCP	1433	Autorise l'accès entrant Microsoft SQL Server depuis les serveurs web
ID du groupe de sécurité du serveur web	TCP	3306	Autorise l'accès entrant MySQL Server depuis les serveurs web

Sortant

Destination	Protocole	Plage de ports	Commentaires
0.0.0.0/0	TCP	80	Autorise l'accès HTTP sortant à Internet sur IPv4
0.0.0.0/0	TCP	443	Autorise l'accès HTTPS sortant à Internet sur IPv4

Pour de plus amples informations sur les groupes de sécurité pour les instances DB Amazon RDS, veuillez consulter Contrôle d'accès par groupes de sécurité dans le Guide de l'utilisateur Amazon RDS.

Créer le VPC

Utilisez la procédure suivante pour créer un VPC avec un sous-réseau public et un sous-réseau privé dans deux zones de disponibilité.

Pour créer le VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Sur le tableau de bord, choisissez Créer un VPC.
3. Sous Ressources à créer, choisissez VPC et plus encore.
4. Configurez le VPC :

    a. Maintenez la génération automatique de balises de nom sélectionnée pour créer des balises de nom pour les ressources VPC ou désactivez-la pour fournir vos propres balises de nom pour les ressources VPC.

    b. Pour Bloc d'adresse CIDR IPv4, vous pouvez conserver la suggestion par défaut ou saisir le bloc d'adresse CIDR requis par votre application ou votre réseau. Pour plus d'informations, consultez the section called "Blocs CIDR VPC".

    c. (Facultatif) Si votre application communique à l'aide d'adresses IPv6, choisissez Bloc d'adresse CIDR IPv6, Bloc d'adresse CIDR IPv6 fourni par Amazon.

    d. Choisissez une option de location. Cette option définit si les instances EC2 que vous lancez dans le VPC s'exécuteront sur du matériel partagé avec d'autres Comptes AWS ou sur du matériel dédié à votre seul usage. Si vous choisissez la location du VPC, les instances EC2

`Default` lancées dans ce VPC utiliseront l'attribut de location spécifié lors du lancement de l'instance. Pour plus d'informations, consultez Lancer une instance à l'aide de paramètres définis dans le guide de l'utilisateur Amazon EC2. Si vous choisissez que la location du VPC est `Dedicated`, les instances s'exécutent toujours en tant qu'instances dédiées sur du matériel dédié à votre utilisation.

5. Configurez les sous-réseaux :

   a. Pour Nombre de zones de disponibilité, choisissez 2 afin de pouvoir lancer des instances dans deux zones de disponibilité et améliorer ainsi la résilience.

   b. Pour Number of public subnets (Nombre de sous-réseaux publics), choisissez 2.

   c. Pour Number of private subnets (Nombre de sous-réseaux privés), choisissez 2.

   d. Vous pouvez conserver les blocs d'adresse CIDR par défaut pour les sous-réseaux, ou bien vous pouvez étendre les blocs d'adresse CIDR personnalisés des sous-réseaux et entrer un bloc d'adresse CIDR. Pour plus d'informations, consultez the section called “Blocs d'adresse CIDR de sous-réseau”.

6. Pour Passerelles NAT, conservez la valeur par défaut, Aucune.

7. Pour Points de terminaison des VPC, conservez la valeur par défaut, Passerelle S3. Bien que cela n'ait aucun effet (sauf si vous accédez à un compartiment S3), l'activation de ce point de terminaison d'un VPC n'entraîne aucuns frais.

8. Pour Options DNS, conservez les deux options sélectionnées. Vos serveurs web recevront des noms d'hôtes DNS publics qui correspondent à leurs adresses IP publiques.

9. Sélectionnez Create VPC (Créer un VPC).

Déploiement de votre application

Idéalement, vous avez déjà testé vos serveurs web et de base de données dans un environnement de développement ou de test et créé les scripts ou les images que vous utiliserez pour déployer votre application en production.

Vous pouvez utiliser des instances EC2 pour vos serveurs web. Il existe plusieurs façons de déployer des instances EC2. Par exemple :

- Assistant de lancement d'instance Amazon EC2
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Afin d'améliorer la disponibilité, vous pouvez utiliser Amazon EC2 Auto Scaling pour déployer des serveurs dans plusieurs zones de disponibilité et maintenir la capacité de serveur minimale requise par votre application.

Vous pouvez utiliser Elastic Load Balancing pour répartir le trafic de manière uniforme entre vos serveurs. Vous pouvez attacher un équilibreur de charge à un groupe Auto Scaling.

Vous pouvez utiliser des instances EC2 pour vos serveurs de base de données ou l'un de nos types de bases de données sur mesure. Pour plus d'informations, voir Bases de données sur AWS : Comment choisir.

Tester votre configuration

Après avoir terminé le déploiement de votre application, vous pouvez la tester. Si votre application ne parvient pas à envoyer ou à recevoir le trafic que vous attendez, vous pouvez utiliser Reachability Analyzer pour résoudre les problèmes. Par exemple, Reachability Analyzer peut identifier les problèmes de configuration liés à vos tables de routage ou à vos groupes de sécurité. Pour plus d'informations, reportez-vous au Guide de l'Analyseur d'accessibilité.

Nettoyage

Lorsque vous avez terminé avec cette configuration, vous pouvez le supprimer. Avant de supprimer le VPC, vous devez résilier vos instances et supprimer l'équilibreur de charge. Pour plus d'informations, voir the section called “Supprimer votre VPC”.

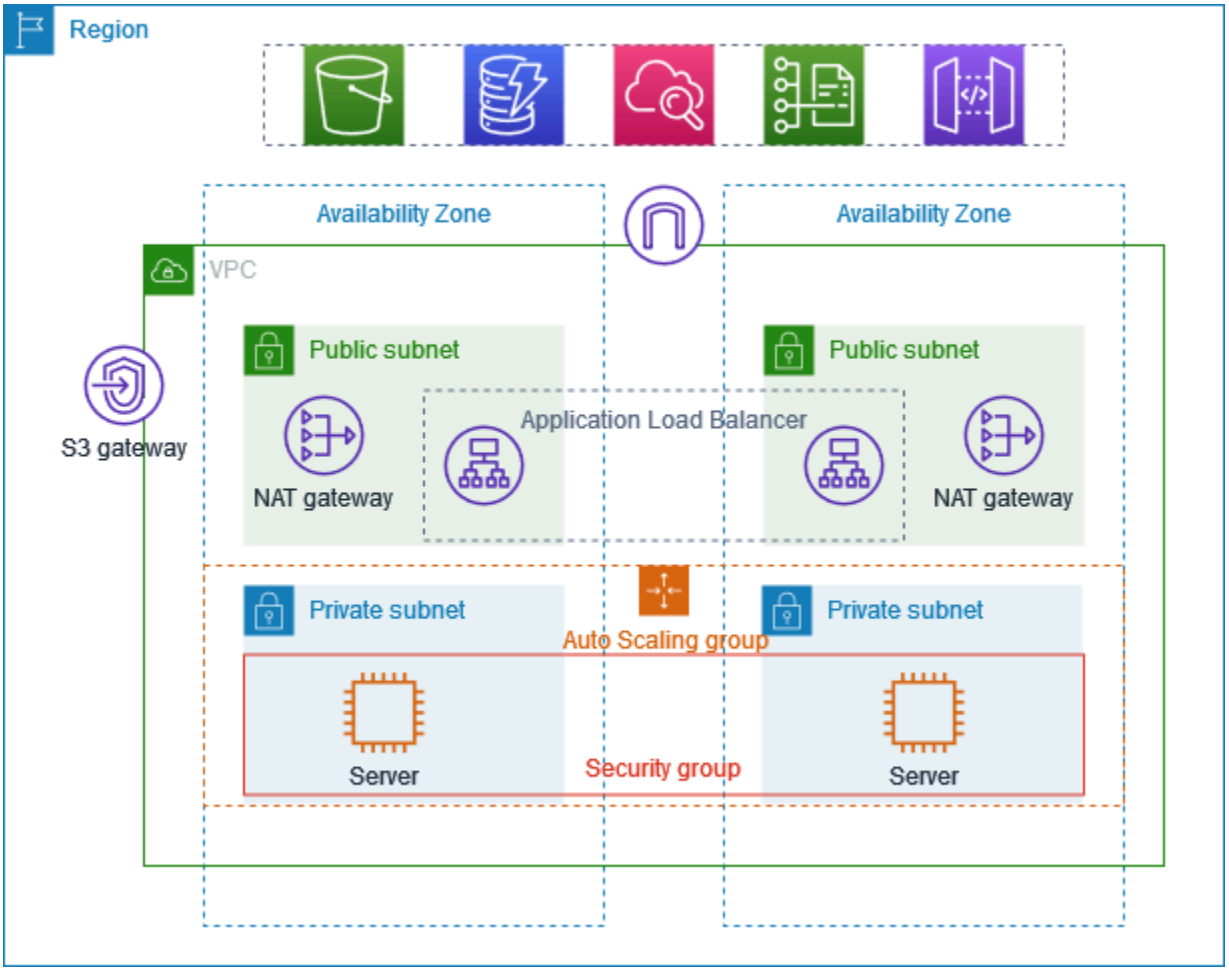
Exemple : VPC avec des serveurs dans des sous-réseaux privés et NAT

Cet exemple montre comment créer un VPC que vous pouvez utiliser pour les serveurs d'un environnement de production. Pour améliorer la résilience, vous déployez les serveurs dans deux zones de disponibilité, à l'aide d'un groupe Auto Scaling et d'un Application Load Balancer. Pour plus de sécurité, vous déployez les serveurs dans des sous-réseaux privés. Les serveurs reçoivent des demandes via l'équilibreur de charge. Les serveurs peuvent se connecter à Internet via une passerelle NAT. Pour améliorer la résilience, vous déployez la passerelle NAT dans les deux zones de disponibilité.

Table des matières

Présentation

Le schéma suivant fournit un aperçu des ressources incluses dans l'exemple. Le VPC contient des sous-réseaux privés et des sous-réseaux publics dans deux zones de disponibilité. Chaque sous-réseau public contient une passerelle NAT et un nœud d'équilibreur de charge. Les serveurs s'exécutent dans les sous-réseaux privés, sont lancés et arrêtés à l'aide d'un groupe Auto Scaling et reçoivent du trafic depuis l'équilibreur de charge. Les serveurs peuvent se connecter à Internet via la passerelle NAT. Les serveurs peuvent se connecter à Amazon S3 via un point de terminaison d'un VPC de passerelle.



Routage

Lorsque vous créez ce VPC à l'aide de la console Amazon VPC, nous créons une table de routage pour les sous-réseaux publics avec des routes locales et des routes vers la passerelle Internet. Nous créons également une table de routage pour les sous-réseaux privés avec des routes locales et des routes vers la passerelle NAT, la passerelle Internet de sortie uniquement et le point de terminaison de VPC de la passerelle.

Voici un exemple de table de routage pour les sous-réseaux publics, avec des routes pour IPv4 et IPv6. Si vous créez des sous-réseaux IPv4 uniquement au lieu de sous-réseaux double pile, votre table de routage inclut uniquement les routes IPv4.

Destination	Cible
10.0.0.0/16	locale
2001:db8:1234:1a00::/56	locale
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Voici un exemple de table de routage pour l'un des sous-réseaux privés, avec des routes pour IPv4 et IPv6. Si vous avez créé des sous-réseaux IPv4 uniquement, la table de routage inclut uniquement les routes IPv4. La dernière route envoie le trafic destiné à Amazon S3 vers le point de terminaison d'un VPC de la passerelle.

Destination	Cible
10.0.0.0/16	locale
2001:db8:1234:1a00::/56	locale
0.0.0.0/0	*nat-gateway-id*
::/0	*eigw-id*
s3-prefix-list-id	*s3-gateway-id*

Sécurité

Voici un exemple des règles que vous pouvez créer pour le groupe de sécurité que vous associez à vos serveurs. Le groupe de sécurité doit autoriser le trafic en provenance de l'équilibreur de charge via le port et le protocole de l'écouteur. Il doit également autoriser le trafic de surveillance de l'état.

Entrant

Source	Protocole	Plage de ports	Commentaires
ID du groupe de sécurité de l'équilibreur de charge	*protocole de l'écouteur*	*port de l'écouteur*	Autorise tout le trafic entrant depuis l'équilibreur de charge sur le port d'écoute
ID du groupe de sécurité de l'équilibreur de charge	*protocole de surveillance de l'état*	*port de surveillance de l'état*	Autorise le trafic de surveillance de l'état entrant depuis l'équilibreur de charge

Créer le VPC

Utilisez la procédure suivante pour créer un VPC avec un sous-réseau public et un sous-réseau privé dans deux zones de disponibilité et une passerelle NAT dans chaque zone de disponibilité.

Pour créer le VPC

1. Ouvrez la console Amazon VPC sur https://console.aws.amazon.com/vpc/.
2. Sur le tableau de bord, choisissez Créer un VPC.
3. Sous Ressources à créer, choisissez VPC et plus encore.
4. Configurer le VPC
    a. Pour Name tag auto-generation (Génération automatique de balises de nom), saisissez un nom pour le VPC.
    b. Pour Bloc d'adresse CIDR IPv4, vous pouvez conserver la suggestion par défaut ou saisir le bloc d'adresse CIDR requis par votre application ou votre réseau.

c. Si votre application communique à l'aide d'adresses IPv6, choisissez Bloc d'adresse CIDR IPv6, Bloc d'adresse CIDR IPv6 fourni par Amazon.

5. Configurer les sous-réseaux

   a. Pour Nombre de zones de disponibilité, choisissez 2 afin de pouvoir lancer des instances dans plusieurs zones de disponibilité et améliorer ainsi la résilience.

   b. Pour Number of public subnets (Nombre de sous-réseaux publics), choisissez 2.

   c. Pour Number of private subnets (Nombre de sous-réseaux privés), choisissez 2.

   d. Vous pouvez conserver le bloc d'adresse CIDR par défaut pour le sous-réseau public ou développer Personnaliser les blocs d'adresse CIDR du sous-réseau et saisir un bloc d'adresse CIDR. Pour de plus amples informations, veuillez consulter the section called "Blocs d'adresse CIDR de sous-réseau".

6. Pour Passerelles NAT, choisissez 1 par zone de disponibilité afin d'améliorer la résilience.

7. Si votre application communique à l'aide d'adresses IPv6, pour Passerelle Internet de sortie uniquement, choisissez Oui.

8. Pour Points de terminaison des VPC, si vos instances doivent accéder à un compartiment S3, conservez l'option par défaut, Passerelle S3. Sinon, les instances de votre sous-réseau privé ne peuvent pas accéder à Amazon S3. Cette option est gratuite. Vous pouvez donc conserver la valeur par défaut si vous souhaitez utiliser un compartiment S3 à l'avenir. Si vous choisissez Aucun, vous pouvez toujours ajouter un point de terminaison de VPC de passerelle ultérieurement.

9. Pour Options DNS, désactivez Activer les noms d'hôte DNS.

10. Sélectionnez Create VPC (Créer un VPC).

Déploiement de votre application

Idéalement, vous avez terminé de tester vos serveurs dans un environnement de développement ou de test et créé les scripts ou les images que vous utiliserez pour déployer votre application en production.

Vous pouvez utiliser Amazon EC2 Auto Scaling pour déployer des serveurs dans plusieurs zones de disponibilité et maintenir la capacité de serveur minimale requise par votre application.

Pour lancer des instances à l'aide d'un groupe Auto Scaling

1. Créez un modèle de lancement pour spécifier les informations de configuration nécessaires au lancement de vos instances EC2 à l'aide d'Amazon EC2 Auto Scaling. Pour plus d'informations, consultez Créer un modèle de lancement pour votre groupe Auto Scaling (langue française non garantie) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.
2. Créez un groupe Auto Scaling, soit un ensemble d'instances EC2 avec une taille minimale, maximale et souhaitée. Pour plus d'informations, consultez Créer un groupe Auto Scaling à l'aide d'un modèle de lancement (langue française non garantie) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.
3. Créez un équilibreur de charge qui répartit le trafic de manière uniforme sur les instances de votre groupe Auto Scaling, puis attachez l'équilibreur de charge à votre groupe Auto Scaling. Pour plus d'informations, consultez le Guide de l'utilisateur Elastic Load Balancing et la section Utiliser Elastic Load Balancing (langue française non garantie) du Guide de l'utilisateur Amazon EC2 Auto Scaling.

Tester votre configuration

Après avoir terminé le déploiement de votre application, vous pouvez la tester. Si votre application ne parvient pas à envoyer ou à recevoir le trafic que vous attendez, vous pouvez utiliser Reachability Analyzer pour résoudre les problèmes. Par exemple, Reachability Analyzer peut identifier les problèmes de configuration liés à vos tables de routage ou à vos groupes de sécurité. Pour plus d'informations, reportez-vous au Guide de l'Analyseur d'accessibilité.

Nettoyage

Lorsque vous avez terminé avec cette configuration, vous pouvez le supprimer. Avant de supprimer le VPC, vous devez supprimer le groupe Auto Scaling, résilier vos instances, supprimer les passerelles NAT et supprimer l'équilibreur de charge. Pour de plus amples informations, veuillez consulter the section called “Supprimer votre VPC”.

Quotas Amazon VPC

Les tableaux suivants répertorient les quotas, anciennement appelés limites, pour les ressources Amazon VPC pour votre AWS compte. Sauf indication contraire, ces quotas s'appliquent par région.

Si vous demandez d'augmenter un quota s'appliquant par ressource, nous l'augmentons pour toutes les ressources de la région.

VPC et sous-réseaux

Nom	Par défaut	Ajustable	Commentaires
VPC par région	5	Oui	L'augmentation de ce quota augmente de la même valeur le quota sur les passerelles Internet par région. Vous pouvez augmenter cette limite afin d'avoir des centaines de VPC par région.
Sous-réseaux par VPC	200	Oui	
Blocs d'adresse CIDR IPv4 par VPC	5	Oui (jusqu'à 50)	Ce bloc d'adresse CIDR principal et tous les blocs d'adresse CIDR secondaires sont pris en compte dans ce quota.
Blocs d'adresse CIDR IPv6 par VPC	5	Oui (jusqu'à 50)	Nombre de CIDR que vous pouvez attribuer à un seul VPC.

DNS

Chaque instance EC2 peut envoyer 1024 paquets par seconde par interface réseau au Route 53 Resolver (spécifiquement l'adresse .2, telle que 10.0.0.2 et 169.254.169.253). Ce quota ne peut pas être augmenté. Le nombre de requêtes DNS par seconde prises en charge par Route 53 Resolver

varie selon le type de requête, la taille de la réponse et le protocole utilisé. Pour plus d'informations sur les recommandations relatives à une architecture DNS évolutive, veuillez consulter le Guide technique DNS hybride AWS avec Active Directory.

Adresses IP Elastic

Nom	Par défaut	Ajustable	Commentaires
Adresses IP Elastic par région	5	Oui	Ce quota s'applique aux Compte AWS VPC individuels et aux VPC partagés.
Adresses IP Elastic par passerelle NAT publique	2	Oui	Vous pouvez demander une augmentation de quota jusqu'à 8.

Passerelles

Nom	Par défaut	Ajustable	Commentaires
Passerelles Internet de sortie uniquement par région	5	Oui	Afin d'augmenter ce quota, augmentez le quota de VPC par région. Vous ne pouvez attacher qu'une seule passerelle Internet de sortie uniquement à un VPC à la fois.
Passerelles Internet par région	5	Oui	Afin d'augmenter ce quota, augmentez le quota de VPC par région. Vous ne pouvez attacher qu'une seule passerelle Internet à un VPC à la fois.
Passerelles NAT par zone de disponibilité	5	Oui	Les passerelles NAT sont prises en compte dans votre quota dans les états `pending`, `active` ou `deleting`.

Nom	Par défaut	Ajustable	Commentaires
Quota d'adresses IP privées par passerelle NAT	8	Non	
Passerelles d'opérateur par VPC	1	Non	

Listes de préfixes gérées par le client

Bien que les quotas par défaut des listes de préfixes gérés par le client soient réglables, vous ne pouvez pas demander une augmentation à l'aide de la console Service Quotas. Vous devez ouvrir un cas visant à augmenter la limite de service à l'aide d' AWS Support Center Console.

Nom	Par défaut	Ajustable	Commentaires
Listes de préfixes par région	100	Oui	
Liste des versions par préfixe	1 000	Oui	Si une liste de préfixes compte 1 000 versions stockées et si vous ajoutez une nouvelle version, la plus ancienne est supprimée pour permettre l'ajout de la nouvelle.
Nombre maximal d'entrées par liste de préfixes	1 000	Oui	Vous pouvez redimensionner une liste de préfixes gérée par le client jusqu'à 1 000. Pour plus d'informations, consultez Redimensionner une liste de préfixes. Lorsque vous faites référence à une liste de préfixes dans une ressource, le nombre maximal d'entrées pour les listes de préfixes est imputé au quota du nombre d'entrées pour la ressource . Par exemple, si vous créez une liste de préfixes avec 20 entrées maximum

Nom	Par défaut	Ajustable	Commentaires
			et que vous faites référence à cette liste de préfixes dans une règle de groupe de sécurité, cela compte pour 20 règles de groupe de sécurité.
Références à une liste de préfixes par type de ressource	5 000	Oui	Ce quota s'applique par type de ressource pouvant référencer une liste de préfixes. Par exemple, vous pouvez avoir 5 000 références à une liste de préfixes dans tous vos groupes de sécurité et 5 000 références à une liste de préfixes dans toutes vos tables de routage de sous-réseau. Si vous partagez une liste de préfixes avec d'autres AWS comptes, les référence s des autres comptes à votre liste de préfixes sont prises en compte dans ce quota.

Listes ACL réseau

Nom	Par défaut	Ajustable	Commentaires
Listes ACL réseau par VPC	200	Oui	Vous pouvez associer une liste ACL réseau à un ou plusieurs sous-réseaux dans un VPC.
Règles par liste ACL réseau	20	Oui	Ce quota détermine à la fois le nombre maximal de règles entrantes et le nombre maximal de règles sortantes. Ce quota peut être augmenté jusqu'à un maximum de 40 règles entrantes et

Nom	Par défaut	Ajustable	Commentaires
			40 règles sortantes (pour un total de 80 règles), mais les performances du réseau peuvent être affectées.

Interfaces réseau

Nom	Par défaut	Ajustable	Commentaires
Interfaces réseau par instance	Varie par type d'instance	Non	Pour plus d'informations, veuillez consulter Interfaces réseau par type d'instance.
Interfaces réseau par région	5 000	Oui	Ce quota s'applique aux Compte AWS VPC individuels et aux VPC partagés. Cette limite est appliquée par zone de disponibilité (AZ). Si, par exemple, les interfaces réseau se trouvent dans trois zones, chaque zone aura une limite de 5 000 et la région aura une limite de 15 000.

Tables de routage

Nom	Par défaut	Ajustable	Commentaires
Tables de routage par VPC	200	Oui	La table de routage principale est prise en compte dans ce quota. Notez que si vous demandez une augmentation de quota pour les tables de routage,

Nom	Par défaut	Ajustable	Commentaires
			vous pouvez également demander une augmentation de quota pour les sous-réseaux. Alors que les tables de routage peuvent être partagées avec plusieurs sous-réseaux, un sous-réseau ne peut être associé qu'à une seule table de routage.
Acheminements par table de routage (acheminements non propagés)	50	Oui	Vous pouvez augmenter ce quota jusqu'à un maximum de 1 000 ; cependant , la performance du réseau risque d'être affectée. Ce quota est appliqué séparément pour les acheminem ents IPv4 et IPv6. Si vous disposez de plus de 125 acheminements, nous vous recommandons de paginer les appels pour décrire vos tables de routes pour optimiser les performances.
Routes propagées par table de routage	100	Non	Si vous avez besoin de préfixes supplémentaires, publiez un acheminem ent par défaut.

Groupes de sécurité

Nom	Par défaut	Ajustable	Commentaires
Groupes de sécurité VPC par région	2 500	Oui	Ce quota s'applique aux Compte AWS VPC individuels et aux VPC partagés.

Nom	Par défaut	Ajustable	Commentaires
			Si vous augmentez ce quota à plus de 5 000 groupes de sécurité dans une région, nous vous recommandons de paginer les appels pour décrire vos groupes de sécurité pour optimiser les performances.
Règles de trafic entrant ou sortant par groupe de sécurité	60	Oui	Ce quota est appliqué séparément pour les règles entrantes et sortantes . Pour un compte avec un quota par défaut de 60 règles, un groupe de sécurité peut avoir 60 règles entrantes et 60 règles sortantes. En outre, ce quota est appliqué séparément pour les règles IPv4 et IPv6. Pour un compte avec un quota par défaut de 60 règles, un groupe de sécurité peut avoir 60 règles entrantes pour le trafic IPv4 et 60 règles entrantes pour le trafic IPv6. Pour plus d'informations, consultez the section called "Taille de groupe de sécurité". Une modification de quota s'applique à la fois aux règles entrantes et sortantes. Ce quota est multiplié par le quota pour les groupes de sécurité par interface réseau ne peut pas être supérieur à 1 000.
Groupes de sécurité par interface réseau	5	Oui (jusqu'à 16)	Ce quota est multiplié par le quota parce que les règles par groupes de sécurité ne peuvent pas être supérieures à 1 000.

Partage de VPC

Tous les quotas de VPC standard s'appliquent à un VPC partagé.

Nom	Par défaut	Ajustable	Commentaires
Comptes participants par VPC	100	Oui	Il s'agit du nombre maximal de comptes participants distincts avec lesquels les sous-réseaux d'un VPC peuvent être partagés. Il s'agit d'un quota par VPC s'appliquant à tous les sous-réseaux partagés dans un VPC. Les propriétaires de VPC peuvent afficher les interfaces réseau et les groupes de sécurité attachés aux ressources des participants.
Sous-réseaux qui peuvent être partagés avec un compte	100	Oui	Il s'agit du nombre maximum de sous-réseaux pouvant être partagés avec un AWS compte.

Utilisation des adresses réseau

L'utilisation des adresses réseau (Network Address Usage, NAU) comprend les adresses IP, les interfaces réseau et les CIDR dans des listes de préfixes gérées. La NAU est une métrique appliquée aux ressources d'un VPC pour vous aider à planifier et à surveiller la taille de votre VPC. Pour plus d'informations, consultez Utilisation des adresses réseau.

Les ressources qui constituent le décompte NAU ont leurs propres quotas de service. Même si un VPC dispose d'une capacité NAU disponible, vous ne pourrez pas lancer de ressources dans le VPC si les ressources ont dépassé leurs quotas de service.

Nom	Par défaut	Ajustable	Commentaires
Utilisation des adresses réseau	64 000	Oui (jusqu'à 256 000)	Nombre maximal d'unités NAU par VPC.
Utilisation des adresses réseau appairées	128 000	Oui (jusqu'à 512 000)	Nombre maximal d'unités NAU pour un VPC et tous ses VPC appairés au sein d'une région. Les VPC qui sont appairés dans différentes régions ne contribuent pas à ce nombre.

Limitation de l'API Amazon EC2

Pour de plus amples informations sur la limitation Amazon EC2, veuillez consulter Limitation de demande d'API dans la Référence d'API Amazon EC2.

Ressources de quotas supplémentaires

Pour en savoir plus, consultez les ressources suivantes :

- AWS Client VPN quotas dans le guide de AWS Client VPN l'administrateur
- Quotas AWS Direct Connect dans le Guide de l'utilisateur AWS Direct Connect
- Quotas d'appairage dans le Guide d'appairage Amazon VPC
- PrivateLink quotas dans le AWS PrivateLink Guide
- Quotas Site-to-Site VPN dans le Guide de l'utilisateur AWS Site-to-Site VPN
- Quotas de mise en miroir du trafic dans le Guide de mise en miroir du trafic Amazon VPC
- Quotas de passerelle de transit dans le Guide des passerelles de transit Amazon VPC

Historique du document

Le tableau ci-après décrit les modifications importantes dans chaque édition du Guide de l'utilisateur Amazon VPC.

Modification	Description	Date
Durée de location préférée pour IPv6	Vous pouvez désormais choisir la fréquence à laquelle une instance en cours d'exécution à laquelle un code IPv6 est attribué doit être renouvelée par DHCPv6.	20 février 2024
AWS mise à jour des politiques gérée	Amazon VPC a mis à jour les politiques AmazonVPCFullAccess et les AmazonVPCReadOnlyAccess a gérées.	8 février 2024
AWS mise à jour des politiques gérée	Amazon VPC a mis à jour la politique AmazonVPCCrossAccountNetworkInterfaceOperations gérée.	25 septembre 2023
EC2-Classic est obsolète	Avec EC2-Classic, les instances EC2 s’exécutent dans un réseau plat unique partagé avec d’autres clients. Amazon VPC remplace EC2-Classic. Avec Amazon VPC, vos instances s'exécutent dans un cloud privé virtuel (VPC) qui est logiquement isolé sur votre Compte AWS.	31 juillet 2023

Ajout d'adresses IPv4 secondaires aux passerelles NAT	Vous pouvez ajouter des adresses IPv4 privées secondaires aux passerelles NAT publiques et privées. Les adresses IPv4 secondaires augmentent le nombre de ports disponibles et, par conséquent, la limite du nombre de connexions simultanées que vos charges de travail peuvent établir à l'aide d'une passerelle NAT.	31 janvier 2023
Alignement sur les bonnes pratiques IAM	Guide mis à jour pour s'aligner sur les bonnes pratiques IAM. Pour de plus amples informations, veuillez consulter Bonnes pratiques de sécurité dans IAM.	4 janvier 2023
Choisissez l'adresse IP privée de votre passerelle NAT	Lorsque vous créez une passerelle NAT, vous pouvez désormais choisir l'adresse IP privée qui est attribuée à la passerelle NAT. Auparavant, l'adresse IP privée était automatiquement attribuée à partir de la plage d'adresses IP du sous-réseau.	17 novembre 2022
Configuration du routeur de passerelle IPv6 par défaut	Trois adresses IPv6 sont désormais réservées à l'utilisation par le routeur VPC par défaut.	11 novembre 2022

Transfert d'adresses IP Elastic	Vous pouvez désormais transférer des adresses IP Elastic d'un AWS compte à un autre.	31 octobre 2022
Métriques d'utilisation des adresses réseau	Vous pouvez activer les métriques d'utilisation des adresses réseau pour votre VPC afin de planifier et de surveiller plus aisément la taille de votre VPC.	4 octobre 2022
Publier des journaux de flux sur Amazon Data Firehose	Vous pouvez spécifier un flux de diffusion Amazon Data Firehose comme destination pour les données du journal de flux.	8 septembre 2022
Bande passante des passerelles NAT	Les passerelles NAT prennent désormais en charge une bande passante allant jusqu'à 100 Gbit/s (une augmentation par rapport à 45 Gbit/s) et peuvent traiter jusqu'à dix millions de paquets par seconde (une augmentation par rapport à quatre millions de paquets).	15 juin 2022
Blocs d'adresse CIDR IPv6 multiples	Vous pouvez associer jusqu'à cinq blocs d'adresse CIDR IPv6 à un VPC.	12 mai 2022
Réorganisation	Réorganisation générale de ce Guide de l'utilisateur Amazon Virtual Private Cloud.	2 janvier 2022

Passerelle NAT IPv6 vers IPv4	La passerelle NAT prend en charge la traduction d'adresses réseau de IPv6 vers IPv4, communément appelée NAT64.	24 novembre 2021
Sous-réseaux IPv6 uniquement dans les VPC	Vous pouvez créer des sous-réseaux IPv6 uniquement dans lesquels vous pouvez lancer des instances EC2 IPv6 uniquement.	23 novembre 2021
Options de diffusion des journaux de flux VPC vers Amazon S3	Vous pouvez spécifier le format de fichier journal Apache Parquet, les partitions horaires et les préfixes S3 compatibles Hive.	13 octobre 2021
Amazon EC2 Global View	Amazon EC2 Global View vous permet de visualiser les VPC, les sous-réseaux, les instances, les groupes de sécurité et les volumes dans plusieurs AWS régions sur une seule console.	1er septembre 2021

Acheminements plus spécifiques	Vous pouvez ajouter à vos tables de routage un acheminement plus spécifique que l'acheminement local. Vous pouvez utiliser des acheminements plus spécifiques pour rediriger le trafic entre les sous-réseaux d'un VPC (trafic Est-Ouest) vers une appliance middlebox. Vous pouvez définir la destination d'un acheminement pour qu'elle corresponde à l'intégralité d'un bloc d'adresse CIDR IPv4 ou IPv6 d'un sous-réseau de votre VPC.	30 août 2021
ID de ressource et prise en charge de l'identification pour les règles de groupes de sécurité	Vous pouvez faire référence aux règles des groupes de sécurité par ID de ressource. Vous pouvez également ajouter des étiquettes aux règles de vos groupes de sécurité.	7 Juillet 2021
Passerelles NAT privées	Vous pouvez utiliser une passerelle NAT privée pour la communication privée sortante uniquement entre des VPC ou entre un VPC et votre réseau sur site.	10 Juin 2021

Identifier à la création	Vous pouvez ajouter des balises lorsque vous créez un VPC, des options DHCP, une passerelle Internet, une passerelle de sortie uniquement, une liste de contrôle d'accès réseau et un groupe de sécurité.	30 juin 2020
Listes de préfixes gérées	Vous pouvez créer et gérer un ensemble de blocs CIDR dans la liste des préfixes.	29 juin 2020
Améliorations des journaux de flux	De nouveaux champs de journal de flux sont disponibles, et vous pouvez spécifier un format personnalisé pour les journaux de flux publiés dans CloudWatch Logs.	4 mai 2020
Prise en charge du balisage pour les journaux de flux	Vous pouvez ajouter des balises à vos journaux de flux.	16 mars 2020
Baliser lors de la création d'une passerelle NAT	Vous pouvez ajouter une balise lorsque vous créez une passerelle NAT.	9 mars 2020
Intervalle d'agrégation maximum pour les journaux de flux	Vous pouvez spécifier la période maximale pendant laquelle un flux est capturé et agrégé dans un enregistrement de journal de flux.	4 février 2020
Configuration de groupes de bordure réseau	Vous pouvez configurer des groupes de bordure réseau pour vos VPC à partir de l'Amazon Virtual Private Cloud Console.	22 janvier 2020

Nom DNS privé	Vous pouvez accéder aux services AWS PrivateLink basés en privé depuis votre VPC à l'aide de noms DNS privés.	6 janvier 2020
Tables de routage de passerelle	Vous pouvez associer une table de routage à une passerelle et acheminer le trafic VPC entrant vers une interface réseau spécifique de votre VPC.	3 décembre 2019
Améliorations des journaux de flux	Vous pouvez spécifier un format personnalisé pour votre journal de flux et choisir les champs qui sont renvoyés dans les enregistrements du journal de flux.	11 septembre 2019
Partage VPC	Vous pouvez partager des sous-réseaux situés dans le même VPC avec plusieurs comptes au sein de la AWS même organisation.	27 novembre 2018
Créer un sous-réseau par défaut	Vous pouvez créer un sous-réseau par défaut dans une zone de disponibilité qui n'en comporte pas un.	9 novembre 2017
Prise en charge du balisage pour les passerelles NAT	Vous pouvez baliser votre passerelle NAT.	7 septembre 2017
CloudWatch Métriques Amazon pour les passerelles NAT	Vous pouvez consulter CloudWatch les métriques de votre passerelle NAT.	7 septembre 2017

Descriptions des règles des groupes de sécurité	Vous pouvez ajouter des descriptions aux règles des groupes de sécurité.	31 août 2017
Blocs d'adresse CIDR IPv4 pour votre VPC	Vous pouvez ajouter plusieurs blocs d'adresse CIDR IPv4 à votre VPC.	29 août 2017
Récupération d'adresses IP Elastic	Si vous avez libéré une adresse IP Elastic, vous pouvez essayer de la récupérer.	11 août 2017
Création d'un VPC par défaut	Si vous supprimez votre VPC par défaut, vous pouvez en recréer un.	27 juillet 2017
Prise en charge d'IPv6	Vous pouvez associer un bloc d'adresse CIDR IPv6 à votre VPC et attribuer des adresses IPv6 aux ressources de votre VPC.	1 décembre 2016
Support de la résolution DNS pour les plages d'adresses IP non RFC 1918	Le serveur DNS d'Amazon peut désormais résoudre les noms d'hôtes DNS privés avec des adresses IP privées pour tous les espaces d'adresses.	24 octobre 2016
Passerelles NAT	Vous pouvez créer une passerelle NAT dans un sous-réseau public et permettre aux instances dans un sous-réseau privé d'initier le trafic sortant vers Internet ou d'autres services AWS .	17 décembre 2015

Journaux de flux VPC	Vous pouvez créer un journal de flux pour capturer des informations sur le trafic IP circulant vers et depuis les interfaces réseau dans votre VPC.	10 juin 2015
ClassicLink	Vous pouvez l'utiliser ClassicLink pour lier votre instance EC2-Classic à un VPC de votre compte. Vous pouvez associer des groupes de sécurité VPC à l'instance EC2-Classic en activant la communication entre votre instance EC2-Classic et des instances de votre VPC à l'aide d'adresses IP privées.	7 janvier 2015
Utilisation de zones hébergées privées	Vous pouvez accéder aux ressources de votre VPC en utilisant des noms de domaine DNS personnalisés que vous définissez dans une zone hébergée privée dans Route 53.	5 novembre 2014
Modifier l'attribut de l'adressage IP public d'un sous-réseau	Vous pouvez modifier l'attribut d'adressage IP public de votre sous-réseau afin d'indiquer si les instances lancées dans ce sous-réseau doivent recevoir une adresse IP publique.	21 juin 2014
Attribution d'une adresse IP publique	Pour attribuer une adresse IPv4 publique à une instance lors du lancement	20 août 2013

Activation des noms d'hôte DNS et désactivation de la résolution DNS	Vous pouvez modifier les valeurs par défaut du VPC, désactiver la résolution DNS et activer les noms d'hôte DNS.	11 mars 2013
VPC Everywhere	Ajout de la prise en charge des VPC dans cinq AWS régions, des VPC dans plusieurs zones de disponibilité, de plusieurs VPC par AWS compte et de plusieurs connexions VPN par VPC.	3 août 2011
Instances dédiées	Les instances dédiées sont des instances Amazon EC2 lancées dans votre cloud privé virtuel (VPC) et qui s'exécutent sur un matériel dédié à un seul client.	27 mars 2011

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.