aws

Guide de l’utilisateur

Amazon Virtual Private Cloud

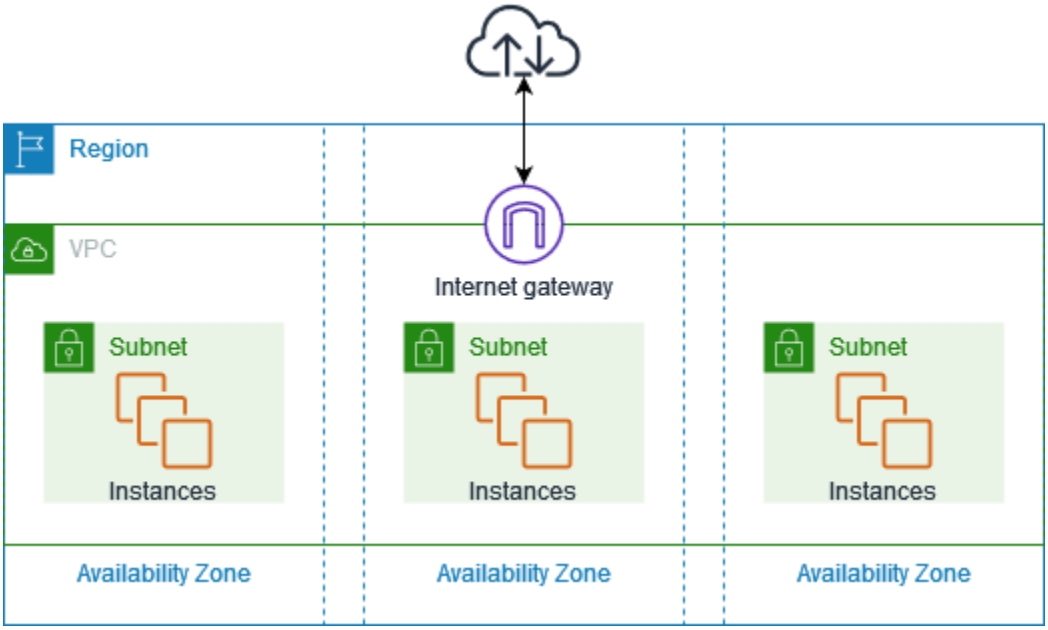
Amazon Virtual Private Cloud: Guide de l’utilisateur

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 chacune des zones de disponibilité de la région, des EC2 instances dans chaque sous-réseau et une passerelle Internet pour permettre la communication entre les ressources de votre VPC et Internet.



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

Caractéristiques

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.

Subnets

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, à la fois IPv4 et IPv6, à vos sous-réseaux VPCs et. Vous pouvez également transférer vos IPv4 adresses publiques et adresses IPv6 GUA et les allouer aux AWS ressources de votre VPC, telles que les EC2 instances, les passerelles NAT 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 VPC pour acheminer le trafic entre les ressources en deux. VPCs

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 VPCs connexions VPN et vos 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-vous VPCs à vos réseaux locaux à l'aide de AWS Virtual Private Network (Site-to-Site VPN).

Mise en route avec Amazon VPC

Vous Compte AWS incluez un VPC par défaut dans chacun d'entre eux. Région AWS Vos paramètres par défaut VPCs sont configurés de telle sorte que vous puissiez immédiatement commencer à lancer des EC2 instances et à vous y connecter. Pour de plus amples informations, veuillez consulter Planifier votre VPC.

Vous pouvez choisir d'en créer d'autres VPCs avec les sous-réseaux, les adresses IP, les passerelles et le routage dont vous avez besoin. Pour de plus amples informations, veuillez consulter the section called “Création d'un VPC”.

Utilisation d'Amazon VPC

Vous pouvez créer et gérer votre compte VPCs à l'aide de l'une des interfaces suivantes :

- AWS Management Console— Fournit une interface Web que vous pouvez utiliser pour accéder à votre VPCs.
- 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 de plus amples informations, veuillez consulter AWS Command Line Interface.
- AWS SDKs— Fournit des informations spécifiques à la langue APIs 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 de plus amples informations, veuillez consulter AWS SDKs.
- 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 le manuel Amazon EC2 API Reference.

Tarification pour Amazon VPC

Il n'y a pas de frais supplémentaires pour l'utilisation d'un VPC. Cependant, des frais sont facturés pour certains composants VPC, tels que les passerelles NAT, le gestionnaire d'adresses IP, la mise en miroir du trafic VPC, l'analyseur d'accessibilité et l'analyseur d'accès réseau. 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 privées IPv4 . Les ressources qui nécessitent un accès direct à Internet utilisent IPv4 toutefois des IPv4 adresses publiques.

Amazon VPC vous permet de lancer des services gérés, tels que Elastic Load Balancing, Amazon RDS et Amazon EMR, sans avoir à configurer un VPC au préalable. Pour ce faire, il utilise le VPC par défaut de votre compte, si vous en avez un. Toutes IPv4 les adresses publiques fournies à votre compte par le service géré seront facturées. Ces frais seront associés au service Amazon VPC de votre entreprise. AWS Cost and Usage Report

Tarification pour les IPv4 adresses publiques

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

Si vous êtes un client existant ou un nouveau client du niveau AWS gratuit, vous bénéficiez de 750 heures d'utilisation gratuite des IPv4 adresses publiques avec le EC2 service. Si vous n'utilisez pas le EC2 service dans le cadre de l' AWS offre gratuite, les IPv4 adresses publiques sont facturées. Pour obtenir des informations tarifaires spécifiques, consultez l'onglet IPv4 Adresse publique dans Amazon VPC Pricing.

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

Les types d' IPv4 adresses publiques sont les suivants :

- Adresses IP élastiques (EIPs) : IPv4 adresses publiques statiques fournies par Amazon que vous pouvez associer à une EC2 instance, à une interface réseau élastique ou à une AWS ressource.
- EC2 IPv4 adresses publiques : IPv4 adresses publiques attribuées à une EC2 instance par Amazon (si l' EC2 instance est lancée dans un sous-réseau par défaut ou si l'instance est lancée dans un sous-réseau configuré pour attribuer automatiquement une IPv4 adresse publique).

- BYOIPv4 adresses : IPv4 adresses publiques comprises dans la plage d' IPv4 adresses que vous avez amenée à AWS utiliser Bring your own IP addresses (BYOIP).
- IPv4 Adresses gérées par le service : IPv4 adresses publiques automatiquement provisionnées sur les AWS ressources et gérées par un service. AWS Par exemple, IPv4 les adresses publiques sur Amazon ECS, Amazon RDS ou Amazon WorkSpaces.

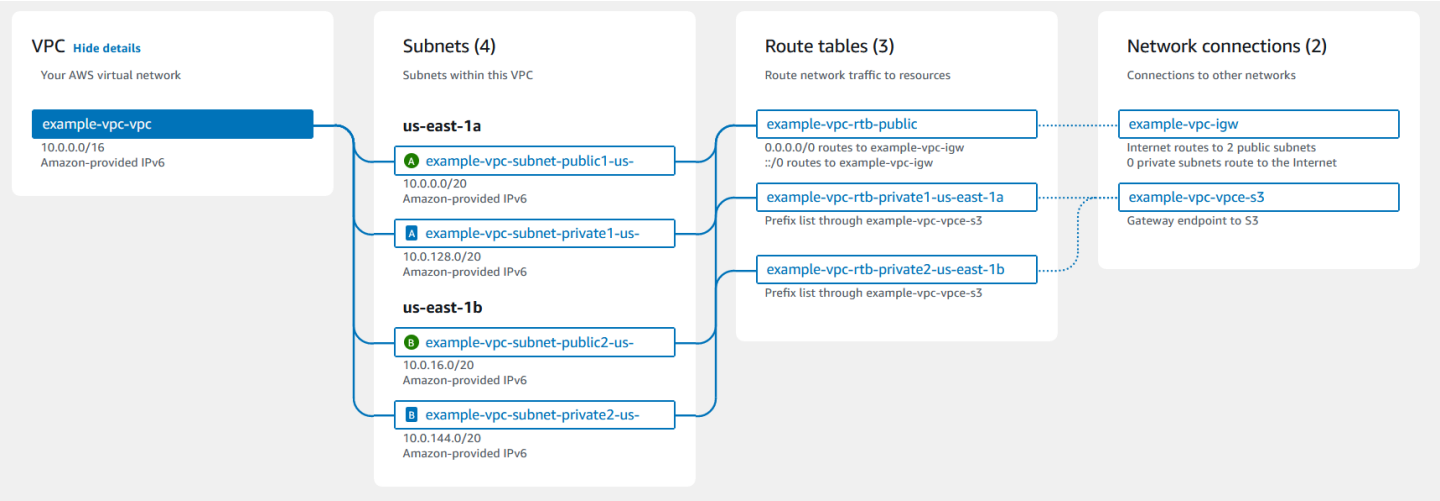
La liste suivante répertorie les AWS services les plus courants qui peuvent utiliser des IPv4 adresses publiques.

- WorkSpaces Applications Amazon
- AWS Client VPN
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR
- GameLift Serveurs Amazon
- 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 des ressources AWS dans un réseau virtuel logiquement isolé 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
- Réseau mondial privé AWS

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 dans le cloud AWS. 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 pour 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 "Par défaut VPCs"
- 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

- Activation de l'accès à Internet pour un VPC à l'aide d'une passerelle Internet
- Activez le IPv6 trafic sortant à l'aide d'une passerelle 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

Si vous le souhaitez, vous pouvez connecter votre VPC à votre propre centre de données d'entreprise à l'aide d'une connexion AWS Site-to-Site VPN IPsec, qui transforme le cloud AWS en une extension de votre centre de données.

Une connexion Site-to-Site VPN se compose de deux tunnels VPN entre une passerelle réseau privé virtuel ou une passerelle de transit côté AWS, et un appareil 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, ce qui peut inclure des VPC, des connexions VPN, des passerelles Direct Connect et des connexions d'appairage de passerelle de transit.

En savoir plus

- Amazon VPC Peering Guide
- Passerelles de transit Amazon VPC

Réseau mondial privé AWS

AWS fournit un réseau mondial privé hautes performances et à faible latence qui offre un environnement de cloud computing sécurisé pour prendre en charge vos besoins de mise en 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 paquets transmis depuis le réseau mondial privé vers une destination qui se trouve au sein de ce même réseau ne passent pas par l'Internet public. Ils restent dans le réseau mondial privé, et ce que la destination soit une adresse IP privée ou publique. Par exemple, si les instances EC2 de deux VPC communiquent à l'aide d'adresses IP publiques, le trafic reste dans le réseau mondial privé. La destination peut se trouver dans la même zone de disponibilité, dans une autre zone de disponibilité de la même région ou dans une autre région, à l'exception des régions de Chine.

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) au niveau du backbone principal raccordant les régions AWS. Nous faisons fonctionner notre réseau backbone en vue d'obtenir un p99 pour le PLR horaire de moins de 0,0001 %.

Planifier votre VPC

Effectuez les tâches suivantes pour préparer la création et la connexion de votre VPCs. 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 l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS 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 de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte 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 VPCs des sous-réseaux, vous pouvez sélectionner leurs plages d'adresses IP. Lorsque vous déployez des ressources dans un sous-réseau, telles que des EC2 instances, elles reçoivent des adresses IP provenant de la plage d'adresses IP du sous-réseau. Pour de plus amples informations, veuillez consulter Adressage IP.

Lorsque vous choisissez la taille de votre VPC, réfléchissez au nombre d'adresses IP dont vous aurez besoin sur votre Comptes AWS bande de distribution. VPCs Assurez-vous que les plages d'adresses IP de votre propre réseau VPCs ne se chevauchent pas avec les plages d'adresses IP de votre propre réseau. Si vous avez besoin d'une connectivité entre plusieurs adresses IP VPCs, vous devez vous assurer qu'elles n'ont pas d'adresses IP qui se chevauchent.

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 de plus amples informations, veuillez consulter the section called “Accéder à Internet à partir d'un sous-réseau privé”.

Créer votre VPC

Une fois que vous avez déterminé le nombre VPCs et les sous-réseaux dont vous avez besoin, les blocs CIDR à attribuer à vos sous-réseaux VPCs et 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 de plus amples informations, veuillez consulter 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 Parc
- 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 EC2 instance. Pour plus d'informations, consultez la section Commencer avec Amazon EC2 dans le guide de EC2 l'utilisateur Amazon.

Adressage IP pour votre réseau VPCs et vos 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 IPv4 adresse individuelle est de 32 bits, avec 4 groupes de 3 chiffres décimaux maximum, de 0 à 255. Par exemple : 10.0.1.0.
- Un bloc IPv4 CIDR possède une IPv4 adresse suivie d'une barre oblique et d'un nombre compris entre 0 et 32. Par exemple, 10.0.0.0/16 représente 65 536 adresses comprises entre 10.0.0.0 et IPv4 10.0.255.255.
- Une IPv6 adresse individuelle est de 128 bits, avec 8 segments de 4 chiffres hexadécimaux. Par exemple, 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Il n'est pas nécessaire d'inclure les zéros de début dans un segment. Vous pouvez également remplacer une fois des segments consécutifs constitués uniquement de zéros par deux signes deux-points (::) dans une adresse. L'adresse donnée en exemple peut donc être compressée sous la forme 2001:db8:85a3::8a2e:370:7334.
- Un bloc IPv6 CIDR possède une IPv6 adresse qui se termine par des segments entièrement nuls, les segments entièrement nuls étant remplacés par deux points, suivis d'une barre oblique et d'un nombre compris entre 0 et 128. Par exemple, 2001:db 8:1234:1 a00 : :/56 représente 2^72 IPv6 adresses comprises entre 2001:db 8:1234:1 a 00:0000:0000:0000:0000 et 2001:db 8:1234:1 aff:ffff:ffff:ffff.

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

Table des matières

- Comparez l'IPv4 et l'IPv6
- Consolidez et gérez les blocs d'adresse CIDR du réseau à l'aide de listes de préfixes gérées
- Plages d'adresses IP AWS
- IPv6 support pour votre VPC
- AWS des services qui soutiennent IPv6

IPv4 Adresses privées

IPv4 Les adresses 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' IPv4 adresses du sous-réseau est attribuée à l'interface réseau principale (par exemple, 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 Interfaces réseau Elastic 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 primaires et secondaires, consultez Plusieurs adresses IP dans le Guide de l'utilisateur Amazon EC2.

Nous appelons adresses IP privées les adresses IP situées dans la plage IPv4 CIDR 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 Direct Connect.

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

IPv4 Adresses publiques

Tous les sous-réseaux possèdent un attribut qui détermine si une interface réseau créée dans le sous-réseau reçoit automatiquement une IPv4 adresse publique (également appelée adresse IP publique dans cette rubrique). Ainsi, lorsque vous lancez une instance dans un sous-réseau pour lequel cet attribut est activé, une adresse IP publique est attribuée à l'interface réseau principale 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 IPv4 adresses publiques, y compris les IPv4 adresses publiques associées aux instances en cours d'exécution et les adresses IP Elastic. Pour plus d'informations, consultez l'onglet IPv4 Adresse publique sur 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 les attributs d'adressage IP 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 de votre instance après le lancement en gérant les adresses IP associées à une interface réseau. Pour plus d'informations, consultez 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 libérons l'adresse IP publique de votre instance ou nous lui en attribuons une nouvelle. Pour plus d'informations, consultez 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 de plus amples informations, veuillez consulter Attributs DNS pour votre VPC.

Si vous utilisez Amazon VPC IP Address Manager (IPAM), vous pouvez obtenir un bloc contigu d' IPv4 adresses publiques AWS et l'utiliser pour allouer des adresses IP élastiques séquentielles aux ressources. AWS L'utilisation de blocs d' IPv4 adresses contigus permet de réduire considérablement les frais de gestion des listes de contrôle d'accès de sécurité et de simplifier l'allocation et le suivi des adresses IP pour les entreprises qui se développent. AWS Pour plus d'informations, consultez la section Allocation d'adresses IP élastiques séquentielles à partir d'un pool IPAM dans le guide de l'utilisateur Amazon VPC IPAM.

IPv6 adresses

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 pour les adresses IP est IPv6, qui fournit un espace d'adressage plus grand que IPv4. IPv6 résout le problème d'épuisement des IPv4 adresses et vous permet de connecter davantage d'appareils à Internet. La transition est progressive, mais à mesure que IPv6 l'adoption se développe, vous pouvez simplifier vos réseaux et tirer parti des fonctionnalités IPv6 avancées pour améliorer la connectivité, les performances et la sécurité.

De nombreux AWS services, tels qu'Amazon EC2, Amazon S3 et Amazon CloudFront, offrent un support à double pile (IPv4 et IPv6) ou IPv6 uniquement, permettant d'attribuer des IPv6 adresses aux ressources et d'y accéder via le IPv6 protocole et de simplifier la configuration et la gestion du réseau pour les clients qui les adoptent. IPv6 D'autres services offrent un support limité ou partiel à double pile et IPv6 uniquement.

Pour plus d'informations sur les services qui prennent en charge IPv6, consultezAWS des services qui soutiennent IPv6.

Notez que certaines IPv6 adresses sont réservées par l'Internet Engineering Task Force. Pour plus d'informations sur les plages d' IPv6 adresses réservées, consultez le registre d'adresses à IPv6 usage spécial de l'IANA et. RFC4291

> **Note**
>
> L' IPv6 adressage public et privé est disponible dans AWS. AWS définit les adresses IP publiques comme celles publiées sur Internet à partir de AWS, tandis que les adresses IP privées ne le sont pas et ne peuvent pas être annoncées sur Internet à partir de. AWS

Table des matières

IPv6 Adresses publiques

Les adresses IPv6 fournies par Amazon sont toujours publiées sur Internet. Il est possible d'y accéder par Internet, car elles sont uniques à l'échelle mondiale. Vous pouvez contrôler si les ressources telles que les instances EC2 sont accessibles à l'aide de leurs IPv6 adresses en contrôlant le routage de vos sous-réseaux ou en utilisant les groupes de sécurité et le réseau. ACLs

Voici quelques-unes des manières dont vous pouvez vous préparer à utiliser des IPv6 adresses publiques pour vos charges de travail :

- Créez un IPAM avec Amazon VPC IP Address Manager et fournissez une plage d'adresses IPv6 publiques appartenant à Amazon à un pool d'adresses IPAM. Pour plus d'informations, consultez la section Créer des IPv6 pools dans le guide de l'utilisateur Amazon VPC IPAM.
- Si vous possédez un IPAM et que vous possédez une plage d' IPv6 adresses publiques, transférez une partie ou la totalité de la plage d' IPv6 adresses publiques à un pool d'adresses IPAM. IPv6 Pour plus d'informations, consultez Didacticiel : Apporter vos adresses IP à IPAM dans le Guide de l'utilisateur Amazon VPC IPAM.
- Si vous n'avez pas d'IPAM mais que vous possédez une plage d' IPv6 adresses publiques, apportez une partie ou la totalité de la plage d' IPv6 adresses publiques à AWS. Pour plus d'informations, consultez Bring your own IP addresses (BYOIP) to Amazon EC2 dans le Guide de l'utilisateur Amazon EC2.

Lorsque vous êtes prêt à utiliser des IPv6 adresses publiques, vous pouvez attribuer des IPv6 adresses publiques aux instances (voir les IPv6 adresses dans le guide de l'utilisateur Amazon EC2), vous pouvez attribuer un bloc d'adresse IPv6 CIDR public à votre VPC (voirAjouter ou supprimer

un bloc d'adresse CIDR de votre VPC) et associer le bloc d'adresse IPv6 CIDR à vos sous-réseaux (voir). Modifier les attributs d'adressage IP de votre sous-réseau

IPv6 Adresses privées

Les IPv6 adresses privées sont IPv6 des adresses qui ne sont pas annoncées et ne peuvent pas être publiées sur Internet à partir de. AWS

Vous pouvez utiliser une IPv6 adresse privée si vous souhaitez que vos réseaux privés soient compatibles IPv6 et que vous n'avez pas l'intention d'acheminer le trafic de ces adresses vers Internet. Si vous souhaitez vous connecter à Internet à partir d'une ressource dotée d'une IPv6 adresse privée, vous pouvez le faire, mais vous devez pour cela acheminer le trafic via une ressource d'un autre sous-réseau doté d'une IPv6 adresse publique.

Il existe deux types d' IPv6 adresses privées :

- IPv6 Plages ULA : IPv6 adresses telles que définies dans RFC4193. Ces plages d'adresses commencent toujours par « fc » ou « fd », ce qui les rend facilement identifiables. L'espace IPv6 ULA valide est tout espace inférieur à fd00 : :/8 qui ne chevauche pas la plage réservée Amazon fd00 : :/16.
- IPv6 Plages GUA : IPv6 adresses telles que définies dans RFC3587. L'option permettant d'utiliser les plages IPv6 GUA comme IPv6 adresses privées est désactivée par défaut et doit être activée avant de pouvoir l'utiliser. Pour plus d'informations, consultez Activer le provisionnement d'une IPv6 GUA privée CIDRs dans le guide de l'utilisateur Amazon VPC IPAM.

Notez ce qui suit :

- Les IPv6 adresses privées ne sont disponibles que via Amazon VPC IP Address Manager (IPAM). L'IPAM découvre les ressources avec des adresses IPv6 ULA et GUA et surveille les pools pour détecter tout chevauchement d'espaces d'adressage IPv6 ULA et GUA.
- Lorsque vous utilisez des gammes IPv6 GUA privées, nous exigeons que vous utilisiez des gammes IPv6 GUA dont vous êtes propriétaire.
- Les IPv6 adresses privées ne sont pas et ne peuvent pas être annoncées sur Internet par AWS. AWS n'autorise pas la sortie directe vers l'Internet public depuis une IPv6 plage privée, même s'il existe une passerelle Internet ou une passerelle Internet de sortie uniquement dans le VPC. Les IPv6 adresses privées sont automatiquement supprimées à la périphérie de la passerelle Internet, ce qui garantit qu'elles ne sont pas routées publiquement.

- AWS réserve les 4 premières IPv6 adresses privées du sous-réseau et la dernière.
- Les plages valides pour les IPv6 ULA privées sont comprises entre /9 et /60, en commençant par fd80 : :/9.
- Si une plage de IPv6 GUA privée est allouée à un VPC, vous ne pouvez pas utiliser d'espace IPv6 GUA public qui chevauche l'espace IPv6 GUA privé du même VPC.
- La communication entre les ressources dotées de plages d'adresses IPv6 ULA et GUA privées est prise en charge (par exemple via Direct Connect, le peering VPC, la passerelle de transit ou les connexions VPN).
- Vous pouvez utiliser des IPv6 adresses privées avec des sous-réseaux VPC à double IPv6 pile ou uniquement, des équilibreurs de charge élastiques et des points de terminaison.AWS Global Accelerator
- Il n'y a aucun frais pour les IPv6 adresses privées.

Voici quelques-unes des manières dont vous pouvez vous préparer à utiliser des IPv6 adresses privées pour vos charges de travail :

- Créez un IPAM avec Amazon VPC IP Address Manager et attribuez une plage d'ULA IPv6 privée à un pool d'adresses IPAM. Pour plus d'informations, consultez la section Créer des IPv6 pools dans le guide de l'utilisateur Amazon VPC IPAM.
- Créez un IPAM avec Amazon VPC IP Address Manager et attribuez une plage GUA IPv6 privée à un pool d'adresses IPAM. L'option permettant d'utiliser les plages IPv6 GUA comme IPv6 adresses privées est désactivée par défaut et doit être activée sur votre IPAM avant de pouvoir l'utiliser. Pour plus d'informations, consultez Activer le provisionnement d'une IPv6 GUA privée CIDRs dans le guide de l'utilisateur Amazon VPC IPAM.

Lorsque vous êtes prêt à utiliser des IPv6 adresses privées, vous pouvez allouer un bloc d'adresse IPv6 CIDR privé d'un pool IPAM à votre VPC (voirAjouter ou supprimer un bloc d'adresse CIDR de votre VPC) et associer le bloc d'adresse IPv6 CIDR à vos sous-réseaux (voir). Modifier les attributs d'adressage IP de votre sous-réseau

Utiliser vos propres adresses IP

Vous pouvez ajouter une partie ou la totalité de votre plage d' IPv4 adresses publiques ou de votre plage d' IPv6 adresses 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 pool d' IPv4 adresses et associer un bloc IPv6 CIDR de votre pool d' IPv6 adresses à un VPC.

Pour plus d'informations, consultez 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 attribuer une adresse IP CIDRs à VPCs l'aide de règles commerciales 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 IPv4 CIDR. Vous pouvez éventuellement associer des blocs d'adresse IPv4 CIDR supplémentaires et un ou plusieurs blocs d'adresse IPv6 CIDR. Pour de plus amples informations, veuillez consulter Adressage IP pour votre réseau VPCs et vos sous-réseaux.

Table des matières

IPv4 Blocs d'adresse CIDR VPC

Lorsque vous créez un VPC, vous devez spécifier un bloc IPv4 CIDR 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 associer des blocs IPv4 CIDR

supplémentaires au VPC. Pour de plus amples informations, veuillez consulter Ajouter ou supprimer un bloc d'adresse CIDR de votre VPC.

Lorsque vous créez un VPC, nous vous recommandons de spécifier un bloc CIDR à partir des plages d' IPv4adresses privées spécifiées dans la 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

Considérations

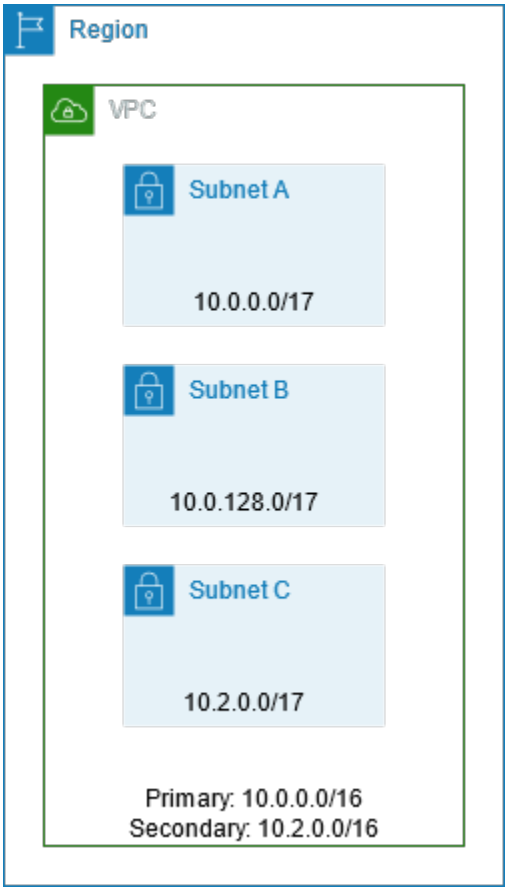
- Vous ne pouvez pas spécifier les blocs CIDR suivants pour votre VPCs :
  - 0.0.0,0/8
  - 127.0.0.0/8 (plage d'adresses de bouclage interne de l'hôte)
  - 169.254.0.0/16 (plage d'adresses lien-local)
  - 224.0.0.0/4 (plage d'adresses multicast)
- Lorsque vous créez un VPC à utiliser avec un AWS service, consultez la documentation du service pour vérifier si sa configuration est soumise à des exigences spécifiques.
- Certains AWS services utilisent la gamme `172.17.0.0/16` CIDR. Les services peuvent être confrontés à des conflits d'adresses IP si la plage d'adresses IP est déjà utilisée sur votre réseau. Par exemple, AWS Cloud9 et l'utilisation d'Amazon SageMaker AI`172.17.0.0/16`. Pour éviter les conflits, n'utilisez pas cette plage lors de la création de votre VPC. 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 CIDR routable publiquement situé en dehors des plages d' IPv4 adresses privées spécifiées dans la RFC 1918. Toutefois, dans le cadre de cette documentation, nous appelons adresses IP privées les IPv4 adresses situées dans la plage CIDR de votre VPC.

- 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.

Gérer les blocs IPv4 CIDR pour un VPC

Vous pouvez associer des blocs d' IPv4 adresse CIDR secondaires 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.
- Les plages d' IPv4 adresses que vous pouvez utiliser sont soumises à des restrictions. Pour de plus amples informations, veuillez consulter IPv4 Restrictions relatives à l'association de blocs CIDR.
- 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 IPv4 CIDR à un VPC faisant partie d'une connexion d'appairage 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 Direct Connect à plusieurs VPCs via une passerelle Direct Connect, les VPCs blocs CIDR associés à la passerelle Direct Connect ne doivent pas se chevaucher. Si vous ajoutez un bloc d'adresse CIDR à l'un des blocs associés 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. VPCs Pour plus d'informations, consultez la section Passerelles Direct Connect du Guide de l'utilisateur 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 dans la console Amazon VPC, choisissez VPCs Votre, cochez la case correspondant à votre VPC, puis cliquez sur l'onglet. CIDRs 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
```

IPv4 Restrictions relatives à l'association de blocs CIDR

Le tableau suivant donne un aperçu des associations autorisées et limitées pour les blocs CIDR VPC existants. 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 IPv4 d'adresses existante	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 d'adresse CIDR provenant de la plage 10.0.0.0/8 entre un masque réseau /16 et un masque réseau /28 qui n'est pas limité. Tout bloc IPv4 CIDR 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.
169.254.0.0/16	Les blocs CIDR du bloc « link local » sont réservés comme décrit dans la RFC 5735 et ne peuvent pas être assignés. VPCs	
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 d'adresse CIDR provenant de la plage 172.16.0.0/12 entre un masque réseau /16 et un masque réseau /28 qui n'est pas limité. Tout bloc IPv4 CIDR 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

Plage IPv4 d'adresses existante	Associations limitées	Associations autorisées
		réseau /16 et un masque réseau /28 compris entre 100.64.0.0/10.
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 d'adresse CIDR provenant de la plage 192.168.0.0/16 entre un masque réseau /16 et un masque réseau /28. Tout bloc IPv4 CIDR 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 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 IPv4 CIDR 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 entre un masque réseau /16 et un masque réseau /28.

Plage IPv4 d'adresses existante	Associations limitées	Associations autorisées
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 IPv4 CIDR 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. Vous pouvez également associer un CIDR dans l'une des plages RFC 1918, mais pour cela, vous devez d'abord ajouter ce CIDR à la création du VPC, puis ajouter le CIDR hors RFC 1918.

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

IPv6 Blocs d'adresse CIDR VPC

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

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

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

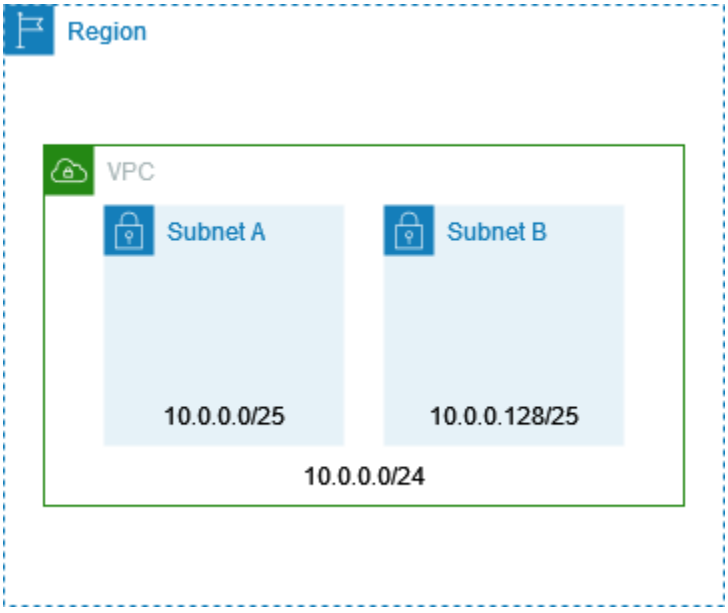
pouvez créer un sous-réseau et associer un bloc IPv6 CIDR à partir de cette plage ; par exemple,. `2001:db8:1234:1a00::/64`

Vous pouvez dissocier un bloc IPv6 CIDR d'un VPC. Après avoir dissocié un bloc d'adresse IPv6 CIDR d'un VPC, vous ne pouvez pas vous attendre à recevoir le même code d'adresse CIDR si vous associez à nouveau un IPv6 bloc d'adresse CIDR 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, à créer IPv4 et à créer des IPv6 sous-réseaux de blocs CIDR. Vous pouvez trouver des outils qui répondent à vos besoins en recherchant des termes tels que « calculateur de sous-réseau » ou « calculateur CIDR ». Votre

groupe d'ingénierie réseau peut également vous aider à déterminer les blocs IPv6 CIDR IPv4 et CIDR à spécifier pour vos sous-réseaux.

Dimensionnement du sous-réseau pour IPv4

La taille de bloc IPv4 CIDR autorisée pour un sous-réseau se situe entre un masque réseau et un `/28` masque réseau. `/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. Dans le VPCs cas de plusieurs blocs d'adresse 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 de plus amples informations, veuillez consulter 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' IPv4 adresses, 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 du sous-réseau pour IPv6

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

Des outils sont disponibles sur Internet pour vous aider à calculer et à créer des blocs CIDR de IPv6 sous-réseau. Vous pouvez trouver des outils adaptés à vos besoins en recherchant des termes tels que « calculateur de IPv6 sous-réseau » ou « calculateur CIDR ». IPv6 Votre groupe d'ingénierie réseau peut également vous aider à déterminer les blocs IPv6 CIDR à spécifier 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 IPv6 adresses suivantes sont réservées au routeur VPC par défaut :

- Une IPv6 adresse lien-local dans la plage FE80 : :/10 générée à l'aide de l'EUI-64. Pour plus d'informations sur les adresses de lien local, voir Adresse de lien local.
- L'adresse locale du lien IPv6 . `FE80:ec2::1`

Si vous devez communiquer avec le routeur VPC IPv6, vous pouvez configurer vos applications pour qu'elles communiquent avec l'adresse qui répond le mieux à vos besoins.

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 services AWS qui prennent en charge la configuration à double pile (IPv4 et IPv6) et les configurations IPv6 uniquement, consultez Des services qui soutiennent IPv6.

Caractéristiques	Caractéristiques et restrictions 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 apporter votre propre bloc CIDR IPv6 sur AWS pour votre VPC, choisissez un bloc CIDR IPv6 fourni par Amazon, ou vous pouvez allouer un bloc 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 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	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

Caractéristiques	Caractéristiques et restrictions IPv4	IPv6
	VPC à l'aide d'une passerelle NAT privée.	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.

Consolidez et gérez les blocs d'adresse CIDR du réseau 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

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 IPv4 des blocs IPv6 CIDR 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 de plus amples informations, veuillez consulter Priorité d'acheminement pour les listes de préfixes.
- 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 de plus amples informations, veuillez consulter 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 de plus amples informations, veuillez consulter 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 politique IAM, consultez Actions, resources, and condition keys for Amazon EC2 dans la Référence de l'autorisation de service.

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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetManagedPrefixListAssociations",
                "ec2:GetManagedPrefixListEntries",
                "ec2:ModifyManagedPrefixList",
                "ec2:RestoreManagedPrefixListVersion"
```

```
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012: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.

Listes de préfixes gérées par le client

Les listes de préfixes gérées par le client vous permettent de définir et de gérer vos propres ensembles de plages d'adresses IP, appelés préfixes, au sein d' AWS. Au lieu de coder en dur ces adresses IP dans vos différentes ressources, vous pouvez créer une liste de préfixes centralisée et y faire référence si nécessaire. Cela simplifie non seulement la gestion de vos adresses IP, mais favorise également la cohérence et la réutilisation dans votre AWS environnement.

L'une des principales caractéristiques des listes de préfixes gérées par les clients est la possibilité de les partager avec d'autres comptes. AWS En accordant l'accès à vos listes de préfixes, vous pouvez permettre à d'autres équipes ou d'autres organisations d'exploiter les plages d'adresses IP que vous avez définies dans leurs propres ressources. Cette approche collaborative favorise une expérience cloud plus cohérente et plus efficace, dans laquelle la gestion des adresses IP est partagée et synchronisée.

Dans les sections qui suivent, nous aborderons plus en détail les aspects pratiques de l'utilisation de listes de préfixes gérées par les clients, notamment des step-by-step conseils sur la création, la gestion et le partage de vos plages d'adresses IP.

> **Note**
>
> Vous pouvez automatiser la gestion des listes de préfixes à l'aide d'Amazon VPC IPAM afin de les CIDRs synchroniser automatiquement en fonction des règles que vous définissez. De cette façon, vous éviterez les mises à jour manuelles lorsque votre infrastructure évolue.

Pour plus d'informations, consultez Automate prefix list updates with IPAM dans le Guide d'utilisation de l'IPAM Amazon VPC.

Tâches

- Utiliser des listes de préfixes gérées par le client

Utiliser des listes de préfixes gérées par le client

Cette section décrit comment utiliser les listes de préfixes gérées par le client.

Table des matières

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, choisissez si la liste de préfixes prend en charge les supports IPv4 ou les IPv6 entrées.
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 consulter IDs les ressources associées à votre liste de préfixes ainsi que leurs propriétaires. 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. Si la liste de préfixes gérée a été configurée comme cible de résolution de liste de préfixes IPAM, une option de synchronisation du résolveur de liste de préfixes IPAM s'affiche.

   Choisissez d'activer ou de désactiver la synchronisation avec le résolveur de liste de préfixes IPAM. Lorsque cette option est activée, la liste des CIDRs préfixes est automatiquement mise à jour en fonction des règles de sélection CIDR du résolveur associé. Lorsque cette option est désactivée, la liste des préfixes n' CIDRs est pas automatiquement mise à jour. Pour plus d'informations sur cette fonctionnalité, consultez Automate prefix list updates with IPAM dans le Guide d'utilisation de l'IPAM Amazon VPC.
6. 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.
7. 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 AWS liste de préfixes gérée.

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.

Partager les listes de préfixes gérées par le client

Avec AWS Resource Access Manager (AWS RAM), le propriétaire d'une liste de préfixes gérée par le client peut partager la liste de préfixes avec les personnes suivantes :

- 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. Pour plus d'informations sur les quotas, consultez la section Quotas de service dans le guide de AWS RAM l'utilisateur.

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

Table des matières

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 IDs AWS ressources qui font référence à la liste des 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.

Utiliser des listes de préfixes partagées

AWS les listes de préfixes constituent un moyen pratique de gérer et de référencer les plages d'adresses IP utilisées par les différents AWS services. Outre les listes de préfixes AWS gérées par les clients, vous pouvez également créer et partager vos propres listes de préfixes gérées par les clients avec d'autres comptes. AWS

Le partage de listes de préfixes peut être particulièrement utile pour les organisations ayant des exigences réseau complexes ou celles qui ont besoin de coordonner l'utilisation des adresses IP

sur plusieurs charges de AWS travail. En partageant une liste de préfixes, vous pouvez garantir une gestion cohérente des adresses IP et simplifier les configurations réseau pour vos collaborateurs.

Cette section explique comment partager des listes de préfixes et comment identifier et utiliser les listes de préfixes partagées avec votre compte.

Table des matières

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.

Important

- 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 .

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

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.

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 IDs ressources qui font référence à la liste de préfixes sont répertoriées dans la colonne Resource ID. 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.

Listes de préfixes gérées par AWS

AWS-les listes de préfixes gérées sont des ensembles de plages d'adresses IP pour les AWS services. Ces listes de préfixes sont gérées par Amazon Web Services et permettent de référencer les adresses IP utilisées par les différentes AWS offres. Cela peut être particulièrement utile lors de la configuration de groupes de sécurité ou d'autres contrôles au niveau du réseau au sein d'un VPC.

Les listes de préfixes couvrent un large éventail de AWS services, notamment S3 et DynamoDB, et bien d'autres. En utilisant les listes de préfixes gérées, vous pouvez vous assurer que les configurations de votre réseau correspondent aux adresses IP utilisées par les AWS services dont vous dépendez up-to-date et en tenir compte correctement. Cela permet de simplifier les tâches de mise en réseau et de réduire les frais administratifs liés à la gestion manuelle des listes d'adresses IP.

Outre les avantages pratiques, l'utilisation des listes de préfixes gérées est également conforme aux meilleures pratiques en AWS matière de sécurité. En vous fiant aux informations d'adresse IP fiables fournies par AWS, vous pouvez minimiser le risque de mauvaise configuration ou de problèmes de connectivité inattendus. Cela peut être particulièrement important pour les applications critiques ou les charges de travail soumises à des exigences de conformité strictes.

Table des matières

Listes AWS de préfixes gérées disponibles

Les services suivants fournissent des listes AWS de préfixes gérées.

Service AWS	Nom de la liste des préfixes	Pondération
Amazon CloudFront	com.amazonaws.global.cloudfront.origin-facing () IPv4	55

Service AWS	Nom de la liste des préfixes	Pondération
	com.amazonaws.global.ipv6.cloudfront.origin-facing () IPv6	
Amazon DynamoDB	com.amazonaws. *region*.dynamodb	1
Amazon EC2 Instance Connect	com.amazonaws. *region*.ec2-instance-connect	2
	com.amazonaws. *region*.ipv6.ec2-instance-connect	2
AWS Ground Station	com.amazonaws.global.groundstation	5
Amazon Route 53	com.amazonaws. *region*.ipv6.route 53 - bilans de santé	25
	com.amazonaws. *region*. route 53 - bilans de santé	25
Amazon S3	com.amazonaws. *region*.s3	1
Amazon S3 Express One Zone	com.amazonaws. *region*.s3 express	6
Amazon VPC Lattice	com.amazonaws. *region*.vpc en treillis	10
	com.amazonaws. *region*.ipv6.vp-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
```

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.

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 de plus amples informations, veuillez consulter Optimisez la gestion de AWS l'infrastructure avec des listes de préfixes.

Optimisez la gestion de AWS l'infrastructure avec des listes de préfixes

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 de plus amples informations, veuillez consulter Groupes de sécurité.

> **Important**
>
> Vous ne pouvez pas modifier une règle existante pour utiliser une liste de préfixes. Vous devez créer une nouvelle règle pour utiliser une liste de préfixes.

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 panneau 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 Personnalisation. Puis, dans le champ suivant, sous Listes de préfixes, choisissez l'ID de la liste de 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 commandes authorize-security-group-ingress et authorize-security-group-egress. 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 CIDRs éléments 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, consultez Gestion des routes de la table de routage de passerelle locale dans le Guide de l'utilisateur AWS Outposts pour les racks.

Plages d'adresses IP AWS

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

Considérations

- Nous publions les plages d'adresses IP des services que les clients utilisent couramment pour effectuer un filtrage de sortie. Nous ne publions pas les plages d'adresses IP pour tous les services.
- Les services utilisent leurs plages d'adresses IP pour communiquer avec d'autres services ou pour communiquer avec un réseau client.
- Les plages d'adresses IP que vous apportez à AWS par le biais de la solution Fourniture de vos propres adresses (BYOIP) ne sont pas incluses dans le fichier `.json`. Pour plus d'informations, consultez Annoncer votre plage d'adresses par le biais d'AWS dans le Guide de l'utilisateur Amazon EC2.

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

Table des matières

- Syntaxe de la plage d'adresses IP AWS JSON
- Notifications des plages d'adresses IP AWS

Téléchargez le fichier JSON

Pour afficher les plages d'adresses actuelles, téléchargez ip-ranges.json. Pour conserver l'historique, enregistrez les versions successives du fichier JSON sur votre propre ordinateur. 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.

Voici un exemple de commande curl qui enregistre le fichier JSON dans le répertoire actuel.

```
curl -O https://ip-ranges.amazonaws.com/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.

Pour recevoir des notifications concernant les mises à jour du fichier JSON, consultez Notifications des plages d'adresses IP AWS.

Contrôle de sortie

Pour permettre aux ressources que vous avez créées avec un service AWS d'accéder uniquement à d'autres services AWS, vous pouvez utiliser les informations relatives à la plage d'adresses IP dans le 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 services AWS sont basés sur EC2 et utilisent l'espace d'adresses 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.

Flux de géolocalisation

Les plages d'adresses IP contenues dans `ip-ranges.json` sont gérées par la Région AWS. Cependant, une zone locale ne se trouve pas au même emplacement physique que sa région parente. Les données de géolocalisation publiées dans le fichier geo-ip-feed.csv concernent les zones locales. Les données sont conformes à la norme technique RFC 8805.

Rechercher les plages d'adresses IP pour Services AWS

Le fichier JSON de plage d'adresses IP AWS fourni par AWS peut être une ressource précieuse pour rechercher les adresses IP de divers services AWS et exploiter ces informations afin d'améliorer la sécurité de votre réseau et votre contrôle d'accès. En analysant les données détaillées contenues dans ce fichier JSON, vous pouvez identifier avec précision les plages d'adresses IP associées à des régions et à des Services AWS spécifiques.

Par exemple, vous pouvez utiliser les plages d'adresses IP pour configurer des politiques de sécurité réseau robustes, en définissant des règles de pare-feu précises visant à autoriser ou refuser l'accès à certaines ressources AWS. Ces informations peuvent également être utiles pour différentes tâches AWS Network Firewall. Ce niveau de contrôle est essentiel pour protéger vos applications et vos données, en garantissant que seul le trafic autorisé peut atteindre les Services AWS nécessaires. En outre, cette intelligence IP peut vous aider à vous assurer que vos applications sont correctement configurées pour communiquer avec les points de terminaison AWS appropriés, améliorant ainsi la fiabilité et les performances globales.

Au-delà des règles de pare-feu, le fichier `ip-ranges.json` peut également être utilisé pour configurer un filtrage de sortie sophistiqué sur votre infrastructure réseau. En comprenant les plages d'adresses IP de destination des différents Services AWS, vous pouvez configurer des politiques de routage ou tirer parti de solutions de sécurité réseau avancées, telles que l'autorisation ou le blocage sélectif du trafic sortant en fonction de sa destination prévue. Ce contrôle de sortie est essentiel pour atténuer le risque de fuite de données et d'accès non autorisé.

Il est important de noter que le fichier `ip-ranges.json` est régulièrement mis à jour. Il est donc essentiel de conserver une copie locale à jour pour garantir que vous disposez des informations les plus précises et les plus récentes. En exploitant en permanence le contenu de ce fichier, vous pouvez gérer efficacement l'accès au réseau et la sécurité de vos applications basées sur AWS, renforçant ainsi votre posture de sécurité globale dans le cloud.

Les exemples suivants peuvent vous aider à filtrer les plages d'adresses IP AWS en fonction de ce que vous recherchez. Sous Linux, vous pouvez télécharger et utiliser l'outil jq pour analyser

une copie locale du fichier JSON. Les AWS Tools for Windows PowerShell incluent une applet de commande, Get-AWSPublicIpAddressRange, que vous pouvez utiliser pour analyser ce fichier JSON. Pour plus d'informations, consultez l'article de blog suivant : Interrogation des plages d'adresses IP publiques pour AWS.

Pour obtenir le fichier JSON, consultez the section called "Téléchargement". Pour plus d'informations sur la syntaxe du fichier JSON, consultez the section called "Syntaxe".

Exemples

- Obtenir la date de création du fichier
- Obtenir les adresses IP d'une région spécifique
- Obtenir toutes les adresses IPv4
- Obtenir toutes les adresses IPv4 pour un service spécifique
- Obtenir toutes les adresses IPv4 pour un service spécifique dans une région spécifique
- Obtenir toutes les adresses IPv6
- Obtenir toutes les adresses IPv6 pour un service spécifique
- Obtenir toutes les adresses IP pour un groupe de bordure spécifique

Obtenir la date de création du fichier

L'exemple suivant permet d'obtenir la date de création du fichier `ip-ranges.json`.

jq

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

"2024-08-01-17-22-15"
```

PowerShell

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

Thursday, August 1, 2024 9:22:35 PM
```

Obtenir les adresses IP d'une région spécifique

L'exemple suivant filtre le fichier JSON pour obtenir les adresses IP de la région spécifiée.

jq

```
$ 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"
},
...
```

PowerShell

```
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
...
```

Obtenir toutes les adresses IPv4

L'exemple suivant filtre le fichier JSON pour obtenir les adresses IPv4.

jq

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

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

PowerShell

```
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
...
```

Obtenir toutes les adresses IPv4 pour un service spécifique

L'exemple suivant filtre le fichier JSON pour obtenir les adresses IPv4 du service spécifié.

jq

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

13.248.117.0/24
15.197.34.0/23
15.197.36.0/22
...
```

PowerShell

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

IpPrefix
--------
13.248.117.0/24
15.197.34.0/23
15.197.36.0/22
```

```
...
```

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

L'exemple suivant filtre le fichier JSON pour obtenir les adresses IPv4 du service spécifié contenu dans la région spécifiée.

jq

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

13.248.124.0/24
99.82.166.0/24
99.82.171.0/24
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1 -ServiceKey GLOBALACCELERATOR
 | where {$_.IpAddressFormat -eq "Ipv4"} | select IpPrefix

IpPrefix
--------
13.248.117.0/24
99.82.166.0/24
99.82.171.0/24
...
```

Obtenir toutes les adresses IPv6

L'exemple suivant filtre le fichier JSON pour obtenir les adresses IPv6.

jq

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

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

```
...
```

PowerShell

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

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

Obtenir toutes les adresses IPv6 pour un service spécifique

L'exemple suivant filtre le fichier JSON pour obtenir les adresses IPv6 du service spécifié.

jq

```
$ jq -r '.ipv6_prefixes[] | select(.service=="GLOBALACCELERATOR") | .ipv6_prefix' <
 ip-ranges.json

2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
2600:9000:a800::/40
...
```

PowerShell

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

IpPrefix
--------
2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
2600:9000:a800::/40
...
```

Obtenir toutes les adresses IP pour un groupe de bordure spécifique

L'exemple suivant filtre le fichier JSON pour obtenir toutes les adresses IP du groupe de bordure spécifié.

jq

```
$ jq -r '.prefixes[] | 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
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.NetworkBorderGroup -eq "us-west-2-
lax-1"} | select IpPrefix

IpPrefix
--------
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

Syntaxe de la plage d'adresses IP AWS JSON

AWS publie ses plages d'adresses IP actuelles au format JSON. Pour obtenir le fichier JSON, consultez the section called "Téléchargement". La syntaxe du fichier 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 AA-MM-JJ-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 qu'AWS peut publier un préfixe dans des plages d'adresses 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 qu'AWS peut publier un préfixe dans des plages d'adresses plus spécifiques.

Type : chaîne

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

network_border_group

Nom du groupe de bordure réseau, qui est un ensemble unique de zones de disponibilité ou de zones locales à partir desquelles AWS publie des adresses IP, ou `GLOBAL`. Le trafic pour les services `GLOBAL` peut être attiré ou provenir de plusieurs (jusqu'à toutes) zones de disponibilité ou zones locales à partir desquelles AWS annonce des adresses IP.

Type : chaîne

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

region

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

Type : chaîne

Valeurs valides: `af-south-1` | `ap-east-1` | `ap-east-2` | `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` | `ap-southeast-5` | `ap-southeast-6` | `ap-southeast-7` | `ca-central-1` | `ca-west-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` | `il-central-1` | `mx-central-1` | `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 | AURORA_DSQL | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | IVS_LOW_LATENCY | 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.

En savoir plus

Cette section fournit des liens vers des informations supplémentaires relatives aux différents codes de service.

- 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 périphériques CloudFront
- `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
- `ROUTE53_HEALTHCHECKS` – Plages d'adresses IP de serveurs Amazon Route
- `ROUTE53_HEALTHCHECKS_PUBLISHING` – Plages d'adresses IP de serveurs Amazon Route
- `WORKSPACES_GATEWAYS` – Serveurs de passerelle PCoIP

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_LOW_LATENCY` .	29 juillet 2025
Ajout du code de service `AURORA_DSQL` .	21 mai 2025
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

Description	Date de publication
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
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

Notifications des plages d'adresses IP AWS

AWS publie ses plages d'adresses IP actuelles au format JSON. Chaque fois qu'une modification de plages d'adresses IP AWS est apportée, nous envoyons des notifications aux abonnés de la rubrique Amazon SNS nommée `AmazonIpSpaceChanged`. Pour plus d'informations sur la syntaxe du fichier JSON, consultez the section called "Syntaxe".

Les données utiles de la notification contiennent 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`. Pour de plus amples informations, consultez the section called "Téléchargement".

Vous pouvez vous abonner pour recevoir des notifications en procédant comme suit.

Pour s'abonner aux notifications de plages d'adresses IP AWS

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 annuler l'abonnement aux notifications de plages d'adresses IP AWS

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 Manuel de développement d'Amazon Simple Notification Service.

IPv6 support pour votre VPC

Si vous disposez d'un VPC existant qui prend IPv4 uniquement en charge et que les ressources de votre sous-réseau sont configurées pour être utilisées IPv4 uniquement, vous pouvez ajouter un IPv6 support pour votre VPC et vos ressources. Votre VPC peut fonctionner en mode double pile : vos ressources peuvent communiquer entre elles ou IPv4 IPv6 les deux. IPv4 et les IPv6 communications 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 entre les sous-réseaux IPv4 uniquement et les sous-réseaux uniquement. IPv6
- 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 nouveau VPC à utiliser avec IPv6, consultez. the section called "Création d'un VPC"
- Avant de commencer à utiliser IPv6, assurez-vous d'avoir lu les fonctionnalités d' IPv6adressage pour Amazon VPC :. Comparez l'IPv4 et l'IPv6

Table des matières

Ajoutez de la IPv6 prise en charge pour votre VPC

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

Table des matières

- Étape 4 : Attribuer IPv6 des adresses à vos instances

Step (Étape)	Remarques
Étape 1 : associer un bloc IPv6 CIDR à votre VPC et à vos sous-réseaux	Associez un IPv6 bloc CIDR fourni par Amazon ou BYOIP à votre VPC et à vos sous-réseaux.
Étape 2 : Mettre à jour vos tables de routage	Mettez à jour vos tables de routage pour acheminer votre IPv6 trafic. Pour un sous-rése au public, créez un itinéraire qui achemine tout le IPv6 trafic du sous-réseau vers la passerelle Internet. Pour un sous-réseau privé, créez un itinéraire qui achemine tout le IPv6 trafic Internet depuis le sous-réseau vers une passerelle Internet de sortie uniquement.
Étape 3 : Mettre à jour les règles de votre groupe de sécurité	Mettez à jour les règles de votre groupe de sécurité pour inclure des règles relatives IPv6 aux adresses. Cela permet au IPv6 trafic de circuler vers et depuis vos instances. Si vous avez créé des règles ACL réseau personnal isées pour contrôler le flux de trafic à destinati on et en provenance de votre sous-réseau, vous devez inclure des règles relatives au IPv6 trafic.
Étape 4 : Attribuer IPv6 des adresses à vos instances	Attribuez IPv6 des adresses à vos instances à partir de la plage d' IPv6 adresses de votre sous-réseau.

Étape 1 : associer un bloc IPv6 CIDR à votre VPC et à vos sous-réseaux

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

Pour associer un bloc IPv6 CIDR à un VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Votre VPCs.
3. Sélectionnez votre VPC.
4. Choisissez Actions, Modifier, CIDRs puis choisissez Ajouter un nouveau IPv6 CIDR.
5. Sélectionnez l'une des options suivantes, puis sélectionnez Sélectionner CIDR) :
   - Bloc d'adresse IPv6 CIDR fourni par Amazon : utilisez un bloc d'adresse IPv6 CIDR provenant du pool d'adresses d'Amazon. IPv6 Pour Network Border Group, choisissez le groupe à partir duquel les AWS adresses IP sont publiées.
   - Bloc d'adresse IPv6 CIDR alloué par IPAM : utilisez un bloc d'adresse IPv6 CIDR provenant d'un pool IPAM. Choisissez le pool IPAM et le bloc IPv6 CIDR.
   - IPv6 CIDR que j'appartiens — Utilisez un bloc IPv6 CIDR de votre pool d' IPv6 adresses (BYOIP). Choisissez le pool IPv6 d'adresses et le bloc IPv6 CIDR.
6. Choisissez Fermer.

Pour associer un bloc IPv6 CIDR 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, IPv6 CIDRs puis Ajouter un IPv6 CIDR.
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 de plus amples informations, veuillez consulter IPv6 Blocs d'adresse CIDR VPC.

Étape 2 : Mettre à jour vos tables de routage

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

Vous devez mettre à jour les tables de routage de vos sous-réseaux publics afin de permettre aux instances (telles que les serveurs Web) d'utiliser la passerelle Internet pour le IPv6 trafic. Vous devez également mettre à jour les tables de routage de vos sous-réseaux privés afin de permettre aux instances (telles que les instances de base de données) d'utiliser une passerelle Internet de sortie uniquement pour le IPv6 trafic, car les passerelles NAT ne sont pas prises 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 de plus amples informations, veuillez consulter Activez le IPv6 trafic sortant à l'aide d'une passerelle 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.

> **Note**
>
> Dans une table de routage, une même destination (::/0) ne peut pas pointer simultanément vers une passerelle Internet et une passerelle Internet de sortie uniquement. Si vous recevez un message d'erreur indiquant « Il existe des routes IPv6 existantes avec le saut suivant comme passerelle Internet » lors de la configuration d'une passerelle Internet de sortie uniquement, vous devez d'abord supprimer la IPv6 route existante vers la passerelle Internet avant de l'ajouter à la passerelle Internet de sortie uniquement.

Pour de plus amples informations, veuillez consulter Exemples d'options de routage.

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

Pour permettre à vos instances d'envoyer et de recevoir du trafic IPv6, vous devez mettre à jour les règles de votre groupe de sécurité afin d'inclure des règles relatives IPv6 aux adresses. 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 l'accès HTTP, HTTPS et SSH entrant à partir IPv6 d'adresses. Il n'est pas nécessaire de modifier les règles entrantes de votre groupe de sécurité de base de données ; la règle qui autorise toutes les communications en provenance `sg-11aa22bb11aa22bb1` inclut les IPv6 communications.

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 IPv4 trafic, choisissez Ajouter une règle et configurez la règle pour autoriser le IPv6 trafic correspondant. Par exemple, pour ajouter une règle autorisant le transfert de tout le trafic HTTP 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 IPv6 CIDR 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 pour votre groupe de sécurité, cette règle n'est pas automatiquement ajoutée et vous devez ajouter des règles sortantes équivalentes pour IPv6 le trafic.

Mettre à jour vos règles de liste ACL réseau

Lorsque vous associez un bloc IPv6 CIDR à un VPC, nous ajoutons automatiquement des règles à l'ACL réseau par défaut pour IPv6 autoriser le trafic. Toutefois, si vous avez modifié votre ACL réseau par défaut ou si vous avez créé un ACL réseau personnalisé, vous devez ajouter manuellement des règles pour IPv6 le trafic. Pour plus d'informations, consultez Add and delete rules.

Étape 4 : Attribuer IPv6 des adresses à vos instances

Tous les types d'instances de la génération actuelle sont pris en charge IPv6. Si votre type d'instance n'est pas compatible IPv6, vous devez redimensionner l'instance selon un type d'instance compatible avant de pouvoir attribuer une IPv6 adresse. 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 à des fins d'assistance IPv6, vous pouvez attribuer une IPv6 adresse à votre instance lors du 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' IPv6 adresse est attribuée à l'interface réseau principale (par exemple, eth0) pour l'instance. Pour plus d'informations, consultez la section Attribuer une IPv6 adresse à une instance dans le guide de l'utilisateur Amazon EC2.

Vous pouvez vous connecter à une instance à l'aide de son IPv6 adresse. Pour plus d'informations, consultez Connect to your Linux instance using an SSH client dans le Guide d'utilisation d'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 un ping à une IPv6 adresse depuis votre instance, consultez la documentation de votre système d'exploitation pour la configurer IPv6.

Exemple de configuration VPC à double pile

Avec une configuration à double pile, vous pouvez utiliser à la fois des IPv6 adresses IPv4 et des adresses pour la communication entre les ressources de votre VPC et les ressources via Internet.

Le schéma suivant présente l'architecture de votre VPC. Votre VPC dispose d'un sous-réseau public et d'un sous-réseau privé. Le VPC et les sous-réseaux doivent comporter à la fois un bloc d'adresse

CIDR IPv4 et un bloc d'adresse CIDR IPv6. Il existe une instance EC2 dans le sous-réseau privé qui possède à la fois une IPv4 adresse et une IPv6 adresse. L'instance peut envoyer du IPv4 trafic sortant vers Internet à l'aide d'une passerelle NAT et IPv6 du trafic sortant vers Internet à l'aide d'une passerelle Internet de sortie uniquement.

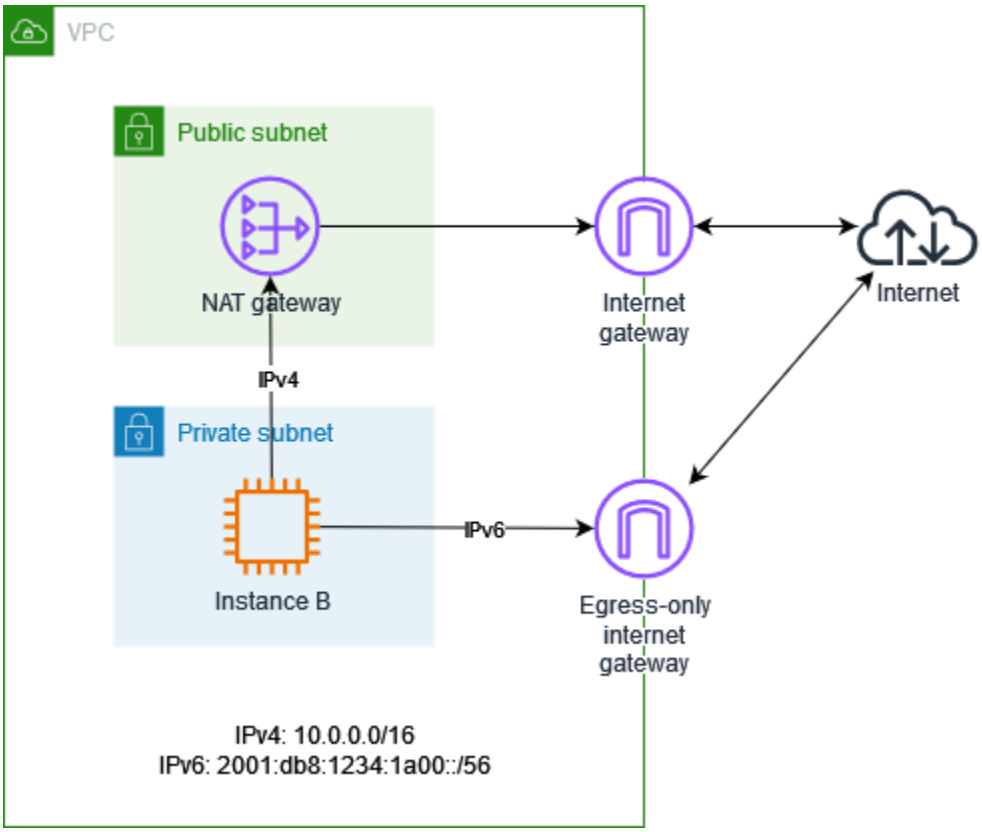


Table de routage pour le sous-réseau public

Voici la table de routage pour le sous-réseau public. Les deux premières entrées correspondent aux routes locales. La troisième entrée envoie tout le trafic IPv4 vers la passerelle Internet. Notez que la quatrième entrée n'est nécessaire que si vous prévoyez de lancer des instances EC2 avec des IPv6 adresses dans le sous-réseau public.

Destination	Target
VPC IPv4 CIDR	local
VPC IPv6 CIDR	locale
0.0.0.0/0	*internet-gateway-id*

Destination	Target
::/0	*internet-gateway-id*

Table de routage pour le sous-réseau privé.

Voici la table de routage pour le sous-réseau privé. Les deux premières entrées correspondent aux routes locales. La troisième entrée envoie tout le IPv4 trafic à la passerelle NAT. La dernière entrée envoie tout le IPv6 trafic vers la passerelle Internet de sortie uniquement.

Destination	Target
VPC IPv4 CIDR	local
VPC IPv6 CIDR	locale
0.0.0.0/0	*nat-gateway-id*
::/0	*egress-only-gateway-id*

AWS des services qui soutiennent 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 pour les adresses IP est IPv6, qui fournit un espace d'adressage plus grand que IPv4.

Services AWS la prise en charge 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 uniquement. IPv6

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 être pris en charge IPv6 via leurs points de terminaison

privés même s'ils ne le font pas IPv6 via leurs points de terminaison publics. Les points de terminaison compatibles IPv6 peuvent répondre aux requêtes DNS avec des enregistrements AAAA.

Des services qui soutiennent IPv6

Le tableau suivant répertorie ceux Services AWS qui fournissent un support double pile, IPv6 uniquement le support, et les points de terminaison qui le prennent en charge IPv6. Nous mettrons à jour ce tableau au fur et à mesure que nous publierons un support supplémentaire pour IPv6. Pour en savoir plus sur le mode de prise en charge d'un service IPv6, reportez-vous à la documentation du service.

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés [1]
AWS Amplify	Oui	Non	Oui	
Amazon API Gateway	Oui	Non	Oui	Oui
AWS App Mesh	Oui	Oui	Oui	Non
AWS App Runner	Oui	Non	Oui	Oui
AWS AppConfig	Oui	Non	Oui	Oui
Application Autoscaling	Non	Non	Oui	Oui
AWS Application Discovery Service	Oui	Non	Oui	Oui
Application Recovery Controller (ARC)	Oui	Non	Oui	
WorkSpaces Applications Amazon	Oui	Non	Non	Non
AWS AppSync[2]	Partielle	Non	Partielle	Oui
Amazon Athena	Oui	Non	Oui	Oui

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés 1
AWS Audit Manager	Non	Non	Oui	Oui
Amazon Aurora	Oui	Non	Oui	Non
Amazon Aurora DSQL	Non	Non	Oui	Oui
AWS Auto Scaling	Non	Non	Oui	Oui
AWS B2B Échange de données	Oui	Non	Oui	Oui
AWS Backup	Oui	Non	Oui	Oui
AWS Batch	Oui	Non	Oui	Oui
Amazon Bedrock	Non	Non	Oui	Oui
AWS Billing and Cost Management Exportations de données	Oui	Non	Oui	Oui
AWS Billing and Cost Management Calculateur de prix	Oui	Non	Oui	Oui
AWS Billing Conductor	Oui	Non	Oui	Oui
AWS Budgets	Oui	Non	Oui	
Amazon Braket	Oui	Oui	Oui	Oui
AWS Certificate Manager	Oui	Non	Oui	Non
Kit SDK Amazon Chime	Oui	Non	Oui	
Amazon Comprehend	Oui	Oui	Oui	Oui

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés 1
AWS Clean Rooms	Oui	Oui	Oui	Oui
AWS Clean Rooms ML	Oui	Oui	Oui	Oui
AWS Cloud9	Oui	Non	Oui	
API de commande du Cloud AWS	Oui	Non	Oui	Oui
CloudFormation	Non	Non	Oui	Oui
Amazon CloudFront	Oui	Oui	Oui	
AWS CloudHSM	Oui	Non	Oui	Oui
AWS CloudTrail	Oui	Non	Oui	Oui
Amazon CloudWatch	Oui	Oui	Oui	Oui
Informations sur les CloudWatch applications Amazon	Non	Non	Oui	Oui
Amazon CloudWatch Internet Monitor	Non	Non	Oui	Oui
Amazon CloudWatch Logs	Oui	Oui	Oui	Oui
Gestionnaire d'accès Amazon CloudWatch Observability	Oui	Oui	Oui	
Amazon CloudWatch Synthetics	Oui	Non	Oui	Oui

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés [1]
AWS Cloud Map	Oui	Oui	Oui	Oui
AWS Réseau WAN dans le cloud	Oui	Non	Oui	Non
AWS CodeArtifact	Oui	Non	Oui	Oui
Profils des clients Amazon Connect	Oui	Non	Oui	Oui
AWS CodeBuild	Non	Non	Oui	Oui
AWS CodeCommit	Non	Non	Oui	Oui
AWS CodeDeploy	Non	Non	Oui	Oui
Optimiseur de calcul AWS	Non	Non	Oui	Oui
Amazon Comprehend Medical	Non	Non	Oui	Oui
Amazon CodeGuru Profiler	Oui	Non	Oui	Oui
Amazon Cognito	Oui	Non	Oui	
AWS Config	Non	Non	Oui	Oui
AWS Control Tower	Non	Non	Oui	Oui
AWS Cost Explorer	Oui	Non	Oui	Oui
Hub d'optimisation des coûts AWS	Oui	Non	Oui	Oui
AWS Data Exchange	Non	Non	Oui	Oui

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés 1
Amazon Data Firehose	Non	Non	Oui	Oui
Amazon Data Lifecycle Manager	Oui	Non	Oui	Oui
AWS Database Migration S	Oui	Non	Non	Oui
AWS DataSync	Oui	Oui	Oui	Oui
Amazon DataZone	Non	Non	Oui	Oui
AWS Deadline Cloud	Oui	Non	Oui	Oui
Amazon Detective	Oui	Oui	Oui	
Direct Connect	Oui	Oui	Non	Oui
Directory Service	Non	Non	Oui	Oui
Amazon EBS direct APIs	Oui	Non	Oui	Oui
Amazon EC2	Oui	Oui	Oui	Non
EC2 Image Builder	Oui	Oui	Oui	Oui
Amazon ECR	Oui	Non	Oui	Non
Amazon ECS	Oui	Oui	Oui	Oui
Amazon EFS	Oui	Oui	Oui	Oui
Amazon EKS	Partielle	Partielle	Oui	Oui
Amazon EMR	Non	Non	Oui	Oui
AWS Elastic Beanstalk	Oui	Non	Oui	Oui

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés 1
AWS Elastic Disaster Recovery	Non	Non	Oui	Oui
Elastic Load Balancing	Partielle	Partielle	Oui	Non
Amazon ElastiCache	Oui	Oui	Non	Oui
AWS Elemental MediaConvert	Non	Non	Oui	Oui
AWS Elemental MediaConnect	Oui	Oui	Oui	Partielle
AWS Messagerie sociale destinée aux utilisateurs finaux	Oui	Non	Oui	Non
Résolution des entités AWS	Oui	Non	Oui	Oui
Amazon EventBridge	Non	Non	Oui	Oui
AWS Fargate	Oui	Non	Oui	Oui
Amazon FSx	Non	Non	Oui	Oui
Amazon GameLift Streams	Oui	Non	Oui	Oui
AWS Global Accelerator	Oui	Non	Oui	
AWS Glue	Oui	Non	Non	Oui
AWS Glue DataBrew	Non	Non	Oui	Oui

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés [1]
Amazon Managed Grafana [3]	Oui	Non	Oui	Oui
AWS Ground Station [4]	Oui	Non	Oui	Oui
Amazon GuardDuty	Non	Non	Oui	Oui
AWS HealthImaging	Non	Non	Oui	Oui
AWS HealthLake	Non	Non	Oui	Oui
AWS HealthOmics	Non	Non	Oui	Oui
Gestion des identités et des accès AWS (JE SUIS)	Oui	Oui	Oui	Non
AWS Analyseur d'accès IAM	Oui	Non	Oui	Oui
AWS IAM Identity Center	Oui	Non	Oui	
AWS Rôles IAM n'importe où	Non	Non	Oui	Oui
Amazon Inspector	Oui	Oui	Oui	Oui
Amazon Interactive Video Service (IVS) [5]	Oui	Non	Oui	Oui
AWS IoT Core	Oui	Non	Oui	Oui
AWS IoT Device Defender	Oui	Non	Oui	Non

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés 1
AWS IoT Device Management	Oui	Non	Oui	Non
AWS IoT FleetWise	Oui	Non	Oui	Oui
AWS IoT Greengrass	Oui	Non	Oui	Non
AWS IoT SiteWise	Oui	Non	Oui	Oui
AWS IoT TwinMaker	Oui	Non	Oui	Oui
AWS IoT Wireless	Oui	Non	Oui	Oui
Amazon Kendra	Non	Non	Oui	Non
AWS Key Management Service	Oui	Partielle	Oui	Oui
Amazon Keyspaces	Oui	Oui	Oui	Oui
Amazon Keyspaces CDC streams	Oui	Oui	Oui	Oui
Amazon Kinesis Data Streams	Oui	Non	Oui	Oui
AWS Lake Formation	Non	Non	Non	Oui
AWS Lambda	Oui	Non	Oui	Oui
AWS Launch Wizard	Non	Non	Oui	Oui
AWS License Manager	Non	Non	Oui	Oui
Amazon Lightsail	Oui	Oui	Oui	Oui

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés [1]
Amazon Location Service	Non	Non	Oui	Oui
Amazon MQ	Non	Non	Oui	Oui
Amazon MWAA	Non	Non	Oui	Oui
Amazon Macie	Oui	Non	Oui	Oui
AWS Mainframe Modernization	Oui	Non	Oui	Oui
Amazon Managed Grafana	Non	Non	Oui	Oui
Amazon Managed Service for Prometheus	Oui	Non	Oui	Oui
Orchestrateur de l'AWS Migration Hub	Non	Non	Oui	Oui
AWS Network Firewall	Oui	Oui	Non	Oui
AWS Network Manager	Oui	Non	Oui	Non
Amazon OpenSearch Service	Oui	Non	Oui	
AWS Organizations	Oui	Non	Oui	Oui
AWS Outposts	Non	Non	Oui	Oui
Amazon Personalize	Oui	Non	Oui	Oui
Amazon Pinpoint	Oui	Non	Oui	Oui
Amazon Polly	Oui	Non	Oui	Oui

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés [1]
AWS Price List	Non	Non	Oui	Non
AWS Autorité de certification privée	Oui	Non	Oui	Oui
AWS CA privée Connecteur pour Active Directory	Oui	Non	Oui	Oui
AWS CA privée Connecteur pour SCEP	Oui	Non	Oui	Oui
AWS PrivateLink	Oui	Oui	Oui	
Amazon Q Business	Non	Non	Oui	Non
Amazon RDS	Oui	Non	Oui	Non
Amazon RDS Data API	Non	Non	Oui	Oui
Amazon RDS Performance Insights	Non	Non	Oui	Oui
Amazon Redshift	Oui	Non	Oui	
Amazon Rekognition	Non	Non	Oui	Oui
Corbeille	Oui	Non	Oui	Oui
AWS re:Post privé	Oui	Non	Oui	Oui
AWS Resource Access Manager	Oui	Non	Oui	Oui
Explorateur de ressources AWS	Oui	Non	Oui	Non

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés 1
Groupes de ressources AWS	Oui	Oui	Oui	Oui
AWS Resource Groups Tagging API	Oui	Oui	Oui	Oui
Amazon Route 53	Oui	Oui	Oui	Oui
Amazon S3	Oui	Non	Oui	Non
Amazon S3 sur Outposts	Non	Non	Oui	Non
Amazon SageMaker	Non	Non	Oui	Oui
AWS Secrets Manager	Oui	Non	Oui	Oui
AWS Security Hub	Non	Non	Oui	Oui
Amazon Security Lake	Oui	Non	Oui	Oui
AWS Security Token Service	Oui	Non	Oui	Oui
AWS Service Catalog	Non	Non	Oui	Oui
AWS Shield	Oui	Oui	Non	Oui
Amazon Simple Email Ser	Oui	Non	Oui	Oui
Amazon Simple Notification Service	Oui	Non	Oui	Oui
Amazon Simple Queue Service	Oui	Non	Oui	Oui

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés [1]
Amazon Simple Workflow Service	Oui	Non	Oui	Oui
AWS Site-to-Site VPN	Oui	Non	Oui	Non
AWS Snow Family	Non	Non	Oui	
AWS Step Functions	Oui	Non	Oui	Oui
AWS Storage Gateway	Oui	Oui	Oui	Oui
AWS Systems Manager	Non	Non	Oui	Oui
AWS Systems Manager Incident Manager	Non	Non	Oui	Oui
AWS Systems Manager pour SAP	Non	Non	Oui	Oui
Amazon Textract	Non	Non	Oui	Oui
Amazon Timestream	Non	Non	Oui	Oui
Amazon Transcribe	Oui	Oui	Oui	Oui
AWS Transfer Family [6]	Oui	Non	Oui	Oui
AWS Transit Gateway	Oui	Non	Oui	Non
Amazon Translate	Oui	Oui	Oui	Oui
AWS Trusted Advisor	Non	Non	Oui	Oui
Notifications des utilisateurs AWS	Non	Non	Oui	Oui

Nom du service	Prise en charge de la double pile	IPv6 support uniquement	Support pour les terminaux publics IPv6	Support IPv6 pour les terminaux privés [1]
Amazon Verified Permissions	Oui	Non	Oui	Oui
VMware Cloud activé AWS	Non	Non	Oui	Oui
Amazon VPC	Oui	Oui	Oui	Non
Amazon VPC Lattice	Non	Non	Oui	Oui
AWS WAF	Oui	Oui	Non	
AWS WAFV2	Non	Non	Oui	Oui
AWS Well-Architected Tool	Non	Non	Oui	Oui
Amazon WorkMail	Non	Non	Oui	Oui
Amazon WorkSpaces	Oui	Non	Oui	Oui
AWS X-Ray	Oui	Non	Oui	Oui

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

[2] Cette entrée représente la IPv6 prise en charge des opérations de configuration de AWS AppSync GraphLQL et d'Event API, via l'API AWS AppSync SDK. IPv6 n'est pas pris en charge pour les connexions client à AWS AppSync GraphQL et Event gérés par le client. APIs

[3] Cette entrée représente la prise en IPv6 charge des opérations de gestion de l'espace de travail Grafana, telles que la mise à jour des espaces de travail et des autorisations de l'espace de travail. Les opérations générales de l'espace de travail Grafana, telles que la création et la modification de tableaux de bord ou l'interrogation de sources de données, ne sont pas prises en IPv6 charge.

[4] Cette entrée représente la IPv6 prise en charge des opérations du plan de AWS Ground Station contrôle, telles que l'appel de l'AWS Ground Station API. IPv6 n'est pas pris en charge par le plan de

AWS Ground Station données. Assurez-vous donc que les ressources auxquelles vous transmettez des données (telles que les instances Amazon EC2) sont accessibles sur ce site. IPv4

[5] Cette entrée représente la IPv6 prise en charge des opérations du plan de contrôle Amazon IVS, telles que l'appel d'un point de terminaison IVS.

[6] Pour plus de détails sur l' IPv6 assistance dans AWS Transfer Family, consultez la section IPv6 Restrictions.

IPv6 Support supplémentaire

Calcul

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

Développement de jeux

- Amazon GameLift Streams prend en charge le streaming IPv6 sur le runtime Microsoft Windows Server 2022 Base.

Réseau et diffusion de contenu

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

Sécurité, identité et conformité

- Amazon Detective prend en charge IPv6 les adresses dans ses résultats liés au réseau et dans ses profils d'entités.
- Gestion des identités et des accès AWS (IAM) prend en charge les IPv6 adresses dans les politiques basées sur l'identité IAM.
- Amazon Macie prend en charge les IPv6 adresses dans les informations personnelles identifiables (PII).

- Amazon Security Lake prend en charge les IPv6 adresses pour toutes les opérations sur les sources de journaux et les abonnés.

Gestion et gouvernance

- AWS CloudTrail les dossiers contiennent des IPv6 informations sur la source.
- AWS CLI La v2 prend en charge le téléchargement via IPv6 des connexions pour les clients IPv6 uniquement.

En savoir plus

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

Configurer un cloud privé virtuel

Amazon Virtual Private Cloud (VPC) est un élément fondamental qui vous permet de mettre en service un réseau virtuel logiquement isolé au sein du cloud AWS. En créant votre propre VPC, vous obtenez un contrôle total sur l'environnement réseau, y compris la possibilité de définir des plages d'adresses IP, des sous-réseaux, des tables de routage et des options de connectivité.

Votre compte AWS contient un VPC par défaut pour chaque région AWS. Ce VPC par défaut est préconfiguré avec des paramètres qui en font une option pratique pour lancer rapidement des ressources. Cependant, le VPC par défaut ne correspond pas toujours à vos besoins à long terme de mise en réseau. C'est là qu'il peut être avantageux de créer des VPC supplémentaires.

La création de VPC supplémentaires présente plusieurs avantages par rapport au VPC par défaut fourni avec chaque nouveau compte AWS. Avec un VPC autogéré, vous pouvez concevoir votre topologie réseau en fonction de vos besoins spécifiques, qu'il s'agisse de mettre en œuvre une application multiniveau, de vous connecter à des ressources sur site ou de séparer les charges de travail par département ou unité commerciale.

En outre, la création de plusieurs VPC peut renforcer la sécurité et l'isolation entre vos différentes applications ou unités commerciales. Chaque VPC agit comme un réseau virtuel distinct, vous permettant d'appliquer des politiques de sécurité, des configurations de routage et des contrôles d'accès distincts et adaptés à chaque environnement.

Enfin, la décision d'utiliser le VPC par défaut ou de créer un ou plusieurs VPC personnalisés doit être basée sur les exigences spécifiques de votre application, vos besoins de sécurité et vos objectifs de capacité de mise à l'échelle à long terme. Investir le temps nécessaire pour concevoir judicieusement votre infrastructure VPC peut porter ses fruits sous la forme d'une base de réseau cloud robuste, sécurisée et adaptable.

Table des matières

- Jeux d'options DHCP dans Amazon VPC
- Attributs DNS pour votre VPC
- Utilisation des adresses réseau pour votre VPC
- Partager vos sous-réseaux VPC avec d'autres comptes
- Étendre un VPC à une zone locale, une zone Wavelength ou Outpost
- Supprimer votre VPC
- Générez des infrastructure-as-code actions à partir de votre console VPC avec Console-to-Code

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, consultez Sous-réseaux.

Table des matières

Plage d'adresses IP de VPC

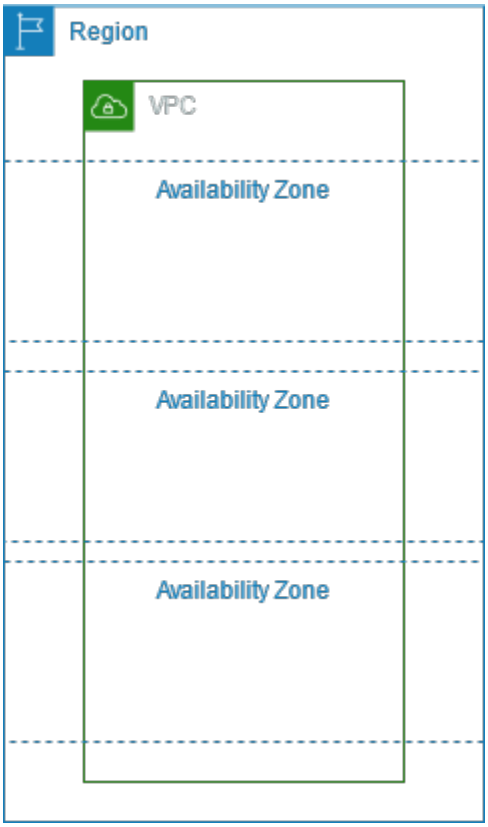
Lorsque vous créez un VPC : vous spécifiez ses adresses IP comme suit :

- 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, consultez Adressage IP pour votre réseau VPCs et vos 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

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 de plus amples informations, consultez Adressage IP pour votre réseau VPCs et vos 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 de plus amples 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, consultez 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 des ressources AWS, 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 que la location du VPC soit `Default`, les instances EC2 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 AWS Outposts, votre Outpost nécessite une connectivité privée ; vous devez utiliser la location `Default`.

Par défaut VPCs

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. Par conséquent, vous pouvez immédiatement lancer des EC2 instances Amazon 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

Composants du VPC par défaut

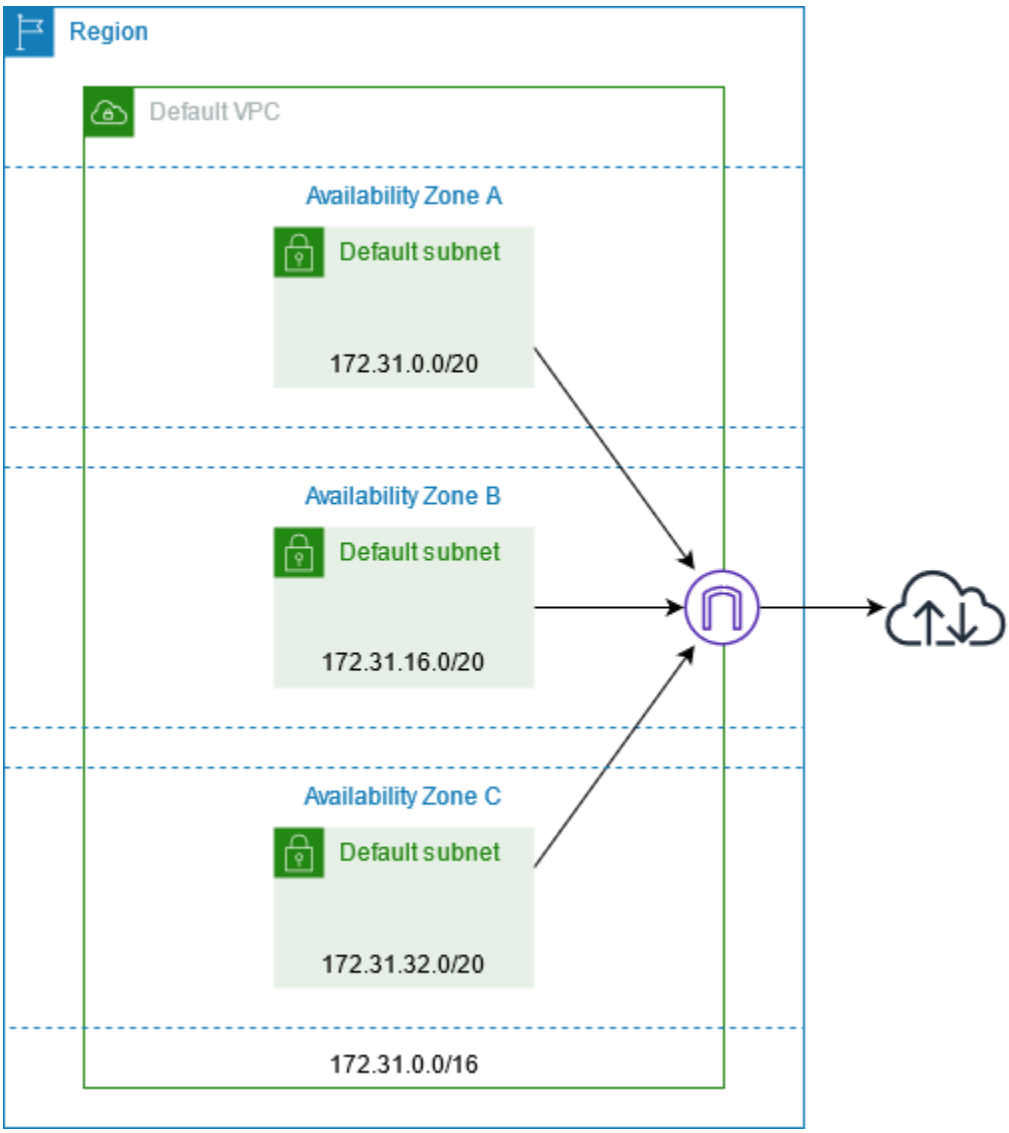
Lorsque nous créons un VPC par défaut, nous le configurons pour vous en procédant comme suit :

- Créez un VPC avec un bloc `/16` IPv4 CIDR de taille (). `172.31.0.0/16` Cela fournit jusqu'à 65 536 adresses privées. IPv4
- 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.

- Associez les options DHCP par défaut définies pour votre AWS compte 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 avez une politique IAM qui refuse la possibilité d'appeler CreateInternetGateway, puis que vous appelez CreateDefaultVpc, la passerelle Internet du VPC par défaut est toujours créée. Pour empêcher Amazon de créer une passerelle Internet, vous devez refuser CreateDefaultVpc et CreateInternetGateway.
> - Pour bloquer tout le trafic à destination et en provenance des passerelles Internet de votre compte, consultez Bloquer l'accès public aux sous-réseaux VPCs et aux sous-réseaux.

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 AWS Site-to-Site VPN des connexions.
- Ajoutez d'autres blocs IPv4 CIDR.
- Accès VPCs dans 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 .

Vous pouvez utiliser un sous-réseau par défaut comme n'importe quel autre sous-réseau ; ajoutez des tables de routage personnalisées et définissez le réseau. ACLs Vous pouvez également spécifier un sous-réseau par défaut spécifique lorsque vous lancez une EC2 instance.

Vous pouvez éventuellement associer un bloc IPv6 CIDR à votre VPC par défaut.

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, dans ce cas, aucune EC2 instance 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 IPv4 adresse publique et une IPv4 adresse privée, ainsi que des noms d'hôte DNS publics et privés. Les instances que vous lancez dans un sous-réseau autre que celui par défaut d'un VPC par défaut ne reçoivent pas d' IPv4 adresse publique ni de nom d'hôte DNS. Vous avez la possibilité de modifier le comportement de votre sous-réseau concernant les adresses IP publiques. Pour de plus amples informations, veuillez consulter Modifier les attributs d'adressage IP de votre sous-réseau.

De temps à autre, une nouvelle zone de disponibilité AWS peut être ajoutée 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.

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

Cette section explique comment utiliser les sous-réseaux par défaut VPCs et par défaut.

Table des matières

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 à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Votre VPCs.
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 le 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 le 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 à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Votre VPCs.
3. Sélectionnez Actions, puis Create Default VPC.
4. Choisissez Créer. Fermez l'écran de confirmation.

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

Vous pouvez utiliser la commande create-default-vpc AWS CLI . 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 PowerShell commande New-EC2DefaultVpcTools for Windows ou l'action CreateDefaultVpcAmazon EC2 API.

Créer un sous-réseau par défaut

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

Vous pouvez créer un sous-réseau par défaut dans une zone de disponibilité qui n'en comporte pas. Par exemple, vous souhaiterez peut-être créer un sous-réseau par défaut si vous avez supprimé un sous-réseau par défaut ou si vous avez ajouté AWS une nouvelle zone de disponibilité sans créer automatiquement de 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 `/20` IPv4 CIDR de taille dans le prochain espace contigu disponible de 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 IPv4 CIDR à votre VPC.

Si vous avez associé un bloc d' IPv6 adresse CIDR à votre VPC par défaut, le nouveau sous-réseau par défaut ne reçoit IPv6 pas automatiquement de bloc d'adresse CIDR. Au lieu de cela, vous pouvez associer un bloc IPv6 CIDR au sous-réseau par défaut après l'avoir créé. Pour de plus amples informations, veuillez consulter Ajouter ou supprimer un bloc d'adresse CIDR IPv6 de votre sous-réseau.

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

Utilisez la create-default-subnet AWS CLI commande 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 plus d'informations sur la configuration du AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur.

Vous pouvez également utiliser la PowerShell commande New-EC2DefaultSubnetTools for Windows ou l'action CreateDefaultSubnetAmazon EC2 API.

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 ou VPC par défaut, vous devez

spécifier explicitement un sous-réseau dans l'un de VPCs vos sous-réseaux lorsque vous lancez 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 les attributs d'adressage IP 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 la modification d'un VPC, consultez the section called "Ajouter ou supprimer un bloc d'adresse CIDR".

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 Resources to create (Ressources à créer), choisissez VPC and more (VPC et autres).
4. Maintenez l'option Génération automatique de balise 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 que la location du VPC soit `Default`, les instances EC2 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 AWS Outposts, votre Outpost nécessite 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 AWS les 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 AWS les 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 de plus amples informations, consultez Tarification des passerelles NAT.

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 plus d'informations, consultez Points de terminaison de 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 de plus amples 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. IPAM est une fonction VPC qui facilite la planification, le suivi et le contrôle des adresses IP pour vos charges de travail AWS. 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. Si vous utilisez le bloc CIDR IPv6 alloué par l'IPAM pour fournir des CIDR IPv6 aux VPC, vous bénéficiez de CIDR IPv6 contigus pour la création de VPC. Les CIDR contigus sont alloués de manière séquentielle. Ils vous permettent de simplifier vos règles de sécurité et de mise en réseau. Les CIDR IPv6 peuvent être regroupés au sein d'une seule entrée dans les structures de réseau et de sécurité telles que les listes de contrôle d'accès, les tables de routage, les groupes de sécurité et les pare-feu.

     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 Groupe de bordures réseau, sélectionnez le groupe à partir duquel AWS publie les adresses IP. 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 la manière d'apporter vos propres plages d'adresses IP à AWS, consultez Apporter vos propres adresses IP (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 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.

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 que la location du VPC soit `Default`, les instances EC2 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 AWS Outposts, votre Outpost nécessite 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 de plus amples informations, consultez Création d'un sous-réseau.

Créer un VPC à l'aide de l'AWS CLI

La procédure suivante contient des exemples de commandes AWS CLI permettant de créer un VPC ainsi que les ressources VPC supplémentaires nécessaires à l'exécution d'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 l'AWS CLI, vous êtes invité à entrer des informations d'identification AWS. 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}]
```

Créer un VPC et des ressources VPC à l'aide de la 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
   ```

Visualiser les ressources de votre VPC

Cette section explique comment 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 représentés en vert.
  - Les sous-réseaux privés sont représentés en bleu.

- 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 à l'adresse 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 la passerelle, il existe une ressource de point de terminaison de passerelle avec le nom du service AWS (Amazon S3 ou Amazon DynamoDB) auquel 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 ou supprimer un bloc d'adresse CIDR de votre VPC

Cette section décrit comment ajouter ou supprimer des blocs d'adresse CIDR IPv4 et IPv6 d'un VPC.

⚠ Important

- Votre VPC peut avoir jusqu'à cinq blocs d'adresse CIDR IPv4 et cinq blocs d'adresse CIDR IPv6 par défaut, mais cette limite est réglable. Pour de plus amples informations, consultez Quotas Amazon VPC. Pour plus d'informations sur les restrictions concernant les blocs d'adresse CIDR pour un VPC, consultez Blocs CIDR 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.
- 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 ajouter ou supprimer un bloc d'adresse CIDR 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 Vos VPC.
3. Sélectionnez le VPC et choisissez Actions, puis Modifier les blocs d'adresse CIDR.
4. Pour supprimer un CIDR, choisissez Supprimer en regard du CIDR.
5. Pour ajouter CIDR, choisissez Ajouter un nouveau CIDR IPv4 ou Ajouter un nouveau CIDR IPv6.
6. Pour ajouter un CIDR pour un 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.
   - Choisissez Enregistrer.
7. Pour ajouter un CIDR pour un bloc d'adresse CIDR IPv6 , effectuez les 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 Groupe de bordures réseau, sélectionnez le groupe à partir duquel AWS publie les adresses IP. 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, consultez Apportez vos propres adresses IP (BYOIP) vers 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.
  - Choisissez Sélectionner le CIDR lorsque vous avez terminé.

8. Choisissez Fermer.
9. Si vous avez ajouté un bloc d'adresse CIDR à votre VPC, vous pouvez créer des sous-réseaux qui utilisent le nouveau bloc d'adresse CIDR. Pour de plus amples informations, consultez Création d'un sous-réseau.

Pour associer ou dissocier un bloc d'adresse CIDR d'un VPC à l'aide de l'AWS CLI

Utilisez les commandes associate-vpc-cidr-block et 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 « AmazonProvidedDNS » est explicitement mentionné dans le jeu d'options DHCP. Si « AmazonProvidedDNS » est absent du jeu d'options, le serveur DHCP IPv4 ne renvoie pas d'adresse, que d'autres serveurs de noms IPv4 soient mentionnés ou non dans le jeu d'options.

Les serveurs DHCP Amazon peuvent également fournir un préfixe IPv4 ou IPv6 complet à une interface réseau de votre VPC à l'aide de la délégation de préfixes (consultez Attribution 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 d'IMDS (consultez Catégories de métadonnées d'instance 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 jeu d'options DHCP n'est configuré pour votre VPC :

- Pour les instances EC2 basées sur Nitro System, AWS configure `169.254.169.253` comme serveur de noms de domaine par défaut.

- Pour les instances EC2 basées sur Xen, aucun serveur de noms de domaine n'est configuré, et puisque les instances du VPC n'ont accès à aucun serveur DNS, elles n'ont pas accès 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 :

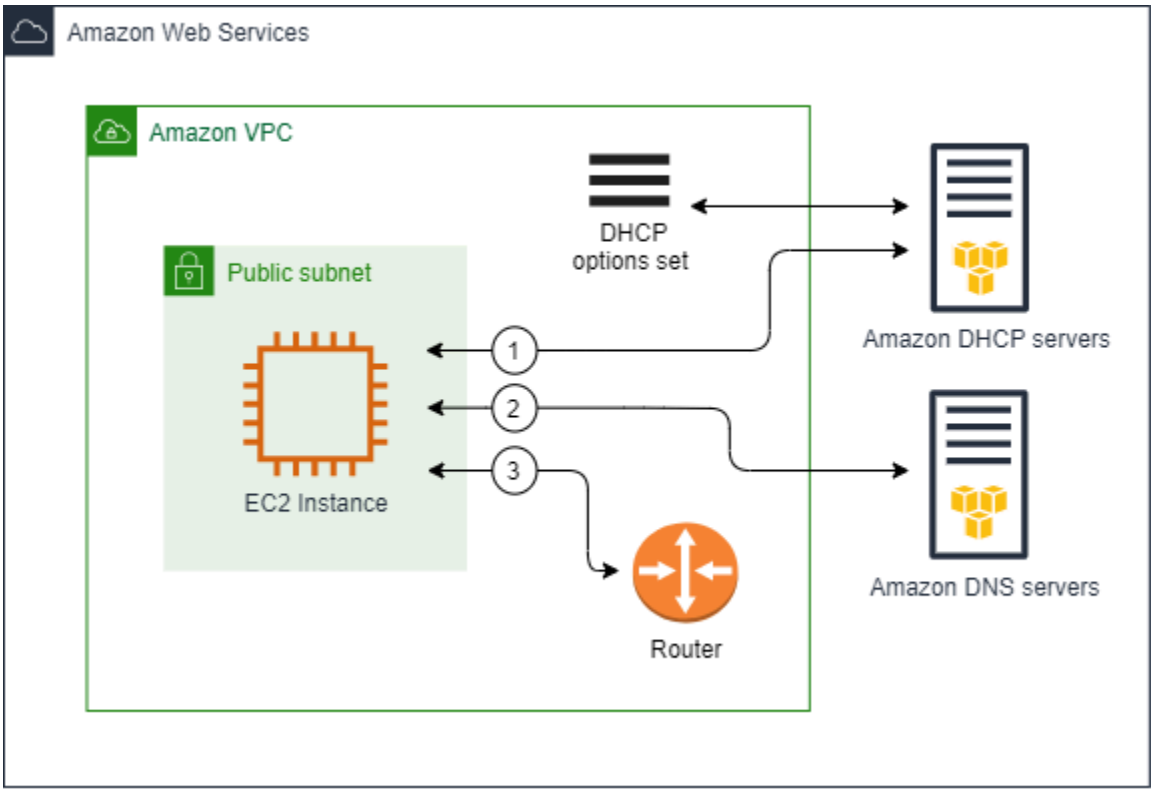
- Serveurs de noms de domaine : les serveurs DNS que vos interfaces réseau utilisent pour la résolution des noms de domaine. Pour un jeu d'options DHCP par défaut, il s'agit toujours d'`AmazonProvidedDNS`. Pour de plus amples informations, consultez Serveur Amazon DNS.
- Nom de domaine : le nom de domaine 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 pour IPv6 : fréquence à laquelle une instance en cours d'exécution à laquelle un IPv6 est attribué est renouvelée par le protocole DHCPv6. Le durée de location par défaut est de 140 secondes. Le renouvellement de la location 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.



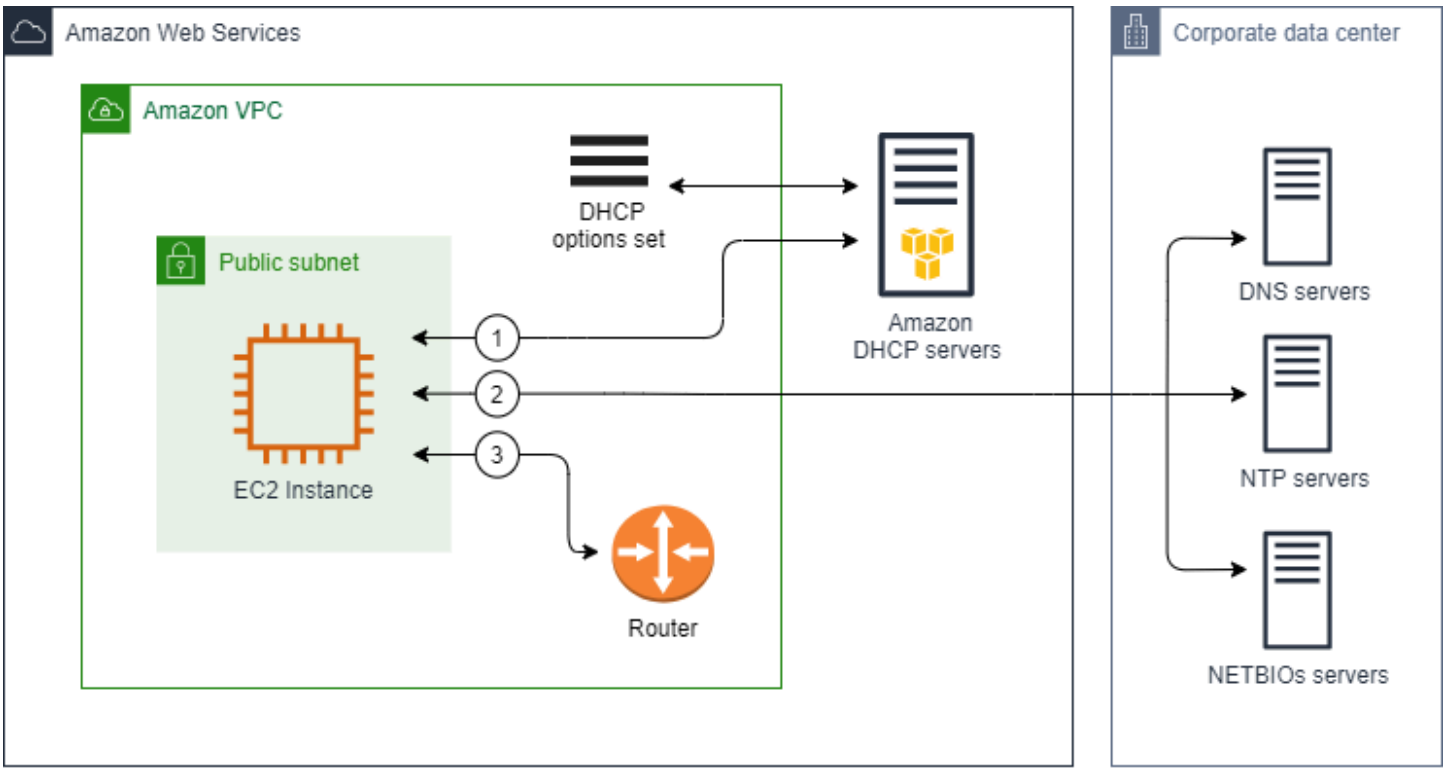
Jeu d'options DHCP personnalisé

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 pour 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 indiquée, la valeur par défaut est de 140 secondes. Si vous utilisez l’adressage à long terme pour les instances EC2, vous pouvez augmenter la durée de location et éviter de fréquentes demandes de renouvellement de location. Le renouvellement de la location 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

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

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.

   - Nom de domaine (facultatif) : entrez le nom de domaine qu'un client devra utiliser lors de la résolution de noms d'hôte à l'aide du système DNS. Si vous n'utilisez pas AmazonProvidedDNS, vos serveurs de noms de domaine personnalisés doivent résoudre le nom d'hôte si nécessaire. Si vous utilisez une zone hébergée privée Amazon Route 53, vous pouvez utiliser AmazonProvidedDNS. Pour de plus amples informations, consultez Attributs DNS pour votre VPC.

     > **Note**
     >
     > Utilisez uniquement des noms de domaine que vous contrôlez entièrement.

     Certains systèmes d'exploitation Linux acceptent plusieurs noms de domaines séparés par des espaces. Cependant, Windows et d'autres systèmes d'exploitation Linux traitent la valeur

comme un domaine unique, ce qui donne lieu à un comportement inattendu. Si votre jeu d'options DHCP est associé à un VPC qui dispose d'instances qui exécutent les 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 AmazonProvidedDNS et le serveur Amazon DNS, consultez Serveur Amazon DNS.

  > **Important**
  >
  > Si votre VPC possède une passerelle Internet, veillez à spécifier votre propre serveur DNS ou le serveur Amazon DNS (AmazonProvidedDNS) pour la valeur Serveurs de nom 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 de synchronisation temporelle d'Amazon, consultez Régler 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 à 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 pour 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 indiquée, la valeur par défaut est de 140 secondes. Si vous utilisez l'adressage à long terme pour les instances EC2, vous pouvez augmenter la durée de location et éviter de fréquentes demandes de renouvellement de location. Le renouvellement de la location 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

- 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

- 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 de plus amples 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

- 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 votre réseau VPCs et vos 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

Comprendre Amazon DNS

En tant qu'architecte ou administrateur AWS, l'un des composants de mise en réseau fondamentaux que vous rencontrerez est le serveur Amazon DNS, également connu sous le nom de Route 53 Resolver. Ce service de résolution DNS est intégré de manière native dans chaque zone de disponibilité de votre région AWS, fournissant une solution fiable et évolutive pour la résolution de noms de domaine au sein de votre cloud privé virtuel (VPC). Dans cette section, vous découvrirez les adresses IP du serveur Amazon DNS, les noms d'hôte DNS privés qu'il peut résoudre et les règles qui régissent son utilisation.

Table des matières

Serveur Amazon DNS

Route 53 Resolver (également appelé « serveur DNS Amazon » ou « AmazonProvidedDNS ») est un service de résolveur DNS intégré à chaque Zone de dDisponibilité d'une région AWS. 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 `2001:db8::/32`, 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 Route 53 Resolver en mode privé et ne sont pas visibles sur le réseau. Dans un sous-réseau IPv6 uniquement, l'adresse locale du lien IPv4 (169.254.169.253) est toujours accessible tant que « AmazonProvidedDNS » est le serveur de noms dans le jeu d'options DHCP.

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 Types de noms d'hôte des instances Amazon EC2 dans le Guide de l'utilisateur Amazon 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 des instances EC2

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 de plus amples informations, consultez Attributs DNS pour votre VPC.

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

Nom DNS IPv4 privé

Le nom d'hôte DNS IPv4 privé d'une instance est résolu en son adresse IPv4 privée. Vous pouvez utiliser le nom d'hôte DNS IPv4 privé pour les communications entre les instances d'un même VPC

ou de VPC connectés. Pour plus d'informations, consultez Private IPv4 addresses dans le Guide d'utilisation d'Amazon EC2.

Nom DNS IPv4 public

Le nom d'hôte DNS IPv4 public d'une instance est résolu en son adresse IPv4 publique (en dehors du réseau de l'instance) et en son adresse IPv4 privée (au sein du réseau de l'instance). Pour plus d'informations, consultez Public IPv4 addresses dans le Guide d'utilisation d'Amazon EC2.

Pour résoudre les noms DNS IPv4 publics en adresses IPv4 privées via une connexion d'appairage de VPC, 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.

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 plus d'informations sur RBN, consultez EC2 instance hostname types dans le Guide d'utilisation d'Amazon EC2.

Attributs DNS pour 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.

Attribut	Description
	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 l'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 de plus amples informati ons, consultez Serveur Amazon DNS. La valeur par défaut de cet attribut est `true`. Notez les règles et considérations relatives à l'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 serveur Route 53 Resolver 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.
  - Le serveur Route 53 Resolver ne peut pas 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 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`.
- Le serveur Route 53 Resolver peut résoudre 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

trouve en dehors des plages d'adresses IPv4 privées spécifiées par la RFC 1918. Toutefois, si vous avez créé votre VPC avant le mois d'octobre 2016, le serveur Route 53 Resolver ne résout pas les noms d'hôte DNS privés lorsque la plage d'adresses IPv4 de votre VPC se situe en dehors de ces plages. Pour activer la prise en charge correspondante, contactez Support.

Quotas DNS

Il existe une limite de 1 024 paquets par seconde (PPS) pour les services qui utilisent des adresses lien-local. Cette limite inclut l'ensemble des requêtes DNS de Route 53 Resolver, des demandes du service de métadonnées d'instance (IMDS), des demandes de NTP (Amazon Time Service Network Time Protocol) et des demandes de Windows Licensing Service (pour les instances basées sur Microsoft Windows). 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 Récupérer les métadonnées d'instance dans le Guide de l'utilisateur Amazon EC2.

Zones hébergées privées

Si vous souhaitez accéder aux ressources de votre VPC à l'aide de noms de domaine DNS personnalisés (comme `example.com`) au lieu d'utiliser des adresses IPv4 privées ou des noms d'hôte DNS privés fournis par AWS, 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`.

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. Il est important de connaître ces noms d'hôtes pour vous connecter à vos ressources.

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

- 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 :

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

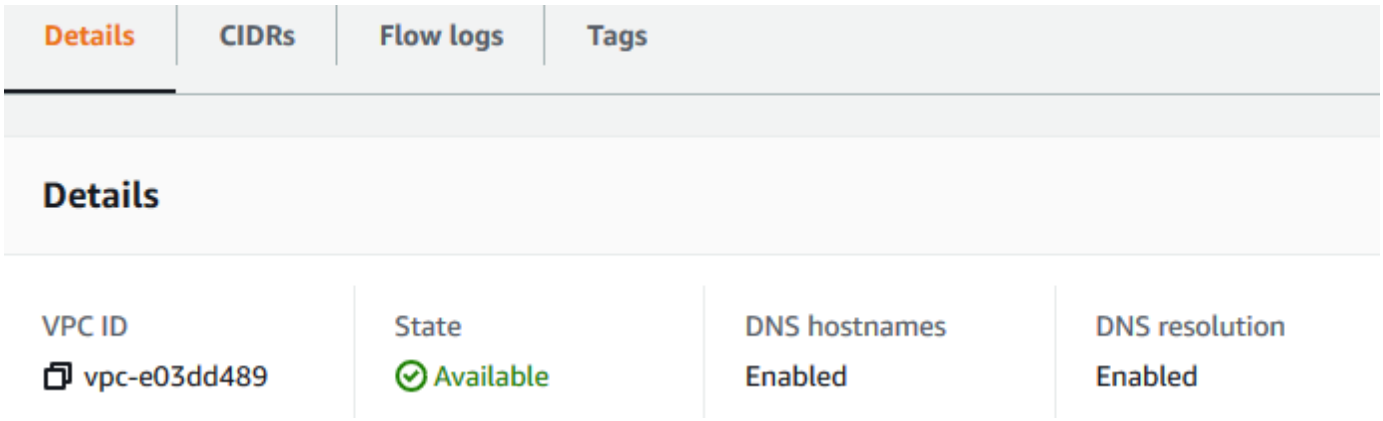
Afficher et mettre à jour les attributs DNS pour votre VPC

Vous pouvez afficher et mettre à jour les attributs de support DNS pour votre VPC à l'aide de la console Amazon VPC. Ces paramètres déterminent si vos instances obtiennent des noms d'hôte DNS publics et si le serveur Amazon DNS peut résoudre vos noms DNS privés. La bonne configuration de ces attributs est essentielle pour garantir une communication fluide au sein de votre 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

- 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 :

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

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.
- Après avoir créé votre VPC, utilisez Amazon CloudWatch pour surveiller l'utilisation de la NAU de celui-ci afin qu'elle ne dépasse pas les limites du quota NAU. Pour de plus amples 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 ressources AWS sont représentées sous la forme d'unités NAU uniques et certaines ressources sont représentées sous la 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 ou chaque adresse IPv6 attribuée 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

Ressource	Unités NAU
Gateway Load Balancer par zone de disponibilité	6
Point de terminaison d'un VPC par zone de disponibilité	6
Réseaux de transit par passerelle	6
fonction Lambda	6
Passerelle NAT	6
Cible de montage EFS	6
Interface EFA (EFA avec un appareil ENA) ou interface EFA uniquement	1
Pod Amazon EKS	1

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 vos sous-réseaux VPC avec d'autres comptes

Le partage de sous-réseaux VPC permet Comptes AWS à plusieurs utilisateurs de créer leurs ressources d'application, telles que les instances Amazon EC2, les bases de données Amazon Relational Database Service (RDS), les clusters Amazon Redshift et les fonctions, dans des clouds

privés virtuels partagés et gérés de manière centralisée (). AWS Lambda VPCs 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 sous-réseaux 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 réduit le nombre de ceux VPCs 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 les sous-réseaux Amazon VPC partagés à l'aide de fonctionnalités de connectivité, telles que les passerelles de transit et le AWS PrivateLink peering VPC. Pour plus d'informations sur les avantages du partage de sous-réseaux VPC, consultez Partage de VPC : une nouvelle approche des comptes multiples et de la gestion des VPC.

Il existe des quotas liés au partage de sous-réseaux VPC. Pour de plus amples informations, veuillez consulter Partage de sous-réseaux VPC.

Table des matières

Conditions préalables relatives aux sous-réseaux partagés

Cette section contient les conditions préalables à l'utilisation de sous-réseaux 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 de plus amples informations, veuillez consulter Activer le partage de ressources dans AWS Organizations dans le Guide de l'utilisateur AWS RAM .

- 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 .

Utilisation des sous-réseaux partagés

Cette section décrit comment utiliser les sous-réseaux partagés dans la AWS console et AWS CLI.

Table des matières

Partager un sous-réseau

Vous pouvez partager des sous-réseaux non définis par défaut avec d'autres comptes au sein de votre organisation comme suit. En outre, vous pouvez partager des groupes de sécurité entre les AWS Organisations. Pour de plus amples informations, veuillez consulter Partagez des groupes de sécurité avec des AWS Organisations.

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

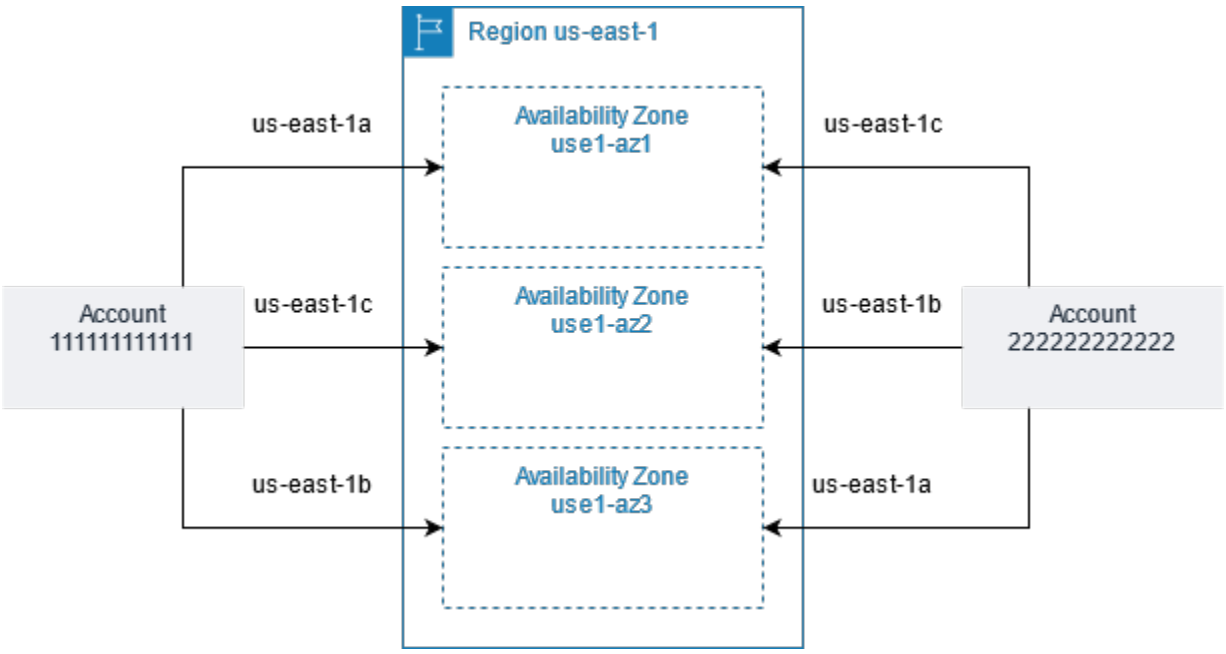
Utilisez les commandes create-resource-share et associate-resource-share.

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 AZ IDs pour déterminer l'emplacement des ressources d'un compte par rapport à un autre. 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 automated/

managed flux de travail (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.

Facturation et mesure pour le propriétaire et les participants

Cette section contient les informations de facturation et de mesure pour les personnes qui possèdent le sous-réseau partagé et pour celles qui utilisent le sous-réseau partagé :

- 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 IPv4 adresses publiques utilisées dans le partage VPCs sont facturées aux propriétaires de VPC. Pour plus d'informations sur la tarification des IPv4 adresses publiques, consultez l'onglet IPv4 Adresse 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

Cette section contient des détails sur les responsabilités et les autorisations des propriétaires du sous-réseau partagé (propriétaire) et des personnes qui utilisent le sous-réseau partagé (participant).

Ressources des propriétaires

Les propriétaires sont responsables des ressources VPC qu'ils possèdent. 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, du réseau, des connexions d'appairage ACLs, des points de terminaison de passerelle, des points de terminaison d'interface, des points de terminaison Route 53 Resolver, des passerelles Internet, des passerelles NAT, des passerelles privées virtuelles et des pièces jointes de passerelle de transit.

Ressources des participants

Les participants sont responsables des ressources VPC qu'ils possèdent. 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 de plus amples informations, veuillez consulter Partage de sous-réseaux VPC.

Ressources en matière de VPC

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

Journaux de flux

- Les participants peuvent créer, supprimer et décrire des journaux de flux pour les interfaces réseau dont ils sont propriétaires dans un sous-réseau VPC partagé.
- Les participants ne peuvent pas créer, supprimer et décrire des journaux de flux pour les interfaces réseau dont ils ne sont pas propriétaires dans un sous-réseau VPC partagé.
- Les participants ne peuvent pas créer, supprimer ou décrire des journaux de flux dans un sous-réseau VPC partagé.
- Les propriétaires de VPC peuvent créer, supprimer et décrire des journaux de flux pour les interfaces réseau dont ils ne sont pas propriétaires dans un sous-réseau VPC partagé.
- Les propriétaires de VPC peuvent créer, supprimer ou décrire des journaux de flux pour un sous-réseau VPC partagé.
- Les propriétaires de VPC ne peuvent pas décrire ni supprimer des 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 des passerelles Internet dans un sous-réseau VPC partagé. Les participants ne peuvent pas décrire des 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 au réseau (NACLs)

- Les participants ne peuvent pas créer, supprimer ou remplacer NACLs dans un sous-réseau VPC partagé. Les participants peuvent décrire la NACLs création 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 appartenant aux participants d'un sous-réseau VPC partagé. Les propriétaires de VPC ne peuvent utiliser les interfaces réseau appartenant à des participants d'une autre manière, comme attacher, détacher ou modifier les interfaces réseau appartenant à des 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 utiliser (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 peuvent utiliser des groupes de sécurité créés par les propriétaires de VPC si le propriétaire du VPC partage le groupe de sécurité avec le participant.

- 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 le groupe de sécurité par défaut du VPC, car il appartient au propriétaire.
- Les participants ne peuvent pas lancer d'instances en utilisant des groupes de sécurité non définis par défaut appartenant au propriétaire du VPC ou à d'autres participants sauf si le groupe de sécurité est partagé avec eux.
- 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 utiliser les groupes de sécurité créés par les participants d'une 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.

Subnets

- 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.

VPCs

- Les participants ne peuvent pas VPCs modifier les attributs qui leur sont associés. Seul le propriétaire du VPC peut le faire. Les participants peuvent décrire VPCs 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.

- Les participants peuvent associer leurs propres groupes de sécurité à un VPC partagé. Cela permet aux participants d'utiliser le groupe de sécurité avec les interfaces réseau Elastic dont ils sont propriétaires dans le VPC partagé.

AWS ressources et sous-réseaux VPC partagés

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

- Amazon Aurora
- AWS Database Migration Service
- Amazon EC2
- Amazon ECS
- Amazon ElastiCache (Redis OSS)
- Amazon EFS
- Amazon Elastic Kubernetes Service
- Elastic Load Balancing
  - Application Load Balancers
  - Équilibreurs de charge de passerelle
  - Network Load Balancers
- Amazon EMR
- AWS Glue
- AWS Lambda
- Amazon MQ exécutant Apache MQ (et non Rabbit MQ)
- Amazon MSK
- AWS Network Manager
  - AWS Réseau WAN dans le cloud
  - Analyseur d'accès réseau
  - Reachability Analyzer
- Amazon OpenSearch Service
- AWS PrivateLink†
- Amazon Relational Database Service (RDS)

- Amazon Redshift
- Amazon Route 53
- Amazon SageMaker Unified Studio
- 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.

Cette liste vise à répertorier tous les services qui prennent en charge le lancement de ressources dans des sous-réseaux VPC partagés. Malgré tous nos efforts, il est possible qu'elle ne soit pas complète. N'hésitez pas à nous faire part de vos commentaires ou de vos questions concernant la documentation.

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.

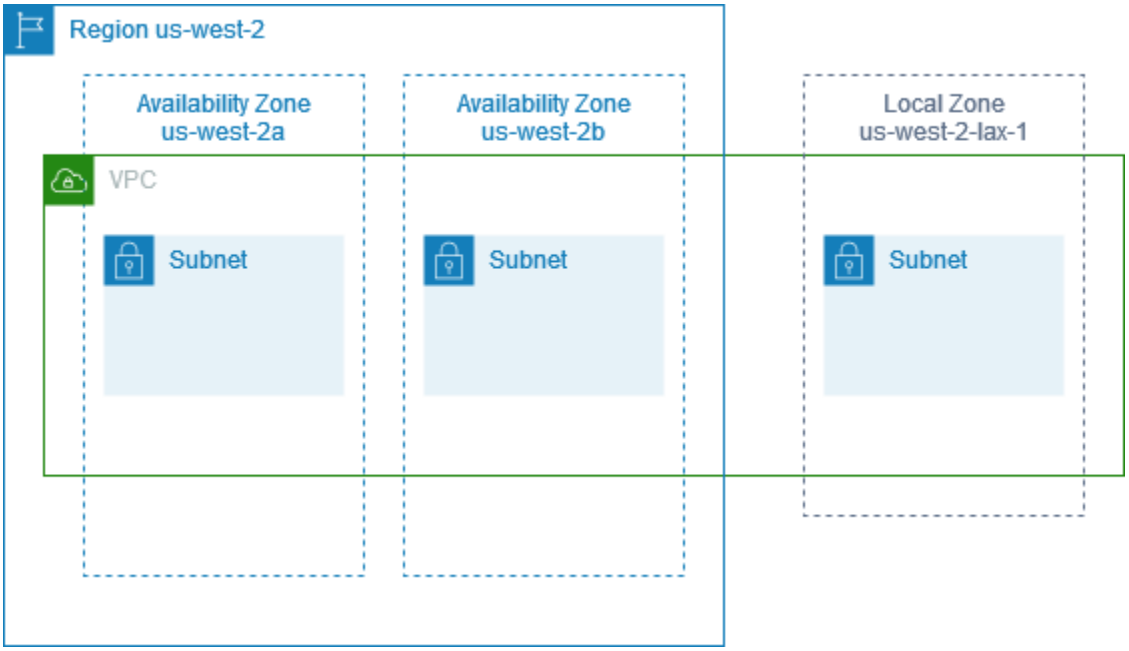
Sous-réseaux dans AWS Local Zones

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 élastiques”.

  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 élastiques”.
- 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 Direct Connect dans une région. Le centre de données local dispose d'une connexion Direct Connect à l'emplacement Direct Connect.

> **Note**
>
> Le trafic destiné à un sous-réseau dans une zone locale utilisant Direct Connect ne passe pas par la région parent 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 console Amazon VPC ou utiliser la commande describe-subnets.

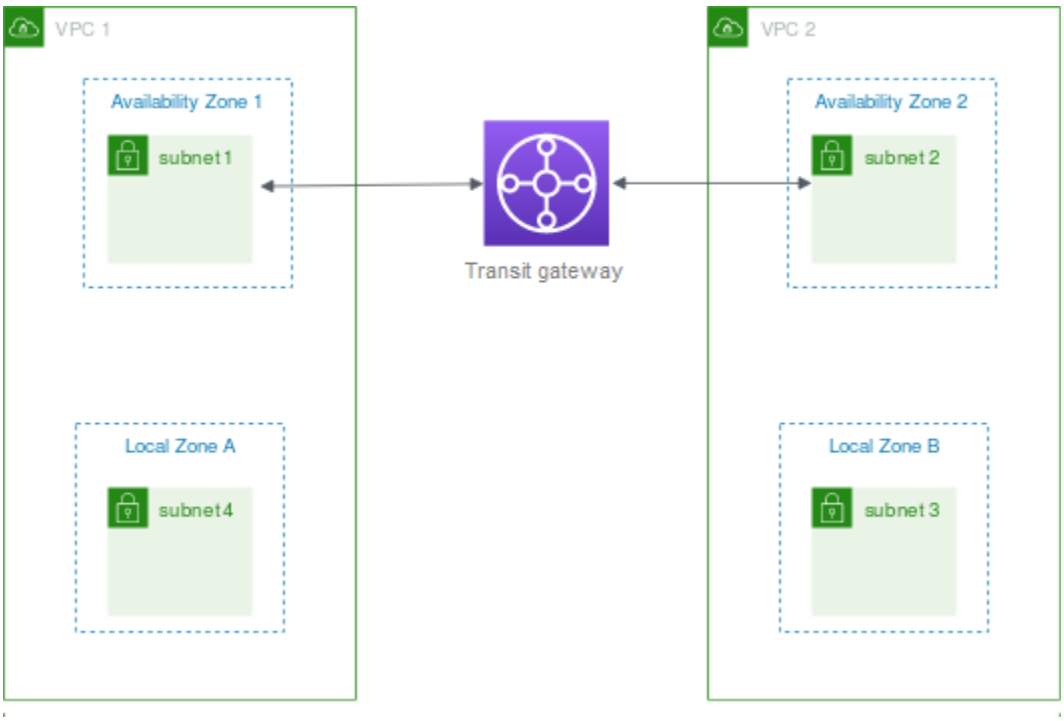
  Pour en savoir plus sur la création d'une passerelle réseau privé virtuel, consultez Création d'une passerelle cible dans le Guide de l'utilisateur AWS Site-to-Site VPN.
- Une connexion Direct Connect. Pour obtenir les meilleures performances de latence, AWS vous recommande d'utiliser l'emplacement Direct 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 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 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 Direct Connect.
- Une interface virtuelle privée sur la connexion depuis l'emplacement 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 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, consultez 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 les tables de routage des sous-réseaux de zone locale qui ont 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, consultez the section called "Routage pour une passerelle de transit".

Voici un exemple de table de routage pour le VPC 1.

Destination	Cible
CIDR VPC	*local*
CIDR VPC	*vpc1-attachment-network-interface-id*

Voici un exemple de table de routage pour le VPC 2.

Destination	Cible
CIDR VPC	*local*
CIDR VPC	*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	*Réseau de transit par passerelle pour le VPC 1*	propagée
CIDR VPC	*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 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 la commande describe-availability-zones pour trouver la zone parent.

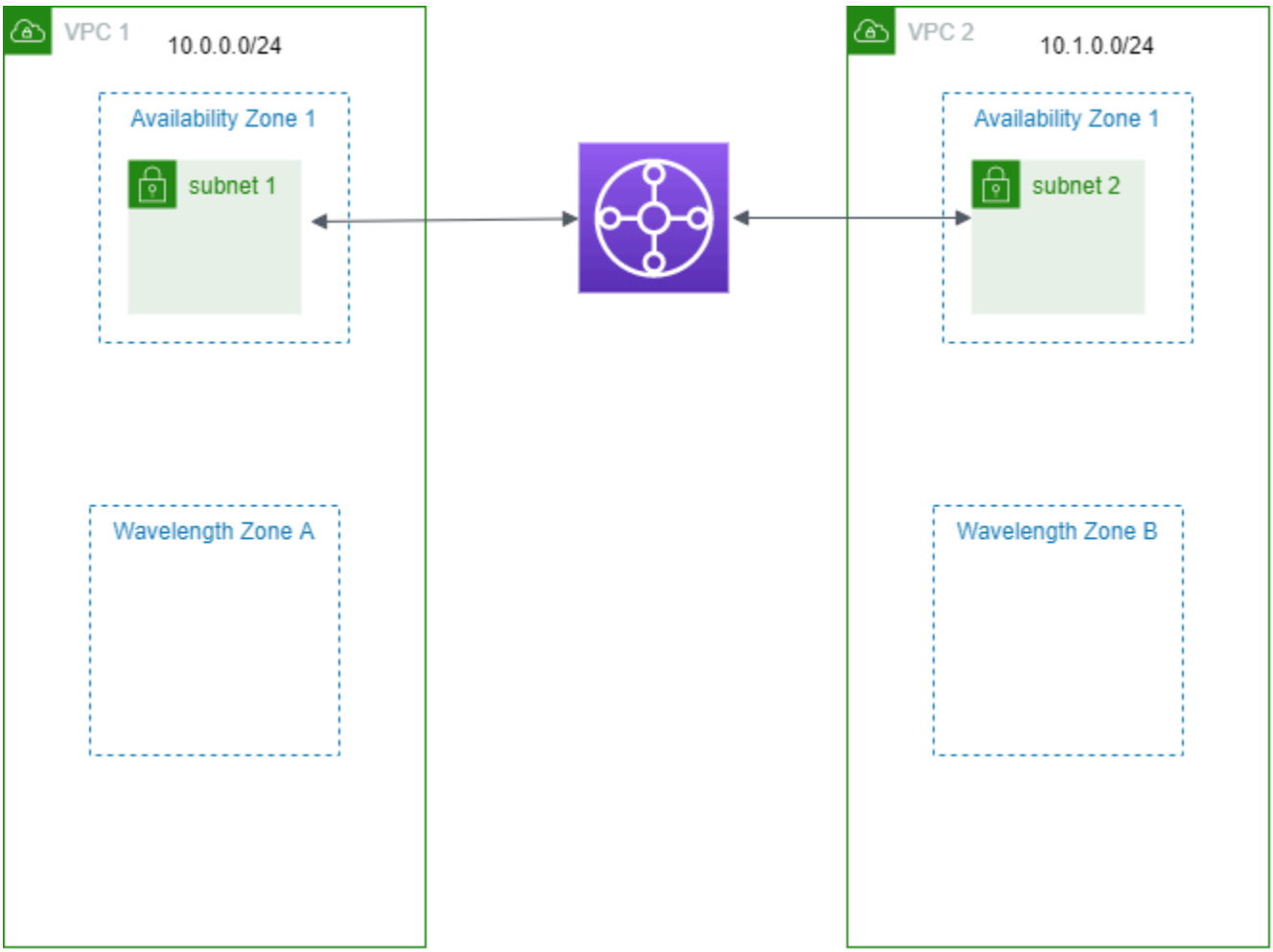
- Une passerelle de transit. La passerelle de transit relie les VPC. Pour plus d'informations sur la création d'une passerelle de transit, consultez Création d'une passerelle de transit dans le Guide Amazon VPC Transit Gateways.
- Pour chaque VPC, un attachement de VPC à la passerelle Transit Gateway 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

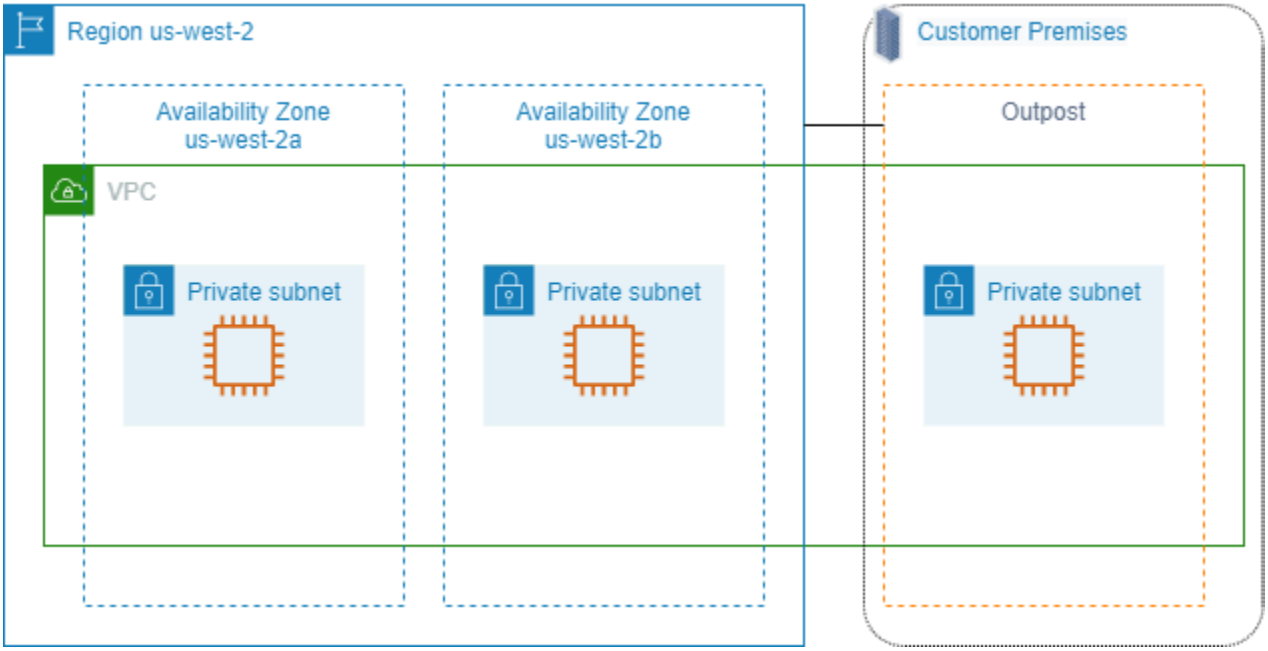
AWS Outposts vous offre les mêmes infrastructure matérielle, services, API et outils AWS pour créer et exécuter vos applications sur site et dans le cloud. AWS Outposts est idéal pour les charges de travail nécessitant un accès à faible latence aux applications ou systèmes sur site, et pour celles ayant 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.

> **Note**
>
> Si vous avez créé un journal de flux pour le VPC que vous supprimez, notez que les journaux de flux des VPC supprimés finissent par être automatiquement supprimés.

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 Résilier une 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 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 de la 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
```

Générez des infrastructure-as-code actions à partir de votre console VPC avec Console-to-Code

La console fournit un parcours guidé pour créer des ressources et tester des prototypes. Si vous souhaitez créer les mêmes ressources à grande échelle, vous aurez besoin d'un code d'automatisation. Console-to-Codeest une fonctionnalité d'Amazon Q Developer qui peut vous aider à démarrer avec votre code d'automatisation. Console-to-Codeenregistre les actions de votre console, y compris les valeurs par défaut et les paramètres compatibles. Il utilise ensuite l'IA générative pour suggérer du code dans votre format préféré infrastructure-as-code (iAc) pour les actions que vous souhaitez. Étant donné que le flux de travail de la console garantit que les valeurs de paramètres que vous spécifiez sont valides ensemble, le code que vous générez à l'aide de ces valeurs Console-to-Code possède des valeurs de paramètres compatibles. Vous pouvez utiliser le code comme point de départ, puis le personnaliser pour qu'il soit prêt pour la production en fonction de votre cas d'utilisation spécifique.

Par exemple, Console-to-Code vous pouvez vous enregistrer à l'aide de la console VPC pour créer des sous-réseaux, des groupes de sécurité NACLs, une table de routage personnalisée et une passerelle Internet et générer du code au CloudFormation format JSON. Vous pouvez ensuite copier ce code et le personnaliser pour l'utiliser dans votre modèle CloudFormation .

Console-to-Code peut actuellement générer infrastructure-as-code (iAc) dans les langues et formats suivants :

- CDK Java
- CDK Python
- CDK TypeScript
- CloudFormation JSON
- CloudFormation YAML

Pour plus d'informations et des instructions d'utilisation Console-to-Code, consultez Automatiser les AWS services avec Amazon Q Developer Console-to-Code dans le guide de l'utilisateur Amazon Q Developer.

Sous-réseaux de votre VPC

Un sous-réseau est une plage d'adresses IP dans votre VPC. Vous pouvez créer des ressources AWS, 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 des ressources AWS dans des zones de disponibilité distinctes, vous pouvez protéger vos applications contre la défaillance d'une 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 disponibles uniquement dans le VPC. Pour des exemples, consultez la section Adresses lien-local dans le Guide de l'utilisateur Amazon EC2.

Pour de plus amples informations, consultez Adressage IP pour votre réseau VPCs et vos sous-réseaux.

Types de sous-réseaux

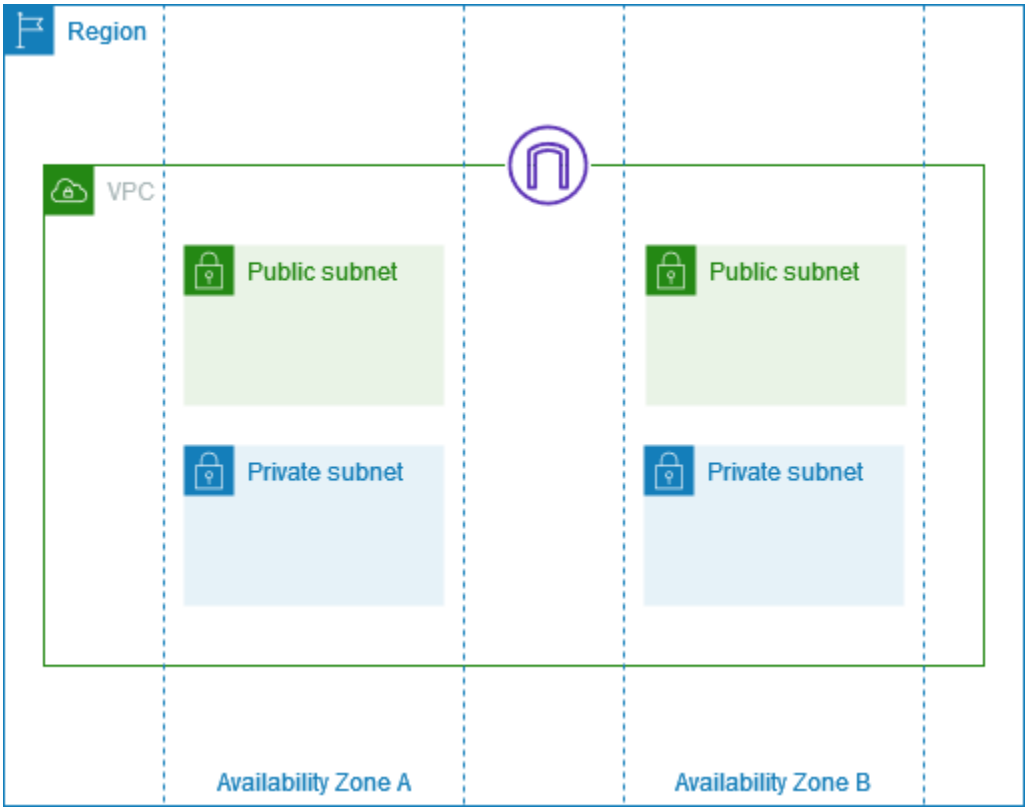
Le type de sous-réseau est déterminé par la façon dont vous configurez le routage pour vos sous-réseaux. Par exemple :

- 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.
- Sous-réseau EVS : ce type de sous-réseau est créé à l'aide d'Amazon EVS. Pour plus d'informations, consultez VLAN subnet dans le Guide d'utilisation d'Amazon EVS.

Diagramme de sous-réseau

Le schéma suivant montre un VPC avec des sous-réseaux dans deux zones de disponibilité et une passerelle Internet. Chaque zone de disponibilité possède un sous-réseau public et un sous-réseau privé.



Pour les schémas illustrant les sous-réseaux dans les zones locales et les zones Wavelength, consultez les sections Fonctionnement des zones locales AWS et Fonctionnement des zones AWS Wavelength.

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 de plus amples 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, par exemple) qui est créée pour une instance lancée 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 Types de noms d'hôte des instances Amazon EC2 dans le Guide de l'utilisateur Amazon EC2.

Sécurité des sous-réseaux

Pour la protection des ressources AWS, 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 de plus amples informations, consultez the section called "Comparez les groupes de sécurité et le réseau ACLs".

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 de plus amples informations, consultez Contrôler le trafic des sous-réseaux à l'aide de listes de contrôle d'accès 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 de plus amples informations, consultez 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 de plus amples informations, consultez Adressage IP pour votre réseau VPCs et vos 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 Availability Zone (Zone de disponibilité), vous pouvez choisir une zone pour votre sous-réseau ou conserver la zone par défaut No Preference (Aucune préférence) pour permettre à AWS de choisir à votre place.
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 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.
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).

Ajouter un sous-réseau à votre VPC à l'aide de la 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 de plus amples informations, consultez Configuration des tables de routage.
- 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 de plus amples informations, consultez Modifier les attributs d'adressage IP de votre 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 de plus amples informations, consultez Contrôler le trafic des sous-réseaux à l'aide de listes de contrôle d'accès réseau.
- Partager le sous-réseau avec d'autres comptes. Pour de plus amples informations, consultez ???.

Ajouter ou supprimer un bloc d'adresse CIDR IPv6 de 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.

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 ajouter ou supprimer 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. Pour ajouter un bloc d'adresse CIDR, cliquez sur Ajouter un bloc d'adresse CIDR IPv6, sélectionnez Bloc d'adresse CIDR VPC, saisissez un Sous-réseau de bloc d'adresses CIDR, puis 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.
5. Pour supprimer un bloc d'adresses CIDR, recherchez le bloc d'adresse CIDR IPv6 et choisissez Supprimer.
6. Choisissez Enregistrer.

Pour associer un bloc d'adresse CIDR IPv6 à un sous-réseau à l'aide de la AWS CLI

Utilisez la commande associate-subnet-cidr-block.

Pour dissocier un bloc d'adresse CIDR IPv6 d'un sous-réseau à l'aide de la AWS CLI

Utilisez la commande disassociate-subnet-cidr-block.

Modifier les attributs d'adressage IP 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.

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 IP 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.
5. 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 de la 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 pour empêcher AWS de 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 : permet d'attribuer un préfixe à une interface réseau unique. Pour plus d'informations, consultez Attribuer des préfixes aux interfaces réseau Amazon EC2 dans le Guide de l'utilisateur Amazon EC2.
- Explicite : permet d'attribuer manuellement une adresse IP individuelle à une interface réseau unique.

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 CIDR dans le même VPC, elles ne doivent 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 être attribuées à vos interfaces réseau par AWS. Supprimer une réservation de sous-réseau n'annule pas l'attribution des adresses IP utilisées.
- Le nombre d'adresses IP disponibles pour le sous-réseau dépend du type de réservation. Si vous créez une réservation de préfixe, ce nombre diminue immédiatement. Si vous créez une réservation de préfixe explicite, il diminue lorsque les adresses IP sont attribuées.

Pour plus d'informations sur la notation CIDR (Routage inter-domaines sans classe), consultez Adressage IP.

Table des matières

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.

Utiliser les réservations de bloc d'adresse CIDR de sous-réseau en utilisant la AWS CLI

Vous pouvez utiliser la AWS CLI pour créer et gérer les réservations de bloc d'adresse 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 sert de contrôleur de trafic pour votre cloud privé virtuel (VPC). Chaque table de routage contient un ensemble de règles, appelées routes, qui déterminent l'orientation du trafic réseau depuis votre sous-réseau ou votre passerelle. Lorsque vous créez un VPC, la table de routage principale de ce VPC est également créée. Vous pouvez créer d'autres tables de routage pour votre VPC, afin d'exercer un contrôle plus précis sur les chemins réseau de votre VPC.

Vous pouvez utiliser des tables de routage pour spécifier les réseaux avec lesquels votre VPC peut communiquer, tels que les autres réseaux VPCs ou les réseaux locaux. Chaque route spécifie une destination (bloc CIDR ou liste de préfixes) et une cible (passerelle Internet, passerelle NAT, connexion d'appairage de VPC ou connexion VPN, par exemple). Le trafic est acheminé vers les cibles en fonction de son adresse IP de destination. Les tables de routage vous permettent de créer des architectures réseau complexes comprenant des sous-réseaux publics et privés, des sous-réseaux VPN uniquement et des sous-réseaux isolés.

Table des matières

Concepts liés aux tables de routage

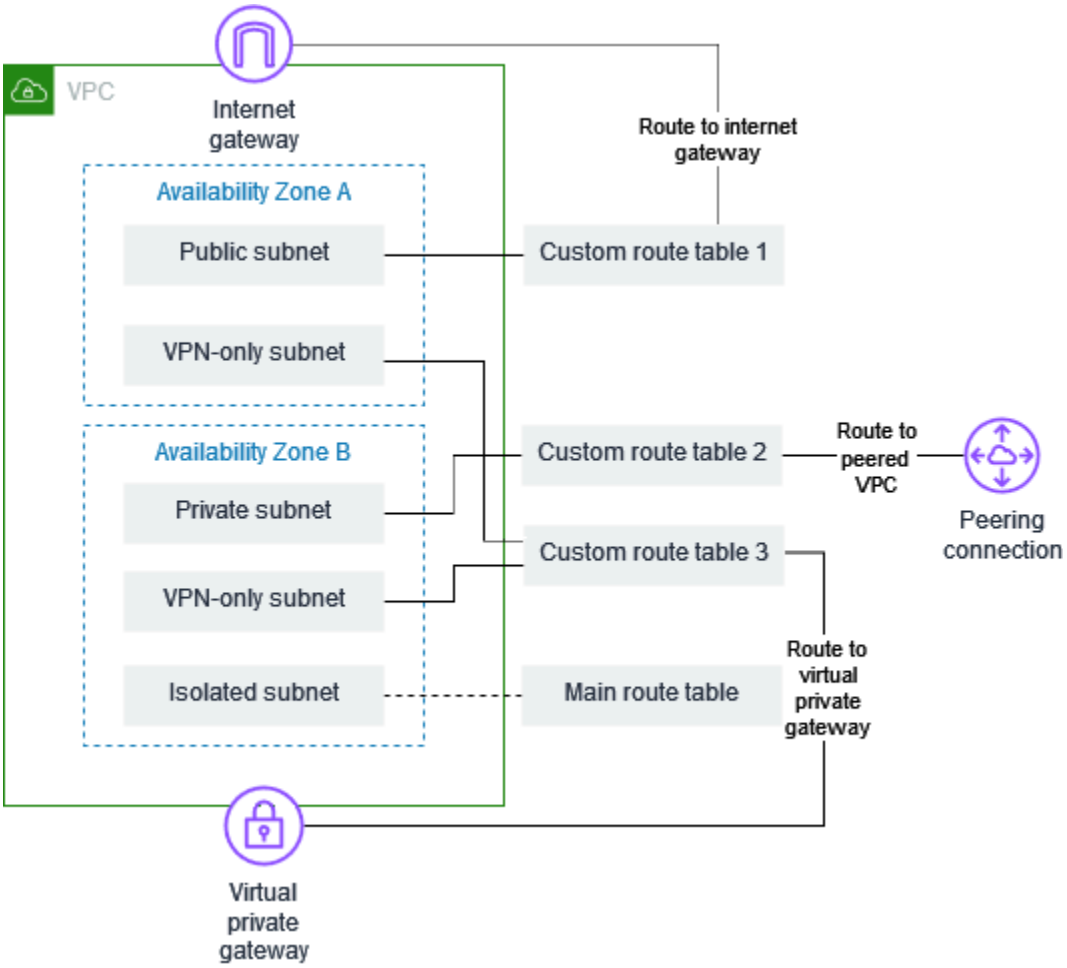
Les concepts clés relatifs aux tables de routage sont les suivants :

- 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.
- Route locale : Il s'agit de la route de communication par défaut au sein du VPC. Si le VPC possède à la fois des IPV6 adresses IPv4 et des adresses, il existe un itinéraire local pour IPv4 et un itinéraire local pour. IPv6
- 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.

- 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, consultez la section Options de routage Site-to-Site VPN dans le Guide de l'utilisateur du 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 un dispositif. 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 dispositif 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 .

Exemple de VPC avec des tables de routage

Le schéma suivant présente un VPC avec cinq sous-réseaux, une table de routage principale et trois tables de routage personnalisées. Les quatre tables de routage disposent de routes locales. La table de routage personnalisée 1, qui est associée au sous-réseau public de la zone de disponibilité A, dispose d'une route vers une passerelle Internet. La table de routage personnalisée 2, qui est associée au sous-réseau privé de la zone de disponibilité B, dispose d'une route vers un VPC appairé. La table de routage personnalisée 3, qui est associée aux sous-réseaux VPN uniquement des deux zones de disponibilité, dispose d'une route vers une passerelle privée virtuelle.



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'itinéraire est`0.0.0.0/0`, qui représente toutes les IPv4 adresses. La cible est la passerelle Internet qui est attachée à votre VPC.

Destination	Cible
0.0.0.0/0	*igw-id*

Les blocs CIDR sont traités séparément IPv4 et IPv6 sont traités séparément. Par exemple, un itinéraire dont le CIDR de destination est n'`0.0.0.0/0`inclut pas automatiquement toutes les IPv6 adresses. Vous devez créer un itinéraire avec un CIDR de destination égal à `::/0` pour toutes les IPv6 adresses.

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 possède plusieurs blocs d'adresse IPv4 CIDR, vos tables de routage contiennent une route locale pour chaque IPv4 bloc d'adresse CIDR. Si vous avez associé un bloc d' IPv6 adresse CIDR à votre VPC, vos tables de routage contiennent une route locale pour IPv6 le bloc d'adresse CIDR. 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 à l'intégralité IPv4 ou au bloc IPv6 CIDR 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'itinéraires vers IPv4 des adresses correspondant exactement ou constituant 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 vers IPv6 des adresses correspondant exactement ou constituant 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 dispositifs middlebox dans les chemins de routage de votre VPC. Pour en savoir plus, consultez the section called "Routage pour un dispositif middlebox".

Exemple

Dans l'exemple suivant, supposons que le VPC possède à la fois un bloc IPv4 CIDR et un IPv6 bloc CIDR. IPv4 et IPv6 le trafic sont traités séparément, comme indiqué dans le tableau d'itinéraires suivant.

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

- IPv4 le trafic à acheminer au sein du VPC (10.0.0.0/16) est couvert par l'itinéraire. Local
- IPv6 le trafic à acheminer au sein du VPC (2001:db 8:1234:1 a00 : :/56) est couvert par la route. Local

- La route pour 172.31.0.0/16 envoie le trafic vers une connexion d'appairage.
- L'itinéraire pour l'ensemble IPv4 du trafic (0.0.0.0/0) envoie le trafic vers une passerelle Internet. Par conséquent, tout IPv4 le trafic, à l'exception du trafic au sein du VPC et vers la connexion d'appairage, est acheminé vers la passerelle Internet.
- L'itinéraire pour l'ensemble IPv6 du trafic (: : /0) envoie le trafic vers une passerelle Internet de sortie uniquement. Par conséquent, tout IPv6 le trafic, à l'exception du trafic au sein 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.

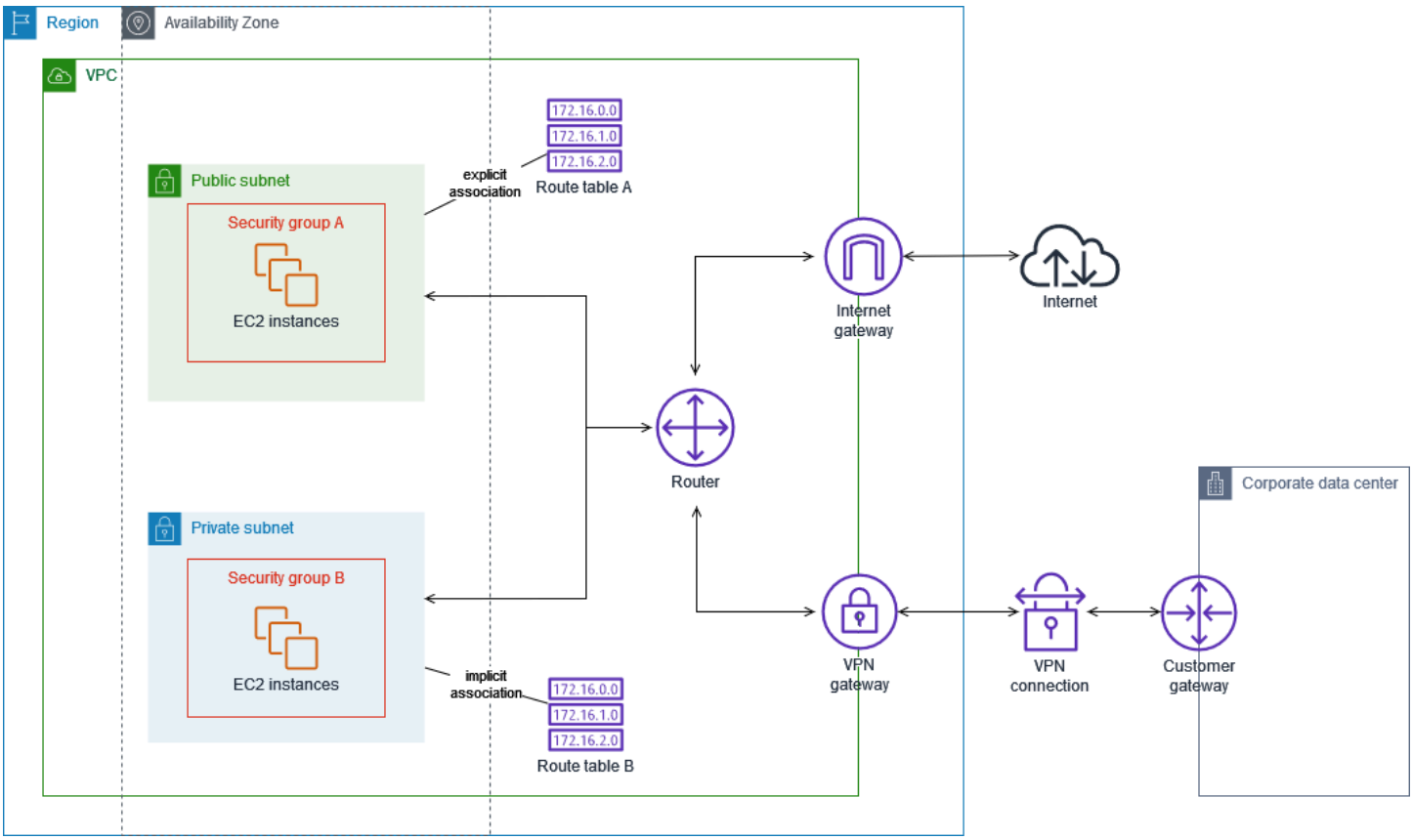
Association de la table de routage du sous-réseau

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 Détermination des associations explicites.

Les sous-réseaux VPCs associés aux Outposts peuvent avoir un type de cible supplémentaire, à savoir 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	Target
VPC CIDR	Local
0.0.0.0/0	*igw-id*

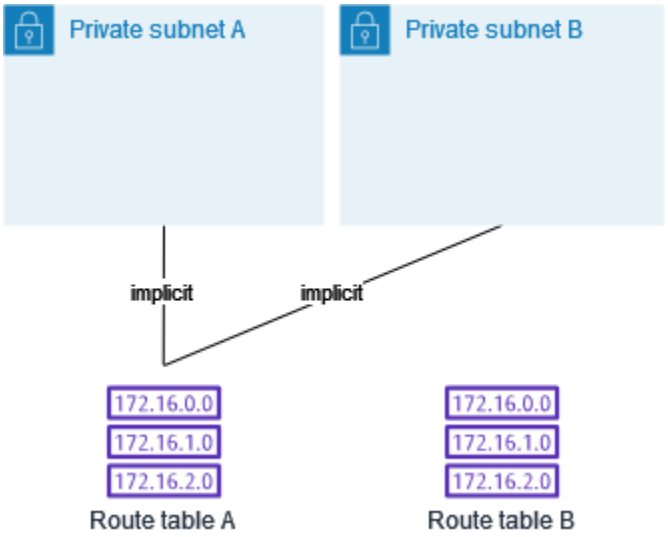
La table de routage B est la table de routage principale. Elle est implicitement associée au sous-réseau privé. Elle dispose d'une route qui envoie tout le trafic vers la passerelle privée virtuelle, mais aucune route vers la passerelle Internet, ce qui fait du sous-réseau un sous-réseau VPN uniquement. 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	Target
VPC CIDR	Local
0.0.0.0/0	*vgw-id*

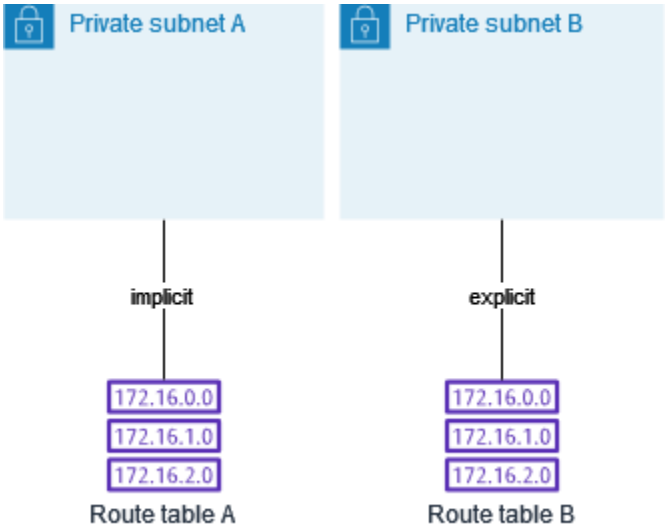
Exemple 2 : Remplacement de la table de routage principale

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.

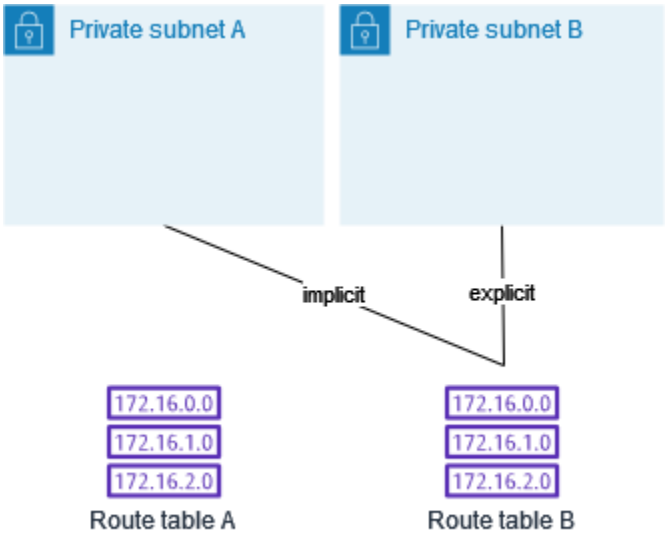
Le schéma suivant montre deux sous-réseaux et deux tables de routage. Le sous-réseau A est implicitement associé à la table de routage A, la table de routage principale. Le sous-réseau B est implicitement associé à la table de routage A. La table de routage B, une table de routage personnalisée, n'est associée à aucun des deux sous-réseaux.



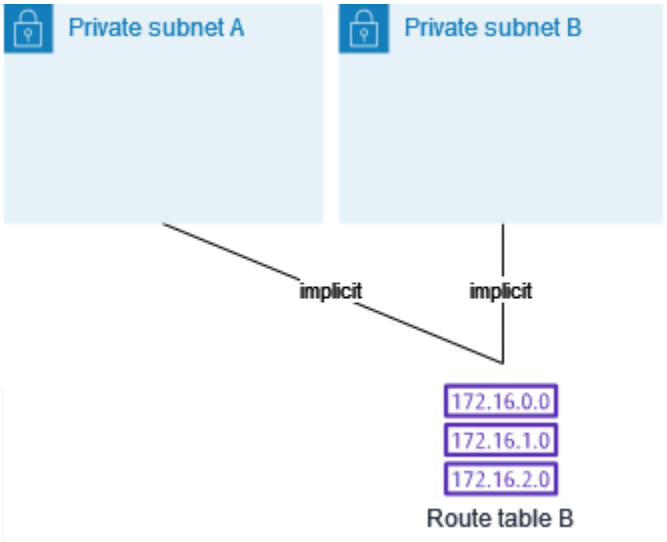
Pour remplacer la table de routage principale, commencez par créer une association explicite entre le sous-réseau B et la table de routage B. Testez la table de routage B.



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 un dispositif middlebox (tel qu'un dispositif 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 un dispositif 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 un dispositif middlebox

Lorsque la cible est un point de terminaison d'équilibreur de charge de passerelle ou une interface réseau, les destinations suivantes sont autorisées :

- Le bloc complet IPv4 ou le bloc IPv6 CIDR de votre VPC. Dans ce cas, vous remplacez la cible de la route locale par défaut.
- Le bloc complet IPv4 ou le bloc IPv6 CIDR d'un sous-réseau de 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 de plus amples informations, veuillez consulter 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 de plus amples informations, veuillez consulter 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 dispositif 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 dispositif middlebox, prenez note des considérations relatives au dispositif.

- Lorsque vous acheminez le trafic via un dispositif middlebox, le trafic de retour du sous-réseau de destination doit être acheminé via le même dispositif. 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 .

Fonctionnement de la priorité de routage

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 :

La liste suivante présente un résumé des priorités de routage avec des liens vers les sections ci-dessous contenant des informations plus détaillées et des exemples :

1. Préfixe le plus long (par exemple, 10.10.2.15/32 prévaut sur 10.10.2.0/24)
2. Routes statiques (comme l'appairage de VPC et les connexions par passerelle Internet)
3. Route par liste de préfixes
4. Routes propagées
   a. Routes BGP Direct Connect (routes dynamiques)
   b. Routes VPN statiques
   c. Routes VPN BGP (routes dynamiques) (comme les passerelles privées virtuelles)

Correspondance du préfixe le plus long

Les itinéraires IPv4 et IPv6 adresses ou les blocs CIDR sont indépendants les uns des autres. Nous utilisons l'itinéraire le plus précis qui correspond au IPv4 trafic ou au IPv6 trafic pour déterminer comment acheminer le trafic.

L'exemple de table de routage de sous-réseau suivant comporte un itinéraire pour le trafic IPv4 Internet (`0.0.0.0/0`) qui pointe vers une passerelle Internet, et un itinéraire pour le `172.31.0.0/16` IPv4 trafic pointant 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 de routage pour les routes statiques et propagées de manière dynamique

Si vous avez connecté une passerelle privée virtuelle à votre VPC et activé la propagation de routes sur la table de routage de votre sous-réseau, les routes représentant votre connexion Site-to-Site VPN apparaissent automatiquement sous forme de routes propagées dans votre table de routage.

Si la destination d'un acheminement propagé est identique à la destination d'un acheminement statique, l'acheminement statique est prioritaire. Les ressources suivantes utilisent des routes statiques :

- 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

Priorité d'acheminement pour les listes de préfixes

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 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.

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 passerelle Internet
- Routage vers un périphérique NAT
- Routage vers une passerelle réseau privé virtuel
- Routage vers une passerelle AWS Outposts locale
- 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 un dispositif 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 une destination pour le IPv4 trafic ou `0.0.0.0/0` `::/0` pour le IPv6 trafic, et une cible pour l'ID de passerelle Internet ()`igw-xxxxxxxxxxxxxxxxx`.

Destination	Cible
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Pour de plus amples informations, veuillez consulter Activation de l'accès à Internet pour un VPC 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. Ajoutez ensuite une route pour la table de routage du sous-réseau privé qui achemine le trafic IPv4 Internet (`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 de plus amples informations, veuillez consulter 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 privée virtuelle ne prend pas en charge IPv6 le trafic. Cependant, nous prenons en charge IPv6 le trafic acheminé via une passerelle privée virtuelle vers une Direct Connect connexion. Pour plus d'informations, consultez le Guide de l'utilisateur 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

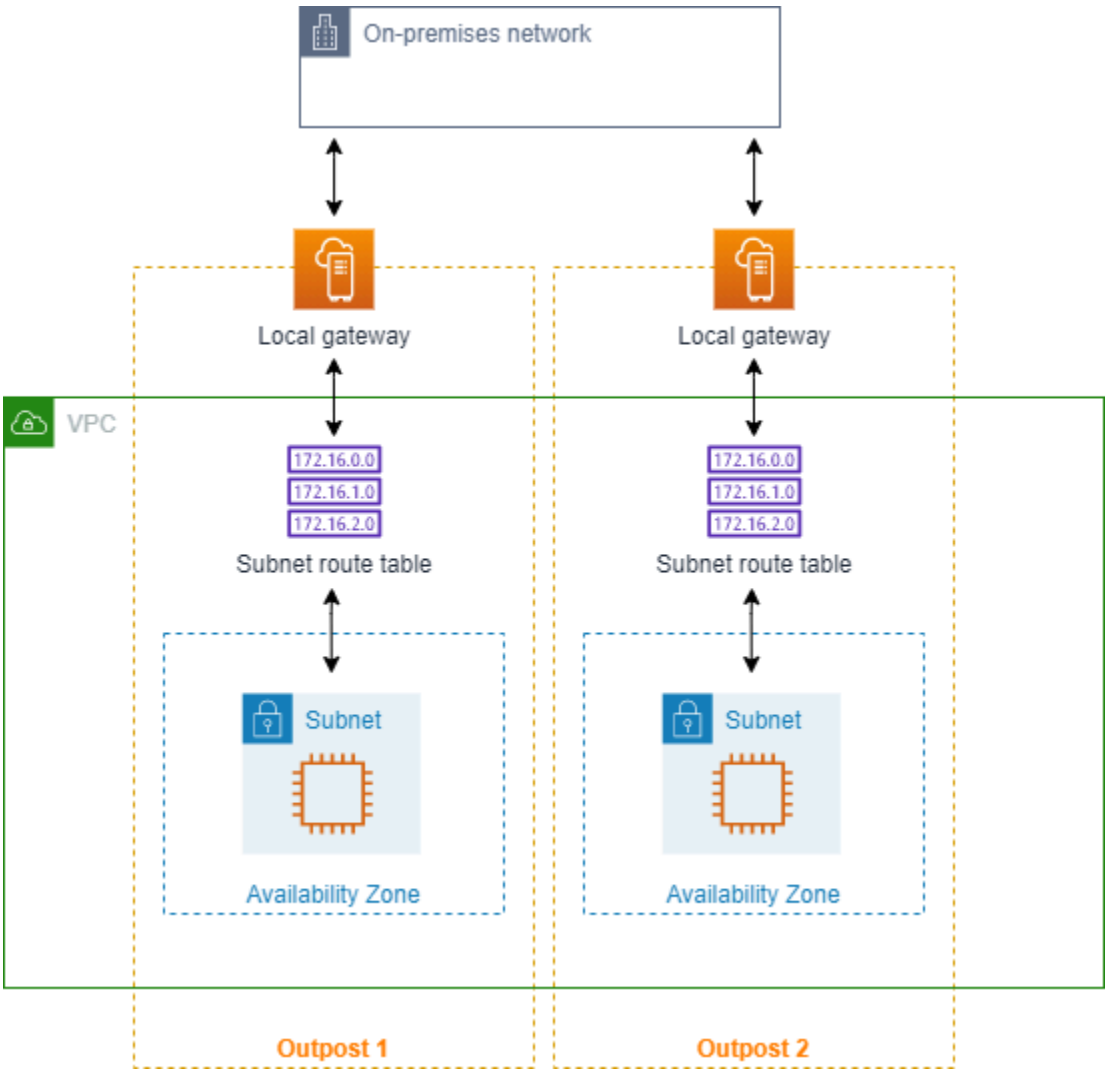
Les sous-réseaux VPCs associés à AWS Outposts peuvent avoir un type de cible supplémentaire, à savoir une passerelle locale. Considérez le cas où vous souhaitez que la passerelle locale route le trafic avec une adresse de destination 192.168.10.0/24 vers le réseau client. Pour ce faire, ajoutez la route 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 multiple (AZ) pour vos applications sur site exécutées sur des racks Outposts en établissant une connectivité entre des racks Outposts ancrés à différents. AZs



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 de l'itinéraire doit correspondre à l'ensemble du IPv4 bloc 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 le groupe de sécurité IDs.
- 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 VPC est une connexion réseau entre deux personnes VPCs qui vous permet d'acheminer le trafic entre elles à l'aide d'adresses privées. IPv4 Les instances des deux VPC peuvent communiquer entre elles comme si elles faisaient partie du même réseau.

Pour activer le routage du trafic entre les VPCs connexions d'appairage VPC, vous devez ajouter une route vers une ou plusieurs tables de routage de sous-réseau pointant vers la connexion d'appairage

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 avez une connexion d'appairage VPC (`pcx-11223344556677889`) entre deux VPCs, 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 activer le trafic entre VPCs et autoriser l'accès à l'ensemble du bloc IPv4 CIDR de l'un ou l'autre VPC, la table de routage du 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 VPC peut également prendre en charge IPv6 la communication entre les instances du VPCs, si les instances VPCs et sont activées pour la communication. IPv6 Pour activer le routage du IPv6 trafic entre les deux VPCs, vous devez ajouter une route à votre table de routage qui pointe vers la connexion d'appairage du VPC pour accéder à tout ou partie du bloc IPv6 CIDR du VPC homologue.

Par exemple, en utilisant la même connexion d'appairage VPC (`pcx-11223344556677889`) ci-dessus, supposons qu' VPCs ils disposent des informations suivantes :

- VPC A : le bloc IPv6 CIDR est `2001:db8:1234:1a00::/56`

- VPC B : le bloc IPv6 CIDR est `2001:db8:5678:2b00::/56`

Pour activer IPv6 la communication via la connexion d'appairage VPC, ajoutez la route suivante à la table de routage du sous-réseau pour le 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 IPv6 le trafic uniquement. Pour configurer le routage d'une passerelle Internet de sortie uniquement, ajoutez une route dans la table de routage du sous-réseau privé qui achemine le trafic IPv6 Internet (`::/0`) vers la passerelle Internet de sortie uniquement.

Destination	Target
::/0	*eigw-id*

Pour de plus amples informations, veuillez consulter Activez le IPv6 trafic sortant à l'aide d'une passerelle 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.

Imaginons le scénario suivant dans lequel vous en avez trois VPCs qui sont rattachés 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 en avez deux VPCs, 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 activer le trafic entre la passerelle de transit VPCs et autoriser l'accès à celle-ci, la table de routage du 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 un dispositif middlebox

Vous pouvez ajouter des dispositifs 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 un dispositif 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 de plus amples informations, veuillez consulter the section called “Assistant de routage middlebox”.
- Direction du trafic entre deux sous-réseaux vers un dispositif 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'un dispositif 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 le dispositif en fonction de vos besoins. Par exemple, vous pouvez configurer un dispositif de sécurité pour filtrer tout le trafic, ou un dispositif d'accélération WAN. Le dispositif est déployé en tant qu'instance Amazon EC2 dans un sous-réseau de votre VPC et est représenté 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 Direct Connect connexion qui prend en charge les trames jumbo).

Pour router 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 de plus amples informations, veuillez consulter Tables de routage de passerelle. Vous pouvez également acheminer le trafic sortant de votre sous-réseau vers un dispositif middlebox figurant dans un autre sous-réseau.

Pour obtenir des exemples de routage middlebox, consultez Scénarios middlebox.

Table des matières

Considérations relatives aux dispositifs

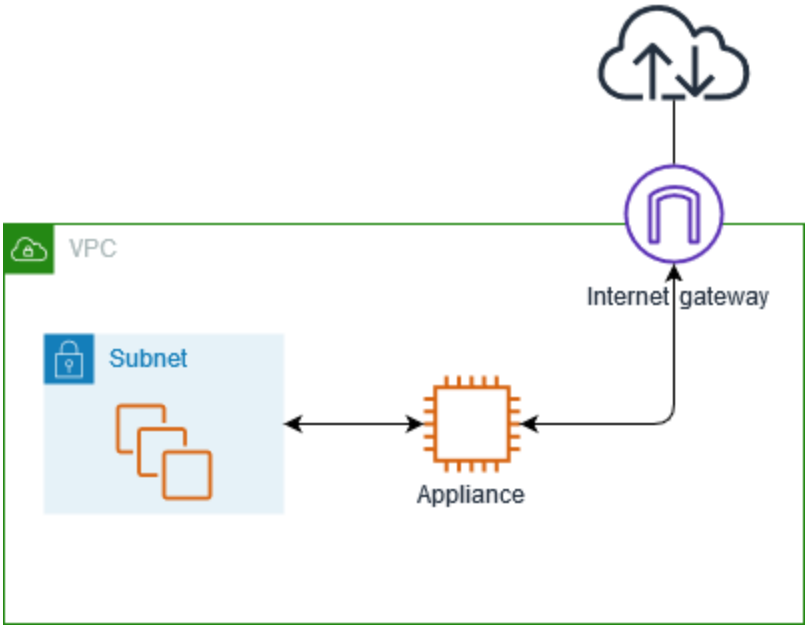
Vous pouvez choisir un dispositif tiers provenant de AWS Marketplace ou configurer votre propre dispositif. Lorsque vous créez ou configurez un dispositif, prenez en compte les éléments suivants :

- Le dispositif doit être configuré dans un sous-réseau distinct du trafic source ou de destination.
- Vous devez désactiver le source/destination contrôle de l'appliance. Pour plus d'informations, consultez Changement de la vérification de source ou de destination dans le Guide utilisateur Amazon EC2.
- Vous ne pouvez pas acheminer le trafic entre les hôtes du même sous-réseau via un dispositif.
- Le dispositif n'est pas tenu 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 un dispositif middlebox. La destination de l'itinéraire doit correspondre à l'intégralité IPv4 ou au bloc IPv6 CIDR d'un sous-réseau de votre VPC.
- Pour intercepter le IPv6 trafic, assurez-vous que votre VPC, votre sous-réseau et votre appliance sont compatibles. IPv6

Acheminement du trafic entre une passerelle et un dispositif

Pour acheminer le trafic VPC entrant vers un dispositif, 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 dispositif comme cible pour le trafic VPC. Dans l'exemple suivant, le VPC dispose d'une passerelle Internet, d'un dispositif et d'un sous-réseau avec des instances. Le trafic en provenance d'Internet est acheminé via un dispositif.



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 IPv4 trafic destiné au sous-réseau à l'interface réseau de l'appliance. Cet acheminement est plus spécifique que l'acheminement local.

Destination	Target
VPC CIDR	Local
Subnet CIDR	*Appliance network interface ID*

Vous pouvez également remplacer la cible de l'acheminement local par l'interface réseau du dispositif. Vous pouvez procéder ainsi pour faire en sorte que l'ensemble du trafic soit acheminé automatiquement vers le dispositif, y compris le trafic destiné aux sous-réseaux que vous ajouterez dans l'avenir au VPC.

Destination	Cible
VPC CIDR	*Appliance network interface ID*

Pour acheminer le trafic de votre sous-réseau vers un dispositif 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 du dispositif. La destination doit être moins spécifique que la destination de la route locale. Par exemple, pour le trafic destiné à Internet, spécifiez `0.0.0.0/0` (toutes les IPv4 adresses) pour la destination.

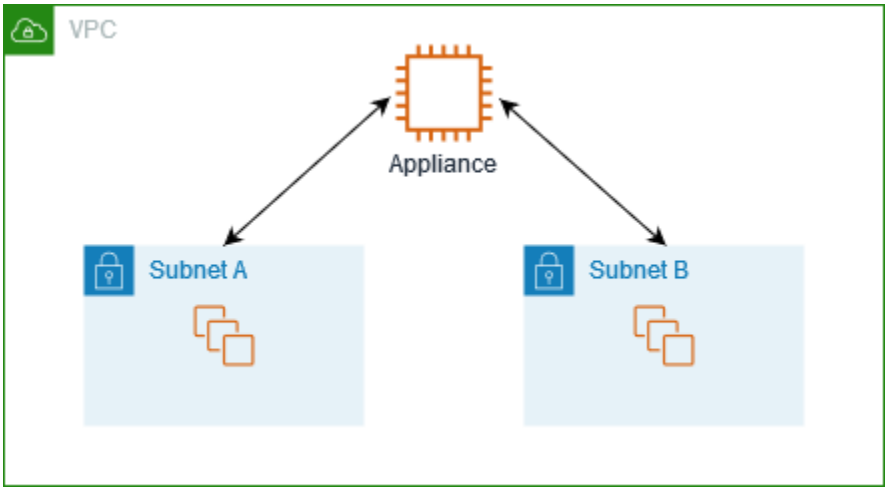
Destination	Target
VPC CIDR	Local
0.0.0.0/0	*Appliance network interface ID*

Ensuite, dans la table de routage associée au sous-réseau du dispositif, ajoutez un acheminement qui renvoie le trafic à la passerelle Internet ou à la passerelle réseau privé virtuel.

Destination	Target
VPC CIDR	Local
0.0.0.0/0	*igw-id*

Acheminement du trafic inter-sous-réseaux vers un dispositif

Vous pouvez acheminer le trafic destiné à un sous-réseau spécifique vers l'interface réseau d'un dispositif. Dans l'exemple suivant, le VPC contient deux sous-réseaux et un dispositif. Le trafic entre les sous-réseaux est acheminé via un dispositif.



Groupes de sécurité

Lorsque vous acheminez le trafic entre les instances de différents sous-réseaux via un dispositif 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 du dispositif.

Destination	Target
VPC CIDR	Local
Subnet B CIDR	*Appliance network interface ID*

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 du dispositif.

Destination	Target
VPC CIDR	Local
Subnet A CIDR	*Appliance network interface ID*

Vous pouvez également remplacer la cible de l'acheminement local par l'interface réseau du dispositif. Vous pouvez procéder ainsi pour faire en sorte que l'ensemble du trafic soit acheminé automatiquement vers le dispositif, y compris le trafic destiné aux sous-réseaux que vous ajouterez dans l'avenir au VPC.

Destination	Cible
VPC CIDR	*Appliance network interface ID*

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. Ils VPCs doivent être en mesure de communiquer avec deux pièces jointes VPC spécifiques dotées des 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 de dispositifs virtuels, tels que des pare-feu. Vous pouvez créer un équilibreur de charge Gateway Load Balancer (GWLB), configurer un service de point de terminaison GWLB, puis créer un point de terminaison GWLB dans votre VPC pour connecter celui-ci 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 de dispositifs 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*

Lorsque votre cible est un point de terminaison GWLB, vous ne pouvez pas spécifier de liste de préfixes comme destination. Si vous tentez de créer ou de remplacer une route de liste de préfixes

ciblant un point de terminaison de VPC, vous recevrez le message d'erreur « Cannot create or replace a prefix list route targeting a VPC Endpoint ».

Pour plus d'informations, consultez Gateway Load Balancers.

Création d'une table de routage pour le VPC

Exécutez les tâches suivantes pour créer et configurer une table de routage personnalisée pour votre VPC. Par défaut, une nouvelle table de routage contient des routes locales qui permettent la communication au sein du VPC. Vous pouvez ajouter des routes pour diriger le trafic réseau vers des cibles spécifiques en fonction de la plage d'adresses IP de destination.

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.

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.

> **Note**
>
> 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 de plus amples informations, veuillez consulter Quotas Amazon VPC.

Tâches

- Création de la table de routage
- Ajout de routes à la table de routage
- Association d'un sous-réseau à la table de routage

Création de la table de routage

Pour créer 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 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 à l'aide du AWS CLI

Utilisez la commande create-route-table.

Ajout de routes à la table de routage

Pour ajouter des routes à 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. Choisissez Ajouter une route.
5. Dans Destination, indiquez l'un des éléments suivants :
   - Une plage d'adresses IP, par exemple, 192.168.0.0/16
   - Une seule adresse IP, par exemple, 192.168.10.1/32
   - L'ID d'une liste de préfixes, par exemple, pl-0abcdef1234567890
6. Dans Cible, sélectionnez un type de ressource (par exemple, une interface réseau), puis entrez l'ID de la ressource (par exemple, eni-11223344556677889).
7. Sélectionnez Enregistrer les modifications.

Pour ajouter des itinéraires à une table de routage à l'aide du AWS CLI

Utilisez la commande create-route.

Association d'un sous-réseau à la table de routage

Pour associer une table de routage à 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 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 ou dissocier un sous-réseau à une table de routage à l'aide du AWS CLI

- associate-route-table
- disassociate-route-table

Gestion des tables de routage des sous-réseaux

Suivez les procédures ci-dessous pour gérer le routage VPC à l'aide de tables de routage.

Tâches

- Déterminer la table de routage associée à un sous-réseau
- Détermination des associations explicites
- Ajout, modification et suppression de routes
- Activer ou désactiver la propagation du routage
- Changer le tableau de routage associé à un sous-réseau

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 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 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 Détermination des associations explicites.

Détermination des associations explicites

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 à l'adresse 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 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 et choisissez l'onglet Edge associations (Associations périphériques).

Pour décrire une ou plusieurs tables de routage et afficher leurs associations à l'aide du AWS CLI

Utilisez la commande describe-route-tables.

Ajout, modification et suppression de routes

Vous pouvez ajouter, modifier et supprimer des routes dans vos tables de routage.

Pour plus d'informations sur l'utilisation des itinéraires statiques pour une connexion Site-to-Site VPN, consultez la section Modification des itinéraires statiques pour une connexion Site-to-Site VPN dans le guide de AWS Site-to-Site VPN l'utilisateur.

Considérations

- Vous pouvez uniquement modifier les routes que vous avez ajoutées.
- La modification ou la suppression d'une route a un impact sur les connexions existantes qui utilisent cette route. Les connexions qui utilisent les autres routes ne sont pas affectées.
- Le nombre de routes que vous pouvez ajouter à chaque table de routage est soumis à un quota. Pour de plus amples informations, veuillez consulter Quotas Amazon VPC.

Pour mettre à jour les routes pour 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). Dans Destination, entrez une plage d'adresses IP, une adresse IP unique ou l'ID d'une liste de préfixes. Dans Cible, sélectionnez le type de ressource, puis entrez l'ID de la ressource.
5. Pour modifier une route, entrez le bloc CIDR ou l'ID de liste de préfixes de la nouvelle destination et choisissez une cible.
6. Pour supprimer une route, sélectionnez Remove (Supprimer).

7. Sélectionnez Enregistrer les modifications.

Pour mettre à jour les itinéraires d'une table de routage à l'aide du AWS CLI

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`.

- créer un itinéraire
- remplacer-route
- supprimer-itinéraire

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, consultez la section Options de routage Site-to-Site VPN dans le Guide de l'utilisateur du Site-to-Site VPN.

Pour activer ou désactiver la propagation de route 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, puis sélectionnez la table de routage.
3. Choisissez Actions, Edit route propagation (Modifier la propagation des acheminements).
4. Cochez ou décochez la case Activer en regard de la passerelle privée virtuelle.
5. Choisissez Enregistrer.

Pour activer ou désactiver la propagation des itinéraires à l'aide du AWS CLI

- enable-vgw-route-propagation
- disable-vgw-route-propagation

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 à l'adresse 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 du AWS CLI

Utilisez la commande replace-route-table-association.

Remplacer la table de routage principale

Cette section explique comment 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 à l'adresse 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 en utilisant AWS CLI

- Utilisez la commande replace-route-table-association.

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 à l'adresse 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).

Contrôle du trafic entrant dans votre VPC à l'aide d'une table de routage de passerelle

Pour contrôler le trafic entrant dans votre VPC à l'aide d'une table de routage de passerelle, vous pouvez associer ou dissocier une passerelle Internet ou une passerelle privée virtuelle à une table de routage. Pour de plus amples informations, veuillez consulter Tables de routage de passerelle.

Pour associer ou dissocier une passerelle à 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, puis sélectionnez la table de routage.
3. Sur l'onglet Associations périphériques, choisissez Modifier les associations périphériques.
4. Cochez ou décochez 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 table de routage spécifiée à la passerelle Internet spécifiée.

```
aws ec2 associate-route-table
```

```
    --route-table-id rtb-01234567890123456 \
    --gateway-id igw-11aa22bb33cc44dd1
```

Pour dissocier une passerelle d'une table de routage à l'aide du AWS CLI

Utilisez la commande disassociate-route-table. Spécifiez l'ID de l'association entre la table de routage et la passerelle.

```
aws ec2 disassociate-route-table \
    --association-id rtbassoc-0abcdef1234567890
```

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 remplacer la route locale 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, 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 à l'adresse 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 l'interface réseau spécifiée.

```
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 pour la table de routage spécifiée.

```
aws ec2 replace-route \
    --route-table-id rtb-01234567890123456 \
    --destination-cidr-block 10.0.0.0/16 \
    --local-target
```

Routage avancé dans votre VPC

Configurez des scénarios de routage avancé pour votre VPC. Cette section couvre les approches de routage statique et dynamique pour la gestion du flux de trafic :

- Routage d'entrée statique : configurez des routes statiques pour diriger le trafic Internet entrant destiné à vos groupes d'adresses BYOIP (apportez votre propre adresse IP) vers des interfaces réseau spécifiques au sein de votre VPC.
- Routage dynamique à l'aide du serveur de routage VPC : utilisez le routage dynamique basé sur le protocole de passerelle frontière (BGP) pour mettre à jour automatiquement les tables de routage de VPC et de passerelle Internet et ainsi assurer une tolérance aux pannes et un basculement automatique pour vos charges de travail.

Table des matières

Acheminement du trafic Internet vers une interface réseau unique

Vous pouvez acheminer le trafic Internet entrant destiné à de grands groupes d'adresses IP publiques vers une ENI unique dans votre VPC.

Auparavant, les passerelles Internet acceptaient uniquement le trafic destiné à des adresses IP publiques directement associées à des interfaces réseau dans le VPC. Le nombre d'adresses IP pouvant être associées à des interfaces réseau est limité pour les types d'instances. Cela entraîne des difficultés pour des secteurs tels que les télécommunications et l'Internet des objets (IoT), qui doivent gérer du trafic pour des groupes d'adresses IP dépassant ces limites.

Cet acheminement élimine les traductions d'adresses complexes sur les connexions Internet entrantes. Vous pouvez apporter vos propres groupes d'adresses IP publiques (BYOIP) et configurer votre passerelle Internet VPC pour qu'elle accepte et achemine le trafic de l'ensemble du groupe vers une interface réseau unique. Cette fonctionnalité est particulièrement utile pour les applications suivantes :

- Télécommunications : gestion de grands groupes d'adresses IP d'abonnés sans frais de traduction d'adresses
- IoT : consolidation du trafic provenant des adresses IP de plusieurs milliers d'appareils
- Tous les scénarios : acheminement de trafic au-delà des limites d'association de l'ENI

Vous pouvez intégrer ce routage au serveur de routage VPC pour des mises à jour dynamiques des routes en cas de basculement.

Principaux avantages

Cette approche du routage offre les avantages suivants :

- Aucune traduction d'adresses requise - Le routage direct permet d'éliminer la complexité liée à la traduction d'adresses réseau.
- Contournement des limites de l'ENI - Permet de gérer des groupes d'adresses IP qui dépassent les limites d'association des instances.
- Fonctionnalité optimisée pour l'industrie - Conçue pour répondre aux besoins des secteurs des télécommunications et de l'IoT.
- Basculement dynamique - S'intègre au serveur de routage pour des mises à jour automatiques.

Disponibilité

Vous pouvez utiliser cette fonctionnalité dans toutes les régions commerciales d'AWS, les régions AWS en Chine et les régions AWS GovCloud.

Table des matières

Avant de commencer

Avant de démarrer ce tutoriel, procédez aux vérifications suivantes :

1. Groupe BYOIP : assurez-vous que vous avez déjà apporté votre propre plage d'adresses IP dans AWS. Suivez la procédure décrite dans Bring your own IP addresses (BYOIP) in Amazon EC2.
2. Assurez-vous que votre groupe BYOIP est prêt à l'aide de la commande suivante :

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Recherchez votre groupe dans la sortie de la commande et vérifiez que `PoolAddressRanges` affiche les adresses `Available`.

3. Autorisations : assurez-vous que votre compte AWS dispose des autorisations requises pour créer des ressources VPC et des instances EC2 et pour gérer des groupes BYOIP.

Fonctionnement de cette fonctionnalité

Cette section présente les concepts techniques sur lesquels repose le routage d'entrée par passerelle Internet et explique comment le trafic circule d'Internet vers votre instance cible.

Pourquoi utiliser le routage d'entrée par passerelle Internet ?

Auparavant, les limites d'association de l'ENI nécessitaient une traduction des adresses pour consolider le trafic d'un grand nombre d'adresses IP. Cette amélioration élimine la complexité liée à cette opération en permettant le routage direct de groupes BYOIP vers des instances cibles.

Fonctionnement du routage

Cette fonctionnalité s'applique uniquement aux CIDR d'adresses IP publiques que vous apportez dans AWS selon le processus BYOIP. Ce processus permet de garantir que votre compte dispose du CIDR d'adresses IP publiques. Une fois que vous disposez du CIDR public BYOIP :

1. Vous devez associer ce groupe d'adresses IP publiques à une table de routage de passerelle Internet. La passerelle Internet doit déjà être associée à un VPC. Cette association permet au VPC d'accepter le trafic destiné au CIDR d'adresses IP. Assurez-vous que la passerelle Internet dispose d'une table de routage dédiée qui n'est partagée avec aucun sous-réseau.
2. Une fois que vous avez associé le groupe BYOIP à la table de routage de la passerelle Internet, vous pouvez entrer dans la table de routage une route dont la destination correspond au CIDR d'adresses IP ou à un sous-ensemble de celui-ci. La cible de cette route doit être l'ENI vers laquelle vous souhaitez acheminer le trafic.
3. Lorsque AWS reçoit le trafic destiné à votre CIDR BYOIP, AWS examine la table de routage de la passerelle Internet et achemine le trafic vers le VPC approprié.
4. Au sein du VPC, la passerelle Internet achemine le trafic vers l'ENI cible.
5. La cible (une ENI associée à votre charge de travail) traite le trafic.

Bonnes pratiques

- Gardez les tables de routage séparées : la table de routage de la passerelle Internet doit être réservée à la passerelle Internet. Ne l'associez à aucun sous-réseau VPC. Utilisez des tables de routage distinctes pour le routage des sous-réseaux.
- N'attribuez pas directement d'adresses IP BYOIP : n'associez pas les adresses IP publiques de votre groupe BYOIP directement à des instances EC2 ou des interfaces réseau. La fonctionnalité de routage d'entrée par passerelle Internet achemine le trafic vers les instances sans qu'une association directe d'adresse IP soit nécessaire.

Important

Lorsque la fonctionnalité Accès public au bloc VPC (BPA) est activée, elle bloque le trafic vers les sous-réseaux qui utilisent le routage d'entrée, même si vous avez défini une exclusion BPA au niveau des sous-réseaux. Les exclusions au niveau des sous-réseaux ne sont pas compatibles avec le routage d'entrée. Pour autoriser le trafic du routage d'entrée lorsque la fonctionnalité BPA est activée :

- désactivez complètement la fonctionnalité BPA ou
- utilisez une exclusion au niveau du VPC.

Étape 1 : Création d'un VPC

Exécutez cette étape pour créer le VPC qui hébergera votre instance cible et votre passerelle Internet.

Note

Assurez-vous que vous n'avez pas atteint votre limite de quota VPC. Pour de plus amples informations, consultez Quotas Amazon VPC.

AWS Console

1. Ouvrez la console VPC Amazon.
2. Sur le tableau de bord VPC, choisissez Create VPC (Créer un VPC).
3. Sous Ressources à créer, choisissez VPC uniquement.
4. Dans Nom de balise, entrez le nom de votre VPC (par exemple, **`IGW-Ingress-VPC`**).

5. Dans Bloc CIDR IPv4, entrez un bloc CIDR (par exemple, **`10.0.0.0/16`**).
6. Sélectionnez Create VPC (Créer un VPC).

AWS CLI

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=IGW-Ingress-VPC}]' --region us-east-1
```

Étape 2 : Création et attachement d'une passerelle Internet

Exécutez cette étape pour créer une passerelle Internet et l'attacher à votre VPC afin d'activer la connectivité Internet.

AWS Console

1. Ouvrez la console VPC Amazon.
2. Dans la console VPC, choisissez Passerelles Internet.
3. Choisissez Créer une passerelle Internet.
4. Dans Nom de balise, entrez le nom de votre passerelle Internet (par exemple, **`IGW-Ingress-Gateway`**).
5. Choisissez Créer une passerelle Internet.
6. Sélectionnez votre passerelle Internet et choisissez Actions, Attacher au VPC.
7. Sélectionnez votre VPC et choisissez Attacher une passerelle Internet.

AWS CLI

```
aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-
gateway,Tags=[{Key=Name,Value=IGW-Ingress-Gateway}]' --region us-east-1

aws ec2 attach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0 --region us-east-1
```

Remarque : remplacez les ID de ressource par les ID réels de l'étape précédente.

Étape 3 : Création d'un sous-réseau pour l'instance cible

Exécutez cette étape pour créer un sous-réseau dans lequel votre instance cible sera déployée.

AWS Console

1. Dans le panneau de navigation de la console VPC, choisissez Subnets (Sous-réseaux).
2. Choisissez Create subnet (Créer un sous-réseau).
3. Dans ID de VPC, choisissez votre VPC.
4. Entrez un nom dans Nom du sous-réseau, (par exemple, **`Target-Subnet`**).
5. Pour Availability Zone (Zone de disponibilité), vous pouvez choisir une zone pour votre sous-réseau ou conserver la zone par défaut No Preference (Aucune préférence) pour permettre à AWS de choisir à votre place.
6. Dans Bloc CIDR IPv4, sélectionnez Saisie manuelle et entrez un bloc CIDR (par exemple, **`10.0.1.0/24`**).
7. Choisissez Create subnet (Créer un sous-réseau).

AWS CLI

```
aws ec2 create-subnet \
    --vpc-id vpc-0123456789abcdef0 \
    --cidr-block 10.0.1.0/24 \
    --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Target-Subnet}]' \
    --region us-east-1
```

Étape 4 : Création d'une table de routage pour le sous-réseau

Exécutez cette étape pour créer une table de routage pour votre sous-réseau et l'associer à celui-ci.

AWS Console

1. Dans le volet de navigation de la console VPC, choisissez Tables de routage.
2. Choisissez Créer une table de routage.
3. Dans Nom, entrez le nom de la table de routage (par exemple, **`Target-Subnet-Route-Table`**).
4. Pour VPC, choisissez votre VPC.
5. Choisissez Créer une table de routage.
6. Sélectionnez votre table de routage et choisissez Actions, Modifier les associations de sous-réseau.
7. Sélectionnez votre sous-réseau et choisissez Enregistrer les associations.

AWS CLI

```
aws ec2 create-route-table \
    --vpc-id vpc-0123456789abcdef0 \
    --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Target-Subnet-
Route-Table}]' \
    --region us-east-1

aws ec2 associate-route-table \
    --route-table-id rtb-0987654321fedcba0 \
    --subnet-id subnet-0123456789abcdef0 \
    --region us-east-1
```

Étape 5 : Création d'un groupe de sécurité pour l'instance cible

Exécutez cette étape pour créer un groupe de sécurité qui contrôlera l'accès réseau à votre instance cible.

AWS Console

1. Dans le panneau de navigation de la console VPC, choisissez Groupes de sécurité.
2. Sélectionnez Create security group (Créer un groupe de sécurité).
3. Entrez un nom dans Nom du groupe de sécurité (par exemple, **`IGW-Target-SG`**).
4. Pour Description, saisissez **`Security group for IGW ingress routing target instance`**.
5. Pour VPC, sélectionnez votre VPC.
6. Pour ajouter des règles entrantes, choisissez Règles entrantes. Pour chaque règle, choisissez Ajouter une règle et spécifiez les informations suivantes :
   - Type : Toutes les ICMP - IPv4, Source : 0.0.0.0/0 (pour les tests ping).
   - Type : SSH, Port : 22, Source : 0.0.0.0/0 (pour EC2 Instance Connect).

> **Note**
>
> Ce groupe de sécurité ouvre les ports SSH à tout le trafic Internet pour ce tutoriel. Ce tutoriel est proposé à des fins pédagogiques. Il ne doit pas être configuré pour les environnements de production. En production, limitez l'accès SSH à des plages d'adresses IP spécifiques.

- Sélectionnez Create security group (Créer un groupe de sécurité).

AWS CLI

```
aws ec2 create-security-group \
    --group-name IGW-Target-SG \
    --description "Security group for IGW ingress routing target instance" \
    --vpc-id vpc-0123456789abcdef0 \
    --region us-east-1

aws ec2 authorize-security-group-ingress \
    --group-id sg-0123456789abcdef0 \
    --protocol icmp \
    --port -1 \
    --cidr 0.0.0.0/0 \
    --region us-east-1

aws ec2 authorize-security-group-ingress \
    --group-id sg-0123456789abcdef0 \
    --protocol tcp \
    --port 22 \
    --cidr 0.0.0.0/0 \
    --region us-east-1
```

Étape 6 : Lancement de l'instance EC2 cible

Exécutez cette étape pour lancer l'instance EC2 qui recevra le trafic de votre groupe BYOIP.

AWS Console

1. Ouvrez la console Amazon EC2.
2. Choisissez Launch instance (Lancer une instance).
3. Dans Nom, entrez le nom de l'instance (par exemple, **`IGW-Target-Instance`**).
4. Dans Images d'applications et de systèmes d'exploitation (Amazon Machine Image), choisissez AMI Amazon Linux 2023.
5. Dans Type d'instance, choisissez t2.micro (éligible à l'offre gratuite).
6. Dans Paire de clés (connexion), sélectionnez une paire de clés existante ou créez-en une.
7. Dans Paramètres réseau, choisissez Modifier et configurez les paramètres suivants :
   - VPC : sélectionnez votre VPC.

- Sous-réseau : sélectionnez votre sous-réseau.
- Attribuer automatiquement l'adresse IP publique : activez ce paramètre.
- Pare-feu (groupes de sécurité) : choisissez Sélectionner un groupe de sécurité existant, puis sélectionnez un groupe de sécurité.

8. Choisissez Launch instance (Lancer une instance).
9. Important : après le lancement, accédez aux détails de l'instance et notez l'ID d'interface réseau (qui commence par « eni- »). Vous en aurez besoin à l'étape 10.

AWS CLI

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name your-key-pair \
    --security-group-ids sg-0123456789abcdef0 \
    --subnet-id subnet-0123456789abcdef0 \
    --associate-public-ip-address \
    --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=IGW-Target-
Instance}]' \
    --region us-east-1
```

Pour rechercher l'ID de l'ENI dans la console :

1. Dans la console EC2, sélectionnez votre instance.
2. Accédez à l'onglet Mise en réseau.
3. Notez l'ID d'interface réseau (par exemple, `eni-0abcdef1234567890`).

Pour rechercher l'ID de ENI à l'aide de l'AWS CLI :

```
aws ec2 describe-instances --instance-ids i-0123456789abcdef0 --query
 'Reservations[0].Instances[0].NetworkInterfaces[0].NetworkInterfaceId' --output text
 --region us-east-1
```

Étape 7 : Création de la table de routage de la passerelle Internet

Exécutez cette étape pour créer pour la passerelle Internet une table de routage dédiée à la gestion du routage d'entrée.

AWS Console

1. Dans la console VPC, choisissez Tables de routage.
2. Choisissez Créer une table de routage.
3. Dans Nom, entrez le nom de la table de routage (par exemple, **`IGW-Ingress-Route-Table`**).
4. Pour VPC, choisissez votre VPC.
5. Choisissez Créer une table de routage.
6. Sélectionnez la table de routage et choisissez l'onglet Associations de périphérie.
7. Choisissez Modifier les associations de périphérie.
8. Sélectionnez votre passerelle Internet et choisissez Enregistrer les modifications.

AWS CLI

```
aws ec2 create-route-table \
    --vpc-id vpc-0123456789abcdef0 \
    --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=IGW-Ingress-
Route-Table}]' \
    --region us-east-1
```

Étape 8 : Association de la table de routage à la passerelle Internet

Exécutez cette étape pour associer la table de routage à la passerelle Internet afin d'activer la fonctionnalité de routage d'entrée.

AWS Console

1. Dans le panneau de navigation de la console VPC, choisissez Tables de routage, puis sélectionnez la table de routage que vous avez créée.
2. Sur l'onglet Associations périphériques, choisissez Modifier les associations périphériques.
3. Cochez la case correspondant à la passerelle Internet.
4. Sélectionnez Enregistrer les modifications.

AWS CLI

```
aws ec2 associate-route-table \
```

```
    --route-table-id rtb-0123456789abcdef0 \
    --gateway-id igw-0123456789abcdef0 \
    --region us-east-1
```

Étape 9 : Association du groupe BYOIP à la passerelle Internet

Exécutez cette étape pour associer le groupe BYOIP à la table de routage de la passerelle Internet afin que le VPC puisse accepter du trafic pour votre plage d'adresses IP.

AWS Console

1. Dans le volet de navigation de la console VPC, choisissez Tables de routage, puis sélectionnez la table de routage de passerelle Internet que vous avez créée.
2. Cliquez sur l'onglet Associations de groupes IPv4.
3. Cliquez sur le bouton Modifier les associations.
4. Sélectionnez votre groupe BYOIP (par exemple, `pool-12345678901234567`).
5. Cliquez sur le bouton Enregistrer les associations.

AWS CLI

```
aws ec2 associate-route-table \
    --route-table-id rtb-0123456789abcdef0 \
    --public-ipv4-pool pool-12345678901234567 \
    --region us-east-1
```

Remarque : remplacez `rtb-0123456789abcdef0` par l'ID de la table de routage de votre passerelle Internet et `pool-12345678901234567` par l'ID de votre groupe BYOIP.

Étape 10 : Ajout d'une route statique pour cibler l'instance

Exécutez cette étape pour ajouter une route qui dirige le trafic de votre plage BYOIP vers l'interface réseau de votre instance cible.

AWS Console

1. Dans le volet de navigation de la console VPC, choisissez Tables de routage, puis sélectionnez la table de routage de passerelle Internet que vous avez créée.
2. Choisissez Actions, Modifier les routes.

3. Choisissez Ajouter une route.
4. Dans Destination, entrez votre CIDR BYOIP ou un sous-ensemble de celui-ci (par exemple, **`203.0.113.0/24`**). Le préfixe doit être compris entre /23 et /28.
5. Dans Cible, sélectionnez Interface réseau et entrez l'ID d'ENI de votre instance (par exemple, `eni-0abcdef1234567890`).
6. Sélectionnez Enregistrer les modifications.

AWS CLI

```
aws ec2 create-route \
    --route-table-id rtb-0123456789abcdef0 \
    --destination-cidr-block 203.0.113.0/24 \
    --network-interface-id eni-0abcdef1234567890 \
    --region us-east-1
```

Étape 11 : Configuration de l'instance cible

Exécutez cette étape pour configurer votre instance cible afin qu'elle gère correctement le trafic destiné aux adresses BYOIP.

Important : exécutez cette étape de configuration de l'instance avant de tester la connectivité (étape 12). Pour garantir le bon fonctionnement du routage d'entrée, l'instance doit être configurée pour répondre aux adresses BYOIP.

AWS Console

1. Connectez-vous à l'instance cible à l'aide d'EC2 Instance Connect :
   - Dans la console EC2, sélectionnez votre instance.
   - Choisissez Actions > Connecter.
   - Sélectionnez l'onglet EC2 Instance Connect.
   - Choisissez Se connecter.
2. Ajoutez une adresse IP BYOIP spécifique à l'interface de l'instance :

   Commencez par rechercher le nom de votre interface réseau :

   ```
   ip link show
   ```

Ajoutez ensuite l'adresse IP (remplacez `203.0.113.10` par une adresse IP de votre plage BYOIP) :

```
sudo ip addr add 203.0.113.10/32 dev eth0
```

Remarque : remplacez `203.0.113.10` par l'adresse IP de votre plage BYOIP que vous souhaitez tester. Le nom de l'interface peut être `eth0`, `ens5` ou une valeur similaire selon le type d'instance.

3. Désactivez la surveillance de la source/destination dans la console EC2 :

   - Sélectionnez votre instance.
   - Accédez à l'onglet Mise en réseau et cliquez sur l'interface réseau.
   - Choisissez Actions, Modifier la surveillance de la source/destination, Désactiver.

AWS CLI

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-0abcdef1234567890 \
    --no-source-dest-check \
    --region us-east-1
```

Étape 12 : Configuration de l'instance pour la gestion du trafic

Exécutez cette étape pour ajouter des adresses BYOIP à votre instance et désactiver la surveillance de la source/destination afin de permettre une gestion appropriée du trafic.

AWS Console

1. Connectez-vous à l'instance cible à l'aide d'EC2 Instance Connect :

   - Dans la console EC2, sélectionnez votre instance.
   - Choisissez Actions > Connecter.
   - Sélectionnez l'onglet EC2 Instance Connect.
   - Choisissez Se connecter.

2. Ajoutez une adresse IP BYOIP spécifique à l'interface de l'instance :

   Commencez par rechercher le nom de votre interface réseau :

```
ip link show
```

Ajoutez ensuite l'adresse IP (remplacez `ens5` par le nom réel de votre interface) :

```
sudo ip addr add 203.0.113.10/32 dev ens5
```

Remarque : remplacez `203.0.113.10` par l'adresse IP de votre plage BYOIP que vous souhaitez tester. Le nom de l'interface peut être `eth0`, `ens5` ou une valeur similaire selon le type d'instance.

3. Désactivez la surveillance de la source/destination dans la console EC2 :

   - Sélectionnez votre instance.
   - Accédez à l'onglet Mise en réseau et cliquez sur l'interface réseau.
   - Choisissez Actions, Modifier la surveillance de la source/destination, Désactiver.

AWS CLI

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-0abcdef1234567890 \
    --no-source-dest-check \
    --region us-east-1
```

Étape 13 : Test de la connectivité

Exécutez cette étape pour vérifier que le trafic Internet est correctement acheminé vers l'instance cible via les adresses BYOIP.

1. Sur l'instance cible, surveillez le trafic entrant à l'aide de la commande tcpdump :

   ```
   sudo tcpdump -i any icmp
   ```

2. Depuis un autre terminal ou ordinateur, testez la connectivité à votre adresse IP BYOIP :

   ```
   ping 203.0.113.10
   ```

3. Résultats attendus :

   - Le ping doit aboutir et afficher les réponses de votre adresse IP BYOIP.

- La commande tcpdump doit afficher les paquets entrants pour l'adresse BYOIP, comme dans l'exemple ci-dessous :

```
12:34:56.789012 IP 203.0.113.100 > 203.0.113.10: ICMP echo request, id 1234, seq
 1, length 64
12:34:56.789123 IP 203.0.113.10 > 203.0.113.100: ICMP echo reply, id 1234, seq 1,
 length 64
```

- Le trafic doit sembler provenir d'adresses IP externes, ce qui prouve que le routage d'entrée par passerelle Internet achemine le trafic Internet vers votre instance.

Résolution des problèmes

Cette section vous aide à résoudre les problèmes courants que vous êtes susceptible de rencontrer lors de la configuration du routage d'entrée par passerelle Internet.

Le trafic n'est pas acheminé jusqu'à l'instance

- Vérifiez que l'ID d'ENI spécifié comme cible pour la table de routage est correct.
- Vérifiez que le groupe BYOIP est associé à la table de routage de la passerelle Internet.
- Vérifiez que la surveillance de la source/destination est désactivée sur l'instance.
- Assurez-vous que les groupes de sécurité autorisent le type de trafic testé.

La création de route échoue

- Vérifiez que le groupe BYOIP est correctement associé à la table de routage.
- Vérifiez que le CIDR de destination se trouve dans votre plage BYOIP.
- Vérifiez que l'ENI cible existe et qu'elle est attachée à une instance en cours d'exécution.
- Assurez-vous que votre préfixe BYOIP est compris entre /23 et /28 (les préfixes situés en dehors de cette plage ne sont pas pris en charge).

Le ping ou la connectivité échoue

- Vérifiez que les adresses IP sont ajoutées à l'interface de l'instance.
- Vérifiez que les groupes de sécurité autorisent le protocole ICMP (pour le ping) ou les ports appropriés.
- Vérifiez que l'instance s'affiche comme étant en cours d'exécution.
- Effectuez des tests à partir de plusieurs emplacements externes.

Option avancée : intégration du serveur de routage pour le routage dynamique

Cette fonctionnalité s'intègre au serveur de routage VPC pour procurer les avantages suivants dans les environnements nécessitant un basculement automatique :

- Mise à jour dynamique des routes en cas de défaillances d'instances.
- Élimination des interventions manuelles pour la gestion des routes.
- Disponibilité de niveau professionnel pour les charges de travail essentielles.

Ces avantages sont particulièrement importants pour les secteurs des télécommunications et de l'IoT, pour lesquels une haute disponibilité est essentielle.

> **Note**
>
> Lorsque vous utilisez le serveur de routage avec plusieurs pairs BGP, vous devez savoir que le nombre de pairs BGP pouvant publier le même préfixe sur la même table de routage à l'aide du serveur de routage est limité à 32.

L'intégration au serveur de routage AWS peut être utile dans les environnements nécessitant un routage dynamique, un basculement automatique et une répartition de la charge entre plusieurs instances. Le serveur de routage permet de remplacer les routes statiques par un routage dynamique basé sur le protocole BGP, ce qui offre les avantages suivants :

- Publication des routes dynamiques par les instances via le protocole BGP.
- Basculement automatique entre plusieurs instances cibles.
- Répartition de la charge entre plusieurs points de terminaison.
- Gestion centralisée des routes via le protocole BGP.

Ce cas d'utilisation est important pour les déploiements d'entreprise nécessitant une haute disponibilité et des capacités de routage dynamique. Pour obtenir des instructions détaillées sur la configuration du serveur de routage, consultez la documentation du serveur de routage AWS.

Nettoyage

Pour éviter des frais continus, supprimez les ressources que vous avez créées pour ce tutoriel :

Étape 1 : Résiliation de l'instance EC2

Exécutez cette étape pour résilier l'instance EC2 et ne plus supporter de frais liés aux ressources de calcul.

AWS Console

1. Ouvrez la console Amazon EC2.
2. Dans le panneau de navigation de la console EC2, choisissez Instances.
3. Sélectionnez l'instance et choisissez État de l'instance, puis Résilier l'instance.
4. Choisissez Résilier pour confirmer.

AWS CLI

```
aws ec2 terminate-instances --instance-ids i-0123456789abcdef0 --region us-east-1
```

Étape 2 : Détachement de la passerelle Internet du VPC

Exécutez cette étape pour détacher la passerelle Internet de votre VPC et la supprimer.

AWS Console

1. Ouvrez la console VPC Amazon.
2. Dans le panneau de navigation de la console VPC, choisissez Passerelles Internet.
3. Sélectionnez la passerelle Internet, puis choisissez Actions, Détacher du VPC.
4. Choisissez Détacher la passerelle Internet.
5. Une fois le détachement effectué, choisissez Actions, Supprimer la passerelle Internet.
6. Choisissez Supprimer la passerelle Internet.

AWS CLI

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0 --region us-east-1

aws ec2 delete-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --region
 us-east-1
```

Étape 3 : Suppression du VPC

Exécutez cette étape pour supprimer le VPC et toutes les ressources associées afin de terminer le processus de nettoyage.

AWS Console

1. Dans la console VPC, sélectionnez Vos VPC.
2. Sélectionnez le VPC approprié, puis choisissez Actions, Supprimer le VPC.
3. Tapez **`delete`** pour confirmation la suppression et choisissez Supprimer.

AWS CLI

```
aws ec2 delete-vpc --vpc-id vpc-0123456789abcdef0 --region us-east-1
```

> **Note**
>
> La suppression du VPC entraîne la suppression des sous-réseaux, des tables de routage et des groupes de sécurité associés.

> **Note**
>
> Ce processus de nettoyage ne supprime pas votre groupe BYOIP. Celui-ci reste disponible pour une utilisation ultérieure.

Routage dynamique dans votre VPC à l'aide du serveur de routage VPC

Le serveur de routage Amazon VPC simplifie le routage du trafic entre les charges de travail déployées au sein d'un VPC et de ses passerelles Internet. Grâce à cette fonctionnalité, le serveur de routage VPC met à jour de manière dynamique les tables de routage VPC et de passerelle Internet avec vos IPv6 itinéraires IPv4 ou itinéraires préférés afin de garantir la tolérance aux pannes de routage pour ces charges de travail. Cela vous permet de réacheminer automatiquement le trafic au sein d'un VPC, ce qui améliore la facilité de gestion du routage VPC et l'interopérabilité avec des charges de travail tierces.

Le serveur de routage prend en charge les types de tables de routage suivants :

- Tables de routage de VPC non associées à des sous-réseaux
- Tables de routage des sous-réseaux
- Tables de routage de passerelle Internet

Le serveur de routage ne prend pas en charge les tables de routage associées à des passerelles privées virtuelles. Pour propager des routes dans une table de routage de passerelle de transit, utilisez la documentation sur Transit Gateway Connect.

Quotas

Pour connaître les quotas associés à un serveur de routage Amazon VPC, consultez la section sur les quotas des serveurs de routage.

Tarification

Pour plus d'informations sur les coûts associés au serveur de routage Amazon VPC, consultez l'onglet Serveur de routage VPC sur la page de tarification d'Amazon VPC.

Table des matières

Terminologie

Ce guide utilise les termes suivants :

- FIB : la base d'informations de transfert (FIB) sert de table de transfert pour les routes que le serveur a déterminées comme étant les routes offrant le meilleur chemin dans la RIB après avoir évalué toutes les informations et stratégies de routage disponibles. Les routes FIB sont installées sur les tables de routage. La FIB est recalculée chaque fois que des modifications sont apportées à la RIB.
- RIB : la base d'informations de routage (RIB) est une base de données qui sert à stocker toutes les informations de routage et les données de topologie de réseau collectées par un routeur ou un système de routage, telles que les routes acquises auprès de pairs BGP. La RIB est constamment

mise à jour à mesure que de nouvelles informations de routage sont reçues ou que les routes existantes changent. Le serveur de routage est ainsi assuré de toujours disposer de la vue de la topologie de réseau la plus récente et de pouvoir prendre des décisions de routage optimales.

- Serveur de routage : le composant du serveur de routage met à jour les tables de routage de votre VPC et de votre passerelle Internet avec les IPv6 routes IPv4 ou de votre base d'informations de transfert (FIB). Le serveur de routage représente une FIB et une RIB uniques.
- Association d'un serveur de routage : l'association d'un serveur de routage est la connexion établie entre un serveur de routage et un VPC.
- Point de terminaison de serveur de route : un point de terminaison de serveur de route est un composant AWS géré au sein d'un sous-réseau qui facilite les connexions BGP (Border Gateway Protocol) entre votre serveur de route et vos homologues BGP.
- homologue du serveur de route : un homologue du serveur de route est une session entre le point de terminaison d'un serveur de route et le périphérique déployé AWS (tel qu'un dispositif de pare-feu ou une autre fonction de sécurité réseau exécutée sur une instance EC2). Le dispositif doit répondre aux exigences suivantes :
  - Disposer d'une interface réseau Elastic dans le VPC
  - Prendre en charge le protocole BGP
  - Être capable de lancer des sessions BGP
- Propagation du serveur de routage : lorsqu'elle est activée, la propagation du serveur de routage installe les routes présentes dans la FIB sur la table de routage que vous avez spécifiée. Supports du serveur de IPv6 routage IPv4 et propagation des itinéraires.

Fonctionnement du serveur de routage Amazon VPC

Cette section décrit le fonctionnement du serveur de routage Amazon VPC et vous aide à comprendre comment il garantit une tolérance aux pannes de routage pour les charges de travail exécutées dans des sous-réseaux.

Table des matières

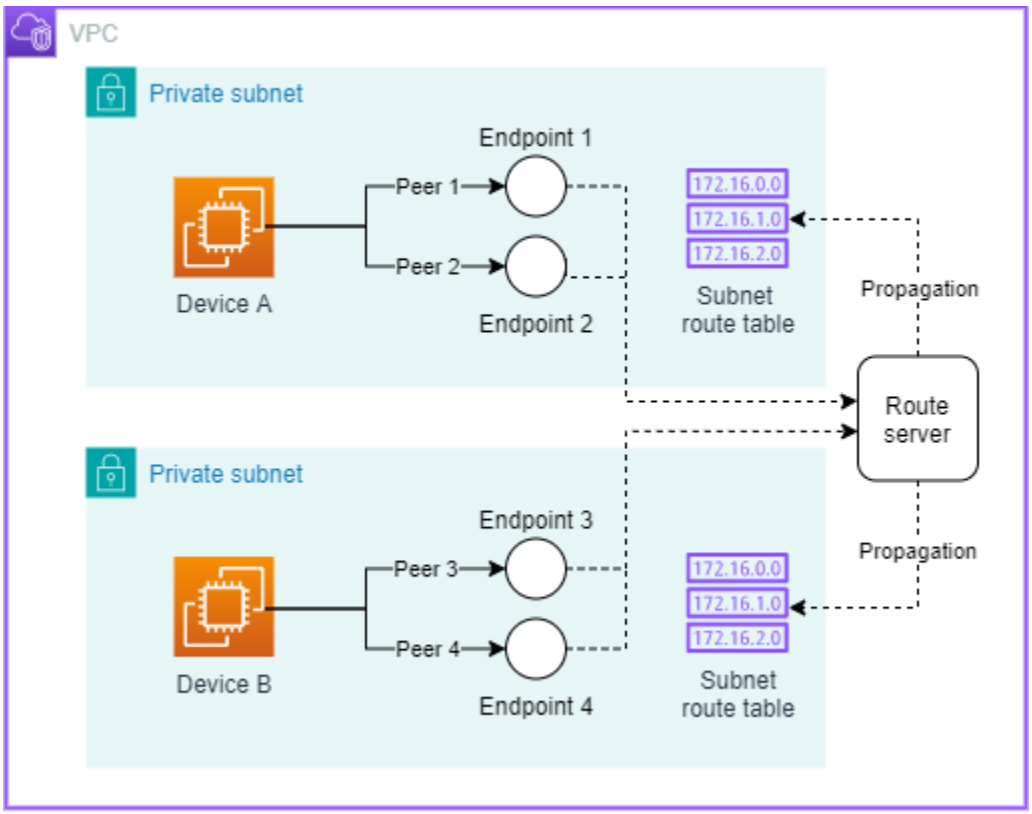
Présentation de

Fonctionnement du serveur de routage Amazon VPC :

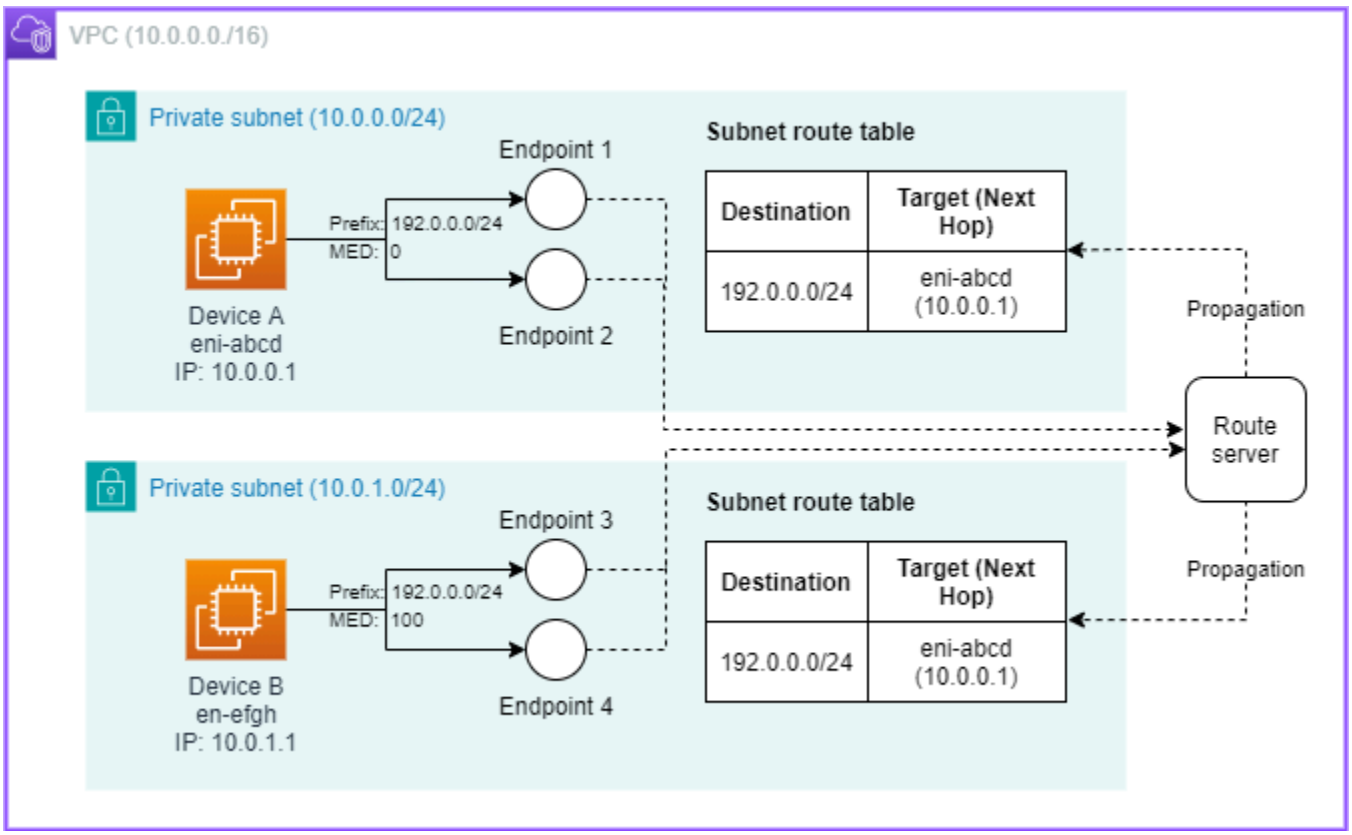
1. Vous avez configuré un dispositif réseau (comme un pare-feu exécuté sur une instance EC2 dans le VPC) de manière à utiliser le serveur de routage Amazon VPC.
2. Le dispositif réseau tombe en panne.
3. Les points de terminaison du serveur de routage détectent la défaillance à travers le protocole de détection de transfert bidirectionnel (BFD) configuré sur le pair du serveur de routage.
4. Les points de terminaison du serveur de routage mettent à jour le serveur de routage afin de retirer les routes présentes dans une base d'informations de routage (RIB) pour lesquelles le dispositif défaillant constitue le prochain saut.
5. Le serveur de routage calcule une base d'informations de transfert (FIB) à partir de la RIB, en sélectionnant les meilleures routes disponibles.
6. Le serveur de routage met à jour les tables de routage configurées avec les routes issues de la FIB.
7. Tout nouveau trafic est transféré vers le dispositif de secours.

Diagrammes

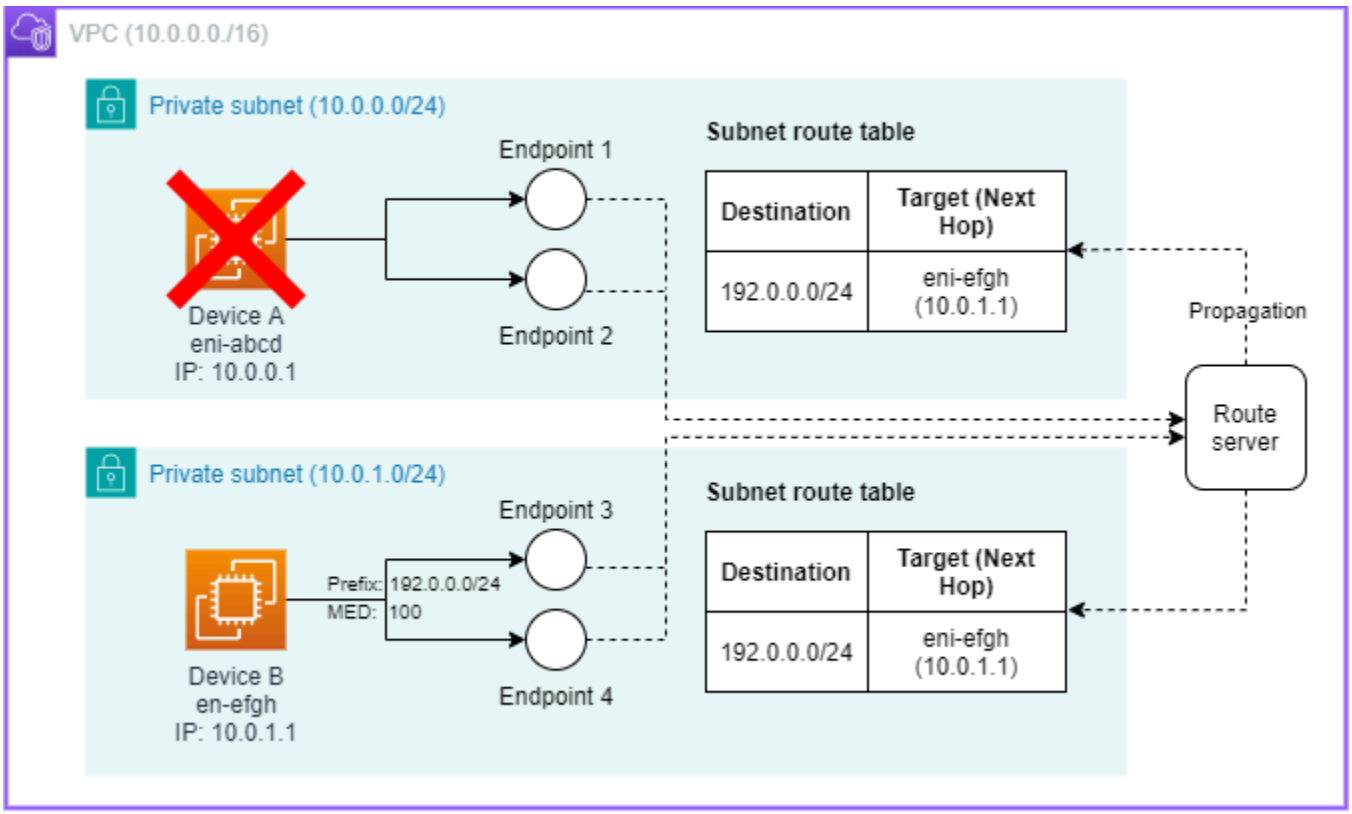
Voici un exemple de diagramme d'un serveur de routage VPC avec des points de terminaison de serveur de routage configurés pour des dispositifs au sein de deux sous-réseaux.



Sur la base de l'exemple ci-dessus, l'exemple suivant présente une conception plus détaillée, dans laquelle le dispositif A et le dispositif B annoncent via le protocole BGP qu'ils peuvent accepter tout trafic dont l'adresse IP de destination se situe dans la plage 192.0.0.0/24 (entre 192.0.0.0 et 192.0.0.255). L'attribut Multi-Exit Discriminator (MED) dont la valeur est 0 indique au serveur de routage que le dispositif A doit être préféré au dispositif B. Le serveur de routage reçoit la route ainsi que l'attribut MED du dispositif A et installe cette route dans les tables de routage des sous-réseaux avec l'interface réseau du dispositif A comme « prochain saut ». Par conséquent, tout trafic au sein du sous-réseau dont l'adresse IP de destination se situe dans la plage 192.0.0.0/24 est envoyé au dispositif A. Le dispositif A traite ensuite le trafic et le retransmet. Le trafic au sein de l'un ou l'autre des sous-réseaux (10.0.0.0/24 ou 10.0.1.0/24) qui est destiné à 192.0.0.0/24 sera acheminé vers le dispositif A eni-abcd (10.0.0.1) comme prochain saut.



Le dernier exemple, présenté ci-dessous, décrit la façon dont le serveur de routage gère le basculement. Dans le cas où l'attribut MED le plus élevé indique au serveur de routage que le dispositif A est à préférer au dispositif B, si le dispositif A eni-abcd (10.0.0.1) tombe en panne, le serveur de routage mettra à jour les tables de routage des sous-réseaux, et le trafic vers 192.0.0.0/24 sera acheminé vers le dispositif B eni-efgh (10.0.1.1) comme prochain saut.



Journalisation par le pair du serveur de routage

Utilisez la journalisation par le pair du serveur de routage VPC lorsque vous devez :

- surveiller l'état de sessions BGP et BFD ;
- résoudre des problèmes de connexion ;
- consulter l'historique des modifications apportées aux sessions ;
- suivre l'état du réseau.

Tarification

- CloudWatch: Les frais d'ingestion de données et d'archivage pour les journaux vendus s'appliquent lorsque vous publiez les journaux homologues du serveur de routage vers CloudWatch Logs.
- S3 : des frais d'ingestion et d'archivage de données s'appliquent pour les journaux payants lorsque vous publiez des journaux de pair du serveur de routage dans Amazon S3.
- Data Firehose : des frais d'ingestion et de diffusion standard s'appliquent.

Les journaux vendus sont des journaux provenant de AWS services spécifiques qui sont disponibles à une tarification par volume et fournis à CloudWatch Logs, Amazon S3 ou Amazon Data Firehose. Pour plus d'informations, ouvrez Amazon CloudWatch Pricing, sélectionnez Logs et recherchez Vended Logs.

Exemple de format de journal

```
{
    "resource_arn": "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0",
    "event_timestamp": 1746643505367,
    "type": "RouteStatus",
    "status": "ADVERTISED",
    "message": {
        "prefix": "10.24.34.0/32",
        "asPath": "65000",
        "med": 100,
        "nextHopIp": "10.24.34.1"
    }
}

{
    "resource_arn": "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0",
    "event_timestamp": 1746643490000,
    "type": "BGPStatus",
    "status": "UP",
    "message": null
}
```

Où :

- L'élément `resource_arn` correspond à l'ARN du pair du serveur de routage.
- L'élément `event_timestamp` correspond à l'horodatage de l'événement.
- L'élément `type` correspond au type des événements du journal que nous produisons (`RouteStatus`, `BGPStatus`, `BFDStatus`).
- Le champ `status` correspond à la mise à jour de l'état.
  - Messages de type `RouteStatus` :
    - `ADVERTISED` signifie que la route a été annoncée par le pair
    - `UPDATED` signifie que la route existante a été mise à jour par le pair.

    - `WITHDRAWN` signifie que la route a été retirée par le pair.
  - Mises à jour associées à `BFDStatus` et `BGPStatus`
    - `UP`, `DOWN`.
- Le `message` champ n'est actuellement utilisé que pour les attributs de route du type de RouteStatus message, mais il peut être rempli avec des informations pertinentes pour n'importe quel type de message.

AWS Management Console

Pour créer des journaux de pair du serveur de routage :

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sous Cloud privé virtuel, sélectionnez Serveurs de routage.
3. Sur la page Serveurs de routage, sélectionnez Serveur de routages pairs.
4. Choisissez l'onglet Livraison des journaux.
5. Choisissez Ajouter la livraison des journaux.
6. Choisissez une destination et configurez les paramètres :
   - Amazon CloudWatch Logs
     - Type de journal : types des journaux à livrer. Le seul type de journal pris en charge est EVENT_LOGS.
     - Groupe de journaux de destination : groupe de journaux dans lequel les journaux seront envoyés. CloudWatch Vous pouvez sélectionner un groupe de journaux existant ou en créer un nouveau (exemple :/aws/vpc/route-server-peers).
     - Sélection du champ : champs de données à inclure dans vos journaux.
     - Format de sortie : mode de formatage des journaux :
       - JSON : format structuré pour le traitement informatique
       - Texte : format texte brut
     - Délimiteur de champs : en cas d'utilisation du format texte, il s'agit du caractère qui sépare les champs (exemple : virgule, tabulation, espace).
   - Amazon S3
     - Compte croisé - Envoi de journaux à différents AWS comptes

- Type de journal : types des journaux à livrer. Le seul type de journal pris en charge est EVENT_LOGS.
- ARN de destination de livraison : nom de ressource Amazon du compartiment S3 dans un autre AWS compte où les journaux seront envoyés.
- Sélection du champ : champs de données à inclure dans vos journaux.
- Suffixe : terminaison ajoutée aux noms des fichiers journaux (exemple : .log, .txt).
- Compatible Hive : lorsque cette option est activée, les journaux sont organisés dans une structure de dossiers compatible avec les outils basés sur Hive pour faciliter les recherches avec des services tels qu'Amazon Athena.
- Délimiteur de champs : en cas d'utilisation du format texte, il s'agit du caractère qui sépare les champs.

- Dans le compte actuel
  - Type de journal : types des journaux à livrer. Le seul type de journal pris en charge est EVENT_LOGS.
  - Compartiment S3 de destination : compartiment S3 de votre compte dans lequel les journaux seront envoyés. Vous pouvez spécifier le chemin d'un sous-dossier.
  - Sélection du champ : champs de données à inclure dans vos journaux.
  - Suffixe : terminaison ajoutée aux noms des fichiers journaux (exemple : .log, .txt).
  - Compatible Hive : lorsque cette option est activée, les journaux sont organisés dans une structure de dossiers compatible avec les outils basés sur Hive pour faciliter les recherches.
  - Délimiteur de champs : en cas d'utilisation du format texte, il s'agit du caractère qui sépare les champs.

- Amazon Data Firehose
  - Compte croisé
    - Type de journal : types des journaux à livrer. Le seul type de journal pris en charge est EVENT_LOGS.
    - ARN de destination de livraison : nom de ressource Amazon du flux de diffusion Firehose dans un autre AWS compte.
    - Sélection du champ : champs de données à inclure dans vos journaux.
    - Délimiteur de champs : en cas d'utilisation du format texte, il s'agit du caractère qui sépare les champs.

- Dans le compte actuel
  - Type de journal : types des journaux à livrer. Le seul type de journal pris en charge est EVENT_LOGS.
  - Flux de destination de diffusion : flux de diffusion Firehose de votre compte dans lequel les journaux seront envoyés. Le flux doit utiliser le type de source « Direct PUT ».
  - Sélection du champ : champs de données à inclure dans vos journaux.
  - Format de sortie : mode de formatage des journaux :
    - JSON : format structuré pour le traitement informatique
    - Texte : format texte brut
  - Délimiteur de champs : en cas d'utilisation du format texte, il s'agit du caractère qui sépare les champs.

Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes de l'AWS CLI . La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Pour créer des journaux de pair du serveur de routage :

1. Utilisez la commande put-delivery-source.
   - Exemple de demande

```
aws logs put-delivery-source --name "source-rsp-1234567890abcdef0" --
resource-arn "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0" --log-type "EVENT_LOGS"
```

   - Exemple de réponse

```
{
     "deliverySource": {
        "name": "source-rsp-1234567890abcdef0",
        "arn": "arn:aws:logs:us-east-1:111122223333:delivery-source:source-
rsp-1234567890abcdef0",
        "resourceArns": [
```

```
            "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0"
        ],
        "service": "ec2",
        "logType": "EVENT_LOGS"
    }
}
```

2. Utilisez la commande put-delivery-destination.

   - L'exemple de AWS CLI suivant crée un journal de serveur de routage. Les journaux sont livrés au groupe de journaux spécifié.
   - Exemple de demande

```
aws logs put-delivery-destination --name "destination-rsp-abcdef01234567890"
 --destination-resource-arn "arn:aws:logs:us-east-1:111122223333:log-group:/
aws/vendedlogs/ec2/route-server-peer/EVENT_LOGS/rsp-abcdef01234567890"
```

   - Exemple de réponse

```
{
     "deliveryDestination": {
        "name": "destination-rsp-abcdef01234567890",
        "arn": "arn:aws:logs:us-east-1:111122223333:delivery-
destination:destination-rsp-abcdef01234567890",
        "deliveryDestinationType": "CWL",
        "deliveryDestinationConfiguration": {
            "destinationResourceArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/vendedlogs/ec2/route-server-peer/
EVENT_LOGS/rsp-abcdef01234567890"
        }
    }
}
```

3. Utilisez la commande create-delivery.

   - Exemple de demande

```
aws logs create-delivery --delivery-source-name "source-rsp-1234567890abcdef0"
 --delivery-destination-arn "arn:aws:logs:us-east-1:111122223333:delivery-
destination:destination-rsp-abcdef01234567890"
```

   - Exemple de réponse

```
{
     "delivery": {
        "id": "1234567890abcdef0",
        "arn": "arn:aws:logs:us-
east-1:111122223333:delivery:1234567890abcdef0",
        "deliverySourceName": "source-rsp-1234567890abcdef0",
        "deliveryDestinationArn": "arn:aws:logs:us-
east-1:111122223333:delivery-destination:destination-rsp-abcdef01234567890",
        "deliveryDestinationType": "CWL",
        "recordFields": [
            "resource_arn",
            "event_timestamp",
            "type",
            "status",
            "message"
        ]
    }
}
```

Didacticiel de premiers pas

Ce tutoriel vous guide tout au long du processus d'installation et de configuration du serveur de routage VPC en vue d'activer le routage dynamique dans votre VPC. Vous apprendrez à créer et à configurer tous les composants nécessaires, à établir un appairage BGP et à en vérifier le bon fonctionnement. Le tutoriel couvre tout, de la configuration IAM initiale jusqu'aux tests, en passant par le nettoyage.

Avant de commencer ce tutoriel, assurez-vous de ce qui suit :

- Accès administratif à votre AWS compte
- Vous disposez d'un VPC avec au moins deux sous-réseaux dans lesquels vous souhaitez activer le routage dynamique.
- Vous disposez de dispositifs réseau (tels que des pare-feu exécutés sur des instances EC2) qui prennent en charge le protocole BGP et peuvent servir de dispositifs pairs du serveur de routage.
- Connaissance de base des concepts BGP et de la mise en réseau AWS

Les étapes peuvent être effectuées à l'aide de la console AWS de gestion ou AWS CLI. Les deux méthodes sont fournies pour chaque étape.

Durée estimée de réalisation des étapes : entre 15 et 30 minutes

Étapes

Étape 1 : configuration des autorisations de rôle IAM requises

Pour utiliser un serveur de routage VPC, assurez-vous que le rôle ou l'utilisateur IAM que vous utilisez dispose des autorisations IAM requises. Vous trouverez ci-dessous un guide indiquant les autorisations requises pour chaque API :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateRouteServer",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteRouteServer",
            "Effect": "Allow",
            "Action": [
                "sns:DeleteTopic"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "CreateRouteServerEndpoint",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteRouteServerEndpoint",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateRouteServerPeer",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteRouteServerPeer",
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Étape 2 : création d'un serveur de routage

Suivez les étapes décrites dans cette section pour créer un serveur de routage.

Le composant du serveur de routage met à jour les tables de routage de votre VPC et de votre passerelle Internet avec les IPv6 routes IPv4 ou de votre base d'informations de transfert (FIB). Le serveur de routage représente une FIB et une RIB uniques.

AWS Management Console

Pour créer un serveur de routage

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sous Cloud privé virtuel, sélectionnez Serveurs de routage.
3. Sur la page Serveurs de routage, sélectionnez Créer un serveur de routage.
4. Sur la page Créer un serveur de routage, configurez les paramètres suivants :
   - Dans Nom, entrez le nom de votre serveur de route (par exemple, « my-route-server -01"). Le nom doit contenir 255 caractères au maximum.
   - Dans ASN côté Amazon, saisissez une valeur ASN BGP. Cette valeur doit se situer dans la plage 1-4294967295. Nous vous recommandons d'utiliser un ASN privé situé dans la plage 64512-65534 (ASN 16 bits) ou dans la plage 4200000000-4294967294 (ASN 32 bits).
   - Dans Conserver les routes, sélectionnez Activer ou Désactiver. Cette option détermine si les routes doivent être maintenues une fois toutes les sessions BGP terminées :
     - Si cette option est activée : les routes seront conservées dans la base de données de routage du serveur de routage, même si toutes les sessions BGP se terminent.
     - Si cette option est désactivée : les routes seront supprimées de la base de données de routage à la fin de toutes les sessions BGP.
   - Si vous avez activé la conservation des routes, dans Durée de conservation, saisissez une valeur comprise entre 1 et 5 minutes. Cette durée indique le temps pendant lequel le serveur de routage doit patienter avant d'annuler la conservation des routes une fois le protocole BGP rétabli. Par exemple, si vous définissez cette durée sur 1 minute, votre dispositif aura une minute après avoir rétabli le protocole BGP pour réacquérir et annoncer ses routes avant que le serveur de routage ne reprenne ses fonctionnalités normales.

Bien qu'une minute soit généralement suffisante, vous pouvez configurer cette durée jusqu'à 5 minutes si votre réseau BGP a besoin de plus de temps pour rétablir et réacquérir entièrement toutes les routes.

- (Facultatif) Pour activer les notifications SNS en cas de changement du statut BGP, activez l'option Activer les notifications SNS. L'activation des notifications SNS permet de conserver les modifications de statut des sessions BGP ou BFD sur les pairs de serveurs de routage et les notifications de maintenance des points de terminaison du serveur de routage dans une rubrique SNS provisionnée par AWS. Pour plus de détails sur ces notifications, consultez le tableau Détails des notifications SNS ci-dessous.

5. (Facultatif) Pour ajouter des balises à votre serveur de routage, faites défiler la page jusqu'à la section Balises – facultatif et sélectionnez Ajouter une nouvelle balise. Saisissez une clé et une valeur facultative pour chaque balise. Vous pouvez ajouter jusqu'à 50 balises.
6. Passez en revue vos paramètres et sélectionnez Créer un serveur de routage.
7. Attendez que le serveur de routage soit créé. Une fois cette étape terminée, vous serez redirigé vers la page Serveurs de routage, sur laquelle vous pourrez voir votre nouveau serveur de routage dans la liste à l'état Disponible.

Command line

Procédez comme suit pour créer un nouveau serveur de routage en vue de gérer le routage dynamique dans un VPC.

Dans `--amazon-side-asn`, saisissez une valeur ASN BGP. Cette valeur doit se situer dans la plage 1-4294967295. Nous vous recommandons d'utiliser un ASN privé situé dans la plage 64512-65534 (ASN 16 bits) ou dans la plage 4200000000-4294967294 (ASN 32 bits).

1. Commande :

```
aws ec2 create-route-server --amazon-side-asn 65000
```

Réponse :

```
{
    "RouteServer": {
        "RouteServerId": "rs-1",
        "AmazonSideAsn": 65000,
        "State": "pending"
    }
```

```
}
```

2. Attendez que le serveur de routage soit disponible.

   Commande :

   ```
   aws ec2 describe-route-servers
   ```

   Réponse :

   ```
   {
       "RouteServer": {
           "RouteServerId": "rs-1",
           "AmazonSideAsn": 65000,
           "State": "available"
       }
   }
   ```

Détails des notifications SNS

Le tableau suivant fournit des détails concernant les messages que le serveur de routage Amazon VPC enverra à l'aide d'Amazon SNS :

Champs standard		Attributs du message (métadonnées)			
Message	Moment auquel il est envoyé	timestamp	eventCode	routeServerEndpointId	affectedRouteServerPeerIds
Le point de terminaison du serveur de routage [ID DU POINT DE TERMINAIS	Maintenance du point de terminaison du serveur de routage	Format : 2025-02-17T15:55:00Z	ROUTE_SERVER_ENDPOINT_MAINTENANCE	ID du point de terminaison affecté	Liste des pairs concernés IDs

Champs standard		Attributs du message (métadonnées)			
ON] fait actuellement l'objet d'une maintenance. Les sessions BFD et BGP peuvent en être affectées.					
Message	Moment auquel il est envoyé	timestamp	eventCode	routeServerPeerId	newBgpStatus
Le protocole BGP du pair du serveur de routage [ID DU PAIR] est désormais défini sur [UP/DOWN].	Modification du statut BGP du pair du serveur de routage	Format : 2025-02-17T15:55:00Z	ROUTE_SERVER_PEER_BGP_STATUS_CHANGE	ID du pair affecté	UP ou DOWN
Message	Moment auquel il est envoyé	timestamp	eventCode	routeServerPeerId	newBfdStatus

Champs standard		Attributs du message (métadonnées)			
Le protocole BFD du pair du serveur de routage [ID DU PAIR] est désormais défini sur [UP/DOWN].	Modification du statut BFD du pair du serveur de routage	Format : 2025-02-17T15:55:00Z	ROUTE_SERVER_PEER_BFD_STATUS_CHANGE	ID du pair affecté	UP ou DOWN

Étape 3 : association du serveur de routage à un VPC

Suivez les étapes décrites dans cette section pour associer le serveur de routage à un VPC.

L'association d'un serveur de routage est la connexion établie entre un serveur de routage et un VPC. Il s'agit d'une étape de configuration fondamentale qui permet au serveur de routage de fonctionner avec les dispositifs associés à votre VPC.

Lorsque vous créez une association de serveur de routage :

- le serveur de routage est relié à un VPC spécifique ;
- le serveur de routage peut interagir avec les tables de routage au sein des sous-réseaux du VPC ;
- le serveur de routage peut recevoir et propager des routes au sein du VPC associé ;
- la portée de fonctionnement du serveur de routage est établie.

Principaux aspects liés à l'association d'un serveur de routage :

- Chaque serveur de routage peut être associé à un VPC. Chaque VPC peut présenter jusqu'à 5 associations de serveur de routage distinctes par défaut. Pour plus d'informations sur les quotas, consultez la section sur les quotas des serveurs de routage.
- L'association doit être créée pour que le serveur de routage puisse gérer des routes.

- L'association peut être surveillée pour suivre son état (Association ou Associé, par exemple).
- L'association peut être supprimée (dissociée) si vous ne souhaitez plus que le serveur de routage fonctionne dans ce VPC.

AWS Management Console

Association d'un serveur de routage à un VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sous Cloud privé virtuel, sélectionnez Serveurs de routage.
3. Sélectionnez le serveur de routage que vous souhaitez associer à un VPC.
4. Dans l'onglet Association, sélectionnez Associer le serveur de routage.
5. Dans la boîte de dialogue Associer le serveur de routage :
   - Le champ ID du serveur de routage est automatiquement renseigné avec le serveur de routage que vous avez sélectionné.
   - Dans ID de VPC, choisissez le VPC que vous souhaitez associer dans la liste déroulante.
6. Sélectionnez Associer le serveur de routage.
7. Attendez que l'association soit terminée. Une fois l'opération terminée, l'État Associé s'affiche dans l'onglet Association.

Command line

Procédez comme suit pour associer un serveur de routage à un VPC.

1. Commande :

```
aws ec2 associate-route-server --route-server-id rs-1 --vpc-id vpc-1
```

Réponse :

```
{
    "RouteServerAssociation": {
        "RouteServerId": "rs-1",
        "VpcId": "vpc-1",
        "State": "associating"
    }
```

```
}
```

2. Attendez que l'association soit terminée.

   Commande :

   ```
   aws ec2 get-route-server-associations --route-server-id rs-1
   ```

   Réponse :

   ```
   {
       "RouteServerAssociation": {
           "RouteServerId": "rs-1",
           "VpcId": "vpc-1",
           "State": "associated"
       }
   }
   ```

Étape 4 : création de points de terminaison de serveur de routage

Suivez les étapes décrites dans cette section pour créer des points de terminaison de serveur de routage. Créez deux points de terminaison par sous-réseau à des fins de redondance.

Un point de terminaison de serveur de route est un composant AWS géré au sein d'un sous-réseau qui facilite les connexions BGP (Border Gateway Protocol) entre votre serveur de route et vos homologues BGP.

Les points de terminaison du serveur de routage sont les « points de contact » au niveau desquels vos dispositifs réseau établissent des sessions BGP avec le serveur de routage. Ce sont les composants qui gèrent réellement les connexions BGP, tandis que le serveur de routage en lui-même gère les décisions de routage et la propagation des routes.

> **Note**
>
> Les points de terminaison de serveur de routage sont facturés 0,75 USD de l'heure.

AWS Management Console

Pour créer des points de terminaison de serveur de routage

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sous Cloud privé virtuel, sélectionnez Serveurs de routage.
3. Sélectionnez le serveur de routage pour lequel vous souhaitez créer des points de terminaison.
4. Dans le volet inférieur, sélectionnez l'onglet Points de terminaison de serveur de routage.
5. Choisissez Créer un point de terminaison de serveur de routage.
6. Sur la page Créer un point de terminaison de serveur de routage, configurez les paramètres suivants :
   - Dans Nom, saisissez un nom descriptif pour votre point de terminaison.
   - Dans Serveur de routage, assurez-vous que le serveur de routage sélectionné est le bon.
   - Dans Sous-réseau, sélectionnez le sous-réseau dans lequel vous souhaitez créer le point de terminaison.
7. (Facultatif) Pour ajouter des balises à votre point de terminaison de serveur de routage, faites défiler la page jusqu'à la section Balises – facultatif et sélectionnez Ajouter une nouvelle balise. Saisissez une clé et une valeur facultative pour chaque balise.
8. Passez en revue vos paramètres et sélectionnez Créer un point de terminaison de serveur de routage.
9. Attendez que le point de terminaison soit créé. Une fois l'opération terminée, vous verrez un message de réussite.
10. Répétez les étapes 5 à 9 pour créer un deuxième point de terminaison dans le même sous-réseau, sous un nom différent.
11. Répétez les étapes 5 à 10 pour chaque sous-réseau au sein duquel vous avez besoin de points de terminaison de serveur de routage.
12. Après avoir créé les points de terminaison, revenez dans l'onglet Points de terminaison de serveur de routage correspondant à votre serveur de routage.
13. Vérifiez que deux points de terminaison sont répertoriés pour chaque sous-réseau.
14. Vérifiez que l'État de chaque point de terminaison est Disponible.

Command line

Procédez comme suit pour créer un point de terminaison de serveur de routage.

1. Commande :

```
aws ec2 create-route-server-endpoint --route-server-id rs-1 --subnet-id subnet-1
```

Réponse :

```
{
    "RouteServerEndpoint": {
        "RouteServerId": "rs-1",
        "RouteServerEndpointId": "rse-1",
        "VpcId": "vpc-1",
        "SubnetId": "subnet-1",
        "State": "pending"
    }
}
```

2. Vous devrez peut-être attendre quelques minutes pour que les points de terminaison deviennent entièrement disponibles après leur création.

Commande :

```
aws ec2 describe-route-server-endpoints
```

Réponse :

```
{
    "RouteServerEndpoint": {
        "RouteServerId": "rs-1",
        "RouteServerEndpointId": "rse-1",
        "VpcId": "vpc-1",
        "SubnetId": "subnet-1",
        "EniId": "eni-123",
        "EniAddress": "10.1.2.3",
        "State": "available"
    }
}
```

Répétez les étapes pour créer un deuxième point de terminaison dans le même sous-réseau sous un nom différent et pour créer des points de terminaison pour chaque sous-réseau au sein duquel vous avez besoin de points de terminaison de serveur de routage.

Étape 5 : activation de la propagation du serveur de routage

Effectuez cette étape pour activer la propagation du serveur de routage.

Lorsqu'elle est activée, la propagation du serveur de routage installe les routes présentes dans la FIB sur la table de routage que vous avez spécifiée. Supports du serveur de IPv6 routage IPv4 et propagation des itinéraires.

La propagation du serveur de routage est le mécanisme qui automatise les mises à jour des tables de routage. Au lieu de mettre à jour manuellement les tables de routage, le serveur de routage propage automatiquement les routes appropriées dans les tables de routage configurées à l'aide des routes provenant de la FIB.

Principaux aspects liés à la propagation du serveur de routage :

- Configuration
  - Lie un serveur de routage à des tables de routage spécifiques
  - Détermine quelles tables de routage recevront les mises à jour de routes dynamiques
  - Peut être activée ou désactivée par table de routage
- Fonctionnalité
  - Met automatiquement à jour les tables de routage avec les routes apprises par les pairs BGP
  - Propage les meilleures routes disponibles sur la base des attributs BGP
  - Maintient la cohérence des itinéraires entre les tables de routage spécifiées
  - Les routes sont mises à jour de manière dynamique lorsque les conditions du réseau changent.
- States
  - La propagation peut être activée (les routes sont propagées).
  - La propagation peut être désactivée (les routes ne sont pas propagées).

AWS Management Console

Pour activer la propagation du serveur de routage

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Sélectionnez le serveur de routage pour lequel vous souhaitez activer la propagation.
3. Sélectionnez l'onglet Propagations dans le panneau de détails du serveur de routage.
4. Sélectionnez Activer la propagation.
5. Dans la boîte de dialogue Activer la propagation :
   - L'ID du serveur de routage sera prérempli.
   - Sous Table de routage, sélectionnez la table de routage de destination des routes récemment propagées dans le menu déroulant.
6. Sélectionnez Activer la propagation pour confirmer votre choix.
7. Attendez que l'état de propagation devienne Disponible dans la liste Propagations.
8. Vérifiez que la table de routage sélectionnée apparaît dans la liste Propagations à l'état Disponible.

Command line

Procédez comme suit pour activer la propagation du serveur de routage.

1. Commande :

```
aws ec2 enable-route-server-propagation --route-table-id rtb-1 --route-server-id
 rs-1
```

Réponse :

```
{
    "RouteServerRoutePropagation": {
        "RouteServerId": "rs-1",
        "RouteTableId": "rtb-1",
        "State": "pending"
    }
}
```

2. Attendez que l'état de propagation devienne Disponible.

Commande :

```
aws ec2 get-route-server-propagations --route-server-id rs-1
```

Réponse :

```
{
    "RouteServerRoutePropagation": {
        "RouteServerId": "rs-1",
        "RouteTableId": "rtb-1",
        "State": "available"
    }
}
```

Étape 6 : création d'un pair du serveur de routage

Un pair de serveur de routage est une session entre le point de terminaison d'un serveur de route et le périphérique dans AWS lequel il est déployé (tel qu'un dispositif de pare-feu ou une autre fonction de sécurité réseau exécutée sur une instance EC2). Le dispositif doit répondre aux exigences suivantes :

- Disposer d'une interface réseau Elastic dans le VPC
- Prendre en charge le protocole BGP
- Être capable de lancer des sessions BGP

> **Note**
>
> Nous vous recommandons de créer un pair du serveur de routage par point de terminaison de serveur de routage à des fins de redondance.

AWS Management Console

Pour créer un pair du serveur de routage

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

2. Dans le chemin de navigation, sélectionnez VPC > Serveur de routages pairs > Créer un pair de serveur de routage.
3. Sous Détails, configurez les éléments suivants :
   - Nom : saisissez un nom pour le pair du serveur de routage (jusqu'à 255 caractères). Exemple : my-route-server-peer -01
   - ID du point de terminaison de serveur de routage : sélectionnez un point de terminaison de serveur de routage dans la liste déroulante. Vous pouvez éventuellement sélectionner Créer un point de terminaison du serveur de routage pour en créer un nouveau.
   - Adresse du pair : entrez l' IPv4 adresse du pair. Il doit s'agir d'une adresse IP valide. L'adresse du pair doit être accessible depuis le point de terminaison du serveur de routage.
   - Pair ASN : saisissez le numéro de système autonome (ASN) du pair BGP. La valeur doit se situer dans la plage 1-4294967295. L'ASN doit généralement utiliser des plages privées (64512-65534 pour 16 bits ou 4200000000-4294967294 pour 32 bits).
   - Détection de vivacité des pairs :
     - Keepalive BGP (valeur par défaut) : mécanisme Keepalive BGP standard
     - BFD : détection de transfert bidirectionnel pour un basculement plus rapide
   - (Facultatif) Sous Balises, sélectionnez Ajouter une nouvelle balise pour ajouter des balises de paire clé-valeur. Les balises permettent d'identifier et de suivre AWS les ressources.
4. Passez en revue vos paramètres et sélectionnez Créer un pair de serveur de routage.

Command line

Procédez comme suit pour créer un pair du serveur de routage.

1. Commande :

```
aws ec2 create-route-server-peer --route-server-endpoint-id rse-1 --peer-address
 10.0.2.3 --bgp-options PeerAsn=65001,PeerLivenessDetection=bfd
```

   Réponse :

   Dans la réponse, les valeurs d'état peuvent être `pending|available|deleting|deleted`.

```
{
```

```
    "RouteServerPeer": {
        "RouteServerPeerId": "rsp-1",
        "RouteServerId": "rs-1",
        "VpcId": "vpc-1",
        "SubnetId": "subnet-1",
        "State": "pending",
        "EndpointEniId": "eni-2,
        "EndpointEniAddress": "10.0.2.4",
        "PeerEniId": "eni-1",
        "PeerAddress": "10.0.2.3",
        "BgpOptions": {
            "PeerAsn": 65001,
   "PeerLivenessDetection": "bfd"
        },
        "BgpStatus": {
            "Status": "Up"
        }
    }
}
```

2. Attendez que l'état de propagation devienne Disponible.

   Commande :

   ```
   aws ec2 describe-route-server-peers
   ```

   Réponse :

   ```
   {
       "RouteServerPeer": {
           "RouteServerPeerId": "rsp-1",
           "RouteServerId": "rs-1",
           "VpcId": "vpc-1",
           "SubnetId": "subnet-1",
           "State": "available",
           "EndpointEniId": "eni-2,
           "EndpointEniAddress": "10.0.2.4",
           "PeerEniId": "eni-1",
           "PeerAddress": "10.0.2.3",
           "BgpOptions": {
               "PeerAsn": 65001,
      "PeerLivenessDetection": "bfd"
           },
   ```

```
        "BgpStatus": {
            "Status": "down"
        }
    }
}
```

Étape 7 : lancement de sessions BGP depuis les dispositifs

Lorsque l'état du pair du serveur de routage est Disponible, configurez votre charge de travail pour lancer la session BGP avec le point de terminaison de serveur de routage.

Le lancement d'une session BGP depuis les dispositifs de vos sous-réseaux n'entre pas dans le cadre de ce tutoriel. Le point de terminaison de serveur de routage ne lance pas la session BGP.

Vous pouvez vérifier que la fonction de serveur de routage VPC fonctionne en vérifiant que la table de routage contient bien les meilleures routes propagées par le serveur de routage.

Étape 8 : nettoyage

La partie création du tutoriel est terminée. Suivez les étapes décrites dans cette section pour supprimer les composants du serveur de routage VPC que vous avez créés.

7.1 : retrait d'une annonce BGP sur les dispositifs

Le retrait d'une annonce BGP sur les dispositifs de vos sous-réseaux n'entre pas dans le cadre de ce tutoriel. Consultez votre fournisseur tiers pour connaître vos configurations BGP, le cas échéant.

7.2 : désactivation la propagation du serveur de routage

Procédez comme suit pour désactiver la propagation du serveur de routage.

AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Sélectionnez le serveur de routage pour lequel vous souhaitez désactiver la propagation.
3. Sélectionnez Actions > Modifier le serveur de routage.
4. Sélectionnez l'onglet Propagations dans le panneau de détails du serveur de routage.
5. Sélectionnez la propagation que vous souhaitez désactiver, puis sélectionnez Désactiver la propagation.

6. Dans la boîte de dialogue, sélectionnez Désactiver la propagation du serveur de routage.

Command line

1. Désactivez la propagation :

```
aws ec2 disable-route-server-route-propagation --route-table-id rtb-1 --route-
server-id rs-1
```

2. Vérifiez que la propagation a bien été supprimée :

```
aws ec2 get-route-server-route-propagations --route-server-id rs-1 [--route-
table-id rtb-1]
```

7.3 : suppression des pairs du serveur de routage

Procédez comme suit pour supprimer les pairs du serveur de routage.

AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le chemin de navigation, sélectionnez Serveurs de routage > Serveur de routages pairs.
3. Sélectionnez un pair du serveur de routage.
4. Sélectionnez Actions > Supprimer le serveur de routage pair.

Command line

1. Supprimez des pairs :

```
aws ec2 delete-route-server-peer --route-server-peer-id rsp-1
```

2. Confirmez la suppression :

```
aws ec2 describe-route-server-peers [--route-server-peer-ids rsp-1] [--filters
 Key=RouteServerId|RouteServerEndpointId|VpcId]
```

7.4 : suppression de points de terminaison de serveur de routage

Procédez comme suit pour supprimer des points de terminaison de serveur de routage.

AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Sélectionnez le serveur de routage pour lequel vous souhaitez supprimer des points de terminaison.
3. Sélectionnez Points de terminaison de serveur de routage.
4. Choisissez le point de terminaison et sélectionnez Actions > Supprimer un point de terminaison de serveur de routage.
5. Saisissez supprimer et sélectionnez Supprimer.

Command line

1. Décrivez les points de terminaison :

```
aws ec2 describe-route-server-endpoints
```

2. Supprimez les points de terminaison de serveur de routage :

```
aws ec2 delete-route-server-endpoint --route-server-endpoint-id rse-1
```

3. Vérifiez que les points de terminaison ont bien été supprimés :

```
aws ec2 describe-route-server-endpoints [--route-server-endpoint-ids rsp-1] [--
filters Key=RouteServerId|VpcId|SubnetId]
```

7.5 : dissociation d'un serveur de routage du VPC

Procédez comme suit pour dissocier le serveur de routage du VPC.

AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Sélectionnez le serveur de routage pour lequel vous souhaitez procéder à la dissociation.
3. Sélectionnez Association.

4. Sélectionnez Dissocier le serveur de routage.
5. Confirmez les modifications qui seront apportées et sélectionnez Dissocier le serveur de routage.

Command line

1. Dissociez un serveur de routage du VPC :

```
aws ec2 disassociate-route-server --route-server-id rs-1 --vpc-id vpc-1
```

2. Confirmez la dissociation :

```
aws ec2 get-route-server-associations --route-server-id rs-1
```

7.6 : suppression d'un serveur de routage

Procédez comme suit pour supprimer le serveur de routage.

AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Sélectionnez le serveur de routage à supprimer.
3. Sélectionnez Actions > Supprimer le serveur de routage.
4. Saisissez supprimer et sélectionnez Supprimer.

Command line

1. Supprimez un serveur de routage :

```
aws ec2 delete-route-server --route-server-id rs-1
```

2. Confirmez la suppression :

```
aws ec2 describe-route-servers [--route-server-ids rs-1] [--filters Key=VpcId]
```

Le tutoriel relatif au serveur de routage Amazon VPC est terminé.

Résolution des problèmes d'accessibilité au sein de votre VPC

L'analyseur d'accessibilité est un outil d'analyse de configuration statique. Utilisez l'analyseur d'accessibilité pour analyser et déboguer l'accessibilité réseau entre deux ressources dans 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.

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 un dispositif 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 un dispositif middlebox, par exemple une instance Amazon EC2 configurée en tant que dispositif 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 de plus amples informations, veuillez consulter 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.

Rediriger le trafic VPC vers un dispositif de sécurité

L'assistant de routage middlebox est disponible dans la console Amazon VPC.

Table des matières

1. 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 à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Votre VPCs.
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 privée virtuelle, pour Destination IPv4 CIDR, entrez le CIDR pour le trafic sur site entrant dans le VPC depuis la passerelle privée virtuelle.

- Pour Middlebox, choisissez l'ID d'interface réseau associé à votre dispositif 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 dispositif middlebox, ou si vous utilisez un point de terminaison Gateway Load Balancer, choisissez l'ID de point de terminaison du VPC.

     Vous devez utiliser le même dispositif 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).

2. 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 à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Votre VPCs.
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 privée virtuelle, pour Destination IPv4 CIDR, 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 dispositif middlebox, ou si vous utilisez un point de terminaison Gateway Load Balancer, choisissez l'ID de point de terminaison du VPC.

     Vous devez utiliser le même dispositif 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).

3. 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.

   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.

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.
- Le dispositif doit être configuré dans un sous-réseau distinct du sous-réseau source ou de destination.
- Vous devez désactiver le source/destination contrôle de l'appliance. Pour plus d'informations, consultez Changement de la vérification de source ou de destination dans le Guide 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.

- Si vous utilisez le routage middlebox pour passer par un dispositif de sécurité, le référencement des groupes de sécurité entre la source et la destination finale après inspection n'est pas pris en charge.

Scénarios middlebox

Amazon Virtual Private Cloud (VPC) fournit un large éventail de fonctionnalités de mise en réseau qui vous permettent de personnaliser et de contrôler le routage du trafic au sein de votre réseau virtuel. L'une de ces fonctionnalités est l'assistant de routage middlebox, qui permet un contrôle précis du chemin de routage du trafic entrant ou sortant de votre VPC.

Si vous devez rediriger le trafic vers une appliance de sécurité, un équilibreur de charge ou un autre périphérique réseau à des fins d'inspection, de surveillance ou d'optimisation, l'assistant de routage middlebox peut simplifier le processus. Cet assistant crée automatiquement les tables de routage et les acheminements (sauts) nécessaires pour rediriger le trafic spécifié selon les besoins, éliminant ainsi les efforts manuels nécessaires pour paramétrer des configurations de routage complexes.

L'assistant de routage middlebox prend en charge plusieurs scénarios différents. Par exemple, vous pouvez l'utiliser pour inspecter le trafic destiné à un sous-réseau spécifique, configurer le routage et l'inspection du trafic middlebox sur l'ensemble de votre VPC, ou inspecter de manière sélective le trafic entre des sous-réseaux spécifiques. Ce contrôle précis du routage du trafic vous permet d'implémenter des politiques de sécurité avancées, de permettre une surveillance centralisée du réseau ou d'optimiser les performances de vos applications basées sur le cloud.

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.

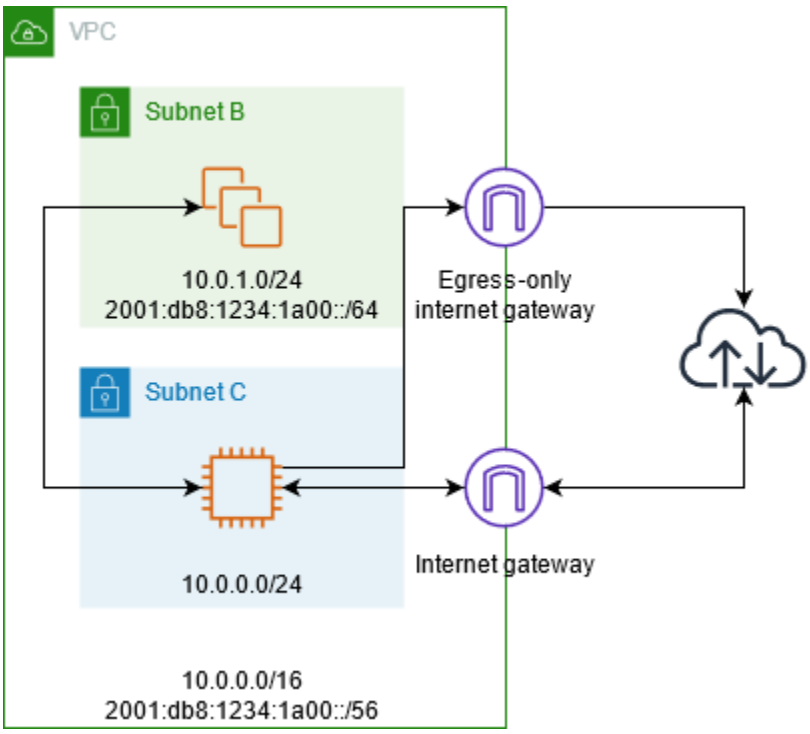


Table de routage de la passerelle Internet

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 »)

Configurer le routage et l'inspection du trafic middlebox dans un VPC

Considérez le scénario dans lequel vous devez inspecter le trafic entrant dans un VPC de la passerelle Internet vers un sous-réseau en utilisant une flotte d'appliances de sécurité configurée derrière un équilibreur de charge Gateway Load Balancer (GWLB). 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.

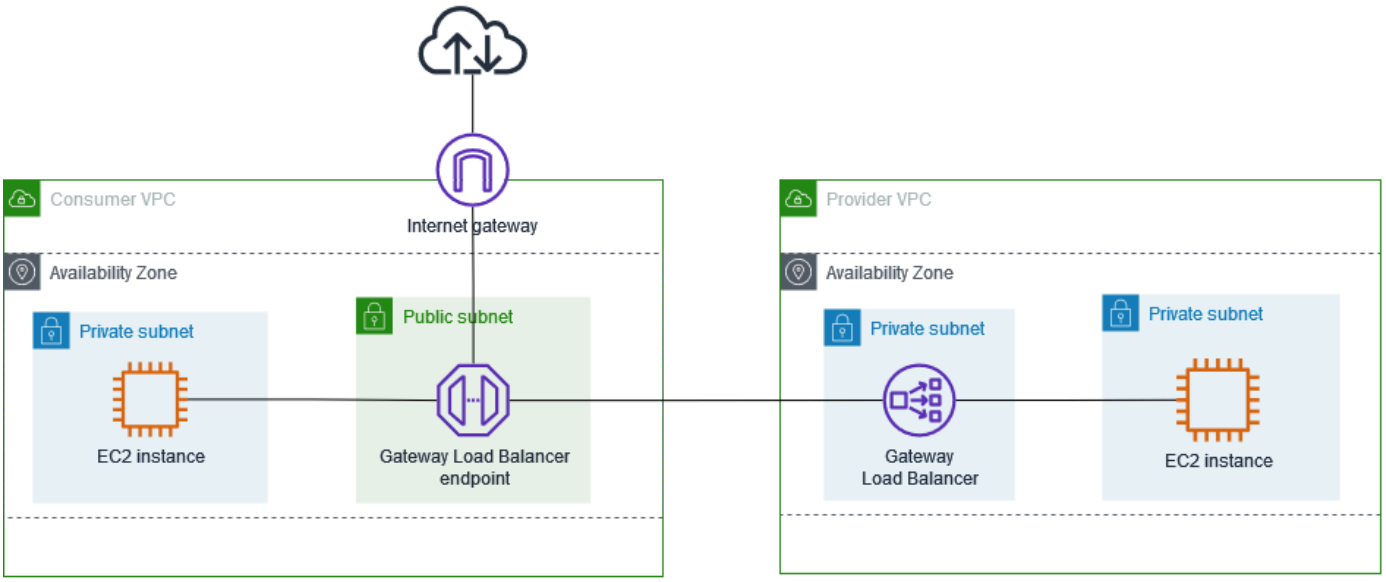


Table de routage de la passerelle Internet

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 GWLB

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*	Achemine le trafic des serveurs d'applications vers le point de terminaison GWLB avant qu'il soit 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'applications

Destination	Cible	Objectif
0.0.0.0/0	*igw-id*	Achemine l'ensemble du trafic vers la passerelle Internet.

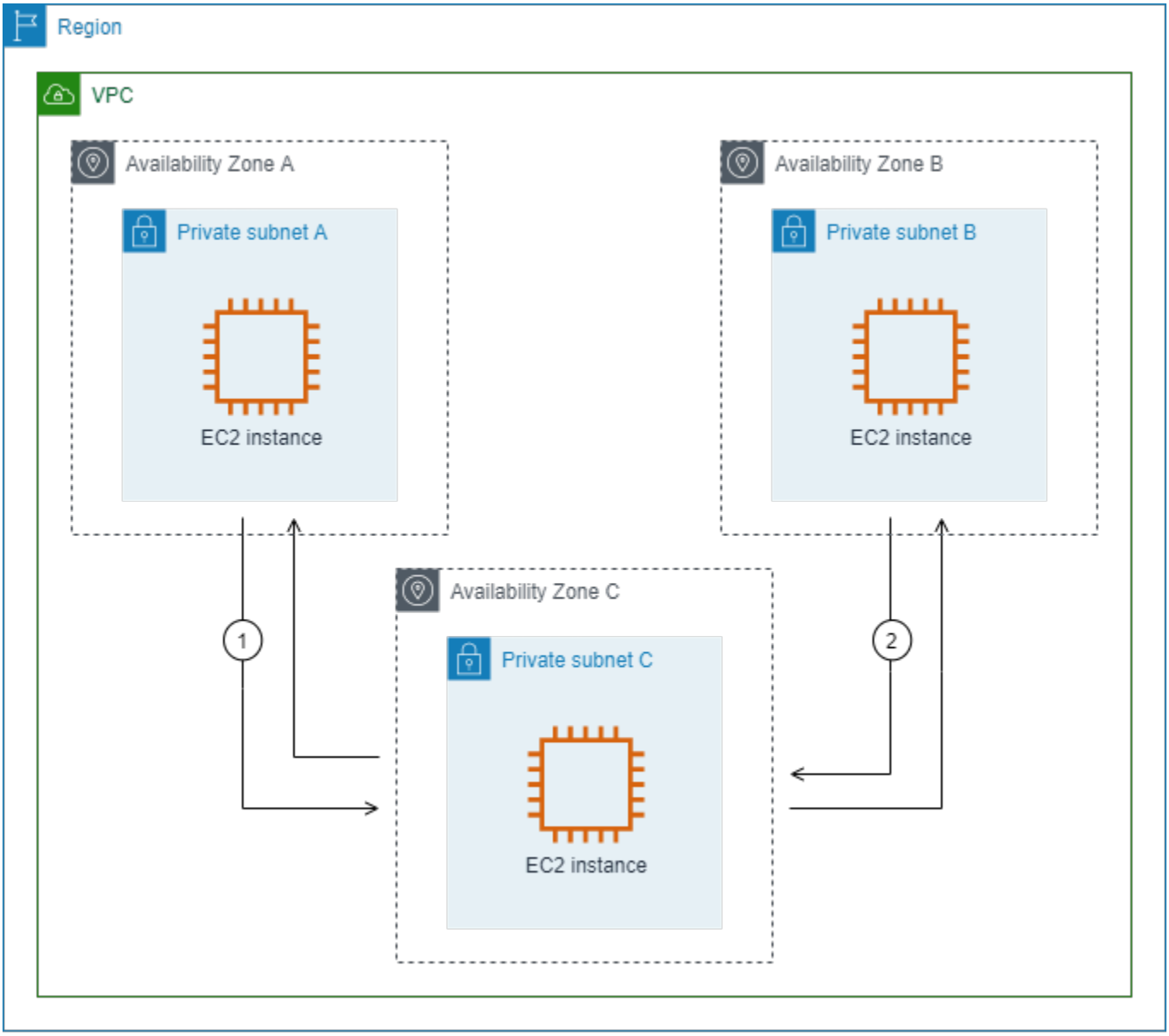
Lorsque vous utilisez l'assistant de routage middlebox, il associe les balises suivantes à la table de routage :

- 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.

Lorsque vous supprimez un sous-réseau, le bloc CIDR associé à ce sous-réseau est renvoyé au groupe d'adresses IP disponible du VPC. Cela signifie que les adresses IP comprises dans la plage CIDR du sous-réseau peuvent être réattribuées à d'autres sous-réseaux ou à d'autres ressources au sein du même VPC.

Il est important de noter que la suppression d'un sous-réseau ne supprime pas automatiquement les ressources qu'il contient. Vous devez d'abord résilier toutes les instances EC2, supprimer toutes les interfaces réseau et supprimer toutes les autres ressources associées au sous-réseau avant de pouvoir procéder à la suppression du sous-réseau.

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

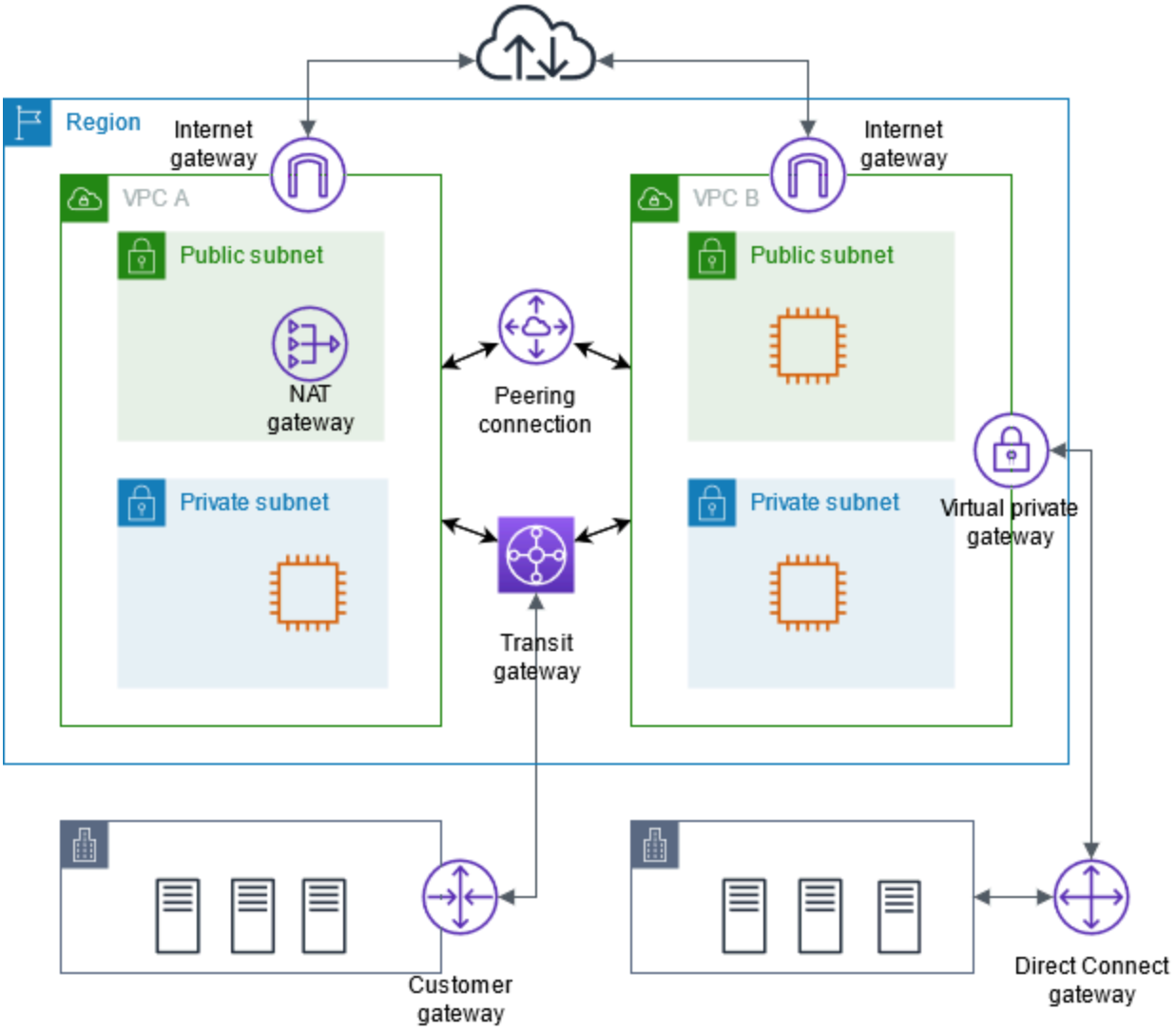
1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Mettez fin à toutes les instances dans le sous-réseau. Pour de plus amples informations, veuillez consulter Résilier une instance dans le Guide de l'utilisateur Amazon EC2.
3. Ouvrez la console Amazon VPC à l'adresse 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, tels que d'autres VPC, Internet ou votre réseau sur site.



Vous pouvez connecter votre cloud privé virtuel (VPC) à d'autres réseaux, tels que d'autres VPC, Internet ou votre réseau sur site.

Ce diagramme illustre certaines de ces options de connectivité. Le VPC A est connecté à Internet via une passerelle Internet, et l'instance EC2 du sous-réseau privé peut se connecter à Internet à l'aide d'une passerelle NAT du sous-réseau public. Le VPC B est également connecté à Internet, mais via une passerelle Internet directe, permettant à l'instance EC2 du sous-réseau public d'accéder à Internet.

De plus, 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, et le VPC B dispose d'une connexion Direct Connect au même centre de données. Cette interconnectivité permet aux organisations d'intégrer leurs ressources cloud à l'infrastructure sur site, créant ainsi un environnement cloud hybride.

La connexion de VPC à d'autres réseaux est un aspect important de la création d'une infrastructure cloud au sein d'AWS. Cela offre aux organisations la flexibilité et le contrôle nécessaires à leurs configurations de mise en réseau, leur permettant de concevoir des architectures VPC conformes à leurs exigences commerciales et à leurs besoins en matière de sécurité. Ces options de connectivité facilitent le flux de données efficace entre les différents composants d'un environnement informatique distribué, qu'ils soient dans le cloud ou sur site.

AWS fournit une gamme d'outils et de fonctionnalités permettant d'activer ces connexions VPC, dont les passerelles Internet, les passerelles NAT, l'appairage de VPC, les passerelles de transit et Direct Connect. En tirant parti de ces fonctionnalités, les organisations peuvent créer des environnements cloud sécurisés qui s'intègrent parfaitement à leur infrastructure informatique existante.

Vous pouvez connecter votre cloud privé virtuel (VPC) à d'autres réseaux. Par exemple, d'autres VPC, Internet ou votre réseau local.

Pour en savoir plus, consultez Cloud privé virtuel d'Amazon Connectivity Options (Options de connectivité de cloud privé virtuel d'Amazon).

Table des matières

Activation de l'accès à Internet pour un VPC 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 dans AWS à l'aide de 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 plus d'informations, consultez Adresses IP et NAT.

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).

Table des matières

Principes de base des passerelles Internet

Pour utiliser une passerelle Internet, vous devez l'attacher à un VPC et configurer le routage.

Configuration du routage

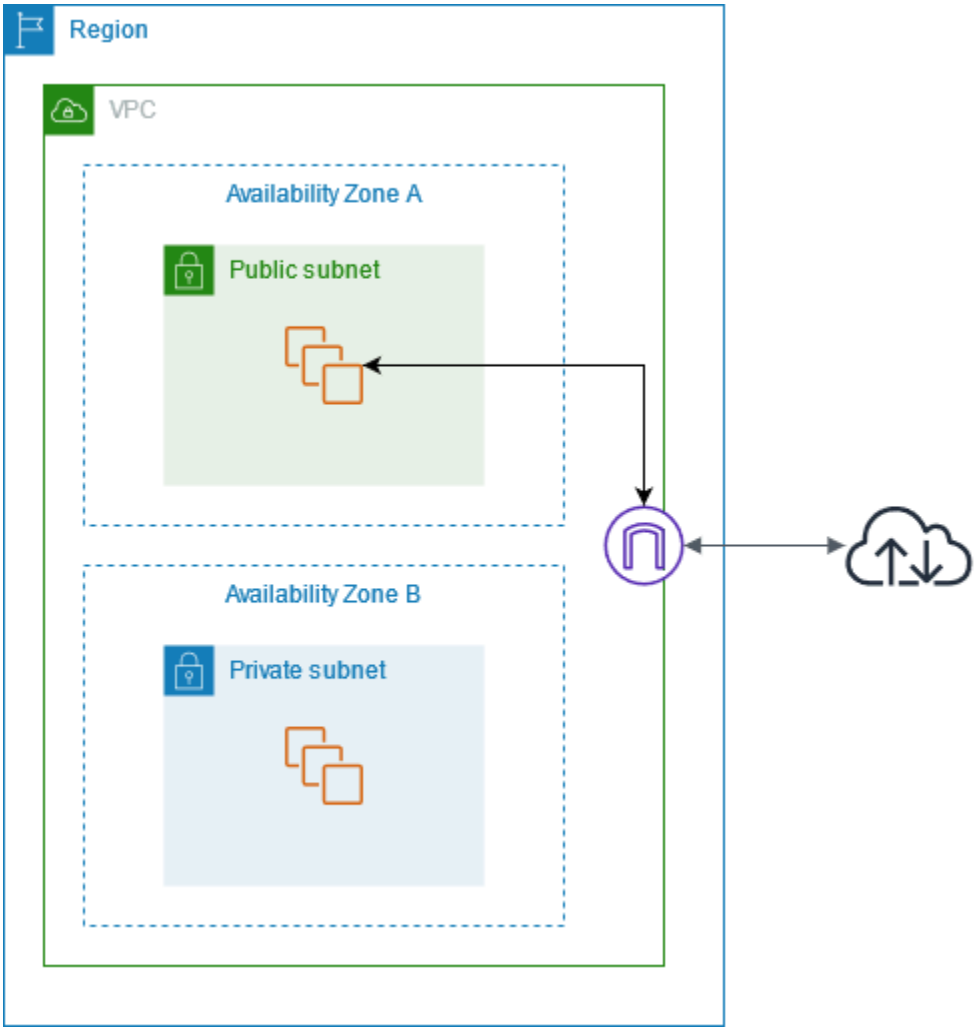
Si un sous-réseau est associé à une table de routage comportant une route vers une passerelle Internet, il est reconnu comme un sous-réseau public. Si un sous-réseau est associé à une table de

routage ne comportant pas de route vers une passerelle Internet, il est reconnu comme un sous-réseau privé.

Dans la table de routage de votre sous-réseau public, vous pouvez spécifier pour la passerelle Internet une route 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 la route vers une plage d'adresses IP plus restreinte, par exemple, les adresses IPv4 publiques des points de terminaison publics de votre entreprise en dehors de AWS, ou les adresses IP Elastic d'autres instances Amazon EC2 situées en dehors de votre VPC.

Schéma de la passerelle Internet

Dans le schéma ci-dessous, le sous-réseau de la zone de disponibilité A est un sous-réseau public, car sa table de routage comporte une route qui dirige tout le trafic IPv4 entrant lié à Internet vers 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. Puisqu'il n'existe aucune route vers la passerelle Internet, les instances du sous-réseau privé ne peuvent pas communiquer avec Internet, même si elles disposent d'adresses IP publiques.



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 la relation NAT un-à-un sur le compte de votre instance, de sorte que lorsque le trafic quitte le sous-réseau de votre VPC et va sur Internet, le champ d'adresse de réponse est défini sur l'adresse IPv4 publique ou l'adresse IP Elastic 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.

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)

Ajouter un accès Internet à un sous-réseau

Cette section décrit la prise en charge de l'accès à Internet à partir d'un sous-réseau qui se trouve dans un VPC autre que celui par défaut à l'aide d'une passerelle Internet. Vous devez créer la passerelle Internet, l'attacher au VPC et configurer le routage pour le sous-réseau.

Après avoir configuré l'accès à Internet pour votre sous-réseau, vous devez vous assurer que les ressources du sous-réseau ont accès à Internet. Par exemple, vos instances EC2 doivent disposer d'une adresse IPv4 ou IPv6 publique et leurs groupes de sécurité doivent autoriser un trafic spécifique vers et depuis Internet.

Pour fournir un accès à Internet à vos instances sans leur attribuer d'adresse IP publique, vous pouvez utiliser un périphérique NAT. Pour de plus amples informations, consultez Périphériques NAT.

Pour supprimer l'accès à Internet, vous pouvez détacher la passerelle Internet de votre VPC, puis la supprimer. Pour de plus amples informations, consultez the section called "Suppression d'une passerelle Internet".

Tâches

- Étape 1 : Création d'une passerelle Internet
- Étape 2 : Attachement de la passerelle Internet au VPC
- Étape 3 : Ajout d'une route à la table de routage du sous-réseau

Étape 1 : Création d'une passerelle Internet

Utilisez la procédure suivante pour créer une passerelle Internet.

Pour créer une passerelle Internet 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 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.

Pour créer une passerelle Internet à l'aide de la ligne de commande

- create-internet-gateway (AWS CLI)
- New-EC2InternetGateway (AWS Tools for Windows PowerShell)

Étape 2 : Attachement de la passerelle Internet au VPC

Pour utiliser une passerelle Internet, vous devez l'associer à un VPC.

Pour attacher une passerelle Internet à un VPC 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 Passerelles Internet.
3. Cochez la case pour la passerelle Internet.
4. Pour l'attacher, choisissez Actions, Attacher au VPC, sélectionnez un VPC disponible, puis choisissez Attacher une passerelle Internet.
5. Pour la détacher, choisissez Actions, Détacher du VPC, puis sélectionnez Détacher la passerelle Internet. Lorsque vous êtes invité à confirmer l'opération, choisissez Détacher la passerelle Internet.

Pour attacher une passerelle Internet à un VPC à l'aide de la ligne de commande

- attach-internet-gateway (AWS CLI)
- Add-EC2InternetGateway (AWS Tools for Windows PowerShell)

Étape 3 : Ajout d'une route à la table de routage du sous-réseau

La table de routage du sous-réseau doit contenir une route qui dirige le trafic Internet vers la passerelle Internet.

Pour configurer la table de routage du 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 Route tables (Tables de routage).
3. Sélectionnez la table de routage du sous-réseau. Par défaut, un sous-réseau utilise la table de routage principale du VPC. Vous pouvez également créer une table de routage, puis associer le sous-réseau à la table de routage créée.
4. Sous l'onglet Routes, choisissez Modifier les routes, puis Ajouter une route.
5. Entrez 0.0.0.0/0 dans Destination et sélectionnez la passerelle Internet dans Cible.
6. Sélectionnez Enregistrer les modifications.

Pour configurer la table de routage du sous-réseau à l'aide de la ligne de commande

- create-route (AWS CLI)
- New-EC2Route (AWS Tools for Windows PowerShell)

Suppression d'une passerelle Internet

Si l'accès à Internet n'est plus nécessaire pour un PVC, vous pouvez détacher la passerelle Internet de votre VPC, puis la supprimer. Vous ne pouvez pas supprimer une passerelle Internet si elle est encore attachée à 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 d'un VPC 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 Passerelles Internet.
3. Cochez la case pour la passerelle Internet.
4. Pour l'attacher, choisissez Actions, Attacher au VPC, sélectionnez un VPC disponible, puis choisissez Attacher une passerelle Internet.
5. Pour la détacher, choisissez Actions, Détacher du VPC, puis sélectionnez Détacher la passerelle Internet. Lorsque vous êtes invité à confirmer l'opération, choisissez Détacher la passerelle Internet.

Pour décrire vos passerelles Internet (y compris les attachements) à l'aide de la ligne de commande

- describe-internet-gateways (AWS CLI)
- Get-EC2InternetGateway (AWS Tools for Windows PowerShell)

Pour détacher une passerelle Internet d'un VPC à l'aide de la ligne de commande

- detach-internet-gateway (AWS CLI)
- Dismount-EC2InternetGateway (AWS Tools for Windows PowerShell)

Pour supprimer une passerelle Internet 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 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.

Pour supprimer une passerelle Internet à l'aide de la ligne de commande

- delete-internet-gateway (AWS CLI)
- Remove-EC2InternetGateway (AWS Tools for Windows PowerShell)

Activez le IPv6 trafic sortant à l'aide d'une passerelle Internet de sortie uniquement

Une passerelle Internet de sortie uniquement est un composant VPC à échelle horizontale, redondant et hautement disponible qui permet les communications sortantes entre les IPv6 instances de votre VPC et Internet et empêche Internet d'établir une connexion avec vos instances. IPv6

Une passerelle Internet de sortie uniquement est destinée à être utilisée avec IPv6 le trafic uniquement. Pour activer les communications Internet uniquement sortantes IPv4, utilisez plutôt une passerelle NAT. Pour de plus amples informations, veuillez consulter Passerelles NAT.

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).

Table des matières

Principes de base sur la passerelle Internet de sortie uniquement

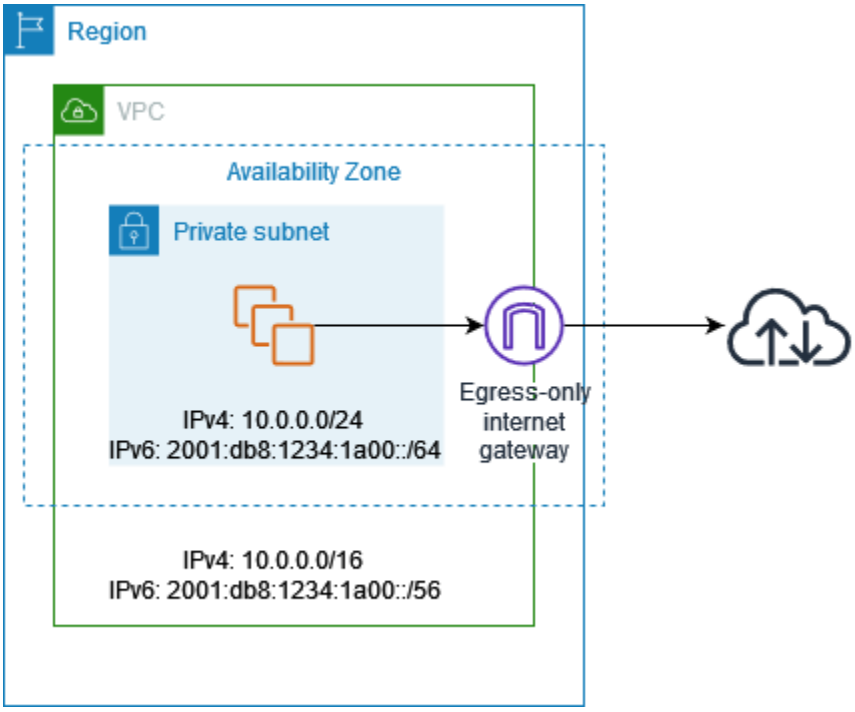
IPv6 les adresses sont uniques au monde et sont donc publiques par défaut. Si vous souhaitez que votre instance puisse accéder à Internet, mais que vous voulez empêcher les ressources sur Internet

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 pointe tout le IPv6 trafic (`::/0`) ou une plage d' IPv6 adresses spécifique vers la passerelle Internet de sortie uniquement. IPv6 le trafic 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.

Vous ne pouvez pas associer un groupe de sécurité à une passerelle Internet de sortie uniquement pour contrôler le trafic autorisé à atteindre ou à quitter la passerelle Internet de sortie uniquement. 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 schéma suivant, le VPC possède à la fois des blocs d'adresse IPv6 CIDR, IPv4 et le sous-réseau comprend à la fois IPv4 des blocs d'adresse CIDR. IPv6 Le VPC a une passerelle Internet de sortie uniquement.



Voici un exemple de table de routage associée au sous-réseau. Il existe une route qui envoie tout le IPv6 trafic Internet (: : /0) vers la passerelle Internet de sortie uniquement.

Destination	Cible
10.0.0.0/16	Locale
2001:db8:1234:1a00::/64	Local
::/0	*eigw-id*

Ajouter un accès Internet de sortie uniquement à un sous-réseau

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

- 1. Création d'une passerelle Internet de sortie uniquement
- 2. Créer une table de routage personnalisée
- 3. Suppression d'une passerelle Internet de sortie uniquement
- Présentation de la ligne de commande

1. 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.

2. 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.

3. 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 de la ligne de commande

Vous pouvez exécuter les tâches décrites sur cette page à l'aide de la ligne de commande.

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)

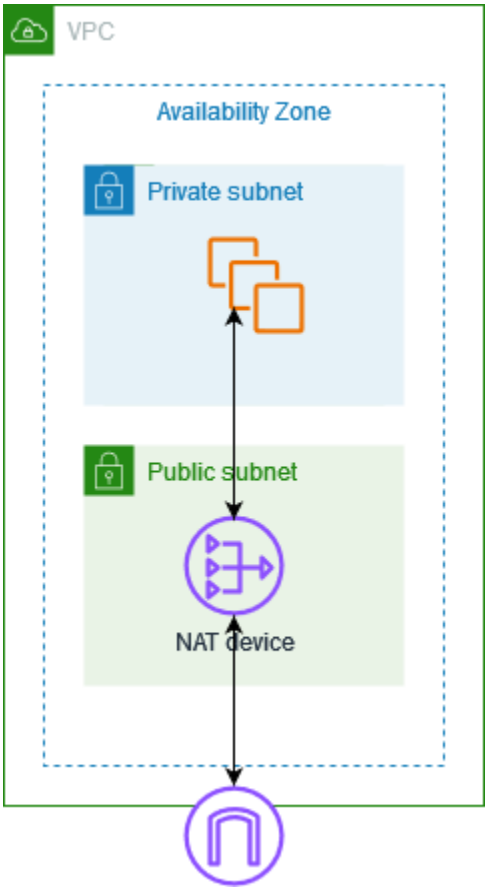
Suppression d'une passerelle Internet de sortie uniquement

- delete-egress-only-internet-passerelle ()AWS CLI
- Remove-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

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 illustre un périphérique NAT d'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 soit utiliser un périphérique NAT géré proposé par AWS appelé passerelle NAT, soit 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 pour permettre aux instances d'un sous-réseau privé de se connecter à des services en dehors de votre VPC tout en empêchant les services externes d'établir une connexion avec ces instances.

Lorsque vous créez une passerelle NAT, vous spécifiez l'un des types de connectivité suivants :

- Publique (par défaut) : les instances des sous-réseaux privés peuvent se connecter à Internet via une passerelle NAT publique, mais ne peuvent pas recevoir de connexions entrantes non sollicitées depuis Internet. Créez dans un sous-réseau public une passerelle NAT publique à laquelle vous associez une adresse IP Elastic. 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 un autre réseau VPCs ou au vôtre. Dans ce cas, vous acheminez le trafic de la passerelle NAT via une passerelle de transit ou une passerelle réseau privé virtuel.
- Privé : les instances situées dans des sous-réseaux privés peuvent se connecter à un autre réseau VPCs ou au vôtre via une passerelle NAT privée, mais elles ne peuvent pas recevoir

de connexions entrantes non sollicitées en provenance de l'autre VPCs réseau ou du réseau local. Vous pouvez acheminer le trafic de la passerelle NAT via une passerelle de transit ou une passerelle réseau privé virtuel. Vous ne pouvez pas associer d'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.

Une passerelle NAT est destinée à être utilisée avec IPv4 IPv6 le trafic (en utilisantDNS64 et NAT64). Une autre option pour activer les communications Internet uniquement sortantes IPv6 consiste à utiliser une passerelle Internet de sortie uniquement.

Les passerelles NAT privées et publiques mappent l' IPv4 adresse privée source des instances à l' IPv4 adresse privée de la passerelle NAT, mais dans le cas d'une passerelle NAT publique, la passerelle Internet mappe ensuite l' IPv4 adresse privée de la passerelle NAT publique à l'adresse IP élastique 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.

Considérations

- Les connexions doivent toujours être lancées depuis le VPC contenant la passerelle NAT.
- 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. La passerelle NAT publique utilise son adresse IP Elastic comme adresse IP source uniquement lorsqu'elle est utilisée conjointement avec une passerelle Internet du même VPC.

Table des matières

- Cas d'utilisation de la passerelle NAT
- DNS64 et NAT64
- Inspectez le trafic provenant des passerelles NAT
- Surveillance des passerelles NAT avec Amazon CloudWatch
- Résoudre les problèmes des passerelles NAT
- Tarification des passerelles NAT

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 de plus amples informations, veuillez consulter Passerelles.

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 IPv4 IPv6 trafic. Pour IPv6 le trafic, la passerelle NAT fonctionne NAT64. En l'utilisant conjointement avec DNS64 (disponible sur le résolveur Route 53), vos IPv6 charges de travail dans un sous-réseau d'Amazon VPC peuvent communiquer avec les ressources. IPv4 Ces IPv4 services 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 IPv4 adresse 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 8 IPv4 adresses à vos passerelles NAT (1 IPv4 adresse principale et 7 IPv4 adresses 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 de plus amples informations, veuillez consulter Adresses IP élastiques.
- Lorsque vous créez une passerelle NAT, vous pouvez sélectionner l' IPv4 adresse privée principale à attribuer à la passerelle NAT. Dans le cas contraire, nous en sélectionnons une en votre nom dans la plage d' IPv4 adresses du sous-réseau. Vous ne pouvez pas modifier ou supprimer l' IPv4 adresse privée principale. Vous pouvez ajouter des IPv4 adresses privées secondaires selon vos besoins.
- 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.
- Une interface réseau gérée par le demandeur est créée pour votre passerelle NAT. Vous pouvez visualiser cette interface réseau à l'aide de la console Amazon EC2. Recherchez l'ID de la passerelle NAT dans la description. Vous pouvez ajouter des balises à l'interface réseau, mais vous ne pouvez modifier aucune autre de ses propriétés.
- 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 de plus amples informations, veuillez consulter Réseau ACLs.
- Vous ne pouvez pas acheminer le trafic vers une passerelle NAT via une connexion d'appairage de VPC. Cependant, le trafic en provenance d'une passerelle NAT via l'appairage de VPC à destination de VPC appairés prend en charge le comportement de « retour à l'expéditeur » : le trafic de retour est automatiquement redirigé vers la passerelle NAT d'origine même si aucune route de retour n'est configurée dans le VPC de destination. Ce comportement est propre aux passerelles NAT et ne s'applique pas aux instances EC2 standard. Pour éviter cela, utilisez NACLs pour bloquer le trafic de retour.

  Non pris en charge :

  ```
  Client # Peering # NAT # Internet
  ```

  Pris en charge :

  ```
  Client # NAT # Peering # Destination
  ```

- Vous ne pouvez pas acheminer le trafic vers une passerelle NAT depuis un Site-to-Site VPN ou Direct Connect à l'aide d'une passerelle privée virtuelle. Vous pouvez acheminer le trafic vers une passerelle NAT depuis un Site-to-Site VPN ou Direct Connect si vous utilisez une passerelle de transit au lieu d'une passerelle privée virtuelle.
- Les passerelles NAT prennent en charge le trafic avec une unité de transmission maximale (MTU) de 8 500, mais il est important de noter ce qui suit :
  - L'unité de transmission maximale (MTU) d'une connexion réseau correspond à la taille, en octets, du paquet le plus volumineux susceptible d'être transmis via la connexion. Plus la MTU d'une connexion est élevée, plus la quantité de données pouvant être transmises dans un seul paquet est importante.
  - Les paquets de plus de 8 500 octets qui parviennent à la passerelle NAT sont supprimés (ou fragmentés, le cas échéant).
  - 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 de la MTU sur une instance, consultez Network MTU for your EC2 instance dans le Guide d'utilisation d'Amazon EC2.
  - Les passerelles NAT prennent en charge la découverte de Path MTU (PMTUD) via les paquets FRAG_NEEDED et les ICMPv4 paquets Packet Too Big (PTB). ICMPv6
  - Les passerelles NAT appliquent la taille maximale du segment (MSS) pour tous les paquets. Pour de plus amples informations, veuillez consulter RFC879.

Utiliser des passerelles NAT

Vous pouvez utiliser la console Amazon VPC pour créer et gérer vos passerelles NAT.

Tâches

- Contrôler l'utilisation des passerelles NAT
- Créer une passerelle NAT
- Modification des associations d'adresses IP secondaires
- Baliser une passerelle NAT
- Supprimer une passerelle NAT
- Présentation de la ligne de commande

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 de plus amples informations, veuillez consulter Identity and Access Management pour Amazon VPC.

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 utilisé le nombre d'adresses IP Elastic allouées à votre compte. Pour de plus amples informations, veuillez consulter Adresses IP élastiques.
- Vous pouvez attribuer jusqu'à 8 IPv4 adresses 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 de plus amples informations, veuillez consulter Adresses IP élastiques.

Créer une passerelle NAT

1. Ouvrez la console Amazon VPC à l'adresse 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 adresse IP Elastic à la passerelle NAT ou Allouer une adresse IP Elastic pour qu'une adresse IP Elastic lui soit attribuée automatiquement. 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 de plus amples informations, veuillez consulter Adresses IP élastiques.

   > **Important**
   >
   > Lorsque vous attribuez une adresse IP élastique à une passerelle NAT publique, le groupe de bordure réseau de cette adresse doit correspondre à celui 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 de plus amples informations, veuillez consulter 1. Allouer une adresse IP Elastic.

2. (Facultatif) Choisissez Paramètres supplémentaires et, sous Adresse IP privée - facultatif, entrez une IPv4 adresse privée pour la passerelle NAT. Si vous n'entrez pas d'adresse, une IPv4 adresse 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 choisi Privé, dans Paramètres supplémentaires, Méthode d'attribution d' IPv4 adresses privées, sélectionnez l'une des options suivantes :

   - Affectation automatique : AWS choisit l' IPv4 adresse privée principale pour la passerelle NAT. Pour Nombre d' IPv4adresses privées attribuées automatiquement, vous pouvez éventuellement spécifier le nombre d' IPv4 adresses privées secondaires pour la passerelle NAT. AWS choisit ces adresses IP au hasard dans le sous-réseau de votre passerelle NAT.
   - Personnalisé : pour IPv4Adresse privée principale, choisissez l' IPv4 adresse privée principale pour la passerelle NAT. Pour les IPv4 adresses privées secondaires, vous pouvez éventuellement spécifier jusqu'à 7 IPv4 adresses 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' IPv4adresses secondaires que vous souhaitez AWS attribuer à cette passerelle NAT privée. Vous pouvez choisir jusqu'à 7 IPv4 adresses.

> **Note**
>
> Les IPv4 adresses 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 (même adresse IP de destination, même port de destination et même protocole). Les IPv4 adresses secondaires augmentent le nombre de ports disponibles et, par conséquent, elles augmentent 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 IPv4 Adresse privée principale, entrez une IPv4 adresse privée.
    2. Sous IPv4 Adresse privée secondaire, entrez jusqu'à 7 IPv4 adresses 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 de plus amples informations, veuillez consulter Échec de la création d'une passerelle NAT.

Modification des associations d'adresses IP secondaires

Chaque IPv4 adresse 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 8 IPv4 adresses à vos passerelles NAT (1 IPv4 adresse principale et 7 IPv4 adresses 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 de plus amples informations, veuillez consulter Adresses IP élastiques.

Vous pouvez utiliser les CloudWatchmétriques ErrorPortAllocationde la passerelle NAT PacketsDropCountpour déterminer si votre passerelle NAT génère des erreurs d'allocation de port ou supprime des paquets. Pour résoudre ce problème, ajoutez des IPv4 adresses secondaires à votre passerelle NAT.

Considérations

- Vous pouvez ajouter des IPv4 adresses privées secondaires lorsque vous créez une passerelle NAT privée ou après avoir créé la passerelle NAT en suivant la procédure décrite dans cette section. Vous pouvez ajouter des adresses IP Elastic secondaires aux passerelles NAT publiques uniquement après avoir créé les passerelles NAT selon la procédure décrite dans cette section.
- Votre passerelle NAT peut être associée à un maximum de 8 IPv4 adresses (1 IPv4 adresse principale et 7 IPv4 adresses secondaires). Vous pouvez attribuer jusqu'à 8 IPv4 adresses 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 de plus amples informations, veuillez consulter Adresses IP élastiques.

Pour modifier les associations IPv4 d'adresses secondaires

1. Ouvrez la console Amazon VPC à l'adresse 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' IPv4 adresses secondaires.
4. Sélectionnez Actions, puis Modifier les associations d'adresses IP secondaires.
5. Si vous modifiez les associations d' IPv4 adresses secondaires d'une passerelle NAT privée, sous Action, choisissez Attribuer de nouvelles IPv4 adresses ou Annuler l'attribution d' IPv4adresses existantes. Si vous modifiez les associations d' IPv4 adresses secondaires d'une passerelle NAT publique, sous Action, choisissez Associer de nouvelles IPv4 adresses ou Dissocier des IPv4 adresses existantes.
6. Effectuez l'une des actions suivantes :

   - Si vous avez choisi d'attribuer ou d'associer de nouvelles IPv4 adresses, procédez comme suit :

1. Cette étape est obligatoire. Vous devez sélectionner une IPv4 adresse privée. Choisissez la méthode d'attribution des IPv4 adresses privées :
   - Attribution automatique : choisit AWS automatiquement une IPv4 adresse privée principale et vous choisissez si vous souhaitez AWS attribuer jusqu'à 7 IPv4 adresses 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.
   - Personnalisé : Choisissez l' IPv4adresse privée principale et jusqu'à 7 IPv4 adresses privées secondaires à attribuer à la passerelle NAT.
2. Sous Elastic IP allocation ID, choisissez une adresse IP Elastic à ajouter avec une IPv4 adresse secondaire. Cette étape est obligatoire. Vous devez sélectionner une adresse IP élastique ainsi qu'une IPv4 adresse privée. Si vous avez choisi Personnalisé pour la méthode d'attribution des adresses IP privées, vous devez également saisir une IPv4 adresse privée pour chaque adresse IP élastique 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 de plus amples informations, veuillez consulter 1. 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, une limite de quota par défaut s'applique aux adresses IP Elastic pour chaque région. Pour de plus amples informations, veuillez consulter Adresses IP élastiques.

- Si vous avez choisi d'annuler l'attribution ou de dissocier de nouvelles IPv4 adresses, 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 Balisage 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 à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez 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 à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Passerelles NAT.
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 de plus amples informations, veuillez consulter 5. Libérer une adresse IP Elastic.

Présentation de la ligne de commande

Vous pouvez exécuter les tâches décrites sur cette page à l'aide de la ligne de commande.

Attribuer une IPv4 adresse privée à une passerelle NAT privée

- assign-private-nat-gateway-adresse ()AWS CLI
- Register-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

Associez des adresses IP élastiques et IPv4 des adresses privées à une passerelle NAT publique

- associate-nat-gateway-address (AWS CLI)
- Register-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

Créer une passerelle NAT

- create-nat-gateway (AWS CLI)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)

Supprimer une passerelle NAT

- delete-nat-gateway (AWS CLI)

- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)

Décrire une passerelle NAT

- describe-nat-gateways (AWS CLI)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)

Dissocier des adresses IP Elastic secondaires d'une passerelle NAT publique

- disassociate-nat-gateway-address (AWS CLI)
- Unregister-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

Baliser une passerelle NAT

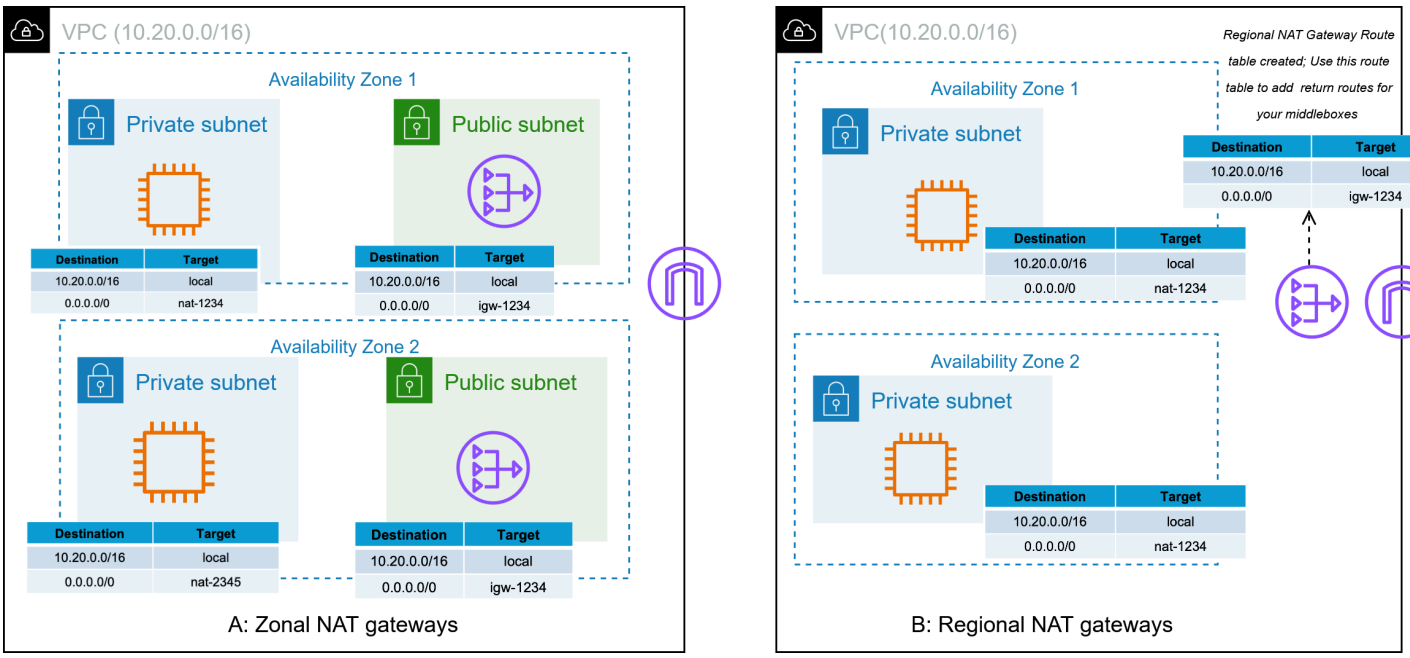
- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Annuler l'attribution d' IPv4 adresses secondaires depuis une passerelle NAT privée

- unassign-private-nat-gateway-adresse ()AWS CLI
- Unregister-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

Passerelles NAT régionales pour une extension multi-AZ automatique

Utilisez des passerelles NAT régionales lorsque vous souhaitez simplifier l'architecture de votre réseau, améliorer votre niveau de sécurité et configurer la haute disponibilité par défaut. Une passerelle NAT régionale s'étend automatiquement aux zones de disponibilité en fonction de la présence de votre charge de travail. Contrairement aux passerelles NAT standard (appelées passerelles NAT zonales), qui fonctionnent dans une seule zone de disponibilité, les passerelles NAT régionales suivent vos charges de travail pour fournir une haute disponibilité automatique.



Le schéma A de gauche représente la configuration actuelle avec une passerelle NAT zonale. Vous créez d'abord des passerelles NAT zonales par zone de disponibilité et vous les hébergez NATs dans des sous-réseaux publics. Vous configurez ensuite des routes distinctes par zone de disponibilité entre vos sous-réseaux privés et le NAT de cette zone de disponibilité. Vous répétez cette étape chaque fois que vos charges de travail s'étendent vers une nouvelle zone de disponibilité, pour une haute disponibilité. En outre, vous devez ajouter des routes pour la passerelle Internet dans la table de routage de votre sous-réseau NAT par zone de disponibilité.

En revanche, avec une passerelle NAT régionale, il n'est pas nécessaire de créer un sous-réseau public pour l'héberger. Vous n'avez pas non plus à créer et à supprimer des passerelles NAT et à modifier vos tables de routage chaque fois que vos charges de travail s'étendent à de nouvelles zones de disponibilité. Au lieu de cela, il vous suffit de créer une passerelle NAT en mode régional, de choisir votre VPC, qui s'étend et se contracte automatiquement en AZs fonction de la présence de votre charge de travail afin d'offrir une haute disponibilité. Comme le montre le diagramme B, vous pouvez acheminer le trafic depuis vos ressources dans un sous-réseau privé AZs vers cet identifiant de passerelle NAT régional unique, ou utiliser la même table de routage sur les sous-réseaux de votre zone de disponibilité pour effectuer la traduction des adresses réseau. Une fois que vous avez créé votre passerelle NAT régionale, elle crée AWS automatiquement une table de routage, qui comprend un itinéraire préconfiguré vers la passerelle Internet. Vous pouvez utiliser cette table de routage pour ajouter des itinéraires de retour à vos middleboxes.

Avantages

Les passerelles NAT régionales offrent les avantages suivants :

- Configuration simplifiée : utilisez un identifiant NAT unique dans toutes les zones de disponibilité dotées d'interfaces réseau, afin de pouvoir utiliser la même entrée de route pour les sous-réseaux des différentes zones de disponibilité.
- Sécurité renforcée : aucun sous-réseau public n'est requis. Une passerelle NAT régionale est une ressource autonome dotée de sa propre table de routage et vous n'avez pas besoin d'un sous-réseau public dans votre VPC pour héberger une passerelle NAT régionale, ce qui réduit les risques de mauvaise configuration des ressources privées dans les sous-réseaux dotés d'une connectivité publique.
- Haute disponibilité automatique : étend et réduit automatiquement l'encombrement de votre charge de travail afin de maintenir l'affinité zonale, ce qui garantit une haute disponibilité par défaut.
- Limites de port et d'IP plus élevées : vos passerelles NAT régionales prennent en charge jusqu'à 32 adresses IP par zone de disponibilité (contre 8 pour les passerelles NAT zonales). Chaque adresse IP augmente la limite de connexions simultanées vers une destination populaire (identifiée par une combinaison unique d'IP de destination, de port de destination et de protocole) de 55 000.

Quand utiliser les passerelles NAT régionales

Envisagez d'utiliser des passerelles NAT régionales pour tous les cas d'utilisation, à l'exception de ceux qui nécessitent une connectivité privée. Les passerelles NAT régionales n'offrent pas de connectivité privée et nous vous recommandons d'utiliser vos passerelles NAT en mode de disponibilité zonale pour les cas d'utilisation de NAT privés.

Comment fonctionnent les passerelles NAT régionales

Lorsque vous lancez des ressources dans une nouvelle zone de disponibilité, la passerelle NAT régionale détecte la présence d'une interface réseau (ENI) dans cette zone de disponibilité et s'étend automatiquement à cette zone. De même, la passerelle NAT contracte à partir de la zone de disponibilité qui n'a aucune charge de travail active.

L'extension de votre passerelle NAT régionale vers une nouvelle zone de disponibilité peut prendre jusqu'à 60 minutes une fois qu'une ressource y a été instanciée. Jusqu'à ce que cette extension soit terminée, le trafic pertinent provenant de cette ressource est traité entre les zones par votre passerelle NAT régionale dans l'une des zones de disponibilité existantes.

Les passerelles NAT régionales prennent en charge deux modes :

- Mode automatique : dans ce mode, gère AWS automatiquement les adresses IP et l'extension de la zone de disponibilité (recommandé). Si vous souhaitez utiliser vos propres adresses IP dans ce mode et que vous utilisez Amazon VPC IPAM, consultez la section Définir une stratégie d' IPv4 allocation publique avec des politiques IPAM dans le guide de l'utilisateur Amazon VPC IPAM.
- Mode manuel : dans ce mode, vous gérez manuellement les adresses IP et contrôlez la traduction des adresses réseau pour chaque zone de disponibilité. En mode manuel, vous êtes responsable de l'extension et de la contraction de votre passerelle NAT entre les zones de disponibilité.

Tarification

Pour plus d'informations sur les tarifs, consultez la section Tarification Amazon VPC.

Création d'une passerelle NAT régionale

Utilisation de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Passerelles NAT.
3. Sélectionnez Créer une passerelle NAT.
4. Pour le mode de disponibilité, choisissez Régional. Il n'est pas nécessaire de spécifier de sous-réseaux lorsque vous choisissez la disponibilité régionale.
5. Choisissez un VPC.
6. Terminez la configuration restante et choisissez Create NAT gateway.

Utilisation de la AWS CLI

Création d'une passerelle NAT régionale

```
aws ec2 create-nat-gateway --vpc-id vpc-12345678 --availability-mode regional
```

Afficher les détails de la passerelle NAT

```
aws ec2 describe-nat-gateways --nat-gateway-ids nat-12345678
```

Ajouter des adresses IP (mode manuel)

```
aws ec2 associate-nat-gateway-address --nat-gateway-id nat-12345678 --availability-zone
 us-east-1b --allocation-ids eipalloc-12345678
```

Supprimer les adresses IP

```
aws ec2 disassociate-nat-gateway-address --nat-gateway-id nat-12345678 --association-
ids eipassoc-12345678
```

Supprimer une passerelle NAT régionale

```
aws ec2 delete-nat-gateway --nat-gateway-id nat-12345678
```

Conversion de passerelles NAT zonales en passerelles NAT régionales

> **Important**
>
> Cela réinitialisera vos connexions existantes. Nous vous recommandons de suivre ces étapes dans votre fenêtre de maintenance.

Vous pouvez convertir des passerelles NAT zonales existantes en passerelle NAT régionale en utilisant l'une des deux approches suivantes :

Si vous êtes d'accord avec l'utilisation de passerelles NAT régionales avec de nouvelles adresses IP :

1. Création d'une nouvelle passerelle NAT régionale
2. Mettre à jour les tables de routage pour qu'elles pointent vers la passerelle NAT régionale
3. Supprimer les anciennes passerelles NAT zonales

Cette approche utilise de nouvelles adresses IP et réinitialise les connexions existantes lorsque les itinéraires sont mis à jour.

Si vous souhaitez réutiliser des adresses IP existantes avec des passerelles NAT régionales :

1. Supprimer les passerelles NAT zonales existantes pour libérer leurs adresses IP
2. Créez une passerelle NAT régionale à l'aide des adresses IP publiées
3. Mettre à jour les tables de routage pour qu'elles pointent vers la passerelle NAT régionale

Cette approche préserve les adresses IP mais nécessite une fenêtre de maintenance car le trafic est interrompu pendant la transition.

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
- Accédez à votre réseau à l'aide d'adresses IP autorisées
- Activer la communication entre des réseaux qui se chevauchent

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.

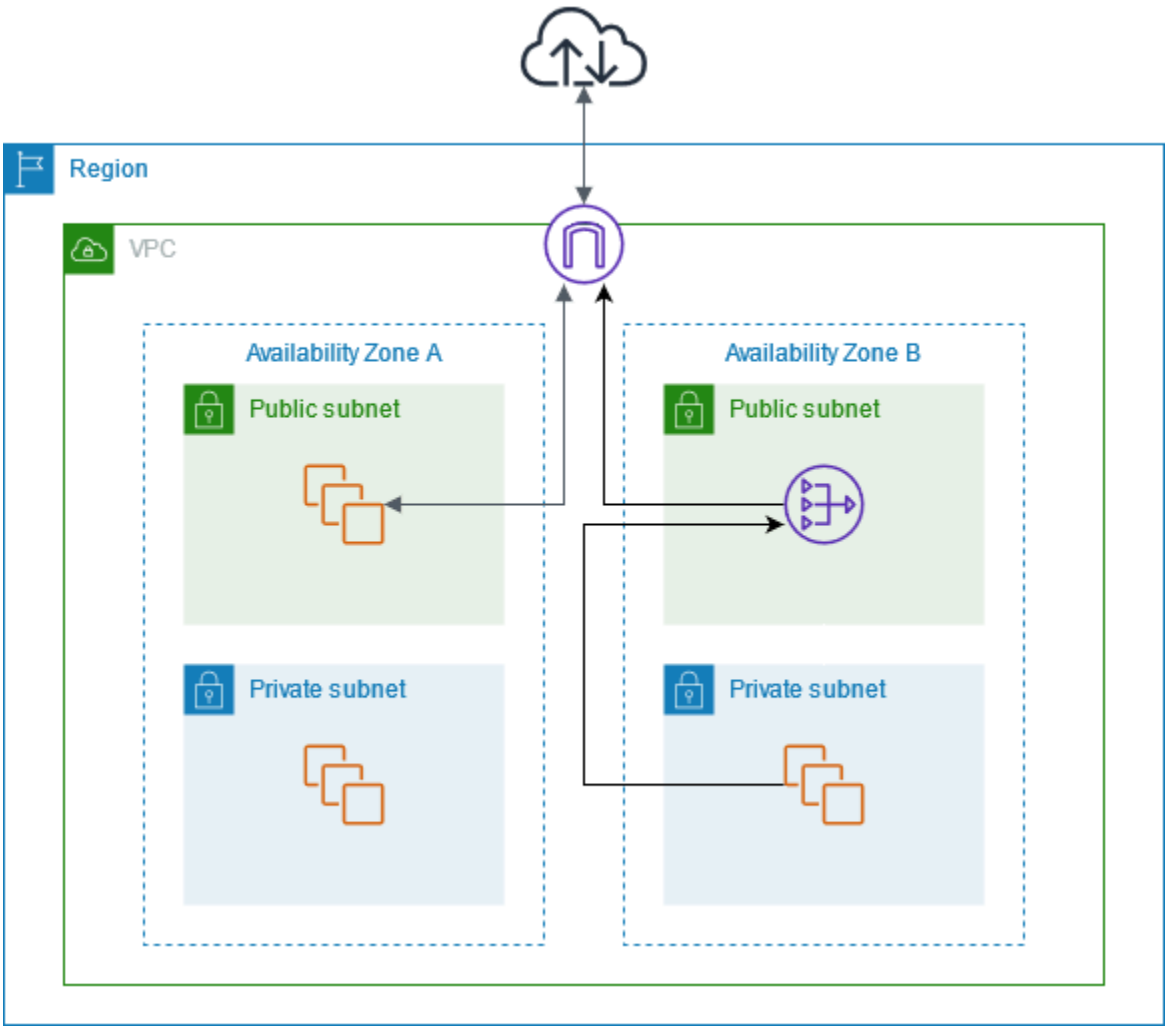
Table des matières

- Présentation de
- Routage
- Tester la passerelle NAT publique

Présentation de

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' IPv4 adresse privée source des instances à l' IPv4 adresse privée de la passerelle NAT privée, mais dans le cas d'une passerelle NAT publique, la passerelle Internet mappe ensuite l' IPv4 adresse privée de la passerelle NAT publique à l'adresse IP élastique 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	Target
VPC CIDR	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	Target
VPC CIDR	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	Target
VPC CIDR	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	Target
VPC CIDR	locale

Destination	Target
0.0.0.0/0	*nat-gateway-id*

Pour de plus amples informations, veuillez consulter the section called "Gestion des tables de routage des sous-réseaux".

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 Convertir votre clé privée à l'aide de Pu TTYgen 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 plus d'informations, consultez Connect to your Linux instance using PuTTY. 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.

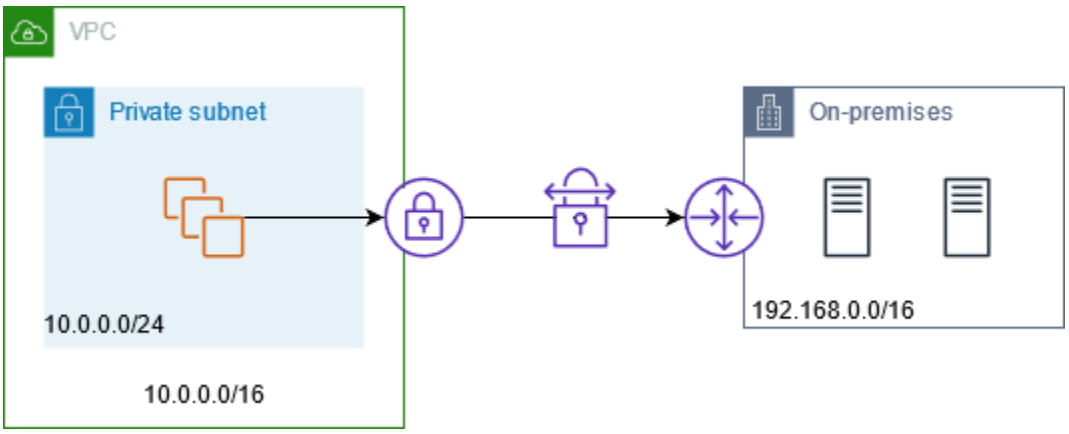
Accédez à votre réseau à l'aide d'adresses IP autorisées

Vous pouvez utiliser une passerelle NAT privée pour permettre la communication entre votre réseau local et votre réseau local VPCs à l'aide d'un pool 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.

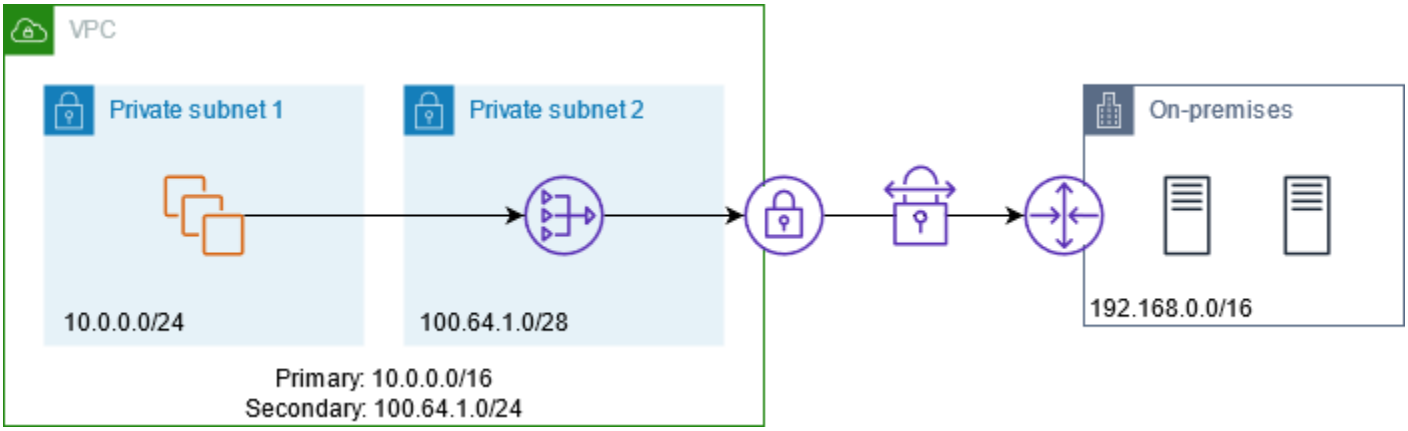
Table des matières

Présentation de

Le schéma suivant montre comment les instances peuvent accéder aux ressources locales via Site-to-Site 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	Target
10.0.0.0/16	local
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	Target
10.0.0.0/16	local
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.

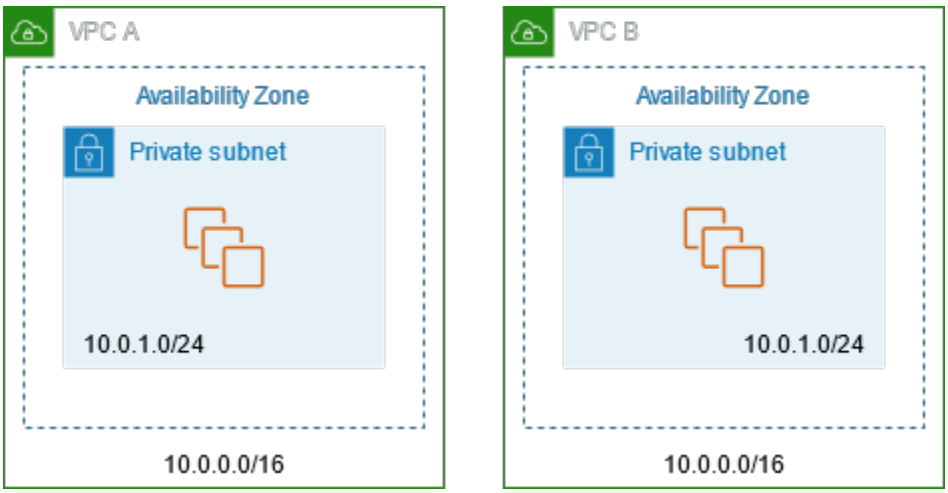


Table des matières

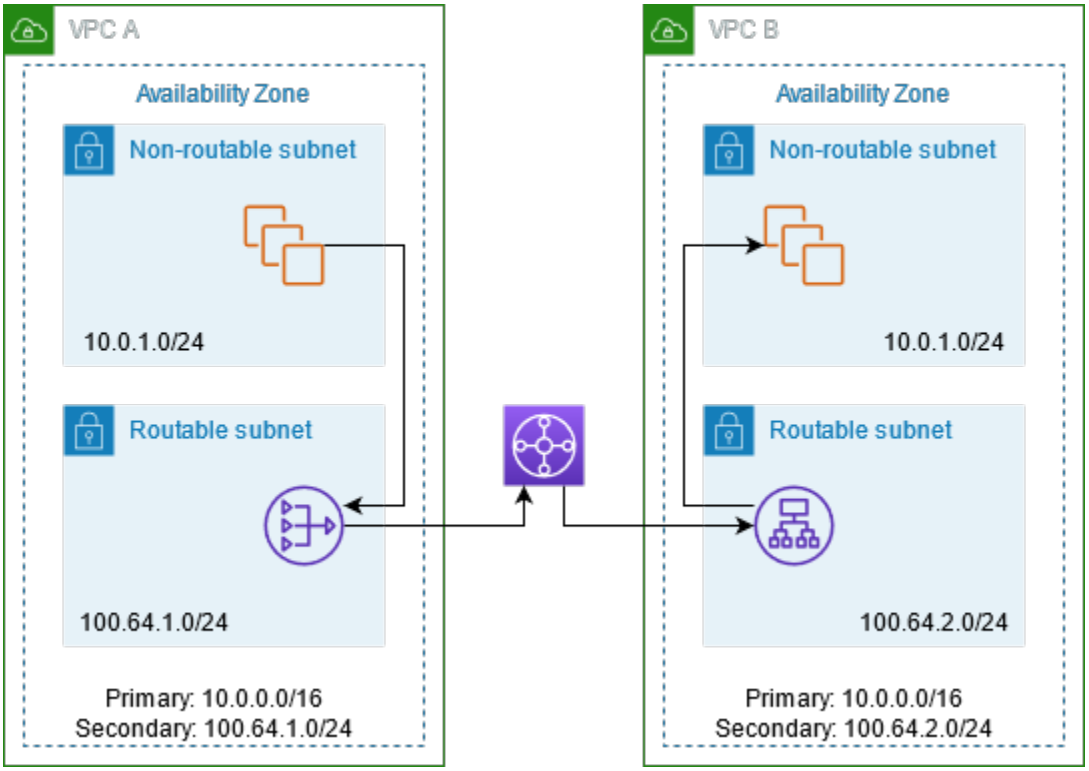
Présentation de

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 plages respectives. VPCs
- 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 le VPCs. 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	Target
10.0.0.0/16	local
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	Target
10.0.0.0/16	local
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	Target
10.0.0.0/16	local
100.64.2.0/24	local

Voici la table de routage pour le sous-réseau routable dans le VPC B.

Destination	Target
10.0.0.0/16	local
100.64.2.0/24	local
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	*Attachment for VPC A*	Statique
100.64.2.0/24	*Attachment for VPC B*	Statique

DNS64 et NAT64

Une passerelle NAT prend en charge la traduction d'adresses réseau de IPv6 vers IPv4, communément appelée NAT64. NAT64 permet à vos IPv6 AWS ressources de communiquer avec les IPv4 ressources du même VPC ou d'un autre VPC, de votre réseau local ou via Internet. Vous pouvez l'utiliser NAT64 avec DNS64 Amazon Route 53 Resolver ou utiliser votre propre DNS64 serveur.

Table des matières

Qu'est-ce que c'est DNS64 ?

Vos charges de travail IPv6 uniquement exécutées ne VPCs peuvent envoyer et recevoir que des paquets IPv6 réseau. Dans le cas contraire DNS64, une requête DNS pour un service IPv4 réservé produira une adresse de IPv4 destination en réponse et votre service IPv6 réservé ne pourra pas communiquer avec lui. Pour combler ce manque de communication, vous pouvez activer DNS64 un sous-réseau et cela 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 demandé et effectue l'une des opérations suivantes :

- Si l'enregistrement contient une IPv6 adresse, il renvoie l'enregistrement d'origine et la connexion est établie sans qu'aucune traduction ne soit effectuée IPv6.
- Si aucune IPv6 adresse n'est associée à la destination dans l'enregistrement DNS, le résolveur Route 53 en synthétise une en ajoutant le `/96` préfixe connu, défini dans RFC6052 (`64:ff9b::/96`), à l' IPv4 adresse de l'enregistrement. Votre service IPv6 réservé uniquement envoie des paquets réseau à l'adresse synthétisée. IPv6 Vous devrez ensuite acheminer ce trafic via la passerelle NAT, qui effectue la traduction nécessaire sur le trafic pour permettre aux IPv6 services de votre sous-réseau d'accéder aux IPv4 services situés en dehors de ce sous-réseau.

Vous pouvez activer ou désactiver DNS64 sur un sous-réseau à l'aide de la modify-subnet-attribute 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 c'est NAT64 ?

NAT64 permet à vos services IPv6 réservés sur Amazon de VPCs communiquer avec des services IPv4 réservés uniquement au sein du même VPC (dans différents sous-réseaux) ou connectés VPCs, dans vos réseaux sur site ou via 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 NAT64 fonctionner.

Après l'activation DNS64, si votre service réservé IPv6 uniquement envoie des paquets réseau à une IPv6 adresse synthétisée via la passerelle NAT, les événements suivants se produisent :

- À partir du `64:ff9b::/96` préfixe, la passerelle NAT reconnaît que la destination d'origine est IPv4 et traduit les IPv6 paquets IPv4 en remplaçant :
  - Source IPv6 avec sa propre adresse IP privée qui est traduite en adresse IP élastique par la passerelle Internet.
  - Destination IPv6 vers IPv4 en tronquant le `64:ff9b::/96` préfixe.
- La passerelle NAT envoie les IPv4 paquets traduits à la destination via la passerelle Internet, la passerelle privée virtuelle ou la passerelle de transit et établit une connexion.

- L'hôte IPv4 -only renvoie les paquets de IPv4 réponse. Une fois la connexion établie, la passerelle NAT accepte les IPv4 paquets de réponse des hôtes externes.
- Les IPv4 paquets de réponse sont destinés à la passerelle NAT, qui reçoit les paquets et NATs les supprime en remplaçant son adresse IP (IP de destination) par l' IPv6 adresse de l'hôte et en commençant `64:ff9b::/96` par l' IPv4 adresse 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 réservées à un sous-réseau de communiquer avec des services IPv4 uniquement situés en dehors du sous-réseau.

Configurez DNS64 et NAT64

Suivez les étapes décrites dans cette section pour configurer DNS64 et NAT64 activer la communication avec les services IPv4 réservés.

Table des matières

Activez la communication avec les services IPv4 uniquement sur Internet à l'aide de la CLI AWS

Si vous avez un sous-réseau avec des IPv6 charges de travail réservées qui doivent communiquer avec des services IPv4 uniquement extérieurs au sous-réseau, cet exemple vous montre comment activer ces services uniquement pour communiquer avec IPv4 des services IPv6 uniquement sur Internet.

Vous devez d'abord configurer une passerelle NAT dans un sous-réseau public (distinct du sous-réseau IPv6 contenant les charges de travail uniquement). Par exemple, le sous-réseau contenant la passerelle NAT doit comporter un acheminement `0.0.0.0/0` pointant vers la passerelle Internet.

Procédez comme suit pour permettre à ces services IPv6 réservés de se connecter à des services IPv4 uniquement sur Internet :

1. Ajoutez les trois itinéraires suivants à la table de routage du sous-réseau IPv6 contenant les charges de travail uniquement :
   - IPv4 route (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 réservées uniquement à des services IPv4 uniquement d'être acheminé via la passerelle NAT.
- IPv6 `::/0`route pointant vers la passerelle Internet de sortie uniquement (ou la passerelle Internet).

Notez que le fait `::/0` de pointer vers la passerelle Internet permettra aux IPv6 hôtes externes (extérieurs au VPC) d'établir une connexion. 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 DNS64 fonctionnalité dans le sous-réseau contenant les charges de IPv6 travail uniquement.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --enable-dns64
```

Désormais, les ressources de votre sous-réseau privé peuvent établir des connexions dynamiques avec les deux réseaux IPv4 et les IPv6 services sur Internet. Configurez votre groupe de sécurité de NACLs manière appropriée pour autoriser le trafic sortant et entrant dans le trafic. `64:ff9b::/96`

Activez la communication IPv4 uniquement avec les services de 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 :

- Vous créez un point de terminaison sortant du résolveur Route 53 dans un VPC et vous lui attribuez les IPv4 adresses à partir desquelles vous souhaitez que le résolveur Route 53 transfère

les requêtes. Pour votre résolveur DNS local, il s'agit des adresses IP d'où proviennent les requêtes DNS et doivent donc être IPv4 des adresses.

- 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. Vous spécifiez également les IPv4 adresses des résolveurs locaux.
- Maintenant que vous avez configuré un point de terminaison sortant Route 53 Resolver, vous devez l'activer DNS64 sur le sous-réseau IPv6 contenant uniquement vos charges de travail et acheminer toutes les données destinées à votre réseau local via une passerelle NAT.

Comment DNS64 fonctionne pour les destinations IPv4 réservées aux réseaux locaux :

1. Vous attribuez une IPv4 adresse au point de terminaison sortant du résolveur Route 53 dans votre VPC.
2. La requête DNS de votre IPv6 service est envoyée au résolveur Route 53. IPv6 Route 53 Resolver fait correspondre la requête à la règle de transfert et obtient une IPv4 adresse pour votre résolveur local.
3. Route 53 Resolver convertit le paquet de requête de 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' IPv4 adresse locale de votre résolveur DNS.
4. Le résolveur local renvoie le paquet de réponse via le point de IPv4 terminaison sortant au résolveur Route 53.
5. En supposant que la requête a été effectuée à partir d'un sous-réseau DNS64 activé, Route 53 Resolver effectue deux opérations :

    a. Il vérifie le contenu du paquet de réponses. Si l'enregistrement contient une IPv6 adresse, il conserve le contenu tel quel, mais s'il ne contient qu'un IPv4 enregistrement. Il synthétise également un IPv6 enregistrement en commençant par `64:ff9b::/96` l' IPv4adresse.

    b. Reconditionne le contenu et l'envoie au service dans votre IPv6 VPC.

Inspectez le trafic provenant des passerelles NAT

Vous pouvez associer un proxy Network Firewall à votre passerelle NAT pour inspecter et filtrer le trafic sur votre passerelle NAT. Ce contrôle de sécurité vous permet de prévenir les fuites de données en dehors de votre périmètre de confiance et de bloquer toute réponse entrante indésirable.

Comment ça marche

Lors de la création d'un proxy Network Firewall, vous devez sélectionner une passerelle NAT existante à laquelle vous souhaitez connecter le proxy. Une fois créé, le proxy :

- Le proxy est fourni avec un nom de domaine complet et vous devez configurer vos applications pour envoyer des demandes de connexion http et https au proxy. Le proxy filtre d'abord le nom de domaine dans la demande de connexion en fonction des règles saisies par le client. Si le client l'autorise, le proxy effectue ensuite une requête DNS pour obtenir l'adresse IP du domaine. Il a ensuite établi une connexion TCP avec la destination finale. Selon que le déchiffrement TLS est activé ou non, le proxy filtre ensuite la connexion TLS en fonction de l'adresse IP et des attributs d'en-tête et n'établit une connexion TLS avec la destination que si les attributs IP et d'en-tête (y compris l'action d'en-tête et le chemin URL) sont autorisés par les politiques.
- L'appliance inspecte et filtre le trafic.
- Le trafic autorisé continue vers la destination (sur Internet, dans un environnement sur site ou dans un autre VPC).

Fixation d'appareils

Les appliances sont connectées aux passerelles NAT via AWS Network Firewall. Pour savoir comment créer et connecter des appliances, consultez le guide du développeur de Network Firewall Proxy.

Affichage des appareils connectés

Pour afficher les appareils connectés à votre passerelle NAT, utilisez la describe-nat-gatewayscommande suivante :

```
aws ec2 describe-nat-gateways --nat-gateway-ids nat-1234567890abcdef0
```

La réponse inclut un `AttachedAppliances` champ indiquant :

- Type — Le type d'appareil (par exemple,`network-firewall-proxy`)
- ApplianceArn— L'ARN de l'appliance connectée
- AttachmentState— État actuel de la pièce jointe (`attacheddetaching`,`detached`,`attach_failed`,`detach_failed`)
- ModificationState— État actuel de la modification (`modifying`,`completed`,`failed`)

- VpcEndpointId— L'ID du point de terminaison VPC utilisé pour acheminer le trafic de l'application vers le proxy VPCs à des fins d'inspection et de filtrage
- FailureCode— Le code d'erreur en cas d'échec de l'opération de fixation ou de modification de l'appliance
- FailureMessage— Un message descriptif expliquant la panne en cas d'échec de l'opération de connexion ou de modification de l'appliance

Surveillance des passerelles NAT avec Amazon CloudWatch

Vous pouvez surveiller votre passerelle NAT avec CloudWatch, qui recueille ses informations et crée des métriques lisibles quasi en temps réel. Vous pouvez utiliser ces informations afin de surveiller et de résoudre les problèmes de votre passerelle NAT. Ces indicateurs vous donnent une visibilité sur l'état et les performances de votre passerelle NAT, ce qui vous permet de surveiller de près son fonctionnement et de résoudre rapidement les problèmes éventuels.

Les métriques de passerelle NAT collectées par CloudWatch incluent des points de données tels que les octets traités, le nombre de paquets, le nombre de connexions et les taux d'erreur. Cela vous permet de bien comprendre le trafic qui passe par votre passerelle NAT et d'identifier les anomalies ou les goulots d'étranglement. CloudWatch fournit ces données métriques à intervalles d'une minute, vous offrant ainsi une vue précise et actualisée du comportement de votre passerelle NAT.

En outre, CloudWatch conserve les données métriques de cette passerelle NAT pendant une période prolongée de 15 mois, ce qui vous permet d'analyser les tendances et les modèles au fil du temps. Vous pouvez utiliser ces données historiques pour planifier les capacités, optimiser les performances et comprendre l'évolution à long terme de l'utilisation de votre passerelle NAT.

Pour tirer parti de ces puissantes fonctionnalités de surveillance, vous pouvez créer des tableaux de bord et des alarmes CloudWatch personnalisés et adaptés à vos besoins spécifiques. Par exemple, vous pouvez configurer des alertes pour vous avertir chaque fois que le transfert de données sortant de votre passerelle NAT dépasse un certain seuil, ce qui vous permet de répondre de manière proactive aux éventuelles contraintes de bande passante.

Pour plus d'informations sur la tarification, consultez Tarification Amazon CloudWatch.

Table des matières

- Créer des alarmes CloudWatch pour surveiller une passerelle NAT

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'Interne t vers les clients qui se trouvent derrière la passerelle NAT. Si la valeur de BytesOutT oSource est inférieure à celle de BytesInFr omDestination , 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 effectuée s sur la passerelle NAT. Cette métrique concerne uniquement la synchronisation initiale. Dans certains cas, la valeur de ConnectionAttemptCount peut être inférieure à celle de ConnectionEstablis hedCount en raison de la retransmission de synchronisation. Si la valeur de ConnectionEstablis hedCount 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. Cette métrique concerne la synchronisation et les retransmissions de synchronisation. 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 abandonnés en pourcentage du trafic de paquets global, utilisez la formule suivante : `PacketsDropCount/(PacketsInFromSource+PacketsInFromDestination)*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 AWS Service Health Dashboard pour identifier tout problème lié au service susceptible d'entraîner l'abandon 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 métriques CloudWatch de la passerelle NAT

Les métriques de la passerelle NAT sont envoyées vers CloudWatch toutes les minutes. 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 console CloudWatch

1. Ouvrez la console CloudWatch 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 afficher les métriques à l'aide de la 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"
```

Créer des alarmes CloudWatch pour surveiller une passerelle NAT

Créez une alarme CloudWatch qui envoie un message Amazon SNS lorsque l'alarme change de statut. 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 console CloudWatch 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 en regard de la métrique BytesOutToDestination de la passerelle NAT, puis choisissez Sélectionner une métrique.
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 console CloudWatch 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 en regard de la métrique ErrorPortAllocation de la passerelle NAT, puis choisissez Sélectionner la métrique.
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 Utilisation des alarmes Amazon CloudWatlh dans le Guide de l'utilisateur Amazon CloudWatch.

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 le paramètre Disponible IPs dans le volet de 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 Ajouter un accès Internet à un sous-réseau.
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 IPs page

Erreur affichée	Cause	Solution
	ressource, et ne peut être associée à la passerelle NAT.	Elastic de la console Amazon VPC et consultez les valeurs spécifiées pour l'ID d'instanc e 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 Commencer à 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 IPs quota Elastic à l'aide de la console Service Quotas.

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 votre réseau ACLs 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, rendez-vous sur la page Passerelles NAT et consultez les informations d'état 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 le réseau ACLs associé au sous-réseau privé et aux sous-réseaux publics ne possède pas de règles bloquant 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.

IPsec la connexion ne peut pas être établie

Problème

Vous ne pouvez pas établir de IPsec connexion avec une destination.

Cause

Les passerelles NAT ne prennent actuellement pas en charge le IPsec protocole.

Solution

Vous pouvez utiliser NAT-Traversal (NAT-T) pour encapsuler le IPsec trafic dans le protocole UDP, qui est pris en charge par les passerelles NAT. Assurez-vous de tester votre NAT-T et votre IPsec configuration pour vérifier que votre IPsec trafic 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 `IdleTimeoutCount`métrique pour CloudWatch surveiller l'augmentation du nombre de 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 IPv4 adresse 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 des passerelles NAT

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 IPv4 trafic sortant vers Internet, mais elles ne peuvent pas recevoir le trafic entrant initié sur Internet.

> **Important**
>
> L'AMI NAT repose sur la dernière version de l'AMI Amazon Linux, 2018.03, qui a atteint la fin de la prise en charge standard le 31 décembre 2020 et la fin de la prise en charge de la 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 de plus amples informations, veuillez consulter Comparer des passerelles NAT et des instances NAT..

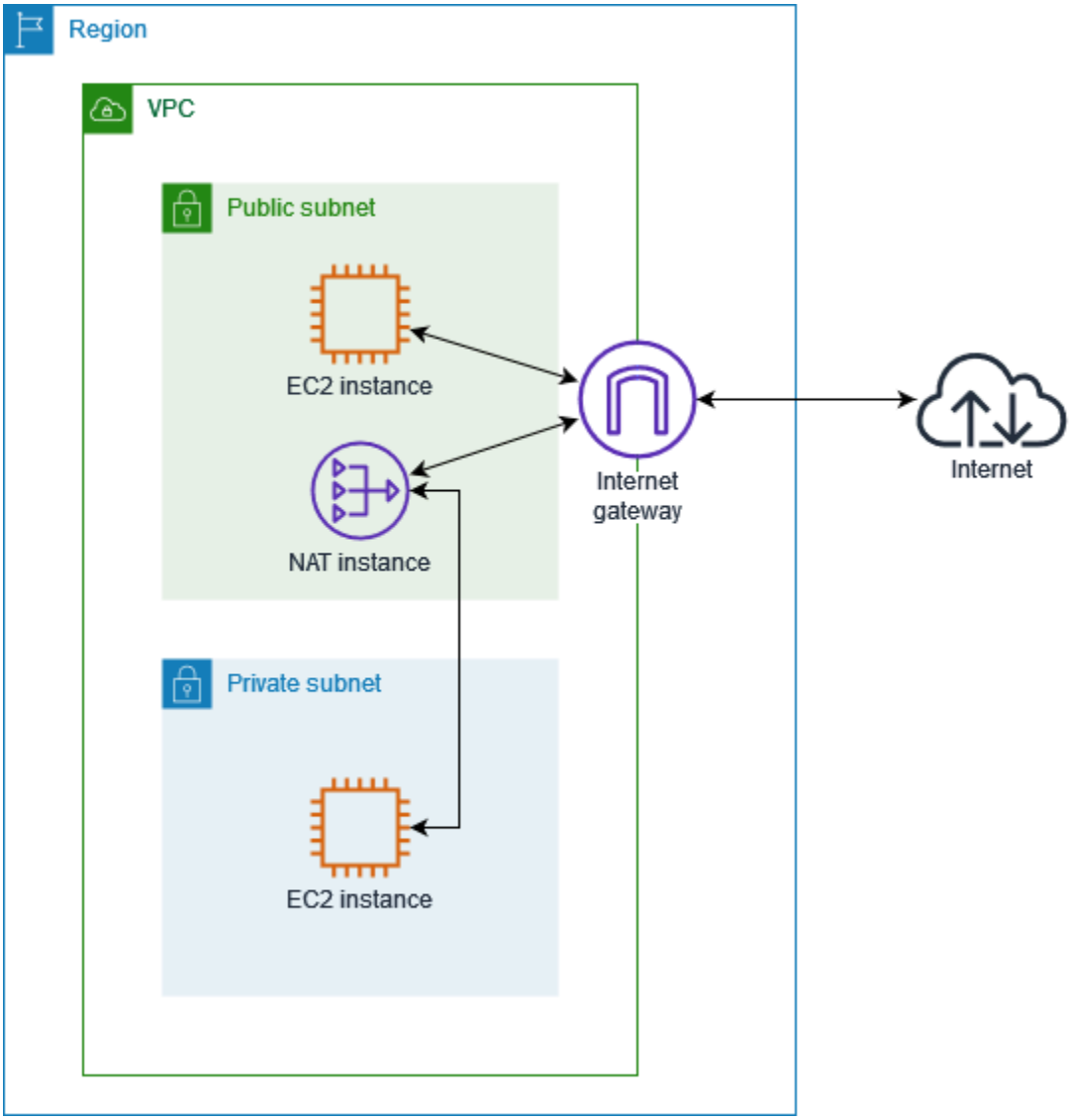
Si les instances NAT sont mieux adaptées à votre cas d'utilisation que les passerelles NAT, vous pouvez créer votre propre AMI NAT à partir de la version actuelle d'Amazon Linux, comme décrit dans the section called "3. Créer une AMI NAT".

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.

Permettre aux ressources privées de communiquer en dehors du VPC

Cette section décrit comment créer et utiliser des instances NAT pour permettre aux ressources d'un sous-réseau privé de communiquer en dehors du cloud privé virtuel.

Tâches

- 1. Créer un VPC pour l'instance NAT

1. 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).

2. 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 entrantes recommandées sont décrites ci-dessous.

Source	Protocole	Plage de ports	Commentaires
Private subnet CIDR	TCP	80	Autorisez le trafic HTTP entrant depuis les serveurs dans le sous-réseau privé
Private subnet CIDR	TCP	443	Autorisez le trafic HTTPS entrant depuis les serveurs dans le sous-réseau privé
Public IP address range of your network	TCP	22	Autoriser l'accès SSH entrant vers l'instance NAT depuis votre réseau (via la passerelle Internet)

Les règles sortantes recommandées sont décrites ci-dessous.

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 de plus amples informations, veuillez consulter Groupes de sécurité.

3. 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 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 ce n'est pas le caseth0, remplacez-la *eth0* par l'interface réseau principale que vous avez indiquée 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 Créer une AMI Linux à partir d'une instance dans le Guide de l'utilisateur Amazon EC2.

4. 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 les images d'applications et de systèmes d'exploitation, sélectionnez votre AMI NAT (choisissez Parcourir davantage AMIs, Mon AMIs).
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. Désactivez les source/destination vérifications pour l'instance NAT (voir5. Désactiver les source/destination chèques).
10. Mettez à jour la table de routage pour envoyer du trafic vers l'instance NAT (voir 6. Mise à jour de la table de routage).

5. Désactiver les source/destination chèques

Chaque instance EC2 effectue source/destination des vérifications 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 vérifications sur l'instance NAT.

Pour désactiver la source/destination vérification

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance NAT.
4. Choisissez Actions, Mise en réseau, source/destination Vérification des modifications.
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).

6. 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 de plus amples informations, veuillez consulter Configuration des tables de routage.

7. 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 Ajouter une règle. Choisissez All 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 Ajouter une règle. Choisissez All ICMP - IPv4 pour Type. Choisissez 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 à l'aide de Pu TTYgen.

   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 source/destination la vérification de votre instance NAT. Pour de plus amples informations, veuillez consulter 5. Désactiver les source/destination chèques.
- Vérifiez que vous avez correctement configuré vos tables de routage. Pour de plus amples informations, veuillez consulter 6. 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.

Attribut	Passerelle NAT	Instance NAT
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.
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.

Attribut	Passerelle NAT	Instance NAT
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.
Métriques du trafic	Affichez les métriques CloudWatch pour la passerelle NAT.	Affichez les métriques CloudWatch pour 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 élastique est une IPv4 adresse publique statique conçue spécifiquement pour la nature dynamique du cloud computing. Cette fonctionnalité vous permet d'associer une adresse IP élastique à n'importe quelle instance ou interface réseau au sein de n'importe quel Virtual Private Cloud (VPC) de votre compte. AWS En tirant parti des adresses IP Elastic, vous pouvez bénéficier de nombreux avantages qui simplifient la gestion et la résilience de votre infrastructure basée sur le cloud.

L'un des principaux avantages des adresses IP Elastic est leur capacité à contourner un problème de défaillance d'une instance. En cas de panne inattendue d'une instance ou si elle doit être remplacée, vous pouvez remapper l'adresse IP Elastic associée à une autre instance au sein de votre VPC. Ce processus de basculement garantit que vos applications et services conservent un point de terminaison public cohérent et fiable, ce qui réduit au maximum la durée d'indisponibilité et offre une expérience utilisateur supérieure.

En outre, les adresses IP Elastic offrent une certaine flexibilité dans la façon dont vous pouvez gérer vos ressources réseau. Vous pouvez associer et dissocier ces adresses par programmation selon vos besoins, ce qui vous permet de diriger le trafic vers différentes instances en fonction de l'évolution des exigences de votre entreprise. Cette allocation dynamique d'adresses IP publiques vous permet de vous adapter à l'évolution de la demande, de mettre à l'échelle votre infrastructure et d'implémenter des architectures innovantes sans les contraintes liées aux attributions d'adresses IP statiques.

Au-delà de leur utilisation pour le basculement d'une instance, les adresses IP Elastic peuvent également servir d'identificateurs stables pour vos ressources basées sur le cloud. Cela peut être utile lors de la configuration de services externes, tels que des enregistrements DNS ou des règles de pare-feu, pour communiquer avec vos applications AWS hébergées. En associant une adresse IP publique permanente, vous pouvez pérenniser vos configurations réseau et éviter de devoir mettre à jour les références externes lorsque des instances sous-jacentes sont remplacées ou mises à l'échelle.

Table des matières

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 Interfaces réseau Elastic 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 élastique à l'interface réseau principale de votre instance, son IPv4 adresse publique actuelle (le cas échéant) est publiée dans le pool d'adresses IP publiques. Si vous dissociez l'adresse IP élastique, une nouvelle IPv4 adresse publique est automatiquement attribuée à l'interface réseau principale 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 de plus amples informations, veuillez consulter Connectez-vous à Internet ou à d'autres réseaux à l'aide de périphériques NAT.
- Les adresses IP élastiques pour ne IPv6 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 plus d'informations, consultez Groupes de sécurité et Réseau ACLs.

- 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 la manière d'apporter vos propres adresses IP, consultez Bring your own IP addresses (BYOIP) dans le Guide de l'utilisateur Amazon EC2.
- Les IPv4 adresses publiques prennent en charge les balises de répartition des coûts. Si vous appliquez des balises aux adresses IP Elastic, vous pouvez les utiliser pour suivre les coûts des IPv4 adresses publiques dans AWS Cost Explorer.

  Avant de pouvoir utiliser les balises comme balises de répartition des coûts, vous devez les activer. Pour plus d'informations, consultez Activation des identifications de répartition des coûts définies par l'utilisateur dans le Guide de l'utilisateur AWS Billing . Veuillez noter qu'après avoir créé et appliqué des balises définies par l'utilisateur à vos ressources, l'activation des clés de balises sur votre page de balises de répartition des coûts peut prendre jusqu'à 24 heures.

  Une fois les balises de répartition des coûts activées...

  - Pour toutes les adresses IPv4 publiques (y compris les adresses IPv4 publiques attribuées aux instances EC2 et les adresses IP Elastic) associées à une interface réseau élastique, vous pouvez consulter les coûts associés aux IPv4 adresses publiques dans Cost Explorer en choisissant Usage type > Public IPv4 InUseAddress (heures).
  - Si une adresse IP élastique balisée n'est pas associée à une ENI ou est associée à une ressource arrêtée (comme une instance EC2 arrêtée), elle est considérée comme une IPv4 adresse inactive. Vous pouvez consulter les coûts associés aux IPv4 adresses inactives dans Cost Explorer en choisissant Type d'utilisation > Public IPv4 IdleAddress (heures).

  Pour plus d'informations sur Cost Explorer, consultez Analyse de vos coûts à l'aide de l' AWS Cost Explorer dans le Guide de l'utilisateur AWS Billing .

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 .

Pour plus d'informations sur la tarification des adresses IP élastiques, consultez la section IPv4 Adresse publique dans la section Tarification d'Amazon VPC.

Commencer à utiliser des adresses IP Elastic

Les sections suivantes expliquent comment commencer à utiliser les adresses IP Elastic.

Tâches

- 1. Allouer une adresse IP Elastic
- 2. Associer une adresse IP Elastic
- 3. Dissocier une adresse IP Elastic
- 4. Transfert d'adresses IP Elastic
- 5. Libérer une adresse IP Elastic
- 6. Récupérer une adresse IP Elastic
- Présentation de la ligne de commande

1. 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 (AZs), de zones locales ou de zones de longueur d'onde à partir duquel AWS une adresse IP publique est annoncée. Les zones Locales et les Zones de longueur d'onde peuvent avoir des groupes de bordure de réseau différents de ceux 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. AZs

> **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 les zones locales ou les zones de longueur d'onde sont activées (pour plus d'informations, voir Activer une zone locale ou Activer les zones de longueur d'onde), vous pouvez choisir un groupe de bordure réseau pour les AZs zones locales ou les zones de longueur d'onde. 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 les zones Local ou Wavelength Zones ne sont pas activées, lorsque vous allouez un EIP, le groupe de bordure du réseau qui représente toutes les zones de la région (par exemple`us-west-2`) est prédéfini pour vous et vous ne pouvez pas le modifier. AZs Cela signifie que l'EIP que vous attribuez à ce groupe frontalier du réseau sera annoncé dans l'ensemble de la région AZs dans laquelle vous vous trouvez.

5. Pour le pool IPv4 d'adresses publiques, choisissez l'une des options suivantes :

   - Le pool d'adresses IP d'Amazon : si vous souhaitez qu'une IPv4 adresse soit attribuée à partir du pool d'adresses IP d'Amazon.
   - Mon pool d' IPv4adresses publiques : si vous souhaitez attribuer une IPv4 adresse à partir d'un pool d'adresses IP que vous avez ajouté à votre AWS compte. Cette option est désactivée si vous ne disposez pas de groupes d'adresses IP.
   - Pool d' IPv4adresses appartenant au client : si vous souhaitez allouer une IPv4 adresse à partir d'un pool créé à partir de votre réseau local 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.

2. 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 volet de navigation, sélectionnez Elastic IPs.
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.

3. 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 volet de navigation, sélectionnez Elastic IPs.

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).

4. 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 à attendre que les nouvelles adresses IP élastiques soient autorisées dans vos groupes de sécurité et NACLs.
- 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 élastiques pour reconfigurer rapidement les charges de travail Internet IPs destinées au public lors d'événements 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 describe-

address-transfers AWS CLI commande). 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 describe-address-transfers AWS CLI commande) pendant 14 jours après l'acceptation des transferts.
- 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' IPv4adresses 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 volet de navigation, sélectionnez Elastic IPs.

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. Sous ID de compte IDs de transfert, entrez les AWS comptes vers lesquels vous souhaitez transférer les adresses IP élastiques.
7. Confirmez le transfert en saisissant **`enable`** dans la zone de texte.
8. Sélectionnez Soumettre.
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 volet de navigation, sélectionnez Elastic IPs.
4. Dans la liste des ressources d'Elastic IPs, assurez-vous que la propriété indiquant la colonne Transfer status 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 Soumettre.

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 describe-address-transfers AWS CLI commande). 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 :

- AddressLimitExceeded: 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 Limite appliquée aux adresses IP Elastic dans le Guide de l'utilisateur Amazon EC2 pour les instructions relatives à l'augmentation de la 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 registre DNS inverse 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 Elastic dans le Guide de l'utilisateur Amazon EC2.

Pour toute autre exception, contactez 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 volet de navigation, sélectionnez Elastic IPs.
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 Soumettre.

5. 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, même non 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 volet de navigation, sélectionnez Elastic IPs.
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.

6. 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 de la ligne de commande

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)

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 Direct Connect.

L'un des principaux avantages de l'utilisation d'une passerelle de transit est la possibilité de centraliser et de simplifier la gestion de la connectivité entre vos VPC et les réseaux sur site. Plutôt que de configurer plusieurs connexions VPN ou plusieurs liens Direct Connect, vous pouvez utiliser la

passerelle de transit comme point d'intégration unique, ce qui peut contribuer à réduire la complexité globale et la charge opérationnelle de votre architecture réseau.

La tarification de l'utilisation d'une passerelle de transit est basée sur le volume de données transférées via la passerelle. Il existe un tarif par Go pour les données transférées à destination et en provenance de la passerelle de transit, ainsi qu'un tarif horaire distinct pour la ressource de passerelle de transit elle-même. La tarification peut varier d'une région AWS à une autre et est sujette à des modifications. Il est donc important de consulter la page de tarification AWS Transit Gateway actuelle pour obtenir les informations les plus récentes. En comprenant le modèle de tarification des passerelles de transit, vous pouvez mieux planifier et budgétiser les coûts permanents associés à ce service réseau AWS. Ceci, combiné aux avantages en termes d'efficacité opérationnelle et de connectivité, fait des passerelles de transit un choix intéressant pour les organisations qui cherchent à créer des solutions de cloud hybride évolutives et rentables.

Le tableau suivant présente des cas d'utilisation courants des passerelles de transit. Pour plus d'informations sur chaque cas d'utilisation, consultez Example transit gateway scenarios dans le Guide d'utilisation d'AWS Transit Gateway.

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.
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.
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 une plus grande flexibilité dans les cas où les routes et les attachements peuvent changer.

Pour plus d'informations, consultez AWS Transit Gateway.

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.

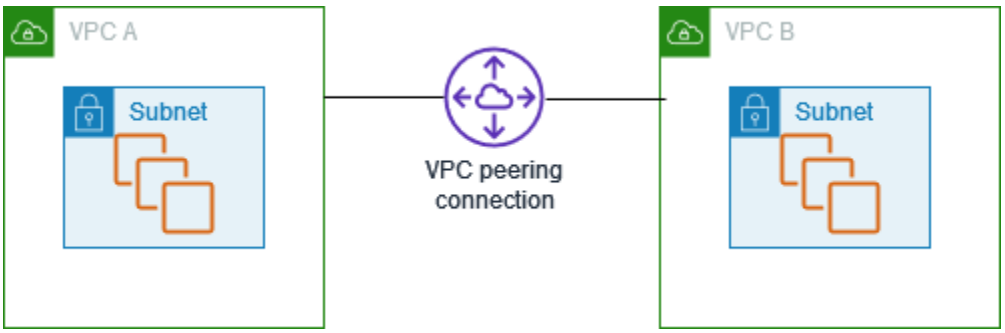
Option de connectivité VPN	Description
AWS Site-to-Site VPN	Vous pouvez créer une connexion VPN IPsec entre votre VPC et votre réseau distant. Du côté AWS de la connexion Site-to-Site VPN, une passerelle réseau privé virtuel ou une passerelle de transit fournit deux points de terminaison VPN (tunnels) 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 disposez de plusieurs réseaux distants (par exemple, plusieurs succursales), vous pouvez créer plusieurs connexions AWS Site-to-Site VPN via votre passerelle privée virtuelle pour permettre la communica tion 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

Option de connectivité VPN	Description
	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 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 Direct Connect dans le Guide de l'utilisateur Direct Connect.

Connexion de VPC avec l'appairage de VPC

Une connexion d'appairage de VPC est une fonctionnalité de mise en réseau qui permet une communication directe et sécurisée entre deux clouds virtuels privés (VPC) au sein de l'infrastructure. AWS Cette connexion privée permet aux ressources des VPC appairés d'interagir les unes avec les autres comme si elles faisaient partie du même réseau, éliminant ainsi le besoin de passer par l'Internet public.



Le processus de création d'une connexion d'appairage de VPC tire parti de l'infrastructure VPC existante pour établir cette connexion, sans nécessiter de passerelle, d'AWS Site-to-Site VPN ou de matériel physique supplémentaire. Cette conception garantit l'absence de point unique de défaillance ou de goulet d'étranglement en termes de bande passante.

L'un des principaux avantages d'une connexion d'appairage de VPC est la possibilité de connecter des VPC entre différents comptes AWS ou même différentes régions AWS. Cette flexibilité permet aux organisations d'intégrer facilement leurs ressources cloud, qu'elles soient au sein d'un même compte ou réparties sur plusieurs comptes et emplacements géographiques. Le caractère privé de

la connexion garantit également que tout le trafic de données entre les VPC appairés reste sur le réseau AWS, sans jamais passer par l’Internet public.

Les cas d’utilisation des connexions d’appairage de VPC sont très variés. Les organisations peuvent tirer parti de cette fonctionnalité pour sécuriser la communication entre les différents niveaux d’une application (tels que les serveurs web et les serveurs de base de données), faciliter le partage des ressources entre plusieurs équipes ou unités commerciales, ou même activer des architectures cloud hybrides en connectant des réseaux sur site à leurs VPC AWS.

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.

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 à destination et en provenance des interfaces réseau de votre. VPCs

Amazon CloudWatch Internet Monitor

Vous pouvez utiliser Internet Monitor pour avoir une idée de l'impact des problèmes Internet sur les performances et la disponibilité entre vos applications hébergées sur AWS et vos utilisateurs finaux. Vous pouvez également découvrir, en temps quasi réel, comment améliorer la latence prévue de votre application en optant pour d'autres services ou en réacheminant le trafic vers votre charge de travail via différents Régions AWS moyens. Pour plus d'informations, consultez la section Utilisation d'Amazon CloudWatch Internet Monitor.

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 fonctionnalité pour copier le trafic réseau depuis l'interface réseau d'une instance Amazon EC2 et l'envoyer aux dispositifs de out-of-band sécurité et de surveillance pour 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 source et de destination, Reachability Analyzer hop-by-hop fournit des détails sur le chemin virtuel qui les relie lorsqu'elles sont accessibles et identifie le composant bloquant lorsqu'elles 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.

CloudTrail journaux

AWS CloudTrail enregistre les appels d'API pour Amazon VPC, tels que :

- Appels d'API effectués (création ou modification de ressources VPC, par exemple)
- Adresse IP source de l'appel
- Auteur de l'appel
- Date et heure de l'appel

Des journaux distincts sont créés pour les actions `CreateVpc`, `DeleteVpc` et `CreateDefaultVpc`. Ces journaux incluent également les ressources par défaut (comme les passerelles Internet ou les groupes de sécurité par défaut) créées et associées au VPC.

Pour plus d'informations, consultez Log Amazon EC2 API calls using AWS CloudTrail dans le Guide d'utilisation d'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. Le chemin de livraison configuré et les autorisations qui permettent d'envoyer les journaux du trafic réseau vers une destination telle que CloudWatch Logs ou S3 sont appelés abonnements. 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 VPCs. Pour plus d'informations sur les journaux de flux pour les passerelles de transit introduites dans la version 6, consultez Journalisation du trafic réseau à l'aide de Transit Gateway Flow Logs dans le Guide de l'utilisateur Amazon VPC Transit Gateways.

Table des matières

Principes de base des journaux de flux

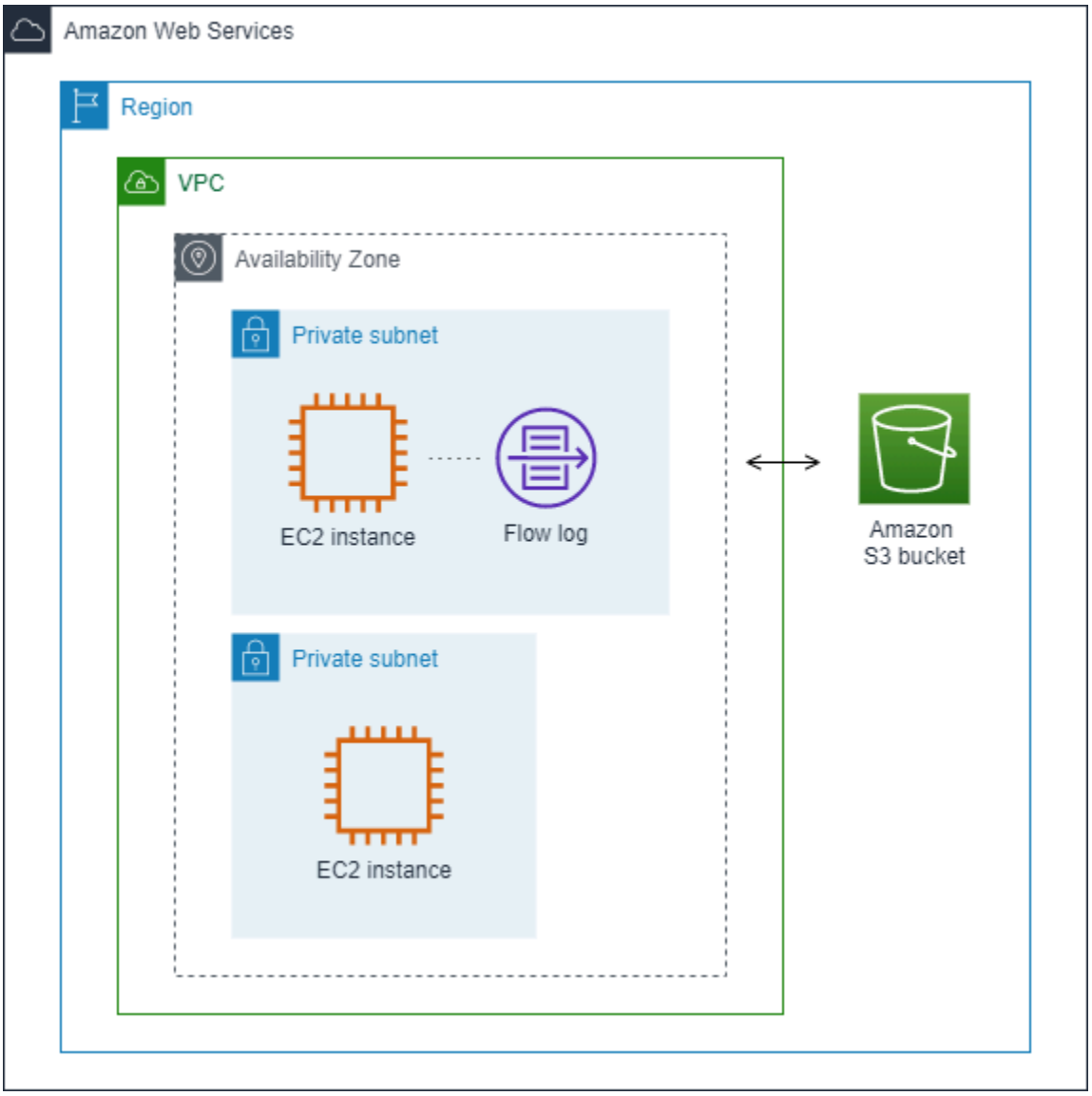
Vous pouvez créer un journal de flux pour un VPC, un sous-réseau ou une interface réseau. Si vous créez un journal de flux pour un sous-réseau ou VPC, chaque interface réseau du sous-réseau ou du VPC est surveillée.

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.

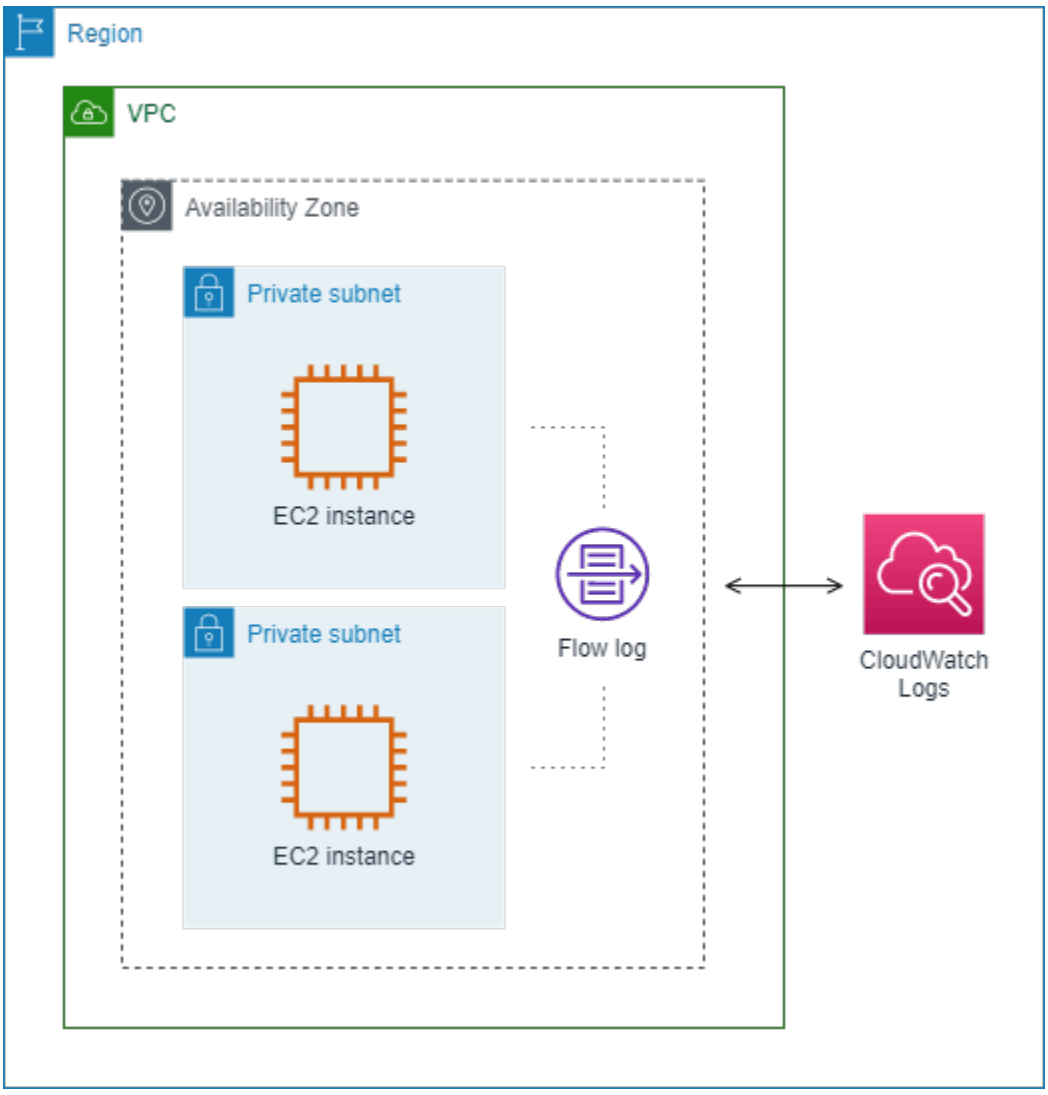
Pour créer un journal de flux, vous spécifiez :

- 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 de plus amples informations, veuillez consulter 2. 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 de plus amples informations, veuillez consulter 4. 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. Renvoie un symbole « - » pour les flux associés à une passerelle NAT régionale. Type de données Parquet : CHAÎNE	2

Champ	Description	Version
srcaddr	Pour le trafic entrant, il s'agit de l'adresse IP de la source du trafic. Pour le trafic sortant, il s'agit de l' IPv4 adresse privée ou de l' IPv6 adresse de l'interface réseau qui envoie le trafic. Pour le trafic sortant de la passerelle NAT régionale, il s'agit de la même adresse IP source au niveau du paquet que dans. pkt-srcaddr Consultez également pkt-srcaddr. Type de données Parquet : CHAÎNE	2
dstaddr	Adresse de destination pour le trafic sortant, ou IPv6 adresse IPv4 ou de l'interface réseau pour le trafic entrant sur l'interface réseau. L' IPv4 adresse de l'interface réseau est toujours son IPv4 adresse privée. Pour le trafic entrant vers la passerelle NAT régionale, il s'agit de la même adresse IP de destination au niveau du paquet que dans. pkt-dstaddr Consultez également 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

Champ	Description	Version
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
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'était pas autorisé par les groupes de sécurité ou le réseau ACLs, ou les paquets sont arrivés après la fermeture de la connexion. Type de données Parquet : CHAÎNE	2

Champ	Description	Version
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'interface 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. Certains enregistrements de journaux de flux peuvent être ignorés pendant l'intervalle d'agrégation (consultez log-status dans Champs disponibles). Cela peut être dû à une contrainte de AWS capacité interne ou à une erreur interne. Si vous utilisez AWS Cost Explorer pour consulter les frais des journaux de flux VPC et que certains journaux de flux sont ignorés pendant l'intervalle d'agrégation des journaux de flux, le nombre de journaux de flux signalés AWS Cost Explorer sera supérieur au nombre de journaux de flux publiés par Amazon VPC. 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
subnet-id	ID du sous-réseau qui contient l'interface réseau pour laquelle le trafic est enregistré. Renvoie un symbole « - » pour les flux associés à la passerelle NAT régionale. Type de données Parquet : CHAÎNE	3

Champ	Description	Version
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 indicateur 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 quelconque, 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 des plages d'adresses IP pour le champ pkt-srcaddr, si l'adresse IP source est prévue pour un service AWS . Si l'adresse IP source appartient à une plage superposée, n'pkt-src-aws-serviceaffiche qu'un seul des codes de AWS service. Les valeurs possibles sont les suivantes : `AMAZON AMAZON_APPFLOW AMAZON_CONNECT API_GATEWAY | AURORA_DSQL | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | IVS_LOW_LATENCY IVS_REALTIME | KINESIS_VIDEO_STREAMS | MEDIA_PACKAGE_V2 | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | 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 — Par le biais d'une autre ressource du même VPC, y compris une interface réseau AWS gérée ou une passerelle locale Outpost • 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 zone locale ou une zone de longueur d'onde • 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
ecs-cluster-name	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 est AWS Fargate, ce champ sera « - ». Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs : ListClusters et ecs :ListContainerInstances. Type de données Parquet : CHAÎNE	7
ecs-container-instance-id	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 est AWS Fargate, ce champ sera « - ». Pour inclure ce champ dans votre abonnement, vous devez être autorisé à appeler ecs : ListClusters et ecs :ListContainerInstances. Type de données Parquet : CHAÎNE	7
ecs-container-id	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
ecs-service-name	Nom du service ECS si le trafic provient d'une tâche ECS en cours d'exécution et que la tâche ECS est lancée par un service ECS. Si la tâche ECS n'est pas lancée 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
ecs-task-id	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

Champ	Description	Version
reject-reason	Motif du rejet du trafic. Valeurs possibles : BPA, EC. Renvoie un « - » pour toute autre motif de rejet. • BPA — Pour plus d'informations sur l'accès public par blocs VPC (BPA), consultez. Bloquer l'accès public aux sous-réseaux VPCs et aux sous-réseaux • EC — Le flux est rejeté par le point de terminaison VPC en raison de contrôles de chiffrement. Pour plus d'informations sur les contrôles de chiffrement VPC, consultez. Appliquer le chiffrement VPC en transit Type de données Parquet : CHAÎNE	8
resource-id	ID de la passerelle NAT régionale qui contient l'interface réseau pour laquelle le trafic est enregistré. Renvoie un symbole « - » pour les flux de trafic non associés à une passerelle NAT régionale. Pour plus d'informations sur les passerelles NAT régionales, consultez Passerelles NAT régionales pour une extension multi-AZ automatique. Type de données Parquet : CHAÎNE	9

Champ	Description	Version

état du chiffrement	État du chiffrement du flux. Pour plus d'informations sur les contrôles de chiffrement VPC, consultez. Appliquer le chiffrement VPC en transit Les valeurs possibles sont :
	• 0 : non chiffré.
	• 1 — crypté nitro. Il est crypté par le matériel du système Nitro.
	• 2 — crypté par application. Seuls les éléments suivants sont considérés comme chiffrés par l'application :
	  • flux sur le port TCP 443 pour le point de terminaison d'interface vers AWS le service*
	  • flux sur le port TCP 443 pour le point de terminaison de la passerelle*
	  • flux vers un cluster Redshift crypté via le point de terminaison VPC**
	• 3 — crypté par nitro et crypté par application.
	
	La valeur est « - » si les contrôles de chiffrement VPC ne sont pas activés ou s'il est FlowLog impossible d'obtenir le statut.
	
	Note
	* Pour les points de terminaison de l'interface et de la passerelle, AWS il ne prend pas en compte les données des paquets pour déterminer l'état du chiffrement, nous nous basons plutôt sur le port utilisé pour assumer l'état du chiffrement.
	** Pour les points de terminaison AWS gérés spécifiés , AWS détermine l'état du chiffrement en fonction des exigences du protocole TLS dans la configuration du service.
	
	Type de données Parquet : INT_32
		10

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) de l'adresse IP 172.31.16.139 vers l'interface réseau avec adresse IP privée est 172.31.16.21 et l'ID eni-1235b8ca123456789 du compte 123456789010 a été autorisé.

```
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
```

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
```

> **Note**
>
> Certains enregistrements de journaux de flux peuvent être ignorés pendant l'intervalle d'agrégation (consultez log-status dans Champs disponibles). Cela peut être dû à une contrainte de AWS capacité interne ou à une erreur interne. Si vous utilisez AWS Cost Explorer pour consulter les frais des journaux de flux VPC et que certains journaux de flux sont ignorés pendant l'intervalle d'agrégation des journaux de flux, le nombre de journaux de flux signalés AWS Cost Explorer sera supérieur au nombre de journaux de flux publiés par Amazon VPC.

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. À l'inverse, le réseau ACLs est apatride. Par conséquent, les réponses au trafic autorisé sont soumises aux règles ACL du 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. Comme le réseau ACLs est apatride, le ping de réponse est supprimé 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.

IPv6 trafic

Voici un exemple d'enregistrement de journal de flux par défaut. Dans l'exemple, le trafic SSH (port 22) entre l' IPv6 adresse 2001:db 8:1234:a 100:8 d6e:3477:df66:f105 et l'interface réseau eni-1235b8ca123456789 du compte 123456789010 était 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 serveur a envoyé au client un indicateur FIN (1) pour la connexion sur le port 43418. En réponse, le client a envoyé au serveur un FIN sur le port 43418.

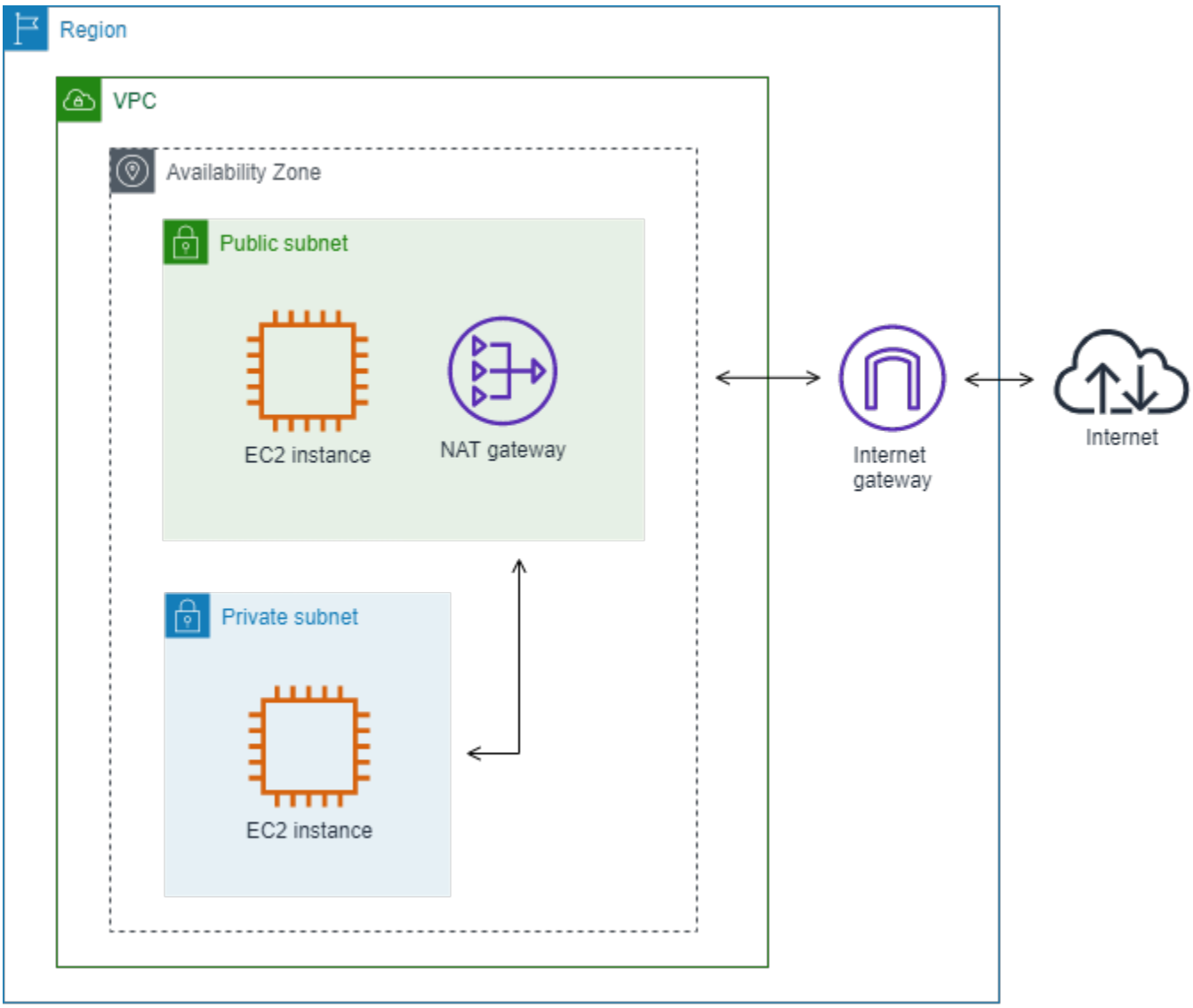
```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 63388 1219 1566848933 1566849113 ACCEPT 1 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 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 zonale

Dans cet exemple, une instance d'un sous-réseau privé accède à Internet via une passerelle NAT zonale située dans un sous-réseau public.



Le journal de flux personnalisé suivant pour l'interface réseau de passerelle NAT zonale capture les champs suivants dans l'ordre suivant.

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

Le journal de flux indique le flux de trafic entre l'adresse IP de l'instance (10.0.1.5) via l'interface réseau de la passerelle NAT zonale et un hôte sur Internet (203.0.113.5). L'interface réseau de la passerelle NAT zonale est une interface réseau gérée par le demandeur. Par conséquent, l'enregistrement du journal de flux affiche un symbole « - » pour le champ. instance-id La ligne suivante montre le trafic entre l'instance source et l'interface réseau de la passerelle NAT zonale. Les valeurs pour les champs dstaddr et pkt-dstaddr sont différentes. Le dstaddr champ affiche l'adresse

IP privée de l'interface réseau de la passerelle NAT zonale, et le pkt-dstaddr champ 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 indiquent le trafic de l'interface réseau de passerelle NAT zonale vers l'hôte cible sur Internet, et le trafic de réponse de l'hôte vers l'interface réseau de 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 de réponse entre l'interface réseau de passerelle NAT zonale et l'instance source. Les valeurs pour les champs srcaddr et pkt-srcaddr sont différentes. Le srcaddr champ affiche l'adresse IP privée de l'interface réseau de la passerelle NAT zonale, et le pkt-srcaddr champ affiche l'adresse IP de l'hôte sur Internet.

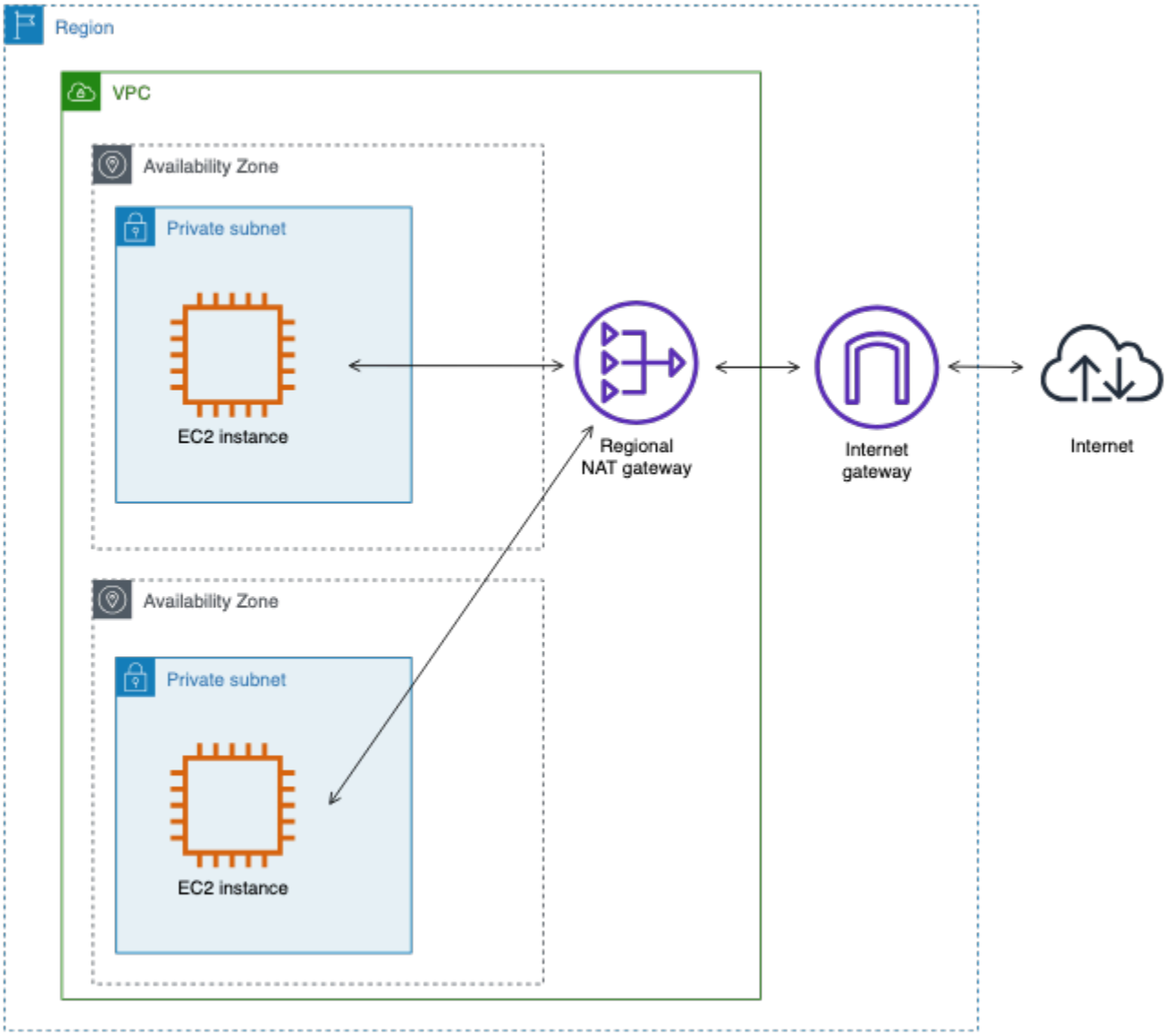
```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

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 de la passerelle NAT zonale, 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 NAT régionale

Une passerelle NAT régionale peut se connecter à plusieurs sous-réseaux dans différentes zones de disponibilité. Dans cet exemple, deux instances de sous-réseaux privés provenant de deux zones de disponibilité différentes accèdent à Internet via la même passerelle NAT régionale. Les journaux de flux suivants indiquent le trafic entre l'une des instances et Internet via la passerelle NAT régionale.



Le journal de flux personnalisé suivant pour la passerelle NAT régionale capture les champs suivants dans l'ordre suivant.

```
resource-id instance-id interface-id subnet-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

Le journal de flux indique le flux de trafic entre l'adresse IP de l'instance (10.0.1.5) via la passerelle NAT régionale et un hôte sur Internet (203.0.113.5). instance-idinterface-id, et subnet-id ne s'appliquent pas à la passerelle NAT régionale. Par conséquent, l'enregistrement du journal de flux affiche un symbole « - » pour ces champs. Le resource-id champ affiche plutôt l'ID de la passerelle NAT régionale. Les pkt-dstaddr champs dstaddr et affichent l'adresse IP de destination finale de l'hôte sur Internet.

```
nat-1234567890abcdef - - - 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
```

Les deux lignes suivantes indiquent le trafic de la passerelle NAT régionale (adresse IP publique 107.22.182.139) vers l'hôte cible sur Internet, et le trafic de réponse de l'hôte vers la passerelle NAT régionale.

```
nat-1234567890abcdef - - - 107.22.182.139 203.0.113.5 107.22.182.139 203.0.113.5
nat-1234567890abcdef - - - 203.0.113.5 107.22.182.139 203.0.113.5 107.22.182.139
```

La ligne suivante montre le trafic de réponse de la passerelle NAT régionale vers l'instance source. Les pkt-srcaddr champs srcaddr et affichent l'adresse IP de l'hôte sur Internet.

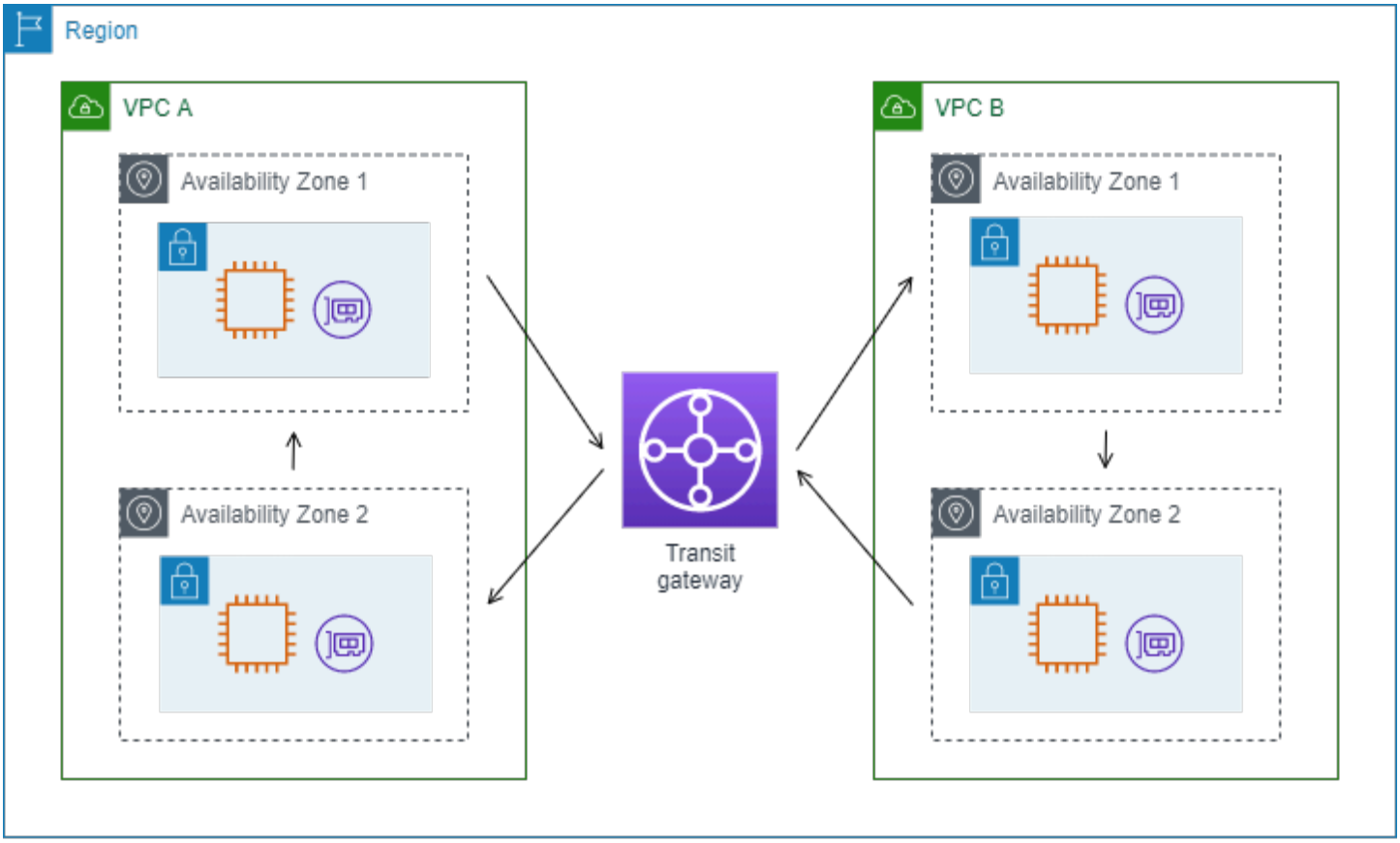
```
nat-1234567890abcdef - - - 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
```

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 instance-id champ renvoie l'ID de l'instance associée à l'interface réseau, et resource-id c'est « - ». Il n'y a aucune différence entre les pkt-dstaddr pkt-srcaddr champs dstaddr srcaddr et et.

```
- i-01234567890123456 eni-1111aaaa2222bbbb3 subnet-aaaaaaaa012345678 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 subnet-aaaaaaaa012345678 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-1111111111111111) et quitte le VPC B en utilisant un autre (par exemple eni-2222222222222222).



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-1111111111111111 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 :

- Après avoir créé un journal de flux, vous ne verrez pas les données du journal de flux tant qu'il n'y aura pas de trafic actif pour l'interface réseau, le sous-réseau ou le VPC que vous avez sélectionné.
- Vous ne pouvez pas activer les journaux de flux VPCs associés à votre VPC, sauf si le VPC homologue figure 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 possède plusieurs IPv4 adresses et que le trafic est envoyé vers une IPv4 adresse privée secondaire, le journal des flux affiche l' IPv4adresse privée principale dans le `dstaddr` champ. Pour capturer l'adresse IP de destination d'origine, créez un journal de flux avec le champ `pkt-dstaddr`.
- Si le trafic est envoyé vers une interface réseau et que la destination n'est aucune des adresses IP de l'interface réseau, le journal des flux affiche l' IPv4 adresse privée principale dans le `dstaddr` champ. 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 aucune des adresses IP de l'interface réseau, lorsque l'enregistrement du journal concerne un flux de sortie, le journal du flux affiche l' IPv4 adresse privée principale dans le `srcaddr` champ. Pour capturer l'adresse IP source d'origine, créez un journal de flux avec le champ `pkt-srcaddr`. Si l'enregistrement de journal concerne un flux entrant dans l'interface réseau, l'adresse IP privée principale de l'interface réseau ne s'affiche pas dans le champ `srcaddr`.
- 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.
- Pour les champs `pkt-srcaddr` et `pkt-dstaddr`, si la préservation des adresses IP client est activée sur la couche intermédiaire, ce champ peut afficher les adresses IP client préservées au lieu des adresses IP de la couche intermédiaire.
- La valeur du champ `traffic-path` est identique pour les flux qui passent par les ressources d'un même VPC et par une passerelle locale Outpost.

- Certains enregistrements de journaux de flux peuvent être ignorés pendant l'intervalle d'agrégation (consultez log-status dans Champs disponibles). Cela peut être dû à une contrainte de AWS capacité interne ou à une erreur interne. Si vous utilisez AWS Cost Explorer pour consulter les frais des journaux de flux VPC et que certains journaux de flux sont ignorés pendant l'intervalle d'agrégation des journaux de flux, le nombre de journaux de flux signalés AWS Cost Explorer sera supérieur au nombre de journaux de flux publiés par Amazon VPC.
- Si vous utilisez la fonctionnalité VPC Block Public Access (BPA) :
  - Les journaux de flux de la fonctionnalité VPC BPA n'incluent pas les enregistrements ignorés.
  - Les journaux de flux de la fonctionnalité VPC BPA n'inclus pas les `bytes` même si vous incluez le champ `bytes` dans votre journal de flux.

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.
- Le trafic mis en miroir du trafic source. Vous verrez uniquement le trafic mis en miroir du trafic cible.
- 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.
- Trafic ARP (Address Resolution Protocol).
- Trafic sur une passerelle NAT régionale de courte durée, qui est supprimée quelques minutes après sa création.

Limitations spécifiques aux champs ECS disponibles dans la version 7 :

- Les champs ECS ne sont pas calculés si les tâches ECS sous-jacentes ne sont pas détenues par le propriétaire de l'abonnement du journal de flux. Par exemple, si vous partagez un sous-réseau (`SubnetA`) avec un autre compte (`AccountB`), puis que vous créez un abonnement du journal de flux pour `SubnetA`, si le `AccountB` lance des tâches ECS dans le sous-réseau partagé,

votre abonnement reçoit les journaux de trafic des tâches ECS lancées par le `AccountB`, mais les champs ECS de ces journaux ne sont pas calculés pour des raisons de sécurité.

- Si vous créez des abonnements aux journaux de flux avec des champs ECS au niveau VPC/Subnet des ressources, tout trafic généré pour les interfaces réseau autres qu'ECS sera également fourni pour vos abonnements. Les valeurs des champs ECS sont « - » pour le trafic IP non ECS. Par exemple, vous avez un sous-réseau (`subnet-000000`) et vous créez un abonnement de 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` et `ECS-Task-1` génèrent du trafic IP, votre abonnement de journaux de flux `fl-00000000` fournit des journaux de trafic pour les deux entités. Toutefois, seule la tâche `ECS-Task-1` dispose des métadonnées ECS réelles pour les champs ECS que vous avez inclus dans votre LogFormat. Pour le trafic `i-0000000` associé, ces champs ont 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 au statut ARRÊTÉ 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. Une fois que vous avez arrêté 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 ayant plus d'une journée de retard et 2) lorsque nous recevons l'événement ECS qui contient les métadonnées de votre tâche ECS indiquant que la tâche n'est plus en cours d'exécution.
- Seules les tâches ECS lancées en mode réseau `awsvpc` sont prises en charge.

Limitations spécifiques au `encryption-status` champ :

- L'état de chiffrement peut être « - » (non disponible) dans certains flux, en raison de la limitation de certains appareils réseau à signaler l'état du chiffrement. Les utilisateurs peuvent ignorer ces flux dans l'analyse.

- L'affichage comme chiffré en mode moniteur ne signifie pas que le flux sera autorisé en mode d'application. Et vice versa.
  - Si un flux est chiffré en mode surveillance, il est possible qu'il ne soit pas conforme en mode application :
    - Si le flux implique une ENI créée par un AWS service, le service doit prendre en charge les contrôles de chiffrement.
    - Si le flux passe par l'appairage VPC, le VPC apparenté peut ne pas forcer les contrôles de chiffrement.
  - Si un flux n'est pas chiffré en mode surveillance, il est possible qu'il soit toujours conforme en mode d'application, étant donné que le service associé au flux est ajouté en tant qu'exclusion.

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
- Marquage de 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

1. Contrôler l'utilisation des journaux de flux avec IAM

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.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

Pour de plus amples informations, veuillez consulter the section called "Fonctionnement d'Amazon VPC avec IAM".

2. Créer un journal de flux

Vous pouvez créer des journaux de flux pour votre VPCs, vos sous-réseaux ou vos 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 "Créer un journal de flux publié dans Amazon Data Firehose"

3. 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 Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Dans le volet de navigation, sélectionnez Votre VPCs. 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).

4. 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 Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Dans le volet de navigation, sélectionnez Votre VPCs. 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 de la ligne de commande

Vous pouvez exécuter les tâches décrites sur cette page à l'aide de la ligne de commande.

Créer un journal de flux

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

Décrire un journal de flux

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

Baliser un journal de flux

- create-tags et delete-tags (AWS CLI)
- New-EC2Tag et Remove-EC2Tag (AWS Tools for Windows PowerShell)

Supprimer un journal de flux

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)

Publier les journaux de flux dans CloudWatch Logs

Les journaux de flux peuvent publier les données des journaux de flux directement sur Amazon CloudWatch. Amazon CloudWatch est un service complet de surveillance et d'observabilité. Il collecte et suit les métriques, les journaux et les données d'événements provenant de diverses AWS ressources, ainsi que de vos propres applications et services. CloudWatch fournit une visibilité sur l'utilisation des ressources, les performances des applications et la santé opérationnelle, ce qui vous permet de détecter les changements de performances et les problèmes potentiels à l'échelle du système et d'y répondre. Vous pouvez ainsi définir des alarmes, visualiser les journaux et les métriques, et réagir automatiquement pour collecter et optimiser vos ressources cloud. CloudWatch Il s'agit d'un outil essentiel pour garantir la fiabilité, la disponibilité et les performances de votre infrastructure et de vos applications basées sur le cloud.

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

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 :

JSON

```
{
  "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.

JSON

```
{
  "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 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. Saisissez un nom pour votre politique ainsi qu'éventuellement une description et des balises, puis choisissez Créer une politique.
5. Dans le panneau de navigation, choisissez 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. Choisissez Créer un rôle.

Créez un journal de flux qui publie dans CloudWatch Logs

Vous pouvez créer des journaux de flux pour votre VPCs, vos sous-réseaux ou vos 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`.

Prérequis

Vérifiez que le principal IAM que vous utilisez pour effectuer la demande disposent des autorisations pour appeler l'action `iam:PassRole`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/flow-log-role-name"
        }
    ]
}
```

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 Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Dans le volet de navigation, sélectionnez Votre VPCs. 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. Si vous saisissez un nom, nous créons le groupe de journaux lorsqu'il y a du trafic à journaliser.
7. Pour l'accès au service, choisissez un rôle de service IAM existant autorisé à publier des journaux dans CloudWatch Logs ou créez un nouveau rôle de service.
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-EC2FlowLog (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 du journal de flux avec CloudWatch Logs

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 de plus amples informations, veuillez consulter 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)
- CWLLogÉvénement Get (AWS 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, saisissez 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 traiter les enregistrements du journal de flux comme vous le feriez pour tout autre événement de journal collecté par CloudWatch Logs. Pour plus d'informations sur la surveillance des données des journaux et des filtres de mesures, consultez la section Création de métriques à partir d'événements de journal à l'aide d'un filtre dans le guide de l'utilisateur Amazon CloudWatch Logs.

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 choisissez 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 terminé 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. Amazon S3 (Simple Storage Service) est un service de stockage d'objets extrêmement évolutif et durable. Il est conçu pour stocker et récupérer n'importe quel volume de données, depuis n'importe où sur le web. S3 offre une durabilité et une disponibilité de pointe, avec des fonctionnalités intégrées de gestion des versions des données, de chiffrement et de contrôle d'accès.

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, consultez Create a bucket dans le Guide d'utilisation d'Amazon S3.

Pour plus d'informations sur la manière de rationaliser l'ingestion des journaux de flux VPC, le traitement des journaux de flux et la visualisation des journaux de flux, consultez la section Journalisation centralisée OpenSearch dans la bibliothèque de AWS solutions.

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

Les journaux de flux VPC collectent les données relatives au trafic IP entrant et sortant de votre VPC dans des enregistrements de journaux, agrègent ces enregistrements dans des fichiers journaux, puis publient les fichiers journaux dans le compartiment Amazon S3 toutes les 5 minutes. Plusieurs fichiers peuvent être publiés et chaque fichier journal peut contenir une partie ou la totalité des enregistrements de journaux de flux pour le trafic IP enregistré au cours des 5 dernières minutes.

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 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.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        }
    ]
}
```

L'ARN que vous spécifiez *my-s3-arn* dépend de l'utilisation de préfixes S3 compatibles avec Hive ou non.

- 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 un individu Compte AWS ARNs. 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.

Notez que le service de livraison de journaux appelle l'action d'API Amazon S3 `HeadBucket` pour vérifier l'existence et l'emplacement du compartiment S3. Il n'est pas nécessaire d'accorder au service de livraison de journaux l'autorisation d'appeler cette action. Il transmettra les journaux de flux VPC même s'il ne peut pas confirmer l'existence et l'emplacement du compartiment S3. Cependant, il y aura une `AccessDenied` erreur liée à l'appel `HeadBucket` dans vos CloudTrail 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 la section 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 politiques de compartiment requises, Amazon S3 utilise des listes de contrôle d'accès (ACLs) pour 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 plus d'informations, consultez Access control list (ACL) overview dans le Guide d'utilisation d'Amazon S3.

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 réseau, vos sous-réseaux et VPCs.

Prérequis

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.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource": "*"
    }
  ]
}
```

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 Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Dans le volet de navigation, sélectionnez Votre VPCs. 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 : journalise uniquement le trafic accepté.
   - 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 (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 dans Amazon S3 à l'aide de la ligne de commande

Utilisez l'une des commandes suivantes :

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (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 avec Amazon S3

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.

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.

Pour afficher des enregistrements de journal de flux publiés dans Amazon S3

1. Ouvrez la console Amazon S3 à l'adresse 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,*prefix*/AWSLogs/*account_idregion*/vpcflowlogs/////. *year month day*
4. Cochez la case à côté du nom de fichier, puis choisissez Download (Télécharger).

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 vers Amazon Data Firehose

Les journaux de flux peuvent publier leurs données directement dans Amazon Data Firehose. Amazon Data Firehose est un service entièrement géré qui collecte, transforme et diffuse des flux de données en temps réel vers divers magasins de AWS données et services d'analyse. Il gère l'ingestion de données en votre nom.

En ce qui concerne les journaux de flux VPC, Firehose peut être utile. Les journaux de flux VPC capture des informations sur le trafic IP circulant vers et depuis les interfaces réseau dans votre VPC.

Ces données peuvent être cruciales pour la surveillance de la sécurité, l'analyse des performances et la conformité réglementaire. Cependant, la gestion du stockage et du traitement de ce flux ininterrompu de données de journal peut s'avérer une tâche complexe et gourmande en ressources.

L'intégration de Firehose à vos journaux de flux VPC vous permet d'envoyer ces données vers votre destination préférée (Amazon S3 ou Amazon Redshift, par exemple). Firehose se mettra à l'échelle pour gérer l'ingestion, la transformation et la diffusion de vos journaux de flux VPC, vous évitant ainsi la charge opérationnelle. Cela vous permet de vous concentrer sur l'analyse des journaux et sur l'obtention d'informations, plutôt que de vous soucier de l'infrastructure sous-jacente.

En outre, Firehose propose des fonctionnalités telles que la transformation, la compression et le chiffrement des données, qui peuvent améliorer l'efficacité et la sécurité de votre pipeline de traitement des journaux de flux VPC. L'utilisation de Firehose pour les journaux de flux VPC peut simplifier la gestion de vos données et vous permettre d'obtenir des informations à partir des données de trafic réseau.

Lors de la publication vers Amazon Data Firehose, les données du journal de flux sont publiées au format texte brut dans un flux de diffusion Amazon Data Firehose.

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 qui se trouve dans le même compte que la ressource à surveiller (le compte source) ou dans un compte différent (le compte de destination). Pour permettre la diffusion des 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.

Roles

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 VPCs interfaces réseau ou les sous-réseaux que vous surveillez à l'aide de la clé `iam:AssociatedResourceARN` de condition.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::123456789012:role/mySourceRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "delivery.logs.amazonaws.com"
                },
                "StringLike": {
                    "iam:AssociatedResourceARN": [
                        "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-00112233344556677"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "logs:GetLogDelivery"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::111122223333: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.

JSON

```
{
  "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 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. Saisissez un nom pour votre politique ainsi qu'éventuellement une description et des balises, puis choisissez Créer une politique.

5. Dans le panneau de navigation, choisissez 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. Choisissez 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.

JSON

```
{
  "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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333: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 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 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. Choisissez Créer un rôle.

Créer un journal de flux publié dans Amazon Data Firehose

Vous pouvez créer des journaux de flux pour votre VPCs, vos sous-réseaux ou vos interfaces réseau.

Conditions préalables

- Créez le flux de diffusion 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.
- Le compte qui crée le journal de flux doit utiliser un rôle IAM qui accorde les autorisations suivantes pour publier les journaux de flux sur Amazon Data Firehose.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "iam:CreateServiceLinkedRole",
                "firehose:TagDeliveryStream"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

- 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 dans 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 Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. Dans le volet de navigation, sélectionnez Votre VPCs. 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 vers Amazon Data Firehose depuis le même compte : le flux de diffusion et la ressource à surveiller se trouvent dans le même compte.
   - Envoyer vers Amazon Data Firehose depuis un compte différent : le flux de diffusion et la ressource à surveiller se trouvent dans des comptes différents.
6. Pour le nom du flux de diffusion Amazon Data Firehose, choisissez le flux de diffusion que vous avez créé.

7. [Diffusion entre comptes uniquement] Dans Accès au service, choisissez un rôle de service IAM existant pour la diffusion entre comptes autorisé à publier des journaux ou sélectionnez Configurer les autorisations pour ouvrir la console IAM et créer un rôle de service.
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 qui publie dans Amazon Data Firehose à l'aide de la ligne de commande

Utilisez l'une des commandes suivantes :

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (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
```

Suite à la création du journal de flux, 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 clouds privés virtuels (VPCs) qui parlent le plus ou les adresses IP dont les connexions TCP sont le 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

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.

Exigences

- 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 volet de navigation, choisissez Votre, VPCs puis sélectionnez votre VPC.
   - Ouvrez la console VPC Amazon. 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 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 flow-logs-subscription-idvpcflowlogsathenadatabase< >.
- Un groupe de travail Athéna. Le nom du groupe de travail est < flow-log-subscription-id>< >< date de début >< date de partition-load-frequencyfin >groupe de travail
- Un tableau Athena partitionné qui correspond à vos enregistrements de journaux de flux. Le nom de la table est < flow-log-subscription-id>< >< date de début partition-load-frequency>< date de fin >.
- 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 CloudFormation modèle.

```
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.

- VpcFlowLogsAcceptedTraffic— Les connexions TCP autorisées en fonction de vos groupes de sécurité et de votre réseau ACLs.
- VpcFlowLogsAdminPortTraffic— Les 10 adresses IP les plus fréquentées, telles qu'elles sont enregistrées par les applications qui répondent aux demandes sur les ports administratifs.
- VpcFlowLogsIPv4Trafic : nombre total d'octets de IPv4 trafic enregistrés.
- VpcFlowLogsIPv6Trafic : nombre total d'octets de IPv6 trafic enregistrés.
- VpcFlowLogsRejectedTCPTraffic— Les connexions TCP rejetées en fonction de vos groupes de sécurité ou de votre réseau ACLs.
- VpcFlowLogsRejectedTraffic— Le trafic rejeté en fonction de vos groupes de sécurité ou de votre réseau ACLs.
- VpcFlowLogsSshRdpTraffic— Le trafic SSH et RDP.
- VpcFlowLogsTopTalkers— Les 50 adresses IP ayant enregistré le plus de trafic.
- VpcFlowLogsTopTalkersPacketLevel— Les 50 adresses IP au niveau des paquets ayant enregistré le plus de trafic.
- VpcFlowLogsTopTalkingInstances— IDs Parmi les 50 instances ayant enregistré le plus de trafic.
- VpcFlowLogsTopTalkingSubnets— Les IDs 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 LogDestinationNotFoundException « » ou « Accès refusé pour LogDestination »
- Dépassement de la limite de politique de compartiment Amazon S3
- LogDestination non livrable
- La taille des données des journaux de flux ne correspond pas aux données de facturation

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 soit survenu lors de la transmission des journaux de flux au groupe de CloudWatch journaux des journaux ou que des SkipData entrées soient présentes.

Solution

Consultez l'onglet Journaux de flux du VPC, du sous-réseau ou de l'interface réseau. Notez que vous ne pouvez pas décrire les journaux de flux pour un VPC ou un sous-réseau partagé avec vous. En revanche, vous pouvez décrire les journaux de flux pour une interface réseau que vous créez dans un VPC ou un sous-réseau partagé avec vous. S'il existe des erreurs, elles apparaissent dans la colonne Statut. Vous pouvez également utiliser la describe-flow-logscommande et vérifier la valeur renvoyée dans le `DeliverLogsErrorMessage` champ.

Valeurs d'erreur possibles pour le statut :

- `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 les quotas CloudWatch de service 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 de plus amples informations, veuillez consulter 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 LogDestinationNotFoundException « » 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.

La taille des données des journaux de flux ne correspond pas aux données de facturation

Problème

La taille totale des données de vos journaux de flux ne correspond pas à la taille indiquée dans les données de facturation.

Causes possibles :

Vos journaux de flux contiennent peut-être des entrées SKIPDATA. Consultez Aucune donnée et enregistrements ignorés pour en savoir plus sur les entrées SKIPDATA.

Solution

Vérifiez que vos entrées de journal contiennent des entrées SKIPDATA en exécutant différentes requêtes dans le champ log-status.

Exemples de requêtes pour la recherche d'entrées SKIPDATA :

CW Insights :

```
fields @timestamp, @message, @logStream, @log
| filter interfaceId = 'eni-123'
| stats count(*) by interfaceId, logStatus
| sort by interfaceId, logStatus
```

Athena :

```
SELECT log_status, interface_id, count(1)
FROM vpc_flow_logs
WHERE interface_id IN ('eni-1', 'eni-2', 'eni-3')
GROUP BY log_status, interface_id
```

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. 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 • 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.

Métrique	Description
	Dimensions • Nom : `Service`, valeur : `EC2` • Nom : `Type`, valeur : `Resource` • Nom : `Resource`, valeur : `VPC` • Nom : `Class`, valeur : `NetworkAddressUsage`
`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 VPC d'Amazon 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"
}
```

Présentation des codes Amazon VPC dans les rapports de facturation et d'utilisation

Lorsque vous utilisez Amazon VPC, nous incluons les codes associés dans vos rapports de facturation et d'utilisation AWS. L'examen de ces codes vous aide à comprendre vos coûts et vos habitudes d'utilisation d'Amazon VPC. Le suivi et la gestion de vos dépenses sont essentiels pour optimiser vos coûts.

Les tableaux suivants décrivent les codes Amazon VPC qui apparaissent dans les rapports de facturation et d'utilisation. Pour obtenir la liste des codes de région utilisés dans les rapports de facturation et d'utilisation, consultez la section AWS Region billing codes.

Codes de facturation pour :

- Gestion des adresses IP
- Points de terminaison d'un VPC
- Passerelles de transit
- Analyse du réseau
- Mise en miroir du trafic
- VPC Lattice
- Ressources entre comptes/régions

Ressources connexes

- Tarification Amazon VPC
- AWS PrivateLink Tarification d
- AWS Transit Gateway Tarification d
- Tarification d'Amazon VPC Lattice

Gestion des adresses IP

Code	Description	Unités	Granularité
region-PublicIPv4:InUseAddress	Durée pendant laquelle les adresses IPv4 publiques sont utilisées par une ressource.	Heures	Par seconde
region-PublicIPv4:IdleAddress	Durée pendant laquelle les adresses IPv4 publiques ne sont pas utilisées par une ressource.	Heures	Par seconde
region-PublicIPv4:ContiguousBlock	Utilisation d'adresses IPv4 publiques dans un bloc IPv4 contigu fourni par Amazon.	Heures	Par heure
region-IPAddressManager-IP-Hours	Durée pendant laquelle les adresses IP sont gérées par l'IPAM (niveau avancé).	Heures	Par heure

Points de terminaison d'un VPC

Code	Description	Unités	Granularité
region-VpcEndpoint-Hours	Durée pendant laquelle les points de terminaison d'un VPC d'interface sont provisionnés.	Heures	Par heure
region-VpcEndpoint-Bytes	Données traitées par les points de terminaison d'un VPC d'interface.	Go	Par heure

Code	Description	Unités	Granularité
region-VpcEndpoint-GWLBE-Hours	Durée pendant laquelle les points de terminaison de l'équilibreur de charge Gateway Load Balancer sont provisionnés.	Heures	Par heure
region-VpcEndpoint-GWLBE-Bytes	Données traitées par les points de terminaison de l'équilibreur de charge Gateway Load Balancer.	Go	Par heure

Passerelles de transit

Code	Description	Unités	Granularité
region-TransitGateway-Hours	Utilisation des attachements de la passerelle de transit.	Heures	Par heure
region-TransitGateway-Bytes	Données traitées par les passerelles de transit.	Go	Par heure
region-TGW-Multicast-Consumer-Bytes	Données traitées par les instances de récepteur multicast.	Go	Par heure

Analyse du réseau

Code	Description	Unités	Granularité
region-Analysis-Runs	Nombre de chemins réseau analysés par l'analyseur d'accessibilité.	Nombre	Par analyse
region-NetworkInterface-Assessment	Nombre d'interfaces réseau analysées par l'analyseur d'accès réseau.	Nombre	Par évaluation

Mise en miroir du trafic

Code	Description	Unités	Granularité
region-ENI-Mirror	Durée pendant laquelle une interface réseau est configurée pour la mise en miroir du trafic.	Heures	Par heure

VPC Lattice

Code	Description	Unités	Granularité
region-VPCLattice-Service-Hourly	Durée d'exécution des services VPC Lattice.	Heures	Par heure
region-VPCLattice-DataPr	Données traitées par les services VPC Lattice.	Go	Par heure

Code	Description	Unités	Granularité
ocessing-Bytes			
region-VPCLattice-RequestCount-Free	Requêtes HTTP et connexions TCP gratuites.	Nombre	Par heure
region-VpcLattice-Service-Network-Resource-Hours	Durée d'exécution des réseaux de services VPC Lattice.	Heures	Par heure

Ressources entre comptes/régions

Code	Description	Unités	Granularité
region-VpcResource-Provider-Bytes	Données transférées depuis les ressources du fournisseur entre comptes ou entre régions.	Go	Par heure
region-VpcResource-Consumer-Bytes	Données transférées par les ressources destinées aux consommateurs entre comptes ou entre régions.	Go	Par heure

Description de l'architecture de votre réseau VPC

Amazon VPC vous permet de définir un réseau virtuel logiquement isolé dans le AWS cloud, connu sous le nom de cloud privé virtuel (VPC). Créez une infrastructure séparée VPCs pour isoler l'infrastructure par charge de travail ou entité organisationnelle. Vous pouvez configurer le vôtre en VPCs sélectionnant des plages d'adresses IP, en configurant le routage et en ajoutant des passerelles réseau VPCs pour vous connecter les uns aux autres, à Internet ou à votre propre réseau d'entreprise. Vous lancez AWS des ressources, telles que EC2 des instances ou des instances RDS, dans votre VPCs.

Le tableau suivant décrit les principales caractéristiques d'un réseau VPC. Il contient des indications qui pourront aider un administrateur réseau à décrire l'architecture et la configuration de votre réseau VPC. Ces informations lui permettront de configurer un réseau fonctionnellement équivalent sur site ou en faisant appel à un autre fournisseur de cloud.

Caractéristiques	Description
Emplacement géographique	Amazon VPC est hébergé dans toutes les AWS régions du monde. Vous pouvez sélectionner les régions de votre réseau VPC qui placent vos AWS ressources au plus près de vos clients.
Sous-réseaux	Les sous-réseaux que vous définissez pour vous VPCs définissent les limites du réseau et déterminent les adresses IP de vos AWS ressources. Vous pouvez ajouter des sous-réseaux dans plusieurs zones de disponibilité pour augmenter la disponibilité de vos ressources.
Connectivité réseau	Les passerelles que vous attachez à votre réseau VPCs ou à vos sous-réseaux pour fournir une connectivité entre votre réseau VPC et d'autres réseaux, tels que d'autres réseaux VPCs ou sous-réseaux, Internet ou vos réseaux sur site.

Caractéristiques	Description
Contrôles de sécurité	Les groupes de sécurité que vous créez pour VPCs contrôler le trafic à destination et en provenance des ressources associées, telles que les ressources de calcul, les ressource s de base de données et les équilibreurs de charge. Chaque sous-réseau possède une ACL réseau qui contrôle le trafic en provenance et à destination du sous-réseau.
Gestion du trafic	Les règles de routage contrôlent le flux de trafic entre les sous-réseaux et VPCs les emplaceme nts externes. Les équilibreurs de charge fournis par Elastic Load Balancing répartissent le trafic entrant sur plusieurs cibles, telles que les EC2 instances, les conteneurs et les fonctions Lambda.

Situation géographique

Amazon VPC est disponible dans toutes les AWS régions du monde. Chaque région constitue une zone géographique séparée. Vous pouvez réduire la latence du réseau lorsque vous créez des ressources VPCs pour vos régions proches de la majorité de vos utilisateurs.

Vous pouvez utiliser Amazon EC2 Global View pour répertorier vos produits VPCs dans toutes les régions à l'aide d'une interface utilisateur graphique (il n'existe pas d'interface de programmation équivalente). Avec la console Amazon VPC, l' AWS API et les interfaces de ligne de AWS commande, vous devez répertorier les ressources et VPCs VPC pour chaque région individuellement.

Pourquoi est-ce important

Après avoir déterminé où vous vous VPCs trouvez, vous pouvez décider de configurer un réseau fonctionnellement équivalent aux mêmes emplacements ou à des emplacements différents, en fonction de vos besoins.

Pour obtenir un résumé de votre situation VPCs dans toutes les régions

1. Ouvrez la console Amazon EC2 Global View à la https://console.aws.amazon.com/ec2globalview/maison.
2. Dans l'onglet Explorateur de régions, sous Résumé, vérifiez le nombre de ressources pour VPCs, qui inclut le nombre VPCs et le nombre de régions. Cela inclut à la fois la valeur par défaut VPCs AWS créée en votre nom et la valeur non par défaut VPCs que vous créez. Cliquez sur le texte souligné pour visualiser la répartition du nombre de VPC entre les régions. Si une région ne possède qu'un VPC, il s'agit probablement de son VPC par défaut.
3. Dans l'onglet Recherche globale, sélectionnez le filtre client Type de ressource = Vpc. Vous pouvez filtrer davantage les résultats en spécifiant une région ou une balise.

Pour obtenir le VPCs dans une région à l'aide du AWS CLI

Utilisez la commande describe-vpcs ci-dessous. Vous devez exécuter cette commande dans chaque région où vous en avez VPCs. Le `--query` paramètre inclut uniquement le VPC IDs dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws ec2 describe-vpcs \
    --region us-east-2 \
    --query "Vpcs[*].VpcId"
```

Chaque région est associée à un VPC par défaut. Si vous n'utilisez pas le filtre par défaut VPCs, vous pouvez les exclure des résultats en ajoutant le filtre suivant.

```
--filters Name=is-default,Values=false
```

Subnets

Un sous-réseau est une limite de réseau logique dans un VPC. Lorsque vous créez un sous-réseau, vous attribuez un bloc d'adresses IP. Les ressources que vous lancez dans un sous-réseau reçoivent des adresses IP issues du bloc d'adresses IP du sous-réseau. Les adresses IP permettent aux ressources de communiquer entre elles via un réseau local ou Internet.

Le mappage des ressources de la console Amazon VPC offre une représentation visuelle des sous-réseaux de votre VPC.

Pourquoi est-ce important ?

Les sous-réseaux permettent aux administrateurs réseau de mettre en place des limites de sécurité et de contrôler le trafic entre les différents niveaux d'application. En notant les adresses IP de vos sous-réseaux, vous pouvez garantir que les ressources d'un réseau fonctionnellement équivalent peuvent communiquer avec les mêmes clients ou applications qu'au sein de votre réseau VPC.

Pour afficher les sous-réseaux d'un VPC à l'aide du mappage des ressources

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez VPCs.
3. Cochez la case correspondant au VPC.
4. Sélectionnez l'onglet Mappage des ressources.
5. Dans le volet VPC, sélectionnez Afficher les détails. Le volet Sous-réseaux répertorie tous les sous-réseaux du VPC et leurs plages d'adresses IP. Survolez un sous-réseau avec la souris pour mettre en évidence la table de routage et les connexions réseau associées. Pour plus d'informations, cliquez sur le lien vers la page de détails du sous-réseau.

Pour décrire les sous-réseaux d'un VPC à l'aide du AWS CLI

Utilisez la commande describe-subnets ci-dessous. Le paramètre `--filters` définit le périmètre de la recherche pour décrire les sous-réseaux du VPC spécifié. Le paramètre `--query` inclut uniquement les champs spécifiés dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws ec2 describe-subnets \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query Subnets[*].
[SubnetId,AvailabilityZoneId,CidrBlock,Ipv6CidrBlockAssociationSet[0].Ipv6CidrBlock] \
    --output table
```

Voici un exemple de sortie. Les colonnes sont l'ID de sous-réseau, l'ID AZ, la plage d' IPv4 adresses et la première plage d' IPv6 adresses (le cas échéant).

```
-------------------------------------------------------------------------------------
|                                  DescribeSubnets                                  |
+---------------------------+-----------+----------------+---------------------------+
|  subnet-0d2d1b81e0bc9c6d4 |  usw2-az1 |  10.0.144.0/20 |  2600:1f14:1e6e:a003::/64  |
|  subnet-0e01d500780bb7468 |  usw2-az1 |  10.0.16.0/20  |  2600:1f14:1e6e:a001::/64  |
|  subnet-0eb17d85f5dfd33b1 |  usw2-az2 |  10.0.128.0/20 |  2600:1f14:1e6e:a002::/64  |
```

```
|  subnet-0e990c67809773b19 |  usw2-az2 |  10.0.0.0/20   |  2600:1f14:1e6e:a000::/64  |
+---------------------------+-----------+----------------+----------------------------+
```

La connectivité réseau

Les options de connectivité proposées par Amazon VPC vous permettent de créer un réseau qui couvre VPCs plusieurs comptes, régions et réseaux distants.

Vous pouvez utiliser la carte des ressources de la console Amazon VPC pour savoir si vous VPCs utilisez des passerelles Internet, des passerelles Internet de sortie uniquement, des passerelles NAT ou des points de terminaison VPC de passerelle. Le mappage des ressources n'affiche pas les passerelles de transit, les connexions d'appairage, les passerelles privées virtuelles et les autres types de point de terminaison de VPC utilisés. Vous pouvez obtenir la liste complète des passerelles et des connexions d'appairage d'un VPC en les décrivant une par une à l'aide de la console, de l'API ou d'une interface de ligne de commande.

Pourquoi est-ce important ?

Lorsque vous comprenez la connectivité fournie par votre réseau VPC, vous pouvez vous assurer que les ressources d'un réseau fonctionnellement équivalent peuvent communiquer avec les mêmes ressources locales et distantes.

Pour afficher les connexions réseau d'un VPC à l'aide du mappage des ressources

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez VPCs.
3. Cochez la case correspondant au VPC.
4. Sélectionnez l'onglet Mappage des ressources.
5. Dans le volet VPC, sélectionnez Afficher les détails. Le volet Connexions réseau répertorie les passerelles Internet, les passerelles Internet de sortie uniquement, les passerelles NAT et les points de terminaison de VPC de passerelle. En cas de doute concernant le type de ressource, survolez l'icône de lien correspondant à la connexion réseau avec la souris et examinez l'URL indiquée. Cette URL est un lien vers la ressource dans la console qui indique le type et l'ID de la ressource (par exemple, internetGatewayId=igw-0123456780abcdef).

Pour obtenir les connexions réseau nécessaires à votre VPCs utilisation du AWS CLI

1. Utilisez la describe-internet-gatewayscommande suivante pour obtenir les passerelles Internet pour la région spécifiée. Le paramètre `--query` inclut uniquement les champs spécifiés dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws ec2 describe-internet-gateways \
    --region us-east-2 \
    --query InternetGateways[*].[Attachments[0].VpcId,InternetGatewayId] \
    --output table
```

   Voici un exemple de sortie. Les colonnes indiquent le VPC IDs et la passerelle Internet. IDs

```
-----------------------------------------------------
|             DescribeInternetGateways              |
+------------------------+--------------------------+
|  None                  |  igw-04c61dba10EXAMPLE   |
|  vpc-0bf4c2739bEXAMPLE |  igw-09737a4029EXAMPLE   |
|  vpc-060415a18fEXAMPLE |  igw-0c562bd22aEXAMPLE   |
|  vpc-0ea9d41094EXAMPLE |  igw-0e06f7033dEXAMPLE   |
|  vpc-03b86de356EXAMPLE |  igw-0a9ff72d05EXAMPLE   |
+------------------------+--------------------------+
```

2. Utilisez la commande describe-egress-only-internet-gateways suivante pour obtenir les passerelles Internet de sortie uniquement pour la région spécifiée. Le paramètre `--query` inclut uniquement les champs spécifiés dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws ec2 describe-egress-only-internet-gateways \
    --region us-east-2 \
    --query EgressOnlyInternetGateways[*].
[Attachments[0].VpcId,EgressOnlyInternetGatewayId] \
    --output table
```

   Voici un exemple de sortie. Les colonnes indiquent le VPC IDs et la passerelle Internet de sortie uniquement. IDs

```
-----------------------------------------------------
|        DescribeEgressOnlyInternetGateways         |
+------------------------+--------------------------+
```

```
|  vpc-060415a18fEXAMPLE |  eigw-0b8ca558acEXAMPLE  |
+------------------------+--------------------------+
```

3. Utilisez la describe-nat-gatewayscommande suivante pour obtenir les passerelles NAT pour la région spécifiée. Le paramètre `--query` inclut uniquement les champs spécifiés dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws ec2 describe-nat-gateways \
    --region us-east-2 \
    --query NatGateways[*].[VpcId,NatGatewayId,SubnetId] \
    --output table
```

Voici un exemple de sortie. Les colonnes indiquent le VPC IDs, la passerelle NAT et le IDs sous-réseau. IDs

```
-------------------------------------------------------------------------------
|                            DescribeNatGateways                              |
+------------------------+-------------------------+---------------------------+
|  vpc-060415a18fEXAMPLE |  nat-026316334aEXAMPLE  |  subnet-0eb17d85f5EXAMPLE  |
|  vpc-060415a18fEXAMPLE |  nat-0f08bc5f52EXAMPLE  |  subnet-0d2d1b81e0EXAMPLE  |
+------------------------+-------------------------+---------------------------+
```

4. Utilisez la commande describe-transit-gateway-vpc-attachments suivante pour obtenir les pièces jointes VPC de la passerelle de transit pour la région spécifiée. Le paramètre `--query` inclut uniquement les champs spécifiés dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws ec2 describe-transit-gateway-vpc-attachments \
    --region us-east-2 \
    --query TransitGatewayVpcAttachments[*].
[VpcId,TransitGatewayId,length(SubnetIds[])] \
    --output table
```

Voici un exemple de sortie. Les colonnes indiquent le VPC IDs, la passerelle de transit et IDs le nombre de sous-réseaux.

```
-----------------------------------------------------------
|         DescribeTransitGatewayVpcAttachments          |
+------------------------+-------------------------+----+
|  vpc-0bf4c2739bEXAMPLE |  tgw-055dc4e47bEXAMPLE  |  4 |
```

```
|  vpc-0ea9d41094EXAMPLE |  tgw-055dc4e47bEXAMPLE  |  2 |
+------------------------+-------------------------+----+
```

5. Utilisez la describe-vpc-peering-connectionscommande suivante pour obtenir les connexions d'appairage pour VPCs la région spécifiée. Le paramètre `--query` inclut uniquement les champs spécifiés dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws ec2 describe-vpc-peering-connections \
    --region us-east-2 \
    --query VpcPeeringConnections[*].[AccepterVpcInfo.VpcId,RequesterVpcInfo.VpcId]
 \
    --output table
```

Voici un exemple de sortie. Les colonnes indiquent le VPC accepteur, les propriétaires du VPC accepteur IDs, le VPC demandeur et les propriétaires du VPC demandeur. IDs

```
-------------------------------------------------------------------------------
|                          DescribeVpcPeeringConnections
 |
+------------------------+--------------+------------------------+---------------
+
|  vpc-0ea9d41094EXAMPLE |  123456789012 |  vpc-03b86de356EXAMPLE |  123456789012
 |
+------------------------+--------------+------------------------+---------------
+
```

6. Utilisez la describe-vpn-gatewayscommande suivante pour obtenir les passerelles privées virtuelles pour la région spécifiée. Le paramètre `--query` inclut uniquement les champs spécifiés dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws ec2 describe-vpn-gateways \
    --region us-east-2 \
    --query VpnGateways[*].[VpcAttachments[0].VpcId,VpnGatewayId] \
    --output table
```

Voici un exemple de sortie. Les colonnes indiquent le VPC IDs et la passerelle privée virtuelle. IDs

```
-------------------------------------------------
```

```
|               DescribeVpnGateways               |
+-------------------------+-------------------------+
|  vpc-0bf4c2739bEXAMPLE |  vgw-0cb3226c4aEXAMPLE  |
+-------------------------+-------------------------+
```

7. Utilisez la describe-vpc-endpointscommande suivante pour obtenir les points de terminaison VPC pour la région spécifiée. Le paramètre `--query` inclut uniquement les champs spécifiés dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws ec2 describe-vpc-endpoints \
    --region us-east-2 \
    --query 'VpcEndpoints[*].[VpcId,VpcEndpointType,ServiceName||
ServiceNetworkArn||ResourceConfigurationArn]' \
    --output table
```

Voici un exemple de sortie. La première colonne indique l'ID des VPC et la deuxième le type de point de terminaison des VPC. La troisième colonne dépend du type de point de terminaison. Elle indique le nom du service, l'ARN de configuration des ressources ou l'ARN du réseau de services.

```
-------------------------------------------------------------------------------------------
|                                                    DescribeVpcEndpoints
                                                 |
+-------------------------+-----------------
+-------------------------------------------------------------------------------------------
+
|  vpc-060415a18fcc9afde |  Interface      |  com.amazonaws.vpce.us-west-2.vpce-
svc-007832a03d60fc387                              |
|  vpc-060415a18fcc9afde |  Interface      |  com.amazonaws.vpce.us-west-2.vpce-
svc-007832a03d60fc387                              |
|  vpc-0bf4c2739bc05a694 |  Gateway        |  com.amazonaws.us-west-2.s3
                                                   |
|  vpc-0ea9d410947d27b7d |  Interface      |  com.amazonaws.us-west-2.logs
                                                   |
|  vpc-0bf4c2739bc05a694 |  Resource       |  arn:aws:vpc-lattice:us-
east-2:123456789012:resourceconfiguration/rcfg-07129f3acded87625  |
|  vpc-0bf4c2739bc05a694 |  ServiceNetwork |  arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetwork/sn-0808d1748faee0c1e           |
|  vpc-0bf4c2739bc05a694 |  ServiceNetwork |  arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetwork/sn-0808d1748faee0c1e           |
```

```
+------------------------+----------------
+-------------------------------------------------------------------------------------------------
+
```

Contrôles de sécurité

Les contrôles de sécurité fournis par Amazon VPC déterminent l'accès réseau à votre entreprise VPCs et aux ressources qui y sont déployées. VPCs

Pourquoi est-ce important

Après avoir déterminé le trafic entrant autorisé vers vos sous-réseaux et ressources et le trafic sortant autorisé à quitter vos sous-réseaux et ressources, vous pouvez planifier les règles de pare-feu nécessaires pour un réseau fonctionnellement équivalent.

Contrôles de sécurité

- Groupes de sécurité
- Réseau ACLs

Groupes de sécurité

Un groupe de sécurité autorise un trafic entrant et sortant spécifique au niveau des ressources. Les groupes de sécurité constituent le principal mécanisme permettant de contrôler l'accès aux ressources de votre VPCs.

Pour obtenir les groupes de sécurité pour votre VPCs

Utilisez la describe-security-groupscommande suivante pour afficher les groupes de sécurité pour le VPC spécifié.

```
aws ec2 describe-security-groups \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query SecurityGroups[*].GroupId
```

Pour obtenir les règles entrantes pour un groupe de sécurité

Utilisez la describe-security-group-rulescommande suivante pour afficher les règles du groupe de sécurité spécifié où se `IsEgress` trouve`false`.

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-0abcdef1234567890 \
    --query 'SecurityGroupRules[?IsEgress==`false`]'
```

Pour obtenir les règles sortantes pour un groupe de sécurité

Utilisez la describe-security-group-rulescommande suivante pour afficher les règles du groupe de sécurité spécifié où se `IsEgress` trouve`true`.

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-0abcdef1234567890 \
    --query 'SecurityGroupRules[?IsEgress==`true`]'
```

Réseau ACLs

Une liste de contrôle d'accès (ACL) réseau autorise ou refuse un trafic entrant et sortant spécifique au niveau du sous-réseau. Vous pouvez utiliser ACLs le réseau comme defense-in-depth si une ressource était déployée sans le bon groupe de sécurité.

Pour obtenir le réseau ACLs pour vos sous-réseaux

Utilisez la describe-network-aclscommande suivante pour afficher le réseau ACLs du VPC spécifié et ses associations de sous-réseaux.

```
aws ec2 describe-network-acls \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query "NetworkAcls[*].{ID:NetworkAclId,Subnets:Associations[].SubnetId}"
```

Pour obtenir les règles entrantes d'une ACL réseau

Utilisez la describe-network-aclscommande suivante pour afficher les règles de l'ACL réseau spécifiée où se `Egress` trouve`false`.

```
aws ec2 describe-network-acls \
    --network-acl-ids acl-0abcdef1234567890 \
    --query 'NetworkAcls[*].Entries[?Egress==`false`]'
```

Pour obtenir les règles sortantes d'une ACL réseau

Utilisez la describe-network-aclscommande suivante pour afficher les règles de l'ACL réseau spécifiée où se `Egress` trouve`true`.

```
aws ec2 describe-network-acls \
    --network-acl-ids acl-0abcdef1234567890 \
    --query 'NetworkAcls[*].Entries[?Egress==`true`]'
```

Gestion du trafic

Une gestion efficace du trafic combine les décisions de routage au niveau du réseau fournies par les tables de routage aux stratégies de distribution au niveau des applications fournies par l'équilibrage de charge.

Pourquoi est-ce important ?

Les administrateurs réseau doivent concevoir les sous-réseaux, le routage, la résolution DNS et l'équilibrage de charge de manière à optimiser le flux de trafic tout en préservant les limites de sécurité et les exigences de performance. En notant la configuration de ces composants dans votre réseau VPC, vous pouvez garantir que les ressources d'un réseau fonctionnellement équivalent peuvent communiquer avec les mêmes clients ou dispositifs qu'au sein de votre réseau VPC.

Gestion du trafic

- Tables de routage
- Jeu d'options DHCP
- Équilibreurs de charge

Tables de routage

Les tables de routage déterminent la manière dont le trafic réseau traverse les limites du réseau, telles que les sous-réseaux VPCs, les réseaux locaux et Internet.

Le mappage des ressources de la console Amazon VPC offre une représentation visuelle des tables de routage de votre VPC.

Pour afficher les tables de routage d'un VPC à l'aide du mappage des ressources

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez VPCs.
3. Cochez la case correspondant au VPC.
4. Sélectionnez l'onglet Mappage des ressources.

5. Le volet Tables de routage répertorie toutes les tables de routage du VPC. Survolez une table de routage avec la souris pour mettre en évidence les sous-réseaux et les connexions réseau associés. Pour plus d'informations, cliquez sur le lien vers la page de détails de la table de routage.

Pour décrire vos tables de routage

Utilisez la describe-route-tablescommande pour décrire les tables de routage pour le VPC spécifié et leurs associations de sous-réseaux.

```
aws ec2 describe-route-tables \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query "RouteTables[*].{ID:RouteTableId,Subnets:Associations[].SubnetId}"
```

Pour obtenir les routes d'une table de routage

Utilisez la describe-route-tablescommande pour décrire les itinéraires pour la table de routage spécifiée.

```
aws ec2 describe-route-tables \
    --route-table-ids rtb-02ec01715bEXAMPLE \
    --query RouteTables[*].Routes
```

Jeu d'options DHCP

Votre VPC dispose d'un jeu d'options DHCP que vous pouvez utiliser pour configurer différents paramètres réseau. Par exemple, vous pouvez configurer des serveurs DNS personnalisés afin que vos EC2 instances puissent résoudre les noms d'hôtes internes à l'aide de votre infrastructure DNS existante. Pour de plus amples informations, veuillez consulter the section called "Concepts des jeux d'options DHCP".

Pour décrire les options DHCP de votre VPC

Utilisez la describe-dhcp-optionscommande pour décrire les options DHCP spécifiées. L'exemple donné permet également d'obtenir l'ID des options DHCP du VPC spécifié à l'aide de la commande describe-vpcs.

```
aws ec2 describe-dhcp-options \
    --dhcp-options-id "$(aws ec2 describe-vpcs \
        --vpc-id vpc-1234567890abcdef0 \
```

```
        --query Vpcs[].DhcpOptionsId --output text)"
```

L'exemple ci-dessous présente la sortie obtenue pour un VPC qui utilise les options DHCP par défaut.

```
{
    "DhcpOptions": [
        {
            "OwnerId": "415546850671",
            "Tags": [],
            "DhcpOptionsId": "dopt-1234567890abcdef0",
            "DhcpConfigurations": [
                {
                    "Key": "domain-name",
                    "Values": [
                        {
                            "Value": "us-west-2.compute.internal"
                        }
                    ]
                },
                {
                    "Key": "domain-name-servers",
                    "Values": [
                        {
                            "Value": "AmazonProvidedDNS"
                        }
                    ]
                }
            ]
        }
    ]
}
```

Équilibreurs de charge

L'équilibrage de charge répartit le trafic entrant des clients sur plusieurs cibles. Les équilibreurs de charge surveillent l'état des cibles et suppriment automatiquement les cibles défectueuses de la distribution du trafic, garantissant ainsi que seules les cibles saines sont utilisées. Cette approche améliore la disponibilité et les performances de votre application et optimise l'utilisation des ressources. Pour plus d'informations, consultez le Guide de l'utilisateur Elastic Load Balancing.

Pour décrire vos équilibreurs de charge

Utilisez la describe-load-balancerscommande pour afficher les équilibreurs de charge pour le VPC spécifié.

```
aws elbv2 describe-load-balancers \
    --query 'LoadBalancers[?VpcId==`vpc-1234567890abcdef0`].LoadBalancerArn'
```

Ressources connexes

Vous pouvez utiliser les services ou fonctionnalités facultatifs suivants dans votre réseau VPC :

- Direct Connect
- AWS Network Firewall
- IPAM
- Mise en miroir du trafic
- Journaux de flux VPC

Gérer les responsabilités en matière de sécurité pour 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 ceci 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

- Validation de conformité pour cloud privé virtuel d'Amazon
- Bloquer l'accès public aux sous-réseaux VPCs et aux sous-réseaux
- Bonnes pratiques de sécurité pour votre VPC

Assurer la 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 d'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 Gestion des identités et des accès AWS (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.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- 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 140-3 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 disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

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 Nom. Cela inclut lorsque vous travaillez avec Amazon VPC ou autre à Services AWS l'aide de la console, de l'API ou. AWS CLI AWS SDKs 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.

Assurer la 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 de plus amples informations, veuillez consulter Groupes de sécurité.
- Listes de contrôle d'accès réseau (ACL) : le réseau ACLs autorise ou refuse un trafic entrant et sortant spécifique au niveau du sous-réseau. Pour de plus amples informations, veuillez consulter Contrôler le trafic des sous-réseaux à l'aide de listes de contrôle d'accès 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 de plus amples informations, veuillez consulter 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.

Appliquer le chiffrement VPC en transit

Les contrôles de chiffrement VPC sont une fonctionnalité de sécurité et de conformité qui vous offre un contrôle centralisé faisant autorité pour surveiller l'état de chiffrement de vos flux de trafic, vous aide à identifier les ressources qui permettent la communication en texte clair et vous fournit éventuellement des mécanismes pour appliquer le chiffrement en transit au sein et entre votre région VPCs

VPC Encryption Controls utilise à la fois le chiffrement de la couche application et la capacité de chiffrement intégrée en transit du matériel du système AWS Nitro pour garantir l'application du chiffrement. Cette fonctionnalité étend également le chiffrement natif de la couche matérielle au-delà des instances Nitro modernes à d'autres services AWS tels que Fargate, Application Load Balancer, Transit Gateways et bien d'autres.

Cette fonctionnalité est conçue pour tous ceux qui souhaitent garantir la visibilité et le contrôle de l'état de chiffrement de l'ensemble de leur trafic. Il est particulièrement utile dans les industries où le chiffrement des données est essentiel pour respecter les normes de conformité telles que HIPAA FedRamp et PCI DSS. Les administrateurs de sécurité et les architectes du cloud peuvent l'utiliser pour appliquer de manière centralisée le chiffrement dans les politiques de transit dans leur AWS environnement

Cette fonctionnalité peut être utilisée dans deux modes : le mode surveillance et le mode application.

Modes de contrôle du chiffrement

Mode de surveillance

En mode surveillance, Encryption Controls fournit une visibilité sur l'état de chiffrement des flux de trafic entre vos AWS ressources internes et entre celles-ci VPCs. Il vous aide également à identifier les ressources VPC qui n'appliquent pas le chiffrement en transit. Vous pouvez configurer vos journaux de flux VPC pour émettre le champ enrichi - `encryption-status` - qui vous indique si votre trafic est chiffré. Vous pouvez également utiliser la console ou la `GetVpcResourcesBlockingEncryptionEnforcement` commande pour identifier les ressources qui n'appliquent pas le chiffrement en transit.

> **Note**
>
> L'existant ne VPCs peut d'abord être activé qu'en mode moniteur. Cela vous donne une visibilité sur les ressources qui sont ou peuvent autoriser le trafic en texte clair. Vous ne pouvez activer le mode d'application sur votre VPC qu'une fois que ces ressources ont commencé à appliquer le chiffrement (ou que vous avez créé des exclusions pour elles).

Mode appliquer

En mode d'application, les contrôles de chiffrement VPC vous empêchent d'utiliser les fonctionnalités ou les services qui autorisent le trafic non chiffré à l'intérieur des limites du VPC. Vous ne pouvez pas activer les contrôles de chiffrement en mode d'application directement sur votre système existant VPCs. Vous devez d'abord activer les contrôles de chiffrement en mode surveillance, identifier et modifier les ressources non conformes pour appliquer le chiffrement en transit, puis activer le mode d'application. Vous pouvez toutefois activer les contrôles de chiffrement en mode d'application pour les nouveaux VPCs lors de la création.

Lorsqu'il est activé, le mode d'application vous empêche de créer ou de joindre des ressources VPC non chiffrées, telles que les anciennes instances EC2 qui ne prennent pas en charge le chiffrement intégré natif, ou les passerelles Internet, etc. Si vous souhaitez exécuter une ressource non conforme dans un VPC basé sur le chiffrement, vous devez créer une exclusion pour cette ressource.

Surveillance de l'état de chiffrement des flux de trafic

Vous pouvez vérifier l'état de chiffrement des flux de trafic à l'intérieur du VPC à l'aide du `encryption-status` champ figurant dans vos journaux de flux VPC. Elle peut avoir les valeurs suivantes :

- `0`= non crypté
- `1`= crypté nitro (géré par VPC Encryption Controls)
- `2`= crypté par application
  - flux sur le port TCP 443 pour le point de terminaison d'interface vers le AWS service *
  - flux sur le port TCP 443 pour le point de terminaison de la passerelle *
  - flux vers un cluster Redshift chiffré via le point de terminaison VPC**
- `3`= Nitro ET application cryptées

- (-)= État du chiffrement inconnu ou les contrôles de chiffrement VPC sont désactivés

Remarque :

* Pour les points de terminaison de l'interface et de la passerelle, AWS il ne prend pas en compte les données des paquets pour déterminer l'état du chiffrement, nous nous basons plutôt sur le port utilisé pour assumer l'état du chiffrement.

** Pour les points de terminaison AWS gérés spécifiés, AWS détermine l'état du chiffrement en fonction des exigences du protocole TLS dans la configuration du service.

Limites du journal de flux VPC

- Pour activer les journaux de flux pour les contrôles de chiffrement VPC, vous devez créer manuellement de nouveaux journaux de flux avec le champ d'état du chiffrement. Le champ d'état du chiffrement n'est pas automatiquement ajouté aux journaux de flux existants.
- Il est recommandé d'ajouter les champs $ {traffic-path} et $ {flow-direction} aux journaux de flux pour obtenir des informations plus détaillées dans les journaux de flux.

  Exemple :

```
aws ec2 create-flow-logs \
--resource-type VPC \
--resource-ids vpc-12345678901234567 \
--traffic-type ALL \
--log-group-name my-flow-logs \
--deliver-logs-permission-arn arn:aws:iam::123456789101:role/publishFlowLogs
--log-format '${encryption-status} ${srcaddr} ${dstaddr} ${srcport} ${dstport}
 ${protocol} ${traffic-path} ${flow-direction} ${reject-reason}'
```

Exclusions relatives aux contrôles de chiffrement VPC

Le mode d'application des contrôles de chiffrement VPC exige que toutes les ressources du VPC appliquent le chiffrement. Cela garantit le chiffrement au AWS sein d'une région. Cependant, il se peut que vous disposiez de ressources telles qu'une passerelle Internet, une passerelle NAT ou une passerelle privée virtuelle qui permettent AWS la connectivité à des réseaux extérieurs où vous êtes responsable de la configuration et de la maintenance du end-to-end chiffrement. Pour exécuter ces ressources dans le cadre du chiffrement appliqué VPCs, vous pouvez créer des exclusions de

ressources. Une exclusion crée une exception vérifiable pour les ressources pour lesquelles le client est responsable du maintien du chiffrement (généralement au niveau de la couche application).

Seules 8 exclusions sont prises en charge pour les contrôles de chiffrement VPC. Si vous disposez de ces ressources dans votre VPC et que vous souhaitez passer en mode d'application, vous devez ajouter ces exclusions lorsque vous passez du mode moniteur au mode d'application. Aucune autre ressource n'est exclue. Vous pouvez faire migrer votre VPC vers le mode d'application en créant des exclusions pour ces ressources. Vous êtes responsable du chiffrement des flux de trafic à destination et en provenance de ces ressources.

- Internet Gateway
- Passerelle NAT
- Internet Gateway uniquement pour les sorties
- Les connexions d'appairage VPC au chiffrement ne sont pas appliquées (VPCs voir la section relative au support de peering VPC pour des scénarios détaillés)
- Passerelle privée virtuelle
- Fonctions Lambda au sein de votre VPC
- Treillis en VPC
- Système de fichiers Elastic

Flux de travail d'implémentation

1. Activer la surveillance : créer un contrôle de chiffrement VPC en mode moniteur
2. Analyser le trafic : consultez les journaux de flux pour surveiller l'état de chiffrement du flux de trafic
3. Analyser les ressources : utilisez la console ou la `GetVpcResourcesBlockingEncryptionEnforcement` commande pour identifier les ressources qui n'appliquent pas le chiffrement en transit.
4. Préparation [Facultatif] - Planifiez les migrations de ressources et les exclusions requises si vous souhaitez activer le mode d'application
5. Appliquer [Facultatif] - Passez en mode d'application avec les exclusions requises configurées
6. Audit - Surveillance continue de la conformité par le biais de journaux de flux

Pour obtenir des instructions de configuration détaillées, consultez le blog Présentation des contrôles de chiffrement VPC : appliquez le chiffrement en transit au sein d'une région et entre VPCs celles-ci.

État des contrôles de chiffrement VPC

Les contrôles de chiffrement VPC peuvent avoir l'un des états suivants :

creating

Les contrôles de chiffrement VPC sont en cours de création sur le VPC.

modify-in-progress

Les contrôles de chiffrement VPC sont en cours de modification sur le VPC

deleting

Les contrôles de chiffrement VPC sont en cours de suppression sur le VPC

available

Les contrôles de chiffrement VPC ont réussi à implémenter le mode de surveillance ou le mode d'application sur le VPC

AWS support technique et compatibilité

Pour être conforme au chiffrement, une ressource doit toujours appliquer le chiffrement en transit, que ce soit au niveau de la couche matérielle ou au niveau de la couche application. Pour la plupart des ressources, aucune action n'est requise de votre part.

Services avec mise en conformité automatique

La plupart AWS des services pris en charge par PrivateLink, y compris Cross-Region, PrivateLinks acceptent le trafic chiffré au niveau de la couche application. Vous n'êtes pas obligé d'apporter des modifications à ces ressources. AWS supprime automatiquement tout trafic qui ne l'est pas application-layer-encrypted. Certaines exceptions incluent les clusters Redshift (provisionnés et sans serveur, où vous devez migrer manuellement les ressources sous-jacentes)

Ressources qui migrent automatiquement

Les équilibreurs de charge réseau, les équilibreurs de charge d'application, les clusters Fargate et le plan de contrôle EKS migreront automatiquement vers du matériel prenant en charge le chiffrement

de manière native une fois que vous aurez activé le mode moniteur. Vous n'êtes pas obligé de modifier ces ressources. AWS gère automatiquement la migration.

Ressources nécessitant une migration manuelle

Certaines ressources et certains services VPC nécessitent que vous sélectionniez les types d'instances sous-jacents. Toutes les instances EC2 modernes prennent en charge le chiffrement en transit. Vous n'avez aucune modification à apporter si vos services utilisent déjà des instances EC2 modernes. Vous pouvez utiliser la console ou la GetVpcResourcesBlockingEncryptionEnforcement commande pour identifier si l'un de ces services utilise des instances plus anciennes. Si vous identifiez de telles ressources, vous devez les mettre à niveau vers l'une des instances EC2 modernes prenant en charge le chiffrement natif du matériel du système Nitro. Ces services incluent les instances EC2, les groupes Auto Scaling, RDS (toutes les bases de données et Document-DB), Elasticache Provisioned, Amazon Redshift Provisioned Clusters, EKS, ECS-EC2, Provisioned et EMR. OpenSearch

Ressources compatibles :

Les ressources suivantes sont compatibles avec les contrôles de chiffrement VPC :

- Instances EC2 basées sur Nitro
- Équilibreurs de charge réseau (avec limitations)
- Application Load Balancers
- AWS Clusters de Fargate
- Amazon Elastic Kubernetes Service (EKS)
- Groupes Amazon EC2 Auto Scaling
- Amazon Relational Database Service (RDS - Toutes les bases de données)
- Clusters basés sur ElastiCache des nœuds Amazon
- Clusters provisionnés et sans serveur Amazon Redshift
- Amazon Elastic Container Service (ECS) - Instances de conteneur EC2
- Amazon OpenSearch Service
- Amazon Elastic MapReduce (EMR)
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Les contrôles de chiffrement VPC appliquent le chiffrement au niveau de la couche application pour tous les AWS services accessibles via. PrivateLink Tout trafic non chiffré au niveau de la couche

application est supprimé par les PrivateLink points de terminaison hébergés dans le VPC avec des contrôles de chiffrement en mode appliqué.

Limitations spécifiques au service

Limites du Network Load Balancer

Configuration TLS : vous ne pouvez pas utiliser un écouteur TLS pour déléguer le travail de chiffrement et de déchiffrement à votre équilibreur de charge lorsque vous appliquez des contrôles de chiffrement sur le VPC contenant. Vous pouvez toutefois configurer vos cibles pour effectuer le chiffrement et le déchiffrement TLS.

Redshift provisionné et sans serveur

Les clients ne peuvent pas passer en mode Enforce sur un VPC doté d'un cluster/point de terminaison existant. Pour utiliser les contrôles de chiffrement VPC avec Redshift, vous devez restaurer votre cluster ou votre espace de noms à partir d'un instantané. Pour les clusters provisionnés, créez un instantané de votre cluster Redshift existant, puis restaurez à partir de cet instantané à l'aide de l'opération de restauration à partir d'un instantané de cluster. Pour Serverless, créez un instantané de votre espace de noms existant, puis restaurez à partir de cet instantané à l'aide de l'opération de restauration à partir d'un instantané sur votre groupe de travail sans serveur. Notez que les contrôles de chiffrement VPC ne peuvent pas être activés sur des clusters ou des espaces de noms existants sans exécuter le processus de capture instantanée et de restauration. Reportez-vous à la documentation Amazon Redshift pour la création d'instantanés.

Amazon MSK (streaming géré pour Apache Kafka)

Cette fonctionnalité est prise en charge dans les nouveaux clusters pour la version 4.1 dans leur propre VPC. Les étapes suivantes vous aideront à utiliser le chiffrement VPC avec MSK.

- Le client active le chiffrement VPC sur un VPC sans aucun autre cluster MSK
- Le client crée un cluster avec la version 4.1 de Kafka et le type d'instance est m7G

Limitations régionales et de zone

- Sous-réseaux de zone locale : non pris en charge en mode d'application - doivent être supprimés du VPC

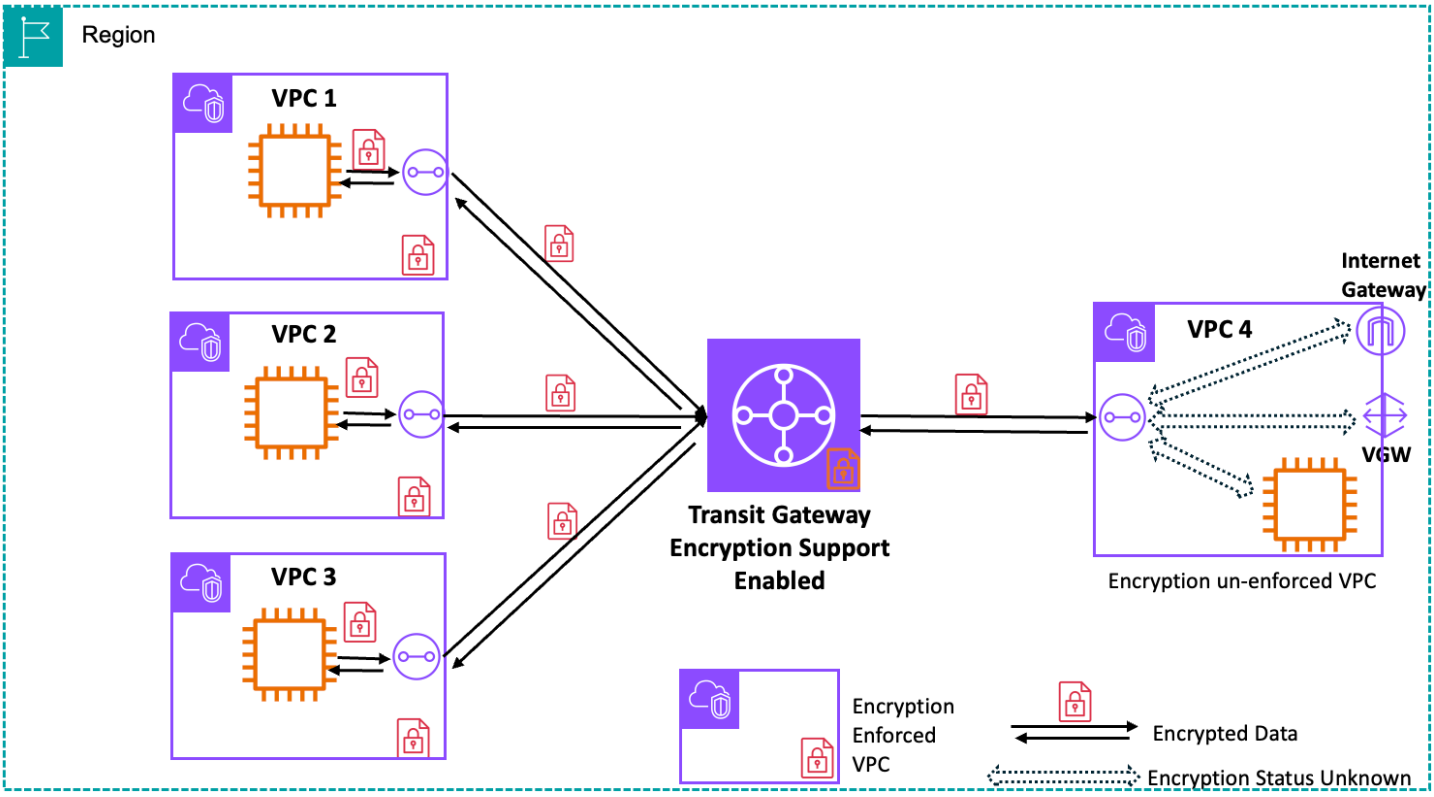
Support de peering VPC

Pour garantir le chiffrement en transit grâce à l'appairage VPC entre deux entités VPCs, les deux VPCs doivent résider dans la même région et les contrôles de chiffrement doivent être activés en mode d'application sans aucune exclusion. Vous devez créer une exclusion d'appairage si vous souhaitez associer un VPC à chiffrement à un autre VPC résidant dans une autre région ou dont les contrôles de chiffrement ne sont pas activés en mode d'application (sans exclusions).

Si deux d'entre eux VPCs sont en mode d'application et s'apparient l'un à l'autre, vous ne pouvez pas passer du mode appliquer au mode surveillance. Vous devez d'abord créer une exclusion de peering, avant de modifier le mode VPC Encryption Controls à surveiller.

Prise en charge du chiffrement Transit Gateway

Vous devez activer explicitement la prise en charge du chiffrement sur un Transit Gateway pour chiffrer le trafic entre ceux VPCs dont les contrôles de chiffrement sont activés. L'activation du chiffrement sur le Transit Gateway existant ne perturbe pas les flux de trafic existants et la migration des pièces jointes VPC vers des voies cryptées se fera de manière fluide et automatique. Le trafic entre deux VPCs personnes en mode forcé (sans exclusions) via le Transit Gateway traverse des voies cryptées à 100 %. Le chiffrement sur Transit Gateway vous permet également d'en connecter deux VPCs qui utilisent des modes de contrôle de chiffrement différents. Vous devez l'utiliser lorsque vous souhaitez appliquer des contrôles de chiffrement dans un VPC connecté à un non-encryption-enforced VPC. Dans un tel scénario, tout le trafic à l'intérieur de votre VPC soumis au chiffrement, y compris le trafic inter-VPC, est chiffré. Le trafic inter-VPC est chiffré entre les ressources du VPC à chiffrement appliqué et du Transit Gateway. En outre, le chiffrement dépend des ressources vers lesquelles le trafic est dirigé dans le VPC non imposé et il n'est pas garanti qu'il soit chiffré (étant donné que le VPC n'est pas en mode d'application). Tous VPCs doivent se trouver dans la même région. (voir les détails ici).



- Dans ce schéma, les VPC 1, VPC 2 et VPC VPC3 disposent de contrôles de chiffrement en mode d'application et ils sont connectés au VPC 4 dont les contrôles de chiffrement sont exécutés en mode moniteur.
- Tout le trafic entre VPC1 VPC2 et VPC3 sera crypté.
- Plus précisément, tout trafic entre une ressource du VPC 1 et une ressource du VPC 4 sera chiffré jusqu'au Transit Gateway en utilisant le cryptage proposé par le matériel du système Nitro. Au-delà de cela, l'état du chiffrement dépend de la ressource dans le VPC 4 et il n'est pas garanti qu'il soit chiffré.

Pour plus de détails sur la prise en charge du chiffrement Transit Gateway, consultez la documentation relative à Transit Gateway.

Tarification

Pour plus d'informations sur les tarifs, consultez la tarification d'Amazon VPC.

AWS CLI référence de commande

Installation et configuration

- AWS EC2 create-vpc-encryption-control
- AWS EC2 modify-vpc-encryption-control
- AWS EC2 TGW modify-transit-gateway

Surveillance et résolution des problèmes

- AWS EC2 describe-vpc-encryption-controls
- aws ec2 get-vpc-resources-blocking -mise en œuvre du chiffrement
- AWS EC2 create-flow-logs
- AWS EC2 describe-flow-logs
- Requête aws Logs

Nettoyage

- AWS EC2 delete-vpc-encryption-control

Ressources supplémentaires

Pour obtenir des instructions de configuration détaillées, consultez le blog Présentation des contrôles de chiffrement VPC : appliquez le chiffrement en transit au sein d'une région et entre VPCs celles-ci.

Pour des informations plus détaillées sur les API, consultez le guide de référence des API EC2.

Identity and Access Management pour Amazon VPC

Gestion des identités et des accès AWS (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 Gestion des identités et des accès AWS (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 en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent 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 qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle utilisateur à un

rôle IAM (console) ou en appelant une opération AWS CLI ou AWS API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM 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 définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant 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. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et 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. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. 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. Vous devez spécifier un principal dans une politique basée sur les ressources.

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 (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session 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. Intégration d'actions dans une politique 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. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, 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 spécifier tous VPCs ceux d'une région spécifique qui appartiennent à un compte spécifique, 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-les ARNs par des virgules.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Pour consulter la liste des types de ressources Amazon VPC et leurs caractéristiques ARNs, consultez la section Types de ressources définis par Amazon EC2 dans le Service Authorization Reference.

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` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. 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 intercompte 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 politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM 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 plus d'informations, consultez la section Grant permission to tag resources during creation du Guide d'utilisation d'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 de plus amples informations, veuillez consulter 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.
- Accordez 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utilisez 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 CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM 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 politiques avec 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 la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec 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.

JSON

```
{
    "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 permet aux rôles de créer des sous-réseaux VPCs, 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.

JSON

```
{
   "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.

JSON

```
{
    "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.

JSON

```
{
    "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"
                },
                "ForAnyValue: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.

JSON

```
{
    "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:us-east-1:123456789012:security-group/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifySecurityGroupRules"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012: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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:us-east-1::image/ami-*",
                "arn:aws:ec2:us-east-1:123456789012:instance/*",
                "arn:aws:ec2:us-
east-1:123456789012:subnet/subnet-1234567890abcdef0",
                "arn:aws:ec2:us-east-1:123456789012:network-interface/*",
                "arn:aws:ec2:us-east-1:123456789012:volume/*",
                "arn:aws:ec2:us-east-1:123456789012:key-pair/*",
                "arn:aws:ec2:us-east-1:123456789012:security-
group/sg-0abcdef1234567890"
            ]
        }
    ]
}
```

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 politique accorde également aux rôles l'autorisation de lancer des instances en utilisant uniquement AMIs les instances portant le tag « `department=dev` ».

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:subnet/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/department": "dev"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:us-east-1:123456789012:instance/*",
                "arn:aws:ec2:us-east-1:123456789012:volume/*",
                "arn:aws:ec2:us-east-1:123456789012:network-interface/*",
                "arn:aws:ec2:us-east-1:123456789012:key-pair/*",
                "arn:aws:ec2:us-east-1:123456789012:security-group/*"
            ]
        }
    ]
}
```

Bloquer l'accès public aux sous-réseaux VPCs et aux sous-réseaux

Les exemples de politique suivants accordent aux rôles l'autorisation d'utiliser la fonctionnalité VPC Block Public Access (BPA) pour bloquer l'accès public aux ressources des sous-réseaux et des sous-réseaux. VPCs

Exemple 1 : autoriser l'accès en lecture seule aux paramètres VPC BPA à l'échelle du compte et aux exclusions du VPC BPA.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAReadOnlyAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Exemple 2 : autoriser un accès complet en lecture et en écriture aux paramètres VPC BPA à l'échelle du compte et aux exclusions du VPC BPA.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAFullAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:ModifyVpcBlockPublicAccessOptions",
        "ec2:CreateVpcBlockPublicAccessExclusion",
        "ec2:ModifyVpcBlockPublicAccessExclusion",
        "ec2:DeleteVpcBlockPublicAccessExclusion"
      ],
      "Effect": "Allow",
      "Resource": "*"
```

```
    }
  ]
}
```

Exemple 3 - Autoriser l'accès à tous les EC2, à l' APIs exception de la modification des paramètres BPA du VPC et de la création d'exclusions.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "EC2FullAccess",
            "Action": [
                "ec2:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "VPCBPAPartialAccess",
            "Action": [
                "ec2:ModifyVpcBlockPublicAccessOptions",
                "ec2:CreateVpcBlockPublicAccessExclusion"
            ],
            "Effect": "Deny",
            "Resource": "*"
        }
    ]
}
```

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 d'un VPC et services de point de terminaison d'un VPC (AWS PrivateLink)
- Appairage de VPC

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, vous devez 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 n'est pas autorisée à transmettre 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 (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, 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 en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM 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 Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : Amazon VPCFull Access

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 Amazon VPCFull Access dans le manuel AWS Managed Policy Reference.

AWS politique gérée : Amazon VPCRead OnlyAccess

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 Amazon VPCRead OnlyAccess dans le AWS Managed Policy Reference.

AWS politique gérée : Amazon VPCCross AccountNetworkInterfaceOperations

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 Amazon VPCCross AccountNetworkInterfaceOperations dans le AWS Managed Policy Reference.

AWS politique gérée : AWSService RoleFor NATGateway

Vous pouvez associer la politique `AWSServiceRoleForNATGateway` à vos identités IAM. Cette politique accorde des autorisations qui permettent à l'identité de travailler en votre nom afin de dimensionner automatiquement les passerelles NAT régionales.

Pour voir les autorisations de cette stratégie, consultez AWSServiceRoleForNATGateway dans le AWS Guide de référence des stratégies gérées par.

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.

Modifier	Description	Date
the section called "Amazon VPCFull Access" – Mise à jour d'une stratégie existante	Actions ajoutées à la politique AWSIPAMService RolePolic y gérée (ec2:ModifyManaged PrefixList,ec2:DescribeMana gedPrefixLists, etec2:Get ManagedPrefixListEntries) pour permettre à IPAM de	31 octobre 2025

Modifier	Description	Date
	modifier et de lire les listes de préfixes gérées.	
the section called "AWSServiceRoleForNATGateway " : nouvelle politique	La nouvelle AWSServic e RoleFor NATGateway politique permet à l'identité de redimensionner automatiq uement les passerelles NAT régionales.	19 novembre 2025
the section called "Amazon VPCFull Access" : mise à jour d'une politique existante	Ajout des DisassociateSecuri tyGroupVpc actions Associate SecurityGroupVpcDe scribeSecurityGroupVpcAssoc iations, et, qui vous permetten t d'associer, de dissocier et de visualiser les associations de groupes de sécurité avec VPCs.	9 décembre 2024
the section called "Amazon VPCRead OnlyAccess" : mise à jour d'une politique existante	Ajout de l'DescribeSecurity GroupVpcAssociationsaction, qui vous permet de visualise r les associations de groupes de sécurité avec VPCs.	9 décembre 2024
the section called "Amazon VPCFull Access" : mise à jour d'une politique existante	Ajout de l'action GetSecuri tyGroupsForVpc, qui vous permet d'obtenir des groupes de sécurité utilisables dans votre VPC.	8 février 2024

Modifier	Description	Date
the section called "Amazon VPCRead OnlyAccess" : mise à jour d'une politique existante	Ajout de l'action GetSecuri tyGroupsForVpc, qui vous permet d'obtenir des groupes de sécurité utilisables dans votre VPC.	8 février 2024
the section called "Amazon VPCCross AccountNe tworkInterfaceOperations" : mise à jour d'une politique existante	Ajout des UnassignIpv6Addres ses actions AssignIpv 6Addresses et, qui vous permettent de gérer les IPv6 adresses associées aux interfaces réseau.	25 septembre 2023
the section called "Amazon VPCRead OnlyAccess" : mise à jour d'une politique existante	Ajout de l'action DescribeS ecurityGroupRules, qui vous permet d'afficher les règles des groupes de sécurité.	2 août 2021
the section called "Amazon VPCFull Access" : mise à jour d'une politique existante	Ajout des actions DescribeS ecurityGroupRules et ModifySecurityGroupRules, qui vous permettent d'affiche r et de modifier les règles des groupes de sécurité.	2 août 2021
the section called "Amazon VPCFull Access" : mise à jour d'une politique existante	Actions ajoutées pour les passerelles d'opérateurs, les IPv6 pools, les passerell es locales et les tables de routage des passerelles locales.	23 juin 2021

Modifier	Description	Date
the section called "Amazon VPCRead OnlyAccess" : mise à jour d'une politique existante	Actions ajoutées pour les passerelles d'opérateurs, les IPv6 pools, les passerell es locales et les tables de routage des passerelles locales.	23 juin 2021

Utilisation de rôles liés à un service pour VPC

Amazon VPC utilise des rôles liés à un Gestion des identités et des accès AWS service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié au VPC. Les rôles liés à un service sont prédéfinis par le VPC et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration du VPC, car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. Le VPC définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul le VPC peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos ressources VPC car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la colonne Rôles liés à un service. Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle liées à un service pour VPC

Le VPC utilise le rôle lié au service nommé AWSServiceRoleForNATGateway— Ce rôle lié au service permet à Amazon VPC d'attribuer des adresses IP élastiques en votre nom afin de dimensionner automatiquement les passerelles NAT régionales, d'associer et de dissocier vos passerelles IPs Elastic existantes aux passerelles NAT régionales à votre demande, et de décrire les interfaces

réseau pour identifier votre infrastructure existante afin de l'étendre automatiquement à de nouvelles zones de disponibilité.

Le rôle AWSService RoleFor NATGateway lié à un service fait confiance aux services suivants pour assumer le rôle :

- `ec2-nat-gateway.amazonaws.com`

La politique d'autorisations de rôle nommée AWSNATGateway ServiceRolePolicy permet au VPC d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `AllocateAddress` sur Service Managed EIPs pour allouer EIPs en votre nom. Service Managed EIPs gère le balisage ultérieur avec des balises gérées par le service et ReleaseAddress automatiquement.
- Action : `AssociateAddress` sur vos adresses IP Elastic préexistantes pour les associer manuellement à votre passerelle NAT régionale à votre demande.
- Action : `DisassociateAddress` sur vos adresses IP Elastic préexistantes pour les supprimer de la passerelle NAT régionale à votre demande.
- Action : `DescribeAddresses` obtenir les informations d'adresse IP publique fournies par le client EIPs sur l'associé.
- Action : `DescribeNetworkInterface` sur vos interfaces réseau existantes pour identifier automatiquement les zones de disponibilité dans lesquelles se trouve votre infrastructure afin de l'étendre automatiquement à de nouvelles zones.

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour VPC

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez une passerelle NAT avec un mode de disponibilité « régional » dans l'API AWS Management Console, le ou l' AWS API AWS CLI, le VPC crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. En outre, si vous utilisiez le service VPC avant le 1er janvier 2017, date à laquelle il a commencé à prendre en charge les rôles liés au service, VPC a créé le rôle dans votre compte. AWSService RoleFor NATGateway Pour en savoir plus, voir Un nouveau rôle est apparu dans mon Compte AWS.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez une passerelle NAT avec un mode de disponibilité « régional », le VPC crée à nouveau le rôle lié au service pour vous.

Vous pouvez également utiliser la console IAM pour créer un rôle lié à un service avec le AWSServiceRoleForNATGatewaycas d'utilisation. Dans l'API AWS CLI ou dans l' AWS API, créez un rôle lié à un service avec le nom du `ec2-nat-gateway.amazonaws.com` service. Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour un VPC

Le VPC ne vous permet pas de modifier le rôle lié au AWSService RoleFor NATGateway service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour un VPC

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service VPC utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources VPC utilisées par AWSService RoleFor NATGateway

- Supprimez toutes les passerelles NAT régionales dans toutes les régions dans lesquelles elles ont été déployées.

Pour supprimer manuellement le rôle lié au service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSService RoleFor NATGateway service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés aux services VPC

Le VPC prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez AWS Régions et points de terminaison.

Le VPC ne prend pas en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Vous pouvez utiliser le AWSService RoleFor NATGateway rôle dans les régions suivantes.

Nom de la région	Identité de la région	Support en VPC
USA Est (Virginie du Nord)	us-east-1	Oui
USA Est (Ohio)	us-east-2	Oui
USA Ouest (Californie du Nord)	us-west-1	Oui
USA Ouest (Oregon)	us-west-2	Oui
Afrique (Le Cap)	af-south-1	Oui
Asie-Pacifique (Hong Kong)	ap-east-1	Oui

Nom de la région	Identité de la région	Support en VPC
Asie-Pacifique (Taipei)	ap-east-2	Oui
Asie-Pacifique (Jakarta)	ap-southeast-3	Oui
Asie-Pacifique (Mumbai)	ap-south-1	Oui
Asie-Pacifique (Hyderabad)	ap-south-2	Oui
Asie-Pacifique (Osaka)	ap-northeast-3	Oui
Asie-Pacifique (Séoul)	ap-northeast-2	Oui
Asie-Pacifique (Singapour)	ap-southeast-1	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	Oui
Asie-Pacifique (Melbourne)	ap-southeast-4	Oui
Asie-Pacifique (Malaisie)	ap-southeast-5	Oui
Asie-Pacifique (Nouvelle Zélande)	ap-southeast-6	Oui
Asie-Pacifique (Thaïlande)	ap-southeast-7	Oui
Canada (Centre)	ca-central-1	Oui
Canada-Ouest (Calgary)	ca-west-1	Oui
Europe (Francfort)	eu-central-1	Oui
Europe (Zurich)	eu-central-2	Oui
Europe (Irlande)	eu-west-1	Oui
Europe (Londres)	eu-west-2	Oui
Europe (Milan)	eu-south-1	Oui

Nom de la région	Identité de la région	Support en VPC
Europe (Espagne)	eu-south-2	Oui
Europe (Paris)	eu-west-3	Oui
Europe (Stockholm)	eu-north-1	Oui
Israël (Tel Aviv)	il-central-1	Oui
Moyen-Orient (Bahreïn)	me-south-1	Oui
Moyen-Orient (EAU)	me-central-1	Oui
Moyen-Orient (Arabie saoudite)	me-west-1	Oui
Mexique (Centre)	mx-central-1	Oui
Amérique du Sud (São Paulo)	sa-east-1	Oui
AWS GovCloud (USA Est)	us-gov-east-1	Non
AWS GovCloud (US-Ouest)	us-gov-west-1	Non

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.

Isolement de réseau

Un cloud privé virtuel (VPC) est un réseau virtuel situé dans votre propre zone logiquement isolée dans le cloud. AWS Utilisez la méthode séparée VPCs 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 principal mécanisme de contrôle de l'accès réseau à votre VPCs. Si nécessaire, utilisez le réseau ACLs pour fournir un contrôle du réseau sans état et grossier. Les groupes de sécurité sont plus polyvalents que les réseaux ACLs, en raison de leur capacité à effectuer un filtrage dynamique des paquets et à créer des règles faisant référence à d'autres groupes de sécurité. Le réseau ACLs peut être efficace en tant que contrôle secondaire (par exemple, pour refuser un sous-ensemble spécifique de trafic) ou en tant que garde-corps de haut niveau. De plus, comme le réseau ACLs s'applique à l'ensemble d'un sous-réseau, il peut être utilisé 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 Direct Connect pour établir des connexions privées entre vos réseaux distants et votre VPCs. Pour plus d'informations, consultez la section Network-to-Amazon Options de connectivité VPC.
- Utilisez des journaux de flux VPC pour surveiller la trafic atteignant vos instances.
- Utilisez AWS Security Hub CSPM 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.

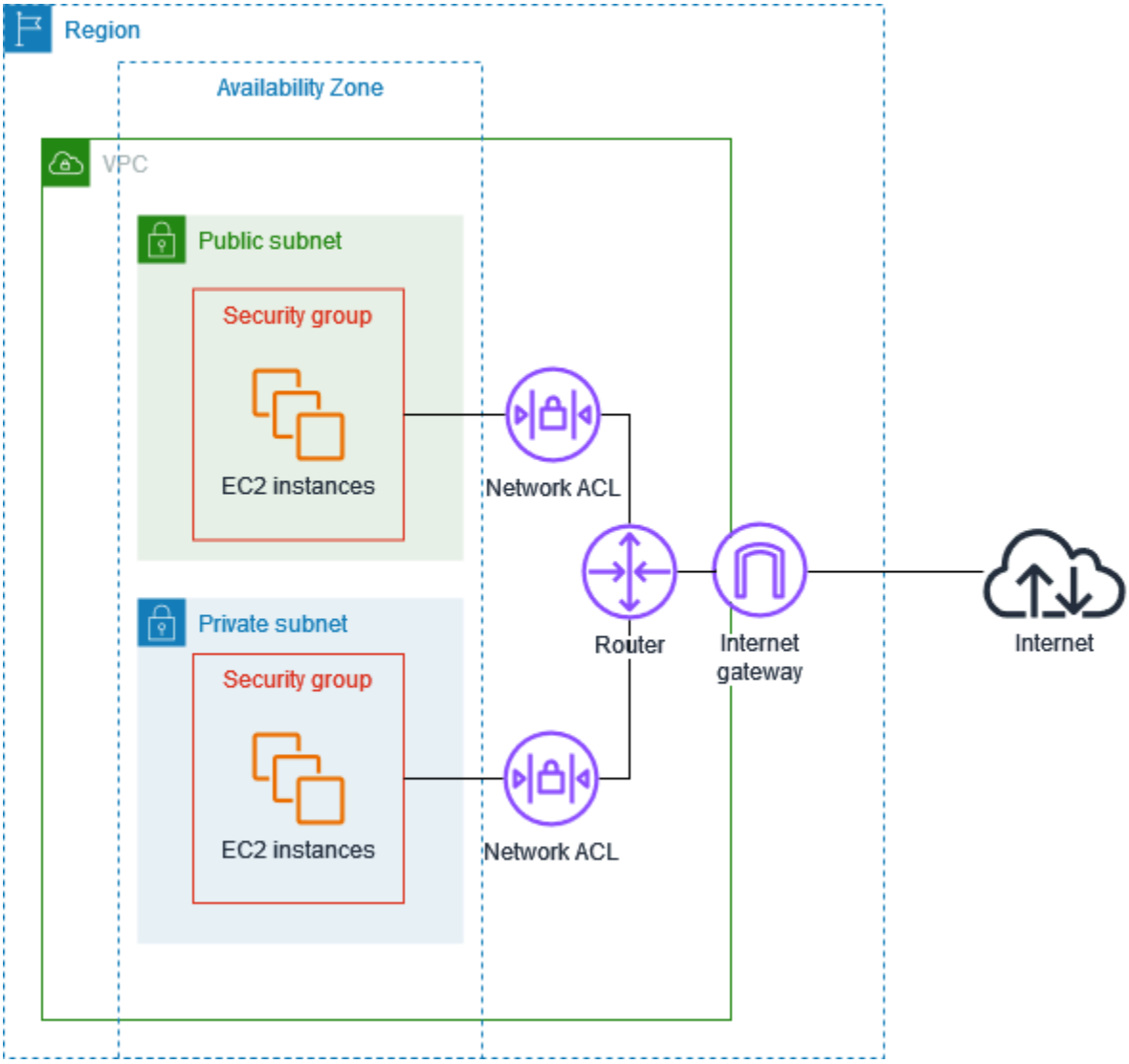
Comparez les groupes de sécurité et le réseau ACLs

Le tableau suivant récapitule les principales différences entre les groupes de sécurité et le réseau ACLs.

Caractéristiques	Groupe de sécurité	Réseau ACL
Niveau de l'opération	Niveau de l'instance	Niveau du sous-réseau
Scope	S'applique à toutes les instances associées au groupe de sécurité	S'applique à toutes les instances présentes dans les sous-réseaux associés
Type de règle	Règles d'autorisation uniquement	Règles d'autorisation et de refus

Caractéristiques	Groupe de sécurité	Réseau ACL
Évaluations des règles	Evalue toutes les règles avant de décider si le trafic doit être autorisé	Évalue les règles par ordre croissant jusqu'à ce qu'une correspondance soit trouvée pour le trafic
Trafic de retour	Autorisé automatiquement (avec état)	Doit être explicitement autorisé (sans état)

Le schéma suivant illustre les couches de sécurité fournies par les groupes de sécurité et le réseau ACLs. 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. Cependant, vous pouvez ajouter un réseau ACLs comme couche de défense supplémentaire. Pour de plus amples informations, veuillez consulter 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.

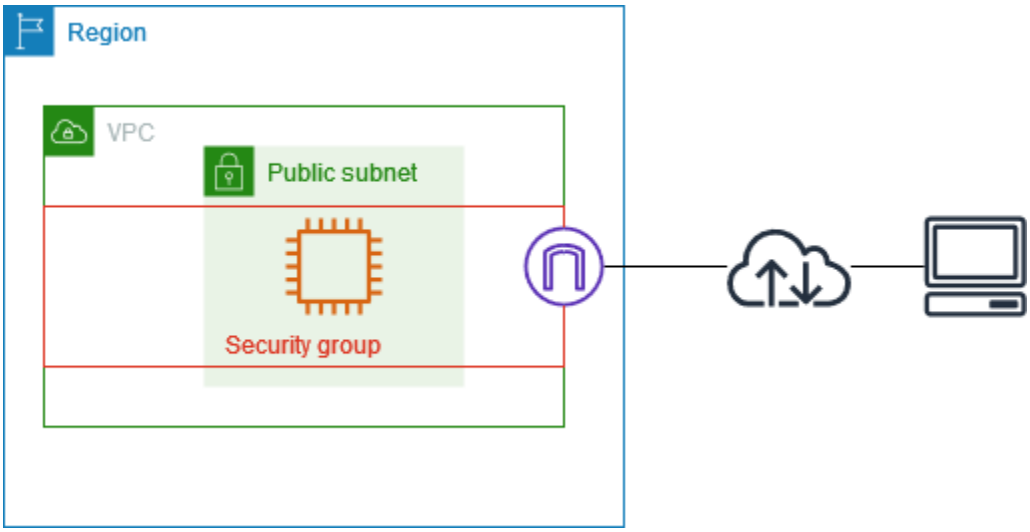


Table des matières

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 à des ressources créées dans le même VPC que le groupe de sécurité ou à des ressources d'un autre groupe VPCs si vous utilisez la fonctionnalité d'association VPC du groupe de sécurité pour associer le groupe de sécurité à d'autres VPCs dans la même région. Vous pouvez également attribuer plusieurs groupes de sécurité à une seule 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 des groupes de sécurité ne sont pas sensibles à la casse.
  - 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 de plus amples informations, veuillez consulter Quotas Amazon VPC.

Bonnes pratiques

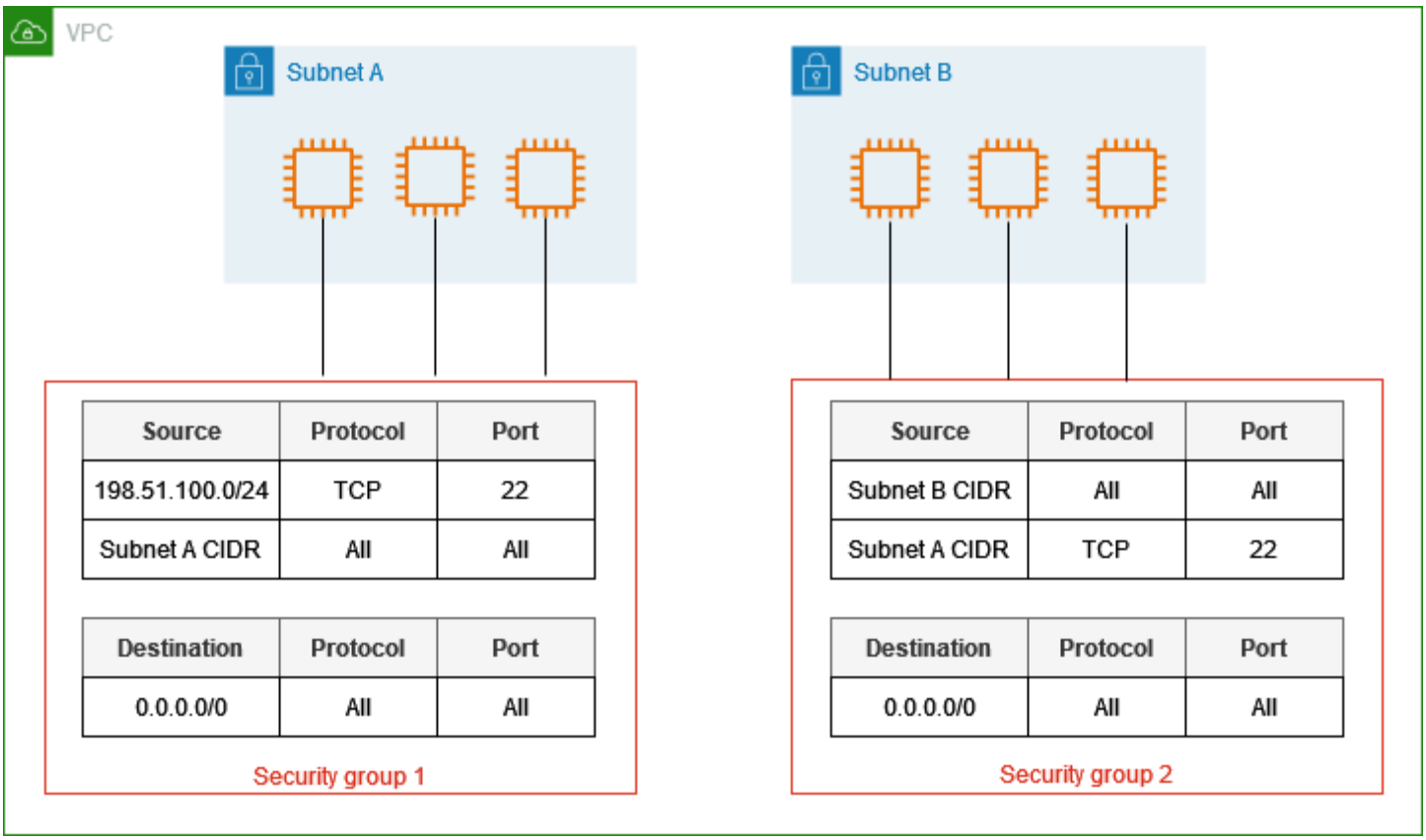
- Autorisez uniquement certains principaux IAM à créer et à modifier les groupes de sécurité.
- Créez le nombre minimum de groupes de sécurité dont vous avez besoin afin de réduire le risque d'erreur. Utilisez chaque groupe de sécurité pour gérer l'accès aux ressources possédant des fonctions et des 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 quiconque d'accéder à vos instances depuis n'importe quelle adresse IP en utilisant 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 ACLs un réseau avec des règles similaires à celles de vos groupes de sécurité, afin d'ajouter une couche de sécurité supplémentaire à votre VPC. Pour plus d'informations sur les différences entre les groupes de sécurité et le réseau ACLs, consultezComparez les groupes de sécurité et le réseau ACLs.

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

- Composants d'une règle de groupe de sécurité
- Référencement des groupes de sécurité
- Taille de groupe de sécurité
- Règles du groupe de sécurité obsolètes

Règles de base de groupe de sécurité

Les caractéristiques des règles des groupes de sécurité sont les suivantes :

- 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. Pour obtenir des instructions, veuillez consulter Configurer des règles de 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 Suivi de connexion 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 Amazon Route 53 Resolverle guide du 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

Les éléments suivants sont les composants des règles entrantes et sortantes des groupes 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 ICMP Echo Request ou le type 128 pour ICMPv6 Echo Request. Pour plus d'informations, consultez la section Rules for ping/ICMP du Guide d'utilisation d'Amazon EC2.
- 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 :
  - Une IPv4 adresse unique. Vous devez utiliser la longueur de préfixe `/32`. Par exemple, `203.0.113.1/32`.
  - Une IPv6 adresse unique. Vous devez utiliser la longueur de préfixe `/128`. Par exemple, `2001:db8:1234:1a00::123/128`.
  - Une plage d' IPv4 adresses, en notation par blocs CIDR. Par exemple, `203.0.113.0/24`.
  - Une plage d' IPv6 adresses, en notation par blocs CIDR. Par exemple, `2001:db8:1234:1a00::/64`.
  - ID d'une liste des préfixes. Par exemple, `pl-1234abc1234abc123`. Pour de plus amples informations, veuillez consulter Listes de préfixes gérées.
  - ID d'un groupe de sécurité. Par exemple, `sg-1234567890abcdef0`. Pour de plus amples informations, veuillez consulter 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 ._-:/()#,@[]+=;{}!$*.

Pour obtenir des exemples, consultez la section Security group rules for different use cases du Guide d'utilisation d'Amazon EC2.

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 :

- Vous pouvez faire référence à un groupe de sécurité dans la règle entrante d'un autre groupe de sécurité si l'une des conditions suivantes est vraie :
  - Les groupes de sécurité sont associés au même VPC.
  - Il existe une connexion d'appairage entre ceux VPCs auxquels les groupes de sécurité sont associés.
  - Il existe une passerelle de transit entre celles VPCs auxquelles les groupes de sécurité sont associés.
- Vous pouvez faire référence à un groupe de sécurité dans la règle sortante si l'une des conditions suivantes est vraie :
  - Les groupes de sécurité sont associés au même VPC.
  - Il existe une connexion d'appairage entre ceux VPCs auxquels les groupes de sécurité sont associés.
- Aucune règle du groupe de sécurité référencé n'est ajoutée au groupe de sécurité le référençant.
- Concernant les règles entrantes, les instances EC2 associées à un groupe de sécurité peuvent recevoir le trafic entrant des adresses IP privées issues des interfaces réseau pour les instances EC2 associées au groupe de sécurité référencé.

- Concernant les règles sortantes, les instances EC2 associées à un groupe de sécurité peuvent envoyer le trafic sortant aux adresses IP privées issues des interfaces réseau pour les instances EC2 associées au groupe de sécurité référencé.
- Nous ne fournissons pas d'autorisation par rapport aux groupes de sécurité référencés dans les actions suivantes : `AuthorizeSecurityGroupIngress`, `AuthorizeSecurityGroupEgress`, `RevokeSecurityGroupIngress`, et `RevokeSecurityGroupEgress`. Nous vérifions uniquement si le groupe de sécurité existe. Il en résulte ce qui suit :
  - La spécification du groupe de sécurité référencé dans les politiques IAM pour ces actions n'a aucun effet.
  - Lorsqu'un groupe de sécurité référencé appartient à un autre compte, le compte propriétaire ne reçoit aucun CloudTrail événement lié à ces actions.

Limitation

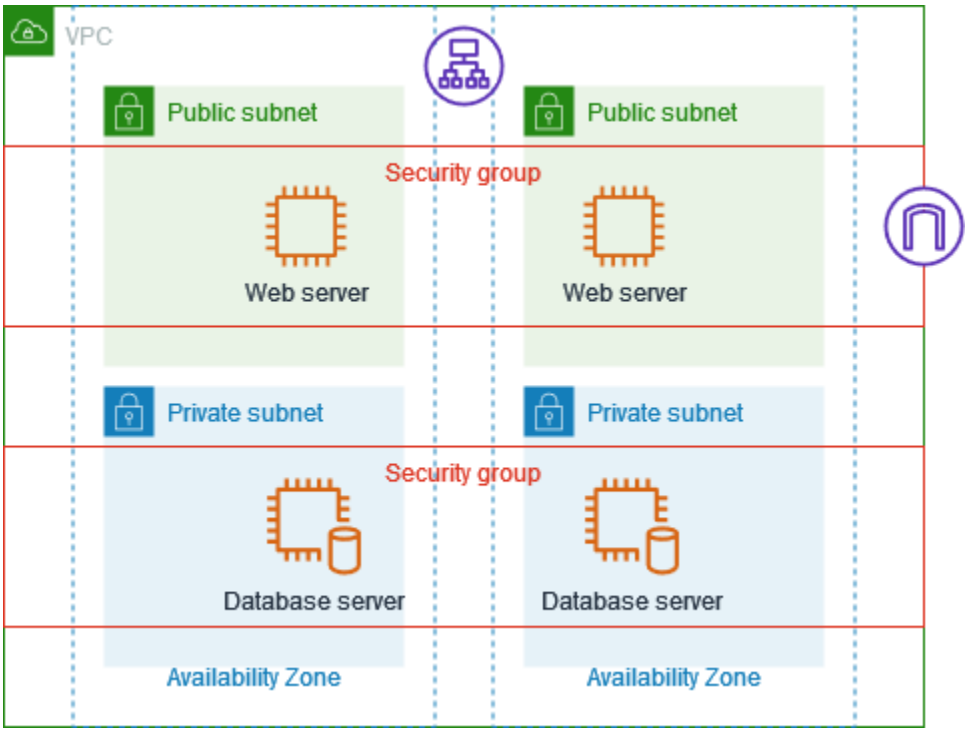
Si vous configurez des acheminements pour transférer le trafic entre deux instances de sous-réseaux différents via un dispositif middlebox, vous devez vous assurer que les groupes de sécurité des deux instances autorisent le trafic à transiter entre les instances. Le groupe de sécurité de chaque instance 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 de plus amples informations, veuillez consulter 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. Pour plus d'informations, consultez Mise à jour de vos groupes de sécurité pour référencer des groupes de sécurité pairs dans le Guide d'appairage Amazon VPC.

Si vous avez une règle de groupe de sécurité qui fait référence à un groupe de sécurité dans un VPC pair ou un VPC partagé, et si le groupe de sécurité du VPC partagé est supprimé ou si la connexion d'appairage de VPC est supprimée, la règle du 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.

Groupes de sécurité par défaut pour votre VPCs

Votre groupe de sécurité par défaut VPCs et tous ceux VPCs 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

Le tableau ci-après décrit les règles entrantes par défaut pour un groupe de sécurité par défaut.

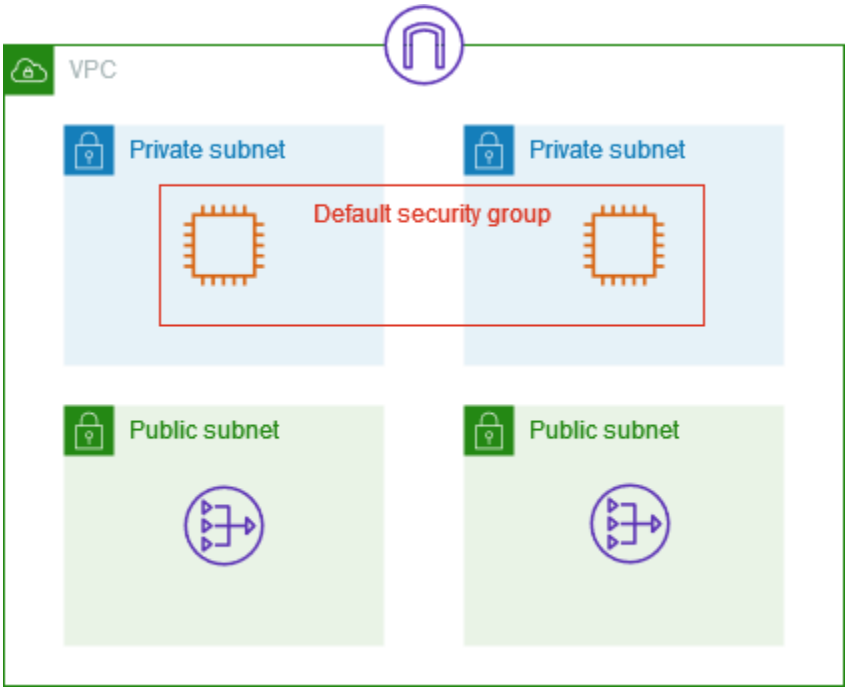
Source	Protocole	Plage de ports	Description
sg-1234567890abcdef0	Tous	Tous	Autorise le trafic entrant à partir de toutes les ressources attribuées à ce groupe de sécurité. La source est l'ID de ce groupe de sécurité.

Le tableau ci-après décrit les règles sortantes par défaut pour un groupe de sécurité par défaut.

Destination	Protocole	Plage de ports	Description
0.0.0.0/0	Tous	Tous	Autorise tout le IPv4 trafic sortant.
::/0	Tous	Tous	Autorise tout le IPv6 trafic sortant. Cette règle est ajoutée uniquement si votre VPC est associé à un bloc IPv6 CIDR.

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.



Créer un groupe de sécurité pour votre VPC

Votre cloud privé virtuel (VPC) est associé à un groupe de sécurité par défaut. Vous pouvez créer des groupes de sécurité supplémentaires. Les groupes de sécurité ne peuvent être utilisés qu'avec les ressources du VPC dans lesquels ils sont créés.

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. Vous pouvez ajouter des règles au moment de créer un groupe de sécurité ou ultérieurement. Pour de plus amples informations, veuillez consulter Règles des groupes de sécurité.

Autorisations nécessaires

Avant de commencer, vérifiez que vous disposez des autorisations requises. Pour plus d'informations, consultez les ressources suivantes :

- Gérer les groupes de sécurité
- Gérer les règles de groupe de sécurité

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. Pour VPC, choisissez le VPC dans lequel vous souhaitez créer les ressources auxquelles associer le groupe de sécurité.
6. (Facultatif) Pour ajouter des règles entrantes, choisissez Règles entrantes. Pour chaque règle, choisissez Ajouter une règle et spécifiez le protocole, le port et la source. Pour de plus amples informations, veuillez consulter Configurer des règles de groupe de sécurité.
7. (Facultatif) Pour ajouter des règles sortantes, choisissez Règles sortantes. Pour chaque règle, choisissez Ajouter une règle et spécifiez le protocole, le port et la destination.
8. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
9. Sélectionnez Create security group (Créer un groupe de sécurité).

Pour créer un groupe de sécurité à l'aide du AWS CLI

Utilisez la commande create-security-group.

Vous pouvez également créer un nouveau groupe de sécurité en copiant un groupe de sécurité existant. Lorsque vous copiez un groupe de sécurité, nous ajoutons automatiquement les mêmes règles entrantes et sortantes qu'au groupe de sécurité d'origine et utilisons le même VPC que le groupe de sécurité d'origine. Vous pouvez saisir un nom et une description pour le nouveau groupe de sécurité. Vous pouvez éventuellement choisir un autre VPC et modifier les règles entrantes et sortantes selon vos besoins. Cependant, vous ne pouvez pas copier un groupe de sécurité d'une région vers une autre région.

Pour créer un groupe de sécurité basé sur un groupe de sécurité existant

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 un groupe de sécurité.
4. Choisissez Actions, Copier vers un nouveau groupe de sécurité.
5. Saisissez un nom et une description pour le groupe de sécurité.
6. (Facultatif) Choisissez un autre VPC si nécessaire.

7. (Facultatif) Ajoutez, supprimez ou modifiez les règles du groupe de sécurité en fonction de vos besoins.
8. Sélectionnez Create security group (Créer un groupe de sécurité).

Configurer des règles de groupe de sécurité

Après avoir créé un groupe de sécurité, vous pouvez ajouter, mettre à jour et supprimer ses règles de groupe de sécurité. Lorsque vous ajoutez, supprimez ou mettez à jour une règle, la modification est automatiquement appliquée aux ressources associées au groupe de sécurité.

Autorisations requises

Avant de commencer, vérifiez que vous disposez des autorisations requises. Pour de plus amples informations, veuillez consulter Gérer les règles de groupe de sécurité.

Protocoles et ports

- Avec la console, lorsque vous sélectionnez un type prédéfini, le Protocole et la Plage de ports sont spécifiés à votre place. Pour saisir une plage de ports, vous devez sélectionner l'un des types personnalisés suivants : TCP personnalisé ou UDP personnalisé.
- Avec le AWS CLI, vous pouvez ajouter une seule règle avec un seul port à l'aide des `--port` options `--protocol` et. Pour ajouter plusieurs règles, ou une règle avec une plage de ports, utilisez plutôt l'option `--ip-permissions`.

Sources et destinations

- Avec la console, vous pouvez spécifier les éléments suivants comme sources pour les règles entrantes ou destinations pour les règles sortantes :
  - Personnalisé : bloc d' IPv4 adresse CIDR, bloc d' IPv6 adresse CIDR, groupe de sécurité ou liste de préfixes.
  - N'importe où- IPv4 — Le bloc CIDR 0.0.0.0/0 IPv4 .
  - N'importe où- IPv6 — Le bloc IPv6 CIDR : :/0.
  - Mon adresse IP — L' IPv4 adresse publique de votre ordinateur local.
- Avec le AWS CLI, vous pouvez spécifier un bloc IPv4 CIDR à l'aide de l'`--cidr`option ou un groupe de sécurité à l'aide de l'`--source-group`option. Pour spécifier une liste de préfixes ou un bloc IPv6 CIDR, utilisez l'`--ip-permissions`option.

> **Warning**
>
> Si vous choisissez Anywhere- IPv4, vous autorisez le trafic provenant de toutes les IPv4 adresses. Si vous choisissez Anywhere- IPv6, vous autorisez le trafic provenant de toutes les IPv6 adresses. Il est recommandé d'autoriser uniquement les plages d'adresses IP spécifiques ayant besoin d'accéder à vos ressources.

Pour configurer des règles 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. Pour modifier les règles entrantes, choisissez Modifier les règles entrantes dans Actions ou dans l'onglet Règles entrantes.
   a. Pour ajouter une règle, choisissez Ajouter une règle et entrez le type, le protocole, le port et la source de la règle.

      Si le type est TCP ou UDP, vous devez entrer 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 tous les autres types, le protocole et la plage de ports sont configurés automatiquement.
   b. Pour mettre à jour une règle, modifiez son protocole, sa description et sa source selon vos besoins. Toutefois, vous ne pouvez pas modifier le type de source. Par exemple, si la source est un bloc d'adresse IPv4 CIDR, vous ne pouvez pas spécifier de bloc d'adresse IPv6 CIDR, de liste de préfixes ou de groupe de sécurité.
   c. Pour supprimer une règle, cliquez sur le bouton Supprimer.
5. Pour modifier les règles sortantes, choisissez Modifier les règles sortantes dans Actions ou dans l'onglet Règles sortantes.
   a. Pour ajouter une règle, choisissez Ajouter une règle et entrez le type, le protocole, le port et la destination de la règle. Vous pouvez également saisir une description facultative.

      Si le type est TCP ou UDP, vous devez entrer 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 tous les autres types, le protocole et la plage de ports sont configurés automatiquement.

b. Pour mettre à jour une règle, modifiez son protocole, sa description et sa source selon vos besoins. Toutefois, vous ne pouvez pas modifier le type de source. Par exemple, si la source est un bloc d'adresse IPv4 CIDR, vous ne pouvez pas spécifier de bloc d'adresse IPv6 CIDR, de liste de préfixes ou de groupe de sécurité.

c. Pour supprimer une règle, cliquez sur le bouton Supprimer.

6. Sélectionnez Enregistrer les règles.

Pour configurer les règles des groupes de sécurité à l'aide du AWS CLI

- Ajouter — Utilisez les authorize-security-group-egresscommandes authorize-security-group-ingresset.
- Supprimer — Utilisez les revoke-security-group-egresscommandes revoke-security-group-ingresset.
- Modifier — Utilisez les modify-security-group-rulescommandes update-security-group-rule-descriptions-ingress et -descriptions-egress. update-security-group-rule

Supprimer un groupe de sécurité

Lorsque vous avez fini d'utiliser un groupe de sécurité que vous avez créé, vous pouvez le supprimer.

Exigences

- Le groupe de sécurité ne peut être associé à aucune ressource.
- Le groupe de sécurité ne peut être référencé par une règle dans un autre groupe de sécurité.
- Le groupe de sécurité ne peut être le groupe de sécurité par défaut du VPC.

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.

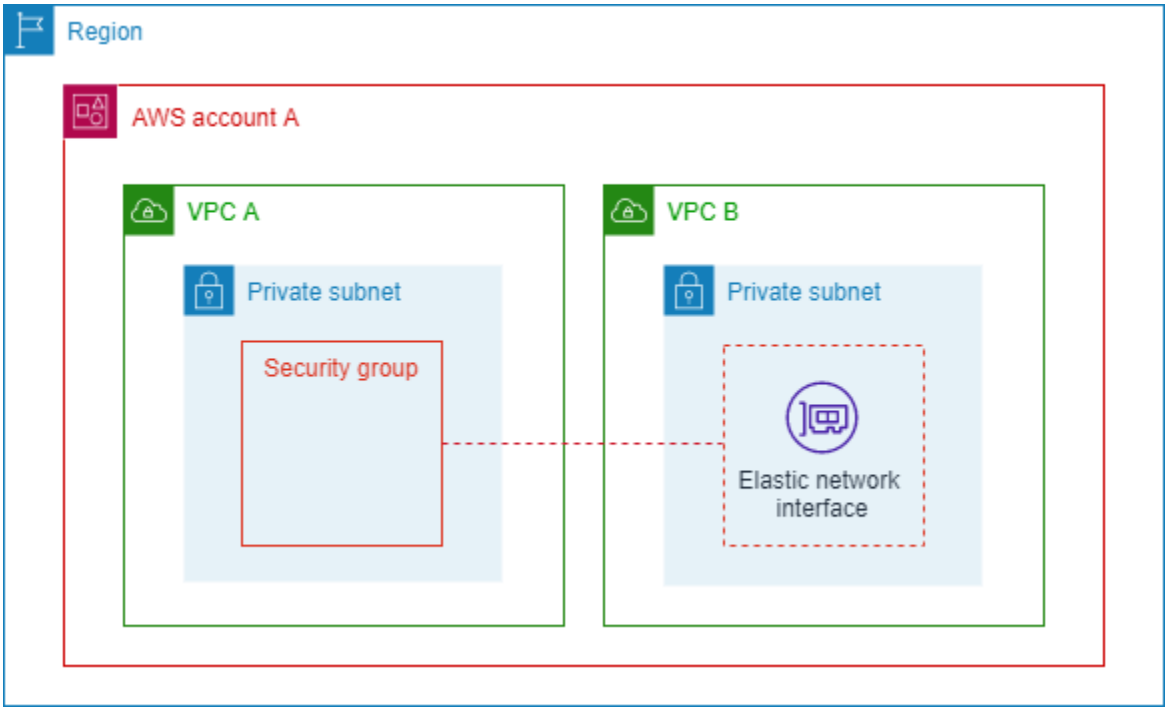
4. Si vous avez sélectionné plusieurs groupes de sécurité, vous êtes invité à confirmer. Si certains groupes de sécurité ne peuvent pas être supprimés, nous affichons le statut de chaque groupe de sécurité, qui indique s'il sera supprimé. Pour confirmer la suppression, saisissez Supprimer.
5. Sélectionnez Delete (Supprimer).

Pour supprimer un groupe de sécurité à l'aide du AWS CLI

Utilisez la commande delete-security-group.

Associer des groupes de sécurité à plusieurs VPCs

Si vous avez des charges de travail exécutées en plusieurs groupes VPCs qui partagent les mêmes exigences de sécurité réseau, vous pouvez utiliser la fonctionnalité Associations VPC de groupe de sécurité pour associer un groupe de sécurité à VPCs plusieurs groupes dans la même région. Cela vous permet de gérer et de gérer les groupes de sécurité en un seul endroit pour plusieurs VPCs groupes de votre compte.



Le schéma ci-dessus montre le AWS compte A contenant deux VPCs comptes. Chacun d'entre eux VPCs a des charges de travail exécutées dans un sous-réseau privé. Dans ce cas, les charges de travail des sous-réseaux des VPC A et B partagent les mêmes exigences en matière de trafic réseau. Le compte A peut donc utiliser la fonctionnalité Associations de VPC et de groupes de sécurité pour associer le groupe de sécurité du VPC A au VPC B. Toutes les mises à jour apportées au groupe de

sécurité associé sont automatiquement appliquées au trafic des charges de travail du sous-réseau du VPC B.

Exigences relatives à la fonctionnalité Associations de VPC et de groupes de sécurité

- Vous devez être le propriétaire du VPC ou disposer de l'un des sous-réseaux VPC partagé avec vous pour associer un groupe de sécurité au VPC.
- Le VPC et le groupe de sécurité doivent se trouver dans la même AWS région.
- Vous ne pouvez pas associer un groupe de sécurité par défaut à un autre VPC ou associer un groupe de sécurité à un VPC par défaut.
- Le propriétaire du groupe de sécurité ainsi que le propriétaire du VPC peuvent consulter les associations de VPC et de groupes de sécurité.

Services qui prennent en charge cette fonctionnalité

- Amazon API Gateway (REST APIs uniquement)
- AWS Auto Scaling
- CloudFormation
- Amazon EC2
- Amazon EFS
- Amazon EKS
- Amazon FSx
- AWS PrivateLink
- Amazon Route 53
- Elastic Load Balancing
  - Application Load Balancer
  - Network Load Balancer

Associer un groupe de sécurité à un autre VPC

Cette section explique comment utiliser le AWS Management Console et AWS CLI pour associer un groupe de sécurité à VPCs.

AWS Management Console

Pour associer un groupe de sécurité à un autre VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, sélectionnez Groupes de sécurité.
3. Choisissez un groupe de sécurité pour afficher les détails.
4. Cliquez sur l'onglet Associations de VPC.
5. Choisissez Associate VPC (Associer un VPC).
6. Sous ID de VPC, choisissez un VPC à associer au groupe de sécurité.
7. Choisissez Associate VPC (Associer un VPC).

Command line

Pour associer un groupe de sécurité à un autre VPC

1. Créez une association VPC avec. associate-security-group-vpc
2. Vérifiez le statut d'une association VPC avec describe-security-group-vpc-associations et attendez que le statut soit le même. `associated`

Le VPC est désormais associé au groupe de sécurité.

Une fois que vous avez associé le VPC au groupe de sécurité, vous pouvez, par exemple, lancer une instance dans le VPC et choisir ce nouveau groupe de sécurité ou référencer ce groupe de sécurité dans une règle de groupe de sécurité existante.

Dissocier un groupe de sécurité d'un autre VPC

Cette section explique comment utiliser le AWS Management Console et AWS CLI pour dissocier un groupe de VPCs sécurité. Vous pouvez le faire si votre objectif est de supprimer le groupe de sécurité. Les groupes de sécurité ne peuvent être supprimés s'ils sont associés. Vous ne pouvez dissocier un groupe de sécurité que s'il n'existe aucune interface réseau dans le VPC associé utilisant ce groupe de sécurité.

AWS Management Console

Pour dissocier un groupe de sécurité d'un VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, sélectionnez Groupes de sécurité.
3. Choisissez un groupe de sécurité pour afficher les détails.
4. Cliquez sur l'onglet Associations de VPC.
5. Choisissez Dissocier le VPC.
6. Sous ID de VPC, choisissez un VPC à dissocier du groupe de sécurité.
7. Choisissez Dissocier le VPC.
8. Consultez l'état de la dissociation dans l'onglet Associations de VPC et attendez que l'état soit `disassociated`.

Command line

Pour dissocier un groupe de sécurité d'un VPC

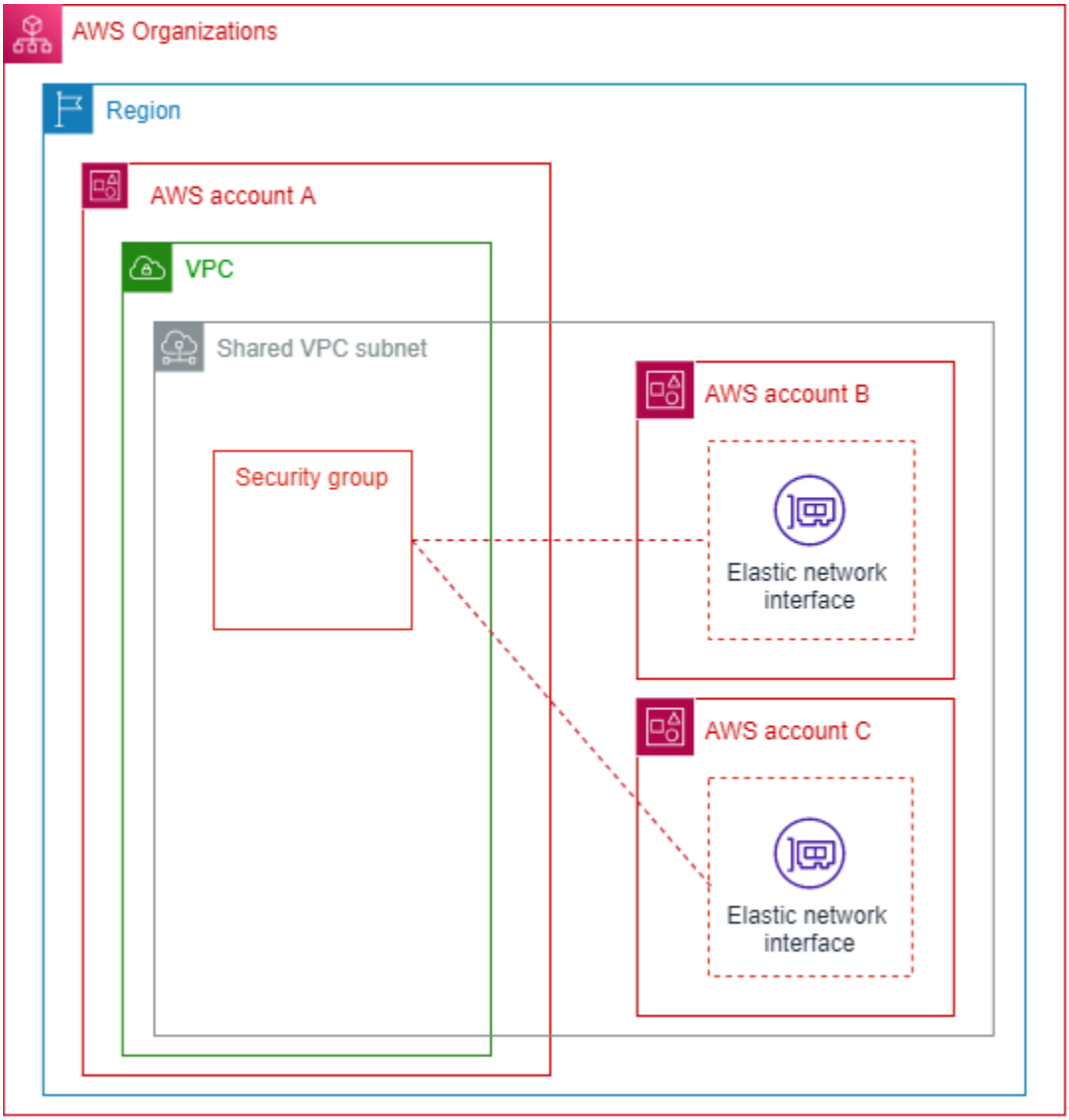
1. Dissocier une association VPC avec. disassociate-security-group-vpc
2. Vérifiez l'état d'une dissociation d'un VPC avec describe-security-group-vpc-associations et attendez que ce soit le cas. `disassociated`

Le VPC est désormais dissocié du groupe de sécurité.

Partagez des groupes de sécurité avec des AWS Organisations

La fonctionnalité de groupe de sécurité partagé vous permet de partager un groupe de sécurité avec d'autres comptes AWS Organizations au sein de la même AWS région et de rendre le groupe de sécurité disponible pour être utilisé par ces comptes.

Le schéma suivant montre comment vous pouvez utiliser la fonctionnalité de groupe de sécurité partagé pour simplifier la gestion des groupes de sécurité entre les comptes de vos AWS Organisations :



Ce diagramme montre trois comptes qui font partie de la même organisation. Le compte A partage un sous-réseau VPC avec les comptes B et C. Le compte A partage le groupe de sécurité avec les comptes B et C à l'aide de la fonctionnalité Groupe de sécurité partagé. Les comptes B et C utilisent ensuite ce groupe de sécurité lorsqu'ils lancent des instances dans le sous-réseau partagé. Cela permet au compte A de gérer le groupe de sécurité : toute mise à jour du groupe de sécurité s'applique aux ressources que les comptes B et C exécutent dans le sous-réseau VPC partagé.

Exigences relatives à la fonctionnalité Groupe de sécurité partagé

- Cette fonctionnalité n'est disponible que pour les comptes d'une même organisation dans AWS Organizations. Le partage des ressources doit être activé dans AWS Organizations.
- Le compte qui partage le groupe de sécurité doit posséder à la fois le VPC et le groupe de sécurité.

- Vous ne pouvez pas partager de groupes de sécurité par défaut.
- Vous ne pouvez pas partager les groupes de sécurité qui se trouvent dans un VPC par défaut.
- Les comptes participants peuvent créer des groupes de sécurité dans un VPC partagé, mais ils ne peuvent pas partager ces groupes de sécurité.
- Un ensemble minimal d'autorisations est requis pour qu'un principal IAM puisse partager un groupe de sécurité avec AWS RAM. Utilisez les politiques IAM gérées `AmazonEC2FullAccess` et `AWSResourceAccessManagerFullAccess` pour vous assurer que vos principaux IAM disposent des autorisations requises pour partager et utiliser des groupes de sécurité partagés. Si vous utilisez une politique IAM personnalisée, les actions `c2:PutResourcePolicy` et `ec2:DeleteResourcePolicy` sont requises. Il s'agit d'actions IAM avec autorisation uniquement. Si ces autorisations ne sont pas accordées à un principal IAM, une erreur se produit lors de la tentative de partage du groupe de sécurité à l'aide d' AWS RAM.

Services qui prennent en charge cette fonctionnalité

- Amazon API Gateway
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Amazon EMR
- Amazon FSx
- Amazon ElastiCache
- AWS Elastic Beanstalk
- AWS Glue
- Amazon MQ
- Amazon SageMaker AI
- Elastic Load Balancing
  - Application Load Balancer
  - Network Load Balancer

Manière dont cette fonctionnalité affecte les quotas existants

Les quotas des groupes de sécurité s'appliquent. Cependant, en ce qui concerne le quota « Groupes de sécurité par interface réseau », si un participant utilise à la fois des groupes détenus et partagés sur une interface réseau Elastic (ENI), le quota minimal du propriétaire et du participant s'applique.

Exemple pour montrer la manière dont le quota est affecté par cette fonctionnalité :

- Quota du compte propriétaire : 4 groupes de sécurité par interface
- Quota du compte participant : 5 groupes de sécurité par interface.
- Le propriétaire partage les groupes SG-O1, SG-O2, SG-O3, SG-O4, SG-O5 avec le participant. Le participant possède déjà ses propres groupes dans le VPC : SG-P1, SG-P2, SG-P3, SG-P4, SG-P5.
- Si le participant crée une ENI et utilise uniquement ses propres groupes, il peut associer les 5 groupes de sécurité (SG-P1, SG-P2, SG-P3, SG-P4, SG-P5), car c'est son quota.
- Si le participant crée une ENI et utilise des groupes partagés, il ne peut associer que 4 groupes au maximum. Dans ce cas, le quota d'une telle ENI est le minimum des quotas du propriétaire et du participant. Les configurations valides possibles se présente comme suit :
  - SG-O1, SG-P1, SG-P2, SG-P3
  - SG-O1, SG-O2, SG-O3, SG-O4

Partager un groupe de sécurité

Cette section explique comment utiliser AWS Management Console et pour AWS CLI partager un groupe de sécurité avec d'autres comptes de votre organisation.

AWS Management Console

Pour partager un groupe de sécurité

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, sélectionnez Groupes de sécurité.
3. Choisissez un groupe de sécurité pour afficher les détails.
4. Cliquez sur l'onglet Sharing (Partager) .
5. Choisissez Partager un groupe de sécurité.
6. Choisissez Créer une ressource. Par conséquent, la AWS RAM console s'ouvre dans laquelle vous allez créer le partage de ressources pour le groupe de sécurité.
7. Saisissez un Nom pour la ressource partagée.

8. Sous Ressources – facultatif, choisissez Groupes de sécurité.
9. Sélectionnez un groupe de sécurité. Le groupe de sécurité ne peut pas être un groupe de sécurité par défaut et ne peut pas être associé au VPC par défaut.
10. Choisissez Suivant.
11. Passez en revue les actions que les principaux seront autorisés à effectuer, puis cliquez sur Suivant.
12. Sous Principaux – facultatif, sélectionnez Autoriser le partage uniquement au sein de votre organisation.
13. Sous Principaux, sélectionnez l'un des types de principaux suivants et saisissez les numéros appropriés :

    - AWS compte : numéro de compte d'un compte au sein de votre organisation.
    - Organisation : The AWS Organizations ID.
    - Unité d'organisation (UO) : ID d'une UO de l'organisation.
    - Rôle IAM : ARN d'un rôle IAM. Le compte qui a créé le rôle doit être membre de la même organisation que le compte qui a créé ce partage de ressources.
    - Utilisateur IAM : ARN d'un utilisateur IAM. Le compte qui a créé l'utilisateur doit être membre de la même organisation que le compte qui a créé ce partage de ressources.
    - Principal de service : vous ne pouvez pas partager un groupe de sécurité avec un principal de service.
14. Choisissez Ajouter.
15. Choisissez Suivant.
16. Choisissez Créer une ressource.
17. Sous Ressources partagées, attendez que l'état soit `Associated`. Si l'association d'un groupe de sécurité échoue, cela peut être dû à l'une des restrictions répertoriées ci-dessus. Consultez les détails du groupe de sécurité et l'onglet Partage de la page de détails pour voir les messages indiquant les raisons pour lesquelles un groupe de sécurité ne peut pas être partagé.
18. Revenez à la liste des groupes de sécurité de la console VPC.
19. Choisissez le groupe de sécurité que vous avez partagé.
20. Cliquez sur l'onglet Sharing (Partager) . Votre AWS RAM ressource doit y être visible. Si ce n'est pas le cas, la création du partage de ressources a peut-être échoué et vous devrez peut-être la recréer.

Command line

Pour partager un groupe de sécurité

1. Vous devez d'abord créer un partage de ressources pour le groupe de sécurité avec lequel vous souhaitez partager AWS RAM. Pour savoir comment créer un partage de ressources à AWS RAM l'aide du AWS CLI, voir Création d'un partage de ressources AWS RAM dans le guide de l'AWS RAM utilisateur.
2. Pour afficher les associations de partage de ressources créées, utilisez get-resource-share-associations.

Le groupe de sécurité est désormais partagé. Vous pouvez sélectionner le groupe de sécurité lors du lancement d'une instance EC2 dans un sous-réseau partagé au sein du même VPC.

Arrêter de partager un groupe de sécurité

Cette section explique comment utiliser AWS Management Console et pour arrêter de AWS CLI partager un groupe de sécurité avec d'autres comptes de votre organisation.

AWS Management Console

Pour arrêter de partager un groupe de sécurité

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, sélectionnez Groupes de sécurité.
3. Choisissez un groupe de sécurité pour afficher les détails.
4. Cliquez sur l'onglet Sharing (Partager) .
5. Choisissez un partage de ressources de groupe de sécurité, puis sélectionnez Arrêter le partage.
6. Choisissez Oui, arrêter le partage.

Command line

Pour arrêter de partager un groupe de sécurité

Supprimez la ressource partagée avec delete-resource-share.

Le groupe de sécurité n’est plus partagé. Lorsque le propriétaire cesse de partager un groupe de sécurité, les règles suivantes doivent être respectées :

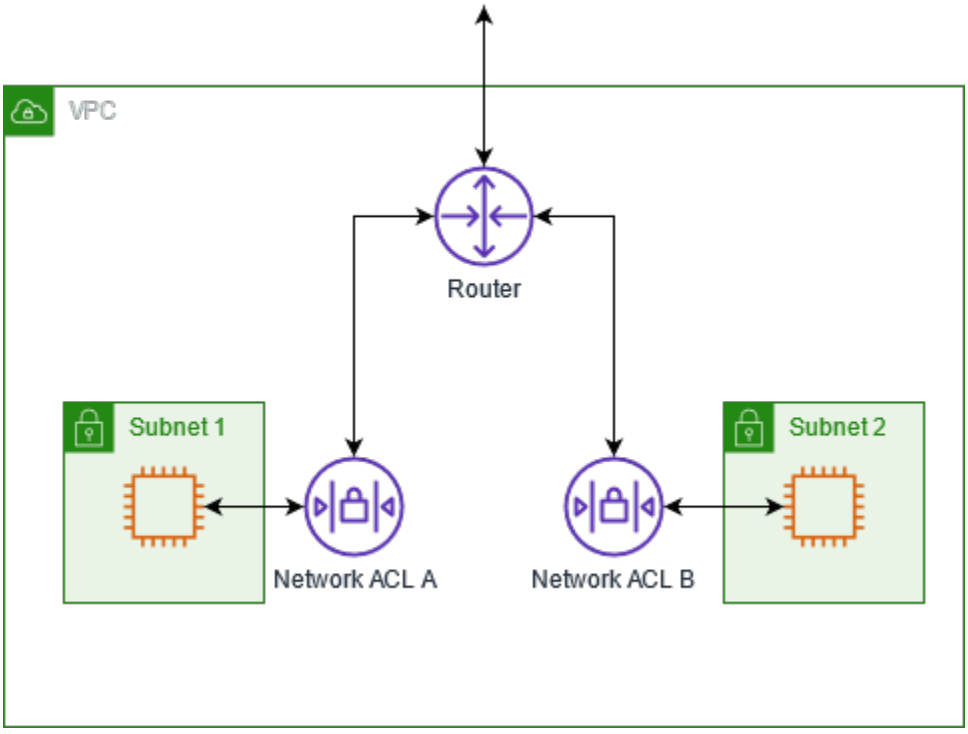
- Les Elastic Network Interfaces (ENIs) des participants existants continuent de recevoir toutes les mises à jour des règles des groupes de sécurité apportées aux groupes de sécurité non partagés. L’annulation du partage empêche uniquement le participant de créer de nouvelles associations avec le groupe non partagé.
- Les participants ne peuvent plus associer le groupe de sécurité non partagé à un groupe qui ENIs leur appartient.
- Les participants peuvent décrire et supprimer ceux ENIs qui sont toujours associés à des groupes de sécurité non partagés.
- Si les participants sont toujours ENIs associés au groupe de sécurité non partagé, le propriétaire ne peut pas supprimer le groupe de sécurité non partagé. Le propriétaire ne peut supprimer le groupe de sécurité qu'une fois que les participants ont dissocié (supprimé) le groupe de sécurité de tous leurs ENIs membres.
- Les participants ne peuvent pas lancer de nouvelles instances EC2 à l’aide d’une ENI associée à un groupe de sécurité non partagé.

Contrôler le trafic des sous-réseaux à l’aide de listes de contrôle d’accès 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.

Il n'y a pas de frais supplémentaires pour l'utilisation du réseau ACLs.

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 plus d'informations sur les différences entre les groupes de sécurité et le réseau ACLs, consultezComparez les groupes de sécurité et le réseau ACLs.

Table des matières

Principes de base des listes ACL réseau

Voici les informations de base à connaître sur le réseau ACLs avant de commencer.

Associations d'ACL 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 ACL réseau, le sous-réseau est automatiquement associé à l'ACL réseau par défaut.
- 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.
- 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.

Règles des listes ACL réseau

- Une ACL réseau possède des règles entrantes et des règles sortantes. Il existe des quotas (ou limites) quant au nombre de règles que vous pouvez avoir par ACL réseau. 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.
- NACLs sont apatrides, ce qui signifie que les informations relatives au trafic précédemment envoyé ou reçu ne sont pas enregistrées. 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.

Limitations

- Il existe des quotas (également appelés limites) pour le réseau ACLs. Pour de plus amples informations, veuillez consulter Réseau ACLs.

- Le réseau ne ACLs peut 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 AmazonProvided DNS). Afin de filtrer les demandes DNS via le résolveur Route 53, vous pouvez activer le pare-feu DNS du résolveur Route 53.
- Le réseau ne ACLs peut 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.
- Le réseau ACLs ne filtre pas le trafic à destination et en provenance des sites 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

Règles des listes ACL réseau

Vous pouvez ajouter ou supprimer des règles de l'ACL réseau par défaut, ou créer un réseau supplémentaire ACLs 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.

Pour obtenir des exemples de règles, consultez la section the section called “Exemple : contrôler l'accès aux instances dans un sous-réseau”.

Considérations

- Il existe des quotas (également appelés limites) pour le nombre de règles par réseau ACLs. Pour de plus amples informations, veuillez consulter Quotas Amazon VPC.
- 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. Les modifications entrent en vigueur après une courte période.
- 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`.
- Vous pouvez ajouter une règle de refus lorsque vous devez ouvrir une grande plage de ports, mais que vous souhaitez refuser certains ports de cette plage. Assurez-vous d'attribuer à la règle de refus un numéro inférieur à celui de la règle qui autorise le trafic de la grande plage de ports.
- Soyez prudent si vous ajoutez des règles dans une ACL réseau et en supprimez de l'ACL réseau en même temps. Si vous supprimez des règles entrantes ou sortantes, puis ajoutez plus de nouvelles entrées que le nombre autorisé (voir 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 tout accès à vos VPC ou depuis ceux-ci.

ACL réseau par défaut d'un VPC

Votre cloud privé virtuel (VPC) est automatiquement associé à une ACL réseau par défaut. L'ACL réseau par défaut est configurée pour autoriser l'ensemble du trafic à entrer et sortir des sous-réseaux auxquels elle est associée. Chaque ACL réseau inclut également des règles dont le numéro est un astérisque (*). Ces règles permettent de s'assurer qu'un paquet sera refusé s'il ne correspond à aucune des autres règles numérotées.

Vous pouvez modifier une ACL réseau par défaut en ajoutant des règles ou en supprimant les règles numérotées par défaut. Vous ne pouvez pas supprimer une règle dont le numéro est un astérisque.

Règles entrantes par défaut

Le tableau suivant illustre les règles entrantes par défaut associées à une ACL réseau par défaut. Les règles pour ne IPv6 sont ajoutées que si vous créez le VPC avec un bloc d'adresse IPv6 CIDR associé ou si vous associez un bloc d'adresse IPv6 CIDR au VPC. Toutefois, si vous avez modifié les règles entrantes d'une ACL réseau par défaut, nous n'ajoutons pas la règle qui autorise tout le IPv6 trafic entrant lorsque vous associez un IPv6 bloc au VPC.

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser
100	Tout IPv4 le trafic	Tous	Tous	0.0.0.0/0	AUTORISER
101	Tout IPv6 le trafic	Tous	Tous	::/0	AUTORISER
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REJETER
*	Tout IPv6 le trafic	Tous	Tous	::/0	REJETER

Règles sortantes par défaut

Le tableau suivant illustre les règles sortantes par défaut associées à une ACL réseau par défaut. Les règles pour ne IPv6 sont ajoutées que si vous créez le VPC avec un bloc d'adresse IPv6 CIDR associé ou si vous associez un bloc d'adresse IPv6 CIDR au VPC. Toutefois, si vous avez modifié les règles sortantes d'une ACL réseau par défaut, nous n'ajoutons pas la règle qui autorise tout le IPv6 trafic sortant lorsque vous associez un IPv6 bloc au VPC.

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/ Refuser
100	Tout le trafic	Tous	Tous	0.0.0.0/0	AUTORISER

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/ Refuser
101	Tout IPv6 le trafic	Tous	Tous	::/0	AUTORISER
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REJETER
*	Tout IPv6 le trafic	Tous	Tous	::/0	REJETER

Réseau personnalisé ACLs pour votre VPC

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. Pour de plus amples informations, veuillez consulter the section called "Créer une ACL réseau".

Chaque ACL réseau inclut une règle entrante par défaut et une règle sortante par défaut dont le numéro est un astérisque (*). Ces règles permettent de s'assurer qu'un paquet sera refusé s'il ne correspond à aucune des autres règles.

Vous pouvez modifier une ACL réseau en ajoutant ou en supprimant des règles. Vous ne pouvez pas supprimer une règle dont le numéro est un astérisque.

Pour chaque règle que vous ajoutez, une règle entrante ou sortante autorisant le trafic de réponse doit exister. Pour savoir comment sélectionner la plage de ports éphémères appropriée, consultez la section Ports éphémères.

Exemples de règles entrantes

Le tableau suivant contient des exemples de règles entrantes pour une ACL réseau. Les règles pour ne IPv6 sont ajoutées que si le VPC est associé à un bloc IPv6 CIDR. IPv4 et IPv6 le trafic sont évalués séparément. Par conséquent, aucune des règles relatives au IPv4 trafic ne s'applique au IPv6 trafic. Vous pouvez ajouter IPv6 des règles à côté IPv4 des règles correspondantes ou les IPv6 ajouter après la dernière IPv4 règle.

Lorsqu'un paquet arrive dans le sous-réseau, nous l'évaluons par rapport aux règles entrantes de l'ACL réseau qui est associée au sous-réseau, en commençant par la règle possédant le numéro le plus bas. Supposons, par exemple, que IPv4 du trafic soit destiné au port HTTPS (443). Le paquet ne

correspond pas à la règle 100 ou 105. Il correspond à la règle 110, qui autorise le trafic à entrer dans le sous-réseau. Si le paquet avait été destiné au port 139 (NetBIOS), il ne correspondrait à aucune des règles numérotées, de sorte que la règle * pour le IPv4 trafic refuse finalement le paquet.

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 IPv4 adresse.
105	HTTP	TCP	80	::/0	AUTORISE	Autorise le trafic HTTP entrant depuis n'importe quelle IPv6 adresse.
110	HTTPS	TCP	443	0.0.0.0/0	AUTORISE	Autorise le trafic HTTPS entrant depuis n'importe quelle IPv4 adresse.
115	HTTPS	TCP	443	::/0	AUTORISE	Autorise le trafic HTTPS entrant depuis n'importe quelle IPv6 adresse.
120	SSH	TCP	22	*192.0.2.0 /24*	AUTORISE	Autorise le trafic SSH entrant depuis la plage d' IPv4 adresses publiques de votre réseau domestique (via la passerelle Internet).
140	TCP personnalisé	TCP	*32768-65535*	0.0.0.0/0	AUTORISE	Autorise le IPv4 trafic entrant en provenance d'Internet (pour les

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser	Commentaires
						demandes provenant du sous-réseau).
145	TCP personnalisé	TCP	32768-65535	::/0	AUTORISE	Autorise le IPv6 trafic entrant en provenance d'Internet (pour les demandes provenant du sous-réseau).
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REJETER	Refuse tout le IPv4 trafic entrant qui n'est pas déjà traité par une règle précédente (non modifiable).
*	Tout le trafic	Tous	Tous	::/0	REJETER	Refuse tout le IPv6 trafic entrant qui n'est pas déjà traité par une règle précédente (non modifiable).

Exemples de règles sortantes

Le tableau suivant contient des exemples de règles sortantes pour une ACL réseau personnalisée. Les règles pour ne IPv6 sont ajoutées que si le VPC est associé à un bloc IPv6 CIDR. IPv4 et IPv6 le trafic sont évalués séparément. Par conséquent, aucune des règles relatives au IPv4 trafic ne s'applique au IPv6 trafic. Vous pouvez ajouter IPv6 des règles à côté IPv4 des règles correspondantes ou les IPv6 ajouter après la dernière IPv4 règle.

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/ Refuser	Commentaires
100	HTTP	TCP	80	0.0.0.0/0	AUTORISE	Autorise le trafic IPv4 HTTP sortant du

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/ Refuser	Commentaires
						sous-réseau vers Internet.
105	HTTP	TCP	80	::/0	AUTORISE	Autorise le trafic IPv6 HTTP sortant du sous-réseau vers Internet.
110	HTTPS	TCP	443	0.0.0.0/0	AUTORISE	Autorise le trafic IPv4 HTTPS sortant du sous-réseau vers Internet.
115	HTTPS	TCP	443	::/0	AUTORISE	Autorise le trafic IPv6 HTTPS sortant du sous-réseau vers Internet.
120	TCP personnalisé	TCP	*1024-655 5*	*192.0.2.(/24*	AUTORISE	Autorise les réponses sortantes au trafic SSH depuis le réseau domestique.
140	TCP personnalisé	TCP	*32768-65 35*	0.0.0.0/0	AUTORISE	Autorise les IPv4 réponses sortantes aux clients sur Internet (par exemple, la diffusion de pages Web).

Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/ Refuser	Commentaires
145	TCP personnalisé	TCP	32768-65535	::/0	AUTORISE	Autorise les IPv6 réponses sortantes aux clients sur Internet (par exemple, la diffusion de pages Web).
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REJETER	Refuse tout le IPv4 trafic sortant qui n'est pas déjà traité par une règle précédente.
*	Tout le trafic	Tous	Tous	::/0	REJETER	Refuse tout le IPv6 trafic sortant qui n'est pas déjà traité par une règle précédente.

Ports éphémères

L'exemple de liste ACL réseau fourni dans la section précédente utilise la plage de ports éphémères 32768-65535. Toutefois, vous souhaiterez peut-être utiliser une plage différente pour votre réseau ACLs 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 ACL réseau doit comporter une règle entrante pour autoriser le trafic destiné aux ports éphémères propres au système d'exploitation de l'instance.

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.

Réseau personnalisé ACLs et autres AWS services

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 d'ACL réseau recommandées pour vos équilibreurs de charge et vos instances principales, consultez les sections relatives aux sujets suivants :

- Réseau ACLs pour votre Application Load Balancer
- Réseau ACLs pour votre Network Load Balancer
- Réseau ACLs pour votre Classic Load Balancer

Résolution des problèmes d'accessibilité

L'analyseur d'accessibilité est un outil d'analyse de configuration statique. Utilisez l'analyseur d'accessibilité pour analyser et déboguer l'accessibilité réseau entre deux ressources dans 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 des listes ACL réseau manquantes ou mal configurées.

Pour plus d'informations, reportez-vous au Guide de l'Analyseur d'accessibilité.

Path MTU Discovery et réseau ACLs

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.

En IPv4 effet, lorsqu'un hôte envoie un paquet supérieur à la MTU de l'hôte récepteur ou supérieur à la MTU d'un périphérique le long du chemin, l'hôte ou le périphérique récepteur abandonne le paquet, puis renvoie 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 IPv6 protocole ne prend pas en charge la fragmentation du 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 Unité de transmission maximale (MTU) du réseau pour votre instance EC2 dans le Guide de l'utilisateur Amazon EC2.

Créer une liste ACL réseau pour votre VPC

Les tâches suivantes vous montrent comment créer un ACL réseau, ajouter des règles à l'ACL réseau, puis associer l'ACL réseau à un sous-réseau.

Tâches

- Étape 1 : création d'une ACL réseau
- Étape 2 : ajout de règles

- Étape 3 : association d'un sous-réseau à une ACL réseau
- (Facultatif) Gérez le réseau ACLs à l'aide de Firewall Manager

Étape 1 : création d'une ACL réseau

Vous pouvez créer une liste ACL réseau personnalisée pour votre VPC. Les règles initiales d'une ACL réseau personnalisée bloquent l'ensemble du trafic entrant et sortant. La nouvelle ACL réseau personnalisée n'est associée à aucun sous-réseau par défaut et doit être explicitement associée à des sous-réseaux.

Pour créer une ACL 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 Network ACLs.
3. Sélectionnez Créer une ACL réseau.
4. (Facultatif) Dans Nom, saisissez un nom pour votre ACL réseau.
5. Dans VPC, sélectionnez le VPC.
6. (Facultatif) Dans Balises, sélectionnez Ajouter une balise et saisissez une clé de balise et une valeur de balise.
7. Sélectionnez Créer une ACL réseau.

Pour créer une ACL réseau à l'aide de la ligne de commande

- create-network-acl (AWS CLI)
- New-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Étape 2 : ajout de règles

Vous pouvez ajouter des règles qui autorisent ou refusent le trafic entrant ou sortant.

Nous traitons les règles dans l'ordre, en commençant par la règle possédant 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.

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 ACL 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 Network ACLs.
3. Sélectionnez l'ACL réseau.
4. Pour ajouter une règle entrante, procédez comme suit :
    a. Choisissez l'onglet Inbound rules (Règles entrantes).
    b. Sélectionnez Modifier les règles entrantes, Ajouter une nouvelle règle.
    c. Saisissez un numéro de règle qui n'est pas encore utilisé, un type, un protocole, une plage de ports et une source, et indiquez s'il faut autoriser ou refuser le trafic. Pour certains types, nous renseignons le protocole et le port à votre place. Si vous êtes invité à saisir une plage de ports, saisissez un numéro de port ou une plage de ports (par exemple, 49152-65535).

        Afin d'utiliser un protocole qui n'est pas répertorié, sélectionnez Protocole personnalisé pour le type, puis sélectionnez le protocole. Pour plus d'informations, consultez la page Protocol Numbers.
    d. Sélectionnez Enregistrer les modifications.
5. Pour ajouter une règle sortante, procédez comme suit :
    a. Choisissez l'onglet Outbound rules (Règles sortantes).
    b. Sélectionnez Modifier les règles sortantes, Ajouter une nouvelle règle.
    c. Saisissez un numéro de règle qui n'est pas encore utilisé, un type, un protocole, une plage de ports et une source, et indiquez s'il faut autoriser ou refuser le trafic. Pour certains types, nous renseignons le protocole et le port à votre place. Si vous êtes invité à saisir une plage de ports, saisissez un numéro de port ou une plage de ports (par exemple, 49152-65535).

        Afin d'utiliser un protocole qui n'est pas répertorié, sélectionnez Protocole personnalisé pour le type, puis sélectionnez le protocole. Pour plus d'informations, consultez la page Protocol Numbers.

d. Sélectionnez Enregistrer les modifications.

Pour ajouter une règle à une ACL réseau à l'aide de la ligne de commande

- create-network-acl-entry (AWS CLI)
- New-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Pour remplacer une règle dans une ACL réseau à l'aide de la ligne de commande

- replace-network-acl-entry (AWS CLI)
- Set-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Pour supprimer une règle d'une ACL réseau à l'aide de la ligne de commande

- delete-network-acl-entry (AWS CLI)
- Remove-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Étape 3 : association d'un sous-réseau à une 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 l'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.

(Facultatif) Gérez le réseau ACLs 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 des listes 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 ACL réseau Firewall Manager, vous pouvez configurer, surveiller et gérer les ensembles de règles minimaux que vous souhaitez définir sur le réseau ACLs que vous utilisez au sein de votre organisation à l'aide d'un seul compte administrateur. 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 du réseau ACLs pour les sous-réseaux concernés, et vous pouvez configurer Firewall Manager pour automatiser la correction des réseaux non conformes. ACLs

Pour plus d'informations, consultez les ressources suivantes dans le Manuel de développement de AWS Firewall Manager :

- AWS Firewall Manager prérequis
- Configuration des politiques ACL AWS Firewall Manager du réseau
- Utilisation des politiques d'ACL réseau avec Firewall Manager

Gestion des associations d'ACL réseau d'un VPC

Chaque sous-réseau est associé à une ACL réseau. Lorsque vous créez un sous-réseau pour la première fois, il est associé à l'ACL réseau par défaut du VPC. Vous pouvez créer une ACL réseau personnalisée et l'associer à un ou plusieurs sous-réseaux, en remplacement de l'association d'ACL réseau précédente.

Tâches

- Description de vos associations d'ACL réseau
- Modification des sous-réseaux associés à une ACL réseau
- Modification de l'ACL réseau associée à un sous-réseau

Description de vos associations d'ACL réseau

Vous pouvez décrire l'ACL réseau associée à un sous-réseau et vous pouvez également décrire les sous-réseaux associés à une ACL réseau.

Pour décrire l'ACL réseau associée à 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 panneau de navigation, choisissez Subnets (Sous-réseaux).
3. Sélectionnez le sous-réseau.
4. Sélectionnez l'onglet ACL réseau.

Pour décrire l'ACL réseau associée à un sous-réseau à l'aide du AWS CLI

Utilisez la describe-network-aclscommande suivante pour répertorier l'ACL réseau associée au sous-réseau spécifié.

```
aws ec2 describe-network-acls --filters Name=association.subnet-
id,Values=subnet-0d2d1b81e0bc9c6d4 --query NetworkAcls[*].NetworkAclId
```

Voici un exemple de sortie.

```
[
    "acl-03701d1f82d8c3fd6"
]
```

Pour décrire les sous-réseaux associés à une ACL 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 Network ACLs.
3. Sélectionnez l'ACL réseau.
4. Sélectionnez l'onglet Associations de sous-réseaux.

Pour décrire les sous-réseaux associés à une ACL réseau à l'aide du AWS CLI

Utilisez la describe-network-aclscommande suivante pour répertorier les sous-réseaux associés à l'ACL réseau spécifiée.

```
aws ec2 describe-network-acls --network-acl-ids acl-060415a18fcc9afde --query
 NetworkAcls[*].Associations[].SubnetId
```

Voici un exemple de sortie.

```
[
    "subnet-0d2d1b81e0bc9c6d4",
    "subnet-0e990c67809773b19",
    "subnet-0eb17d85f5dfd33b1",
    "subnet-0e01d500780bb7468"
]
```

Modification des sous-réseaux associés à une ACL réseau

Vous pouvez dissocier une liste ACL réseau personnalisée d'un sous-réseau. Lorsque vous dissociez un sous-réseau d'une ACL réseau personnalisée, nous associons automatiquement ce dernier à l'ACL réseau par défaut du VPC. Les modifications prennent effet après un court laps de temps.

Pour modifier les sous-réseaux associés à une 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.
3. Sélectionnez l'ACL réseau.
4. Sélectionnez Actions, Modifier les associations de sous-réseau.
5. Supprimez le sous-réseau des Sous-réseaux sélectionnés.
6. Sélectionnez Enregistrer les modifications.

Modification de l'ACL réseau associée à 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 l'ACL réseau par défaut du VPC. Si vous créez une ACL réseau personnalisée, vous devrez appliquer les règles d'ACL réseau en associant l'ACL réseau à un ou plusieurs sous-réseaux.

Une fois que vous aurez modifié l'ACL réseau associée à un sous-réseau, les modifications prendront effet après un court laps de temps.

Pour modifier l'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 panneau de navigation, choisissez Subnets (Sous-réseaux).
3. Sélectionnez le sous-réseau.

4. Sélectionnez Actions, Modifier une association de liste ACL réseau.
5. Dans ID de l'ACL réseau, sélectionnez l'ACL réseau à associer au sous-réseau et passez en revue les règles entrantes et sortantes de l'ACL réseau sélectionnée.
6. Choisissez Enregistrer.

Pour remplacer une association d'ACL réseau à l'aide de la ligne de commande

- replace-network-acl-association (AWS CLI)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Suppression d'une ACL pour un VPC

Lorsque vous n'avez plus besoin d'utiliser une ACL réseau, vous pouvez la supprimer. Vous ne pouvez pas supprimer une ACL réseau si des sous-réseaux y sont associés. Vous ne pouvez pas supprimer la liste ACL réseau par défaut.

Pour supprimer les associations de sous-réseaux d'une ACL 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 Network ACLs. La colonne Associé à indique le nombre de sous-réseaux associés à chaque ACL réseau. Cette colonne contient la mention - en l'absence de sous-réseaux associés.
3. Sélectionnez l'ACL réseau.
4. Sélectionnez Actions, Modifier les associations de sous-réseau.
5. Supprimez les associations de sous-réseaux.
6. Sélectionnez Enregistrer les modifications.

Pour décrire votre réseau ACLs, y compris les associations, à l'aide de la ligne de commande

- describe-network-acls (AWS CLI)
- Get-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Pour remplacer une association d'ACL réseau à l'aide de la ligne de commande

- replace-network-acl-association (AWS CLI)

- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Pour supprimer une ACL réseau à l'aide de la console

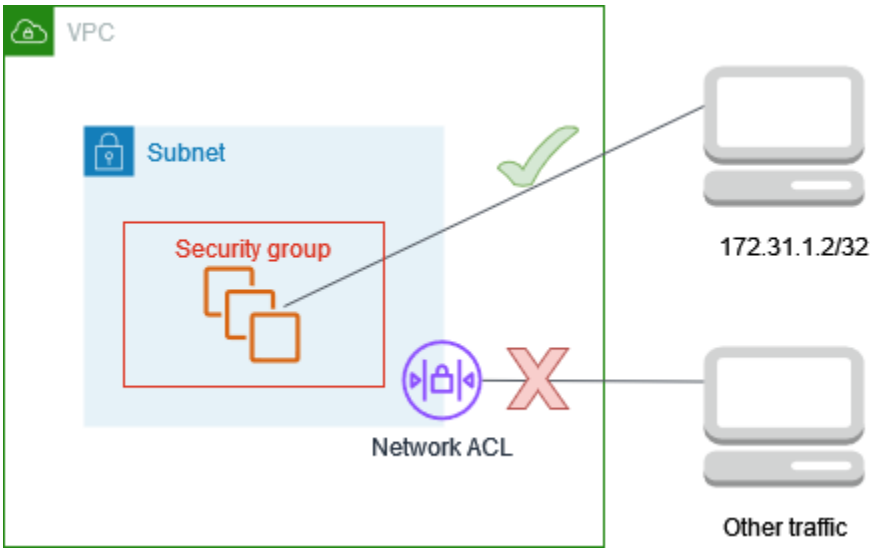
1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Network ACLs.
3. Sélectionnez l'ACL réseau.
4. Choisissez Actions, puis Supprimer le réseau ACLs.
5. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

Pour supprimer une ACL réseau à l'aide de la ligne de commande

- delete-network-acl (AWS CLI)
- Remove-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Exemple : contrôler l'accès aux instances dans un sous-réseau

Dans cet exemple, les instances du sous-réseau peuvent communiquer entre elles et sont accessibles depuis un ordinateur distant fiable afin d'effectuer des tâches administratives. L'ordinateur distant peut être un ordinateur de votre réseau local (comme illustré sur le diagramme) ou une instance d'un autre sous-réseau ou VPC. Les règles d'ACL réseau du sous-réseau et les règles de groupe de sécurité des instances autorisent l'accès à partir de l'adresse IP de votre ordinateur distant. Le reste du trafic provenant d'Internet ou d'autres réseaux est refusé.



Le recours à une ACL réseau vous permet de modifier les groupes de sécurité ou les règles de groupe de sécurité de vos instances, tout en offrant une couche de défense des sauvegardes. Par exemple, si vous mettez accidentellement à jour le groupe de sécurité pour autoriser l'accès SSH entrant à partir de n'importe quel emplacement, mais que l'ACL réseau n'autorise l'accès qu'à partir de la plage d'adresses IP de l'ordinateur distant, l'ACL réseau refuse le trafic SSH entrant en provenance de toute autre adresse IP.

Règles des listes ACL réseau

Voici des exemples de règles entrantes pour l'ACL réseau associée au sous-réseau. Ces règles s'appliquent à toutes les instances du sous-réseau.

Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/ Refuser	Commentaires
100	SSH	TCP	22	*172.31.1.2/32*	AUTORISER	Autorisation du trafic entrant depuis l'ordinateur distant.
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REJETER	Refus de tout autre trafic entrant.

Voici des exemples de règles sortantes pour l'ACL réseau associée au sous-réseau. ACLs Les réseaux sont apatrides. Par conséquent, vous devez inclure une règle qui autorise les réponses au trafic entrant.

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.

Règles des groupes de sécurité

Voici des exemples de règles entrantes pour le groupe de sécurité associé aux instances. Ces règles s'appliquent à toutes les instances associées au groupe de sécurité Un utilisateur disposant de la clé privée pour la paire de clés associée aux instances peut se connecter aux instances depuis l'ordinateur distant à l'aide de SSH.

Type de protocole	Protocole	Plage de ports	Source	Commentaires
Tout le trafic	Tous	Tous	*sg-1234567890abcdef0*	Autorisation de la communication entre les instances associées à ce groupe de sécurité.
SSH	TCP	22	*172.31.1.2/32*	Autorisation de l'accès SSH entrant à partir

Type de protocole	Protocole	Plage de ports	Source	Commentaires
				de l'ordinateur distant.

Voici des exemples de règles sortantes pour le groupe de sécurité associé aux instances. Les groupes de sécurité sont avec état. Par conséquent, vous n'avez pas besoin d'une règle qui autorise les réponses au trafic entrant.

Type de protocole	Protocole	Plage de ports	Destination	Commentaires
Tout le trafic	Tous	Tous	*sg-1234567890abcdef0*	Autorisation de la communication entre les instances associées à ce groupe de sécurité.

Différences entre le réseau ACLs et les groupes de sécurité

Le tableau suivant récapitule les principales différences entre le réseau ACLs et les groupes de sécurité.

Caractéristiques	Réseau ACL	Groupe de sécurité
Niveau de l'opération	Niveau du sous-réseau	Niveau de l'instance
Scope	S'applique à toutes les instances présentes dans les sous-réseaux associés	S'applique à toutes les instances associées au groupe de sécurité
Type de règle	Règles d'autorisation et de refus	Règles d'autorisation uniquement

Caractéristiques	Réseau ACL	Groupe de sécurité
Évaluations des règles	Évalue les règles par ordre croissant jusqu'à ce qu'une correspondance soit trouvée pour le trafic	Evalue toutes les règles avant de décider si le trafic doit être autorisé
Trafic de retour	Doit être explicitement autorisé (sans état)	Autorisé automatiquement (avec état)

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.

Régions AWS sont les principaux éléments constitutifs, chacun représentant un emplacement géographique distinct abritant plusieurs zones de disponibilité physiquement séparées et isolées. Ces zones de disponibilité sont reliées par une structure réseau à latence faible, à débit élevé et à forte redondance, permettant une communication et un transfert de données entre elles sans faille.

L'architecture des zones de disponibilité est un facteur de différenciation clé, car elles sont conçues pour être bien plus robustes et tolérantes aux pannes que les configurations traditionnelles de centres de données uniques ou multiples. En répartissant les ressources entre plusieurs zones de disponibilité au sein d'une région, les applications et les bases de données peuvent être conçues pour basculer automatiquement entre les zones sans interruption de service. Ce niveau de redondance et de haute disponibilité est une exigence essentielle pour les charges de travail critiques et permet aux organisations de créer des solutions natives cloud résilientes.

En outre, l'envergure et la portée mondiale de l' AWS infrastructure permettent aux clients de déployer leurs applications au plus près des utilisateurs finaux, de réduire le temps de latence et d'améliorer l'expérience utilisateur globale. La disponibilité de plusieurs régions à travers le monde permet également une souveraineté et une conformité efficaces des données, car les clients

peuvent stocker et traiter les données dans les limites géographiques requises par leurs besoins réglementaires et commerciaux spécifiques.

En tirant parti de l'infrastructure AWS mondiale, les entreprises peuvent concevoir leurs environnements cloud de manière à ce qu'ils soient hautement disponibles, tolérants aux pannes et évolutifs, avec la flexibilité nécessaire pour s'adapter à l'évolution des exigences et des besoins commerciaux. Cette base solide est essentielle à l'implémentation réussie d'applications et de services modernes basés sur le cloud.

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 votre système VPCs 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. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez AWS la documentation de sécurité.

Bloquer l'accès public aux sous-réseaux VPCs et aux sous-réseaux

La fonctionnalité VPC Block Public Access (BPA) est une fonctionnalité de sécurité centralisée qui vous permet d'empêcher de manière officielle l'accès public à Internet aux ressources VPC sur

l'ensemble d'un compte AWS , en garantissant le respect des exigences de sécurité tout en offrant une flexibilité pour les exceptions spécifiques et les capacités d'audit.

La fonctionnalité VPC BPA dispose des modes suivants :

- Bidirectionnel : tout le trafic à destination et en provenance des passerelles Internet et des passerelles Internet de sortie uniquement dans cette région (à l'exception des réseaux exclus VPCs et des sous-réseaux) est bloqué.
- Entrée uniquement : tout le trafic Internet vers cette région (VPCs à l'exception des VPCs sous-réseaux exclus) est bloqué. Seul le trafic à destination et en provenance des passerelles NAT et des passerelles Internet de sortie uniquement est autorisé, car ces passerelles autorisent uniquement l'établissement de connexions sortantes.

Vous pouvez également créer des « exclusions » pour cette fonctionnalité pour le trafic que vous ne souhaitez pas bloquer. Une exclusion est un mode qui peut être appliqué à un seul VPC ou sous-réseau pour l'exempter du mode VPC BPA du compte et autoriser un accès bidirectionnel ou de sortie uniquement.

Les exclusions peuvent avoir l'un des modes suivants :

- Bidirectionnel : tout le trafic Internet à destination et en provenance des sous-réseaux exclus VPCs est autorisé.
- Sortie uniquement : le trafic Internet sortant des sous-réseaux exclus est autorisé VPCs . Le trafic Internet entrant vers les sous-réseaux exclus VPCs est bloqué. Cela ne s'applique que lorsque la fonctionnalité VPC BPA est réglée sur Bidirectionnel.

Table des matières

Principes de base de la fonctionnalité VPC BPA

Cette section fournit des informations importantes sur la fonctionnalité VPC BPA, notamment les services qui la prennent en charge et la manière dont vous pouvez l'utiliser.

Table des matières

Disponibilité par région

Le VPC BPA est disponible dans toutes les AWS régions commerciales, y compris les régions de GovCloud Chine.

Dans ce guide, vous trouverez également des informations sur l'utilisation de l'analyseur d'accès réseau et de l'analyseur d'accessibilité avec la fonctionnalité VPC BPA. Notez que l'analyseur d'accès réseau et l'analyseur d'accessibilité ne sont pas disponibles dans toutes les régions commerciales. Pour plus d'informations sur la disponibilité régionale de l'analyseur d'accès réseau et de l'analyseur d'accessibilité, consultez les sections Restrictions dans le Guide de l'analyseur d'accès réseau et Considérations dans le Guide de l'analyseur d'accessibilité.

AWS impact sur le service et support

Les ressources et services suivants prennent en charge la fonctionnalité VPC BPA et le trafic vers ces services et ressources est impacté par la fonctionnalité BPA VPC :

- Passerelle Internet : tout le trafic entrant et sortant est bloqué.
- Passerelle Internet de sortie uniquement : tout le trafic sortant est bloqué. Les passerelles Internet de sortie uniquement n'autorisent pas le trafic entrant.
- Gateway Load Balancer (GWLB) : tout le trafic entrant et sortant est bloqué même si le sous-réseau contenant les points de terminaison GWLB est exclu.
- Passerelle NAT : tout le trafic entrant et sortant est bloqué. Les passerelles NAT nécessitent une passerelle Internet pour la connectivité Internet.
- Network Load Balancer connecté à Internet : tout le trafic entrant et sortant est bloqué. Les équilibreurs Network Load Balancers connectés à Internet nécessitent une passerelle Internet pour la connectivité Internet.

- Application Load Balancer connecté à Internet : tout le trafic entrant et sortant est bloqué. Les Application Load Balancers connectés à Internet nécessitent une passerelle Internet pour la connectivité Internet.
- Amazon CloudFront VPC Origins : tout le trafic entrant et sortant est bloqué.
- Direct Connect: Tout le trafic entrant et sortant utilisant des interfaces virtuelles publiques (IPv6 adresses unicast publiques IPv4 ou globales) est bloqué. Ce trafic utilise la passerelle Internet (ou passerelle Internet de sortie uniquement) pour la connectivité.
- AWS Accélérateur global : le trafic entrant VPCs est bloqué, que la cible soit accessible ou non via Internet.
- AWS Network Firewall : tout le trafic entrant et sortant est bloqué même si le sous-réseau contenant les points de terminaison de pare-feu est exclu.
- AWS Wavelength passerelle du transporteur : tout le trafic entrant et sortant est bloqué.

Le trafic lié à la connectivité privée, tel que le trafic pour les services et ressources suivants, n'est ni bloqué ni impacté par la fonctionnalité VPC BPA :

- AWS Client VPN
- AWS Cloud WAN
- AWS Outposts passerelle locale
- AWS Site-to-Site VPN
- Passerelle de transit
- Accès vérifié par AWS

⚠ Important

- Si vous acheminez le trafic entrant et sortant via un dispositif (tel qu'un outil de sécurité ou de surveillance tiers) exécuté sur une instance EC2 d'un sous-réseau, lorsque vous utilisez la fonctionnalité VPC BPA, ce sous-réseau doit constituer une exclusion pour que le trafic y entre et en sorte. Les autres sous-réseaux envoyant du trafic vers le sous-réseau de dispositif et non vers la passerelle Internet n'ont pas besoin d'être ajoutés en tant qu'exclusions.
- Le trafic envoyé en privé depuis les ressources de votre VPC vers d'autres services exécutés dans votre VPC, tels que le résolveur Route 53, est autorisé même lorsque la

fonctionnalité VPC BPA est activée, car il ne passe pas par une passerelle Internet de votre VPC. Il est possible que ces services adressent des demandes à des ressources extérieures au VPC en votre nom, par exemple, afin de résoudre une requête DNS, et qu'ils exposent des informations sur l'activité des ressources au sein de votre VPC s'ils ne sont pas atténués par d'autres contrôles de sécurité.

Restrictions liées à la fonctionnalité VPC BPA

Le mode VPC BPA en entrée uniquement n'est pas pris en charge dans les Zones Locales (LZs) où les passerelles NAT et les passerelles Internet de sortie uniquement ne sont pas autorisées.

Contrôle de l'accès à la fonctionnalité VPC BPA avec une politique IAM

Pour des exemples de politiques IAM qui allow/deny accèdent à la fonctionnalité VPC BPA, consultez. Bloquer l'accès public aux sous-réseaux VPCs et aux sous-réseaux

Activation du mode bidirectionnel de la fonctionnalité VPC BPA pour votre compte

Le mode bidirectionnel VPC BPA bloque tout le trafic à destination et en provenance des passerelles Internet et des passerelles Internet de sortie uniquement dans cette région (à l'exception des réseaux exclus et des sous-réseaux). VPCs Pour plus d'informations sur les exclusions, consultez Créer et supprimer des exclusions.

Important

Nous vous recommandons vivement de passer en revue les charges de travail qui nécessitent un accès à Internet avant d'activer la fonctionnalité VPC BPA dans vos comptes de production.

Note

- Pour activer le VPC BPA sur les sous-réseaux VPCs et de votre compte, vous devez être propriétaire des sous-réseaux et. VPCs
- Si vous partagez actuellement des sous-réseaux VPC avec d'autres comptes, le mode VPC BPA appliqué par le propriétaire du sous-réseau s'applique également au trafic

des participants, mais les participants ne peuvent pas contrôler les paramètres de la fonctionnalité BPA VPC qui ont un impact sur le sous-réseau partagé.

AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Choisissez Modifier les paramètres d'accès public.
4. Choisissez Activer le blocage d'accès public et Bidirectionnel, puis sélectionnez Enregistrer les modifications.
5. Attendez que l'état passe à Activé. Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour.

Le mode bidirectionnel VPC BPA est désormais activé.

AWS CLI

1. Activez la fonctionnalité VPC BPA :

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
```

Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour.

2. Affichez l'état de la fonctionnalité VPC BPA :

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

Changer le mode VPC BPA en mode d'entrée uniquement

Le mode d'entrée BPA VPC uniquement bloque tout le trafic Internet vers cette région (VPCs à l'exception des sous-réseaux exclus). VPCs Seul le trafic à destination et en provenance des passerelles NAT et des passerelles Internet de sortie uniquement est autorisé, car ces passerelles autorisent uniquement l'établissement de connexions sortantes.

AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Choisissez Modifier les paramètres d'accès public.
4. Remplacez la direction par Entrée uniquement.
5. Enregistrez les modifications et attendez que l'état soit mis à jour. Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour.

AWS CLI

1. Modifiez le sens de blocage de la fonctionnalité VPC BPA :

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-ingress
```

   Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour.

2. Affichez l'état de la fonctionnalité VPC BPA :

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

Créer et supprimer des exclusions

Une exclusion VPC BPA est un mode qui peut être appliqué à un seul VPC ou sous-réseau pour l'exempter du mode VPC BPA du compte et autoriser un accès bidirectionnel ou de sortie uniquement. Vous pouvez créer des exclusions VPC BPA pour les sous-réseaux VPCs et les sous-réseaux même lorsque le BPA VPC n'est pas activé sur le compte afin de garantir que le trafic des exclusions n'est pas perturbé lorsque le BPA VPC est activé. Une exclusion pour un VPC s'applique automatiquement à tous les sous-réseaux du VPC.

Vous pouvez créer 50 exclusions au maximum. Pour plus d'informations sur la demande d'une augmentation de limite, consultez Exclusions VPC BPA par compte dans Quotas Amazon VPC.

AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Dans l'onglet Bloquer l'accès public, sous Exclusions, effectuez l'une des opérations suivantes :
   - Pour supprimer une exclusion, sélectionnez-la, puis choisissez Actions > Supprimer les exclusions.
   - Pour créer une exclusion, sélectionnez Créer des exclusions et passez aux étapes suivantes.
4. Choisissez la direction du bloc :
   - Bidirectionnel : autorise tout le trafic Internet à destination et en provenance des VPCs sous-réseaux exclus.
   - Sortie uniquement : autorise le trafic Internet sortant depuis les sous-réseaux exclus. VPCs Bloque le trafic Internet entrant vers les exclus VPCs et les sous-réseaux. Ce paramètre s'applique lorsque la fonctionnalité VPC BPA est réglée sur Bidirectionnel.
5. Choisissez un VPC ou un sous-réseau.
6. Choisissez Créer des exclusions.
7. Attendez que l'état d'exclusion passe à Actif. Vous devrez peut-être actualiser le tableau des exclusions pour voir la modification.

L'exclusion est créée.

AWS CLI

1. Modifiez le sens d'autorisation de l'exclusion :

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. La mise à jour de l'état d'exclusion peut prendre un certain temps. Pour afficher l'état de l'exclusion :

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

Activer la fonctionnalité VPC BPA au niveau de l'organisation

Si vous utilisez AWS Organizations pour gérer les comptes de votre organisation, vous pouvez utiliser une politique déclarative AWS Organizations pour appliquer le BPA VPC aux comptes de l'organisation. Pour plus d'informations sur la politique déclarative de la fonctionnalité VPC BPA, consultez Politiques déclaratives prises en charge dans le Guide de l'utilisateur AWS Organizations.

> **Note**
>
> - Vous pouvez utiliser la politique déclarative de la fonctionnalité VPC BPA pour configurer si les exclusions sont autorisées, mais vous ne pouvez pas créer d'exclusions avec cette politique. Pour créer des exclusions, vous devez toujours les créer dans le compte propriétaire du VPC. Pour plus d'informations sur la création des exclusions VPC BPA, consultez Créer et supprimer des exclusions.
> - Si la politique déclarative VPC BPA est activée, dans les paramètres Bloquer l'accès public, vous verrez Gérer par une politique déclarative et vous ne pourrez pas modifier les paramètres VPC BPA au niveau du compte.

Évaluation de l'impact de la fonctionnalité VPC BPA et surveillance de la fonctionnalité VPC BPA

Cette section contient des informations sur l'évaluation de l'impact de la fonctionnalité VPC BPA avant de l'activer et sur la manière de contrôler si le trafic est bloqué après son activation.

Table des matières

Évaluation de l'impact de la fonctionnalité VPC BPA à l'aide de l'analyseur d'accès réseau

Dans cette section, vous allez utiliser l'analyseur d'accès réseau pour afficher les ressources de votre compte qui utilisent une passerelle Internet avant d'activer la fonctionnalité VPC BPA et de bloquer

l'accès. Utilisez cette analyse pour comprendre l'impact de l'activation de la fonctionnalité VPC BPA sur votre compte et du blocage du trafic.

> **Note**
>
> - Network Access Analyzer n'est pas compatible IPv6 ; vous ne pourrez donc pas l'utiliser pour visualiser l'impact potentiel du BPA VPC sur le trafic sortant des passerelles Internet uniquement en sortie. IPv6
> - Les analyses que vous effectuez avec l'analyseur d'accès réseau vous sont facturées. Pour plus d'informations, consultez la section Pricing du Guide d'utilisation de l'analyseur d'accès réseau.
> - Pour plus d'informations sur la disponibilité régionale de l'analyseur d'accès réseau et de l'analyseur d'accessibilité, consultez les sections Restrictions dans le Guide de l'analyseur d'accès réseau.

AWS Management Console

1. Ouvrez la console AWS Network Insights à l'adressehttps://console.aws.amazon.com/networkinsights/.
2. Choisissez Analyseur d'accès réseau.
3. Choisissez Créer un périmètre Network Access.
4. Choisissez Évaluer l'impact de la fonctionnalité VPC Block Public Access, puis cliquez sur Suivant.
5. Le modèle est déjà configuré pour analyser le trafic à destination et en provenance des passerelles Internet de votre compte. Vous pouvez le consulter sous Source et Destination.
6. Choisissez Suivant.
7. Choisissez Créer un périmètre Network Access.
8. Choisissez le périmètre que vous venez de créer, puis sélectionnez Analyser.
9. Attendez que l'analyse se termine.
10. Affichez les résultats de l'analyse. Chaque ligne sous Résultats indique le chemin réseau qu'un paquet peut emprunter sur un réseau à destination ou en provenance d'une passerelle Internet de votre compte. Dans ce cas, si vous activez le BPA VPC et qu'aucun des sous-réseaux et/ou sous-réseaux qui apparaissent dans ces résultats n'est configuré comme une exclusion VPC BPA, le trafic vers ces réseaux VPCs et sous-réseaux sera restreint. VPCs

11. Analysez chaque résultat pour comprendre l'impact du BPA VPC sur les ressources de votre entreprise. VPCs

L'analyse de l'impact est terminée.

AWS CLI

1. Créez un périmètre d'accès au réseau :

```
aws ec2 create-network-insights-access-scope --region us-east-2 --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
```

2. Lancez l'analyse du périmètre :

```
aws ec2 start-network-insights-access-scope-analysis  --region us-east-2 --
network-insights-access-scope-id nis-id
```

3. Obtenez les résultats de l'analyse :

```
aws ec2 get-network-insights-access-scope-analysis-findings  --region us-east-2
 --network-insights-access-scope-analysis-id nisa-0aa383a1938f94cd1 --max-items
 1
```

   Les résultats indiquent le trafic à destination et en provenance des passerelles Internet VPCs dans l'ensemble de votre compte. Les résultats sont organisés sous forme de « constatations ». FindingId« :" AnalysisFinding -1" indique qu'il s'agit du premier résultat de l'analyse. Notez qu'il existe plusieurs résultats et que chacun indique un flux de trafic affecté par l'activation de la fonctionnalité VPC BPA. La première constatation montrera que le trafic a commencé sur une passerelle Internet (» SequenceNumber « : 1), est passé à une NACL (» SequenceNumber « : 2) à un groupe de sécurité (» SequenceNumber « : 3) et s'est terminé sur une instance (» SequenceNumber « : 4).

4. Analysez les résultats pour comprendre l'impact du BPA VPC sur les ressources de votre entreprise. VPCs

L'analyse de l'impact est terminée.

Surveillance de l'impact de la fonctionnalité VPC BPA à l'aide des journaux de flux

La fonctionnalité de journaux de flux VPC vous permet de capturer des informations sur le trafic IP circulant vers et depuis les interfaces réseau Elastic dans votre VPC. Vous pouvez utiliser cette fonctionnalité pour surveiller le trafic que VPC BPA empêche d'atteindre les interfaces réseau de votre instance.

Créez un journal de flux pour votre VPC en suivant les étapes décrites dans Utiliser des journaux de flux.

Lorsque vous créez le journal de flux, assurez-vous d'utiliser un format personnalisé qui inclut le champ `reject-reason`.

Lorsque vous affichez les journaux de flux, si le trafic vers une interface réseau Elastic (ENI) est rejeté en raison de la fonctionnalité VPC BPA, vous verrez un `reject-reason` de type `BPA` dans l'entrée du journal de flux.

Outre les restrictions standard relatives aux journaux de flux VPC, notez les restrictions suivantes spécifiques à VPC BPA :

- Les journaux de flux de la fonctionnalité VPC BPA n'incluent pas les enregistrements ignorés.
- Les journaux de flux de la fonctionnalité VPC BPA n'inclus pas les `bytes` même si vous incluez le champ `bytes` dans votre journal de flux.

Suivez la suppression des exclusions avec CloudTrail

Cette section explique comment vous pouvez l'utiliser AWS CloudTrail pour surveiller et suivre la suppression des exclusions BPA des VPC.

AWS Management Console

Vous pouvez consulter toutes les exclusions supprimées dans l'historique des CloudTrail événements en recherchant Type de ressource > `AWS::EC2::VPCBlockPublicAccessExclusion` dans la AWS CloudTrail console à l'adressehttps://console.aws.amazon.com/cloudtrailv2/.

AWS CLI

Vous pouvez utiliser la commande `lookup-events` pour afficher les événements liés à la suppression d'exclusions :

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

Vérifier que la connectivité est bloquée à l'aide de l'analyseur d'accessibilité

L'analyseur d'accessibilité VPC peut être utilisé pour évaluer si certains chemins d'accès réseau sont accessibles en fonction de la configuration de votre réseau, y compris les paramètres VPC BPA.

Pour plus d'informations sur la disponibilité régionale de l'analyseur d'accessibilité, consultez Considérations dans le Guide de l'analyseur d'accessibilité.

AWS Management Console

1. Ouvrez la console AWS Network Insights à l'adressehttps://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer.
2. Cliquez sur Créer et analyser le chemin.
3. Pour Type de source, choisissez Passerelles Internet et sélectionnez la passerelle Internet pour laquelle vous souhaitez bloquer le trafic dans le menu déroulant Source.
4. Pour Type de destination, choisissez Instances et sélectionnez l'instance pour laquelle vous souhaitez bloquer le trafic dans le menu déroulant Destination.
5. Cliquez sur Créer et analyser le chemin.
6. Attendez que l'analyse se termine. Cela peut prendre quelques minutes.
7. Une fois l'analyse terminée, vous devriez voir que l'État d'accessibilité est défini sur Non joignable et que les Détails du chemin indiquent que `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` est la cause de ce problème d'accessibilité.

AWS CLI

1. Créez un chemin réseau en utilisant l'ID de la passerelle Internet pour laquelle vous souhaitez bloquer le trafic en provenance (source) et l'ID de l'instance pour laquelle vous souhaitez bloquer le trafic à destination (destination) :

   ```
   aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
   destination instance-id --protocol TCP
   ```

2. Lancez une analyse sur le chemin réseau :

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-path-id nip-id
```

3. Récupérez les résultats de l'analyse :

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-insights-analysis-ids nia-id
```

4. Vérifiez que `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` est le `ExplanationCode` du manque d'accessibilité.

Exemple avancé

Cette section contient un exemple avancé qui vous aidera à comprendre comment fonctionne la fonctionnalité VPC Block Public Access dans différents scénarios. Chaque scénario s'appuie sur le scénario précédent. Il est donc important de suivre les étapes dans l'ordre.

Important

Ne passez pas en revue cet exemple dans un compte de production. Nous vous recommandons vivement de passer en revue les charges de travail qui nécessitent un accès à Internet avant d'activer la fonctionnalité VPC BPA dans vos comptes de production.

Note

Pour bien comprendre la fonctionnalité VPC BPA, vous aurez besoin de certaines ressources dans votre compte. Dans cette section, nous fournissons un CloudFormation modèle que vous pouvez utiliser pour fournir les ressources dont vous avez besoin pour bien comprendre le fonctionnement de cette fonctionnalité. Des coûts sont associés aux ressources que vous fournissez avec le CloudFormation modèle et aux analyses que vous effectuez avec Network Access Analyzer et Reachability Analyzer. Si vous utilisez le modèle de cette section, assurez-vous de suivre les étapes de nettoyage lorsque vous aurez terminé avec cet exemple.

Table des matières

CloudFormation Modèle de déploiement (facultatif)

Pour montrer comment fonctionne cette fonctionnalité, vous avez besoin d'un VPC, de sous-réseaux, d'instances et d'autres ressources. Pour faciliter la réalisation de cette démonstration, nous avons fourni un modèle CloudFormation ci-dessous que vous pouvez utiliser pour obtenir rapidement les ressources requises pour les scénarios de cette démonstration. Cette étape est facultative et vous souhaiterez peut-être simplement afficher les diagrammes dans les scénarios de cette section.

> **Note**
>
> - Certains coûts sont associés aux ressources que vous créez dans cette section avec le CloudFormation modèle, tels que le coût de la passerelle NAT et des IPv4 adresses publiques. Pour éviter les coûts supplémentaires, assurez-vous de suivre les étapes de nettoyage afin de supprimer toutes les ressources créées aux fins de cet exemple.
> - Ce CloudFormation modèle crée les ressources sous-jacentes nécessaires au VPC BPA mais n'active pas la fonctionnalité VPC BPA elle-même. Les ressources déployées ici sont destinées à vous aider à comprendre et à tester la fonctionnalité VPC BPA une fois que vous avez choisi de l'activer séparément.

Le modèle crée les ressources suivantes dans votre compte :

- Passerelle Internet de sortie uniquement
- Passerelle Internet
- Passerelle NAT

- Deux sous-réseaux publics
- Un sous-réseau privé
- Deux instances EC2 avec adresses publiques et privées IPv4
- Une instance EC2 avec une IPv6 adresse et une adresse privée IPv4
- Une instance EC2 avec une IPv4 adresse privée uniquement
- Un groupe de sécurité avec trafic entrant SSH et ICMP autorisé et TOUT le trafic sortant autorisé
- Journal de flux VPC
- Un point de terminaison EC2 Instance Connect dans le sous-réseau B

Copiez le modèle ci-dessous et enregistrez-le dans un fichier .yaml.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Creates a VPC with public and private subnets, NAT gateway, and EC2
 instances for VPC BPA.

Parameters:
  InstanceAMI:
    Description: ID of the Amazone Machine Image (AMI) to use with the instances
 launched by this template
    Type: AWS::EC2::Image::Id
  InstanceType:
    Description: EC2 Instance type to use with the instances launched by this template
    Type: String
    Default: t2.micro

Resources:

  # VPC
  VPCBPA:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsHostnames: true
      EnableDnsSupport: true
      InstanceTenancy: default
      Tags:
        - Key: Name
          Value: VPC BPA

  # VPC IPv6 CIDR
```

```
  VPCBPAIpv6CidrBlock:
    Type: AWS::EC2::VPCCidrBlock
    Properties:
      VpcId: !Ref VPCBPA
      AmazonProvidedIpv6CidrBlock: true

  # EC2 Key Pair
  VPCBPAKeyPair:
    Type: AWS::EC2::KeyPair
    Properties:
      KeyName: vpc-bpa-key

  # Internet Gateway
  VPCBPAInternetGateway:
    Type: AWS::EC2::InternetGateway
    Properties:
      Tags:
        - Key: Name
          Value: VPC BPA Internet Gateway

  VPCBPAInternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      VpcId: !Ref VPCBPA
      InternetGatewayId: !Ref VPCBPAInternetGateway

  # Egress-Only Internet Gateway
  VPCBPAEgressOnlyInternetGateway:
    Type: AWS::EC2::EgressOnlyInternetGateway
    Properties:
      VpcId: !Ref VPCBPA

  # Subnets
  VPCBPAPublicSubnetA:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.1.0/24
      MapPublicIpOnLaunch: true
      Tags:
        - Key: Name
          Value: VPC BPA Public Subnet A

  VPCBPAPublicSubnetB:
```

```
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.2.0/24
      MapPublicIpOnLaunch: true
      Tags:
        - Key: Name
          Value: VPC BPA Public Subnet B

  VPCBPAPrivateSubnetC:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.3.0/24
      MapPublicIpOnLaunch: false
      Ipv6CidrBlock: !Select [0, !GetAtt VPCBPA.Ipv6CidrBlocks]
      AssignIpv6AddressOnCreation: true
      Tags:
        - Key: Name
          Value: VPC BPA Private Subnet C

  # NAT Gateway
  VPCBPANATGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt VPCBPANATGatewayEIP.AllocationId
      SubnetId: !Ref VPCBPAPublicSubnetB
      Tags:
        - Key: Name
          Value: VPC BPA NAT Gateway

  VPCBPANATGatewayEIP:
    Type: AWS::EC2::EIP
    Properties:
      Domain: vpc
      Tags:
        - Key: Name
          Value: VPC BPA NAT Gateway EIP

  # Route Tables
  VPCBPAPublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref VPCBPA
```

```
      Tags:
        - Key: Name
          Value: VPC BPA Public Route Table

  VPCBPAPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: VPCBPAInternetGatewayAttachment
    Properties:
      RouteTableId: !Ref VPCBPAPublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref VPCBPAInternetGateway

  VPCBPAPublicSubnetARouteTableAssoc:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPublicSubnetA
      RouteTableId: !Ref VPCBPAPublicRouteTable

  VPCBPAPublicSubnetBRouteTableAssoc:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPublicSubnetB
      RouteTableId: !Ref VPCBPAPublicRouteTable

  VPCBPAPrivateRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Private Route Table

  VPCBPAPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref VPCBPANATGateway

  VPCBPAPrivateSubnetCRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationIpv6CidrBlock: ::/0
```

```
      EgressOnlyInternetGatewayId: !Ref VPCBPAEgressOnlyInternetGateway

  VPCBPAPrivateSubnetCRouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPrivateSubnetC
      RouteTableId: !Ref VPCBPAPrivateRouteTable

  # EC2 Instances Security Group
  VPCBPAInstancesSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupName: VPC BPA Instances Security Group
      GroupDescription: Allow SSH and ICMP access
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 22
          ToPort: 22
          CidrIp: 0.0.0.0/0
        - IpProtocol: icmp
          FromPort: -1
          ToPort: -1
          CidrIp: 0.0.0.0/0
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Instances Security Group

  # EC2 Instances
  VPCBPAInstanceA:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: t2.micro
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPublicSubnetA
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance A

  VPCBPAInstanceB:
    Type: AWS::EC2::Instance
```

```
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPublicSubnetB
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance B

  VPCBPAInstanceC:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance C

  VPCBPAInstanceD:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      NetworkInterfaces:
        - DeviceIndex: '0'
          GroupSet:
            - !Ref VPCBPAInstancesSecurityGroup
          SubnetId: !Ref VPCBPAPrivateSubnetC
          Ipv6AddressCount: 1
      Tags:
        - Key: Name
          Value: VPC BPA Instance D

  # Flow Logs IAM Role
  VPCBPAFlowLogRole:
    Type: AWS::IAM::Role
    Properties:
```

```
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service: vpc-flow-logs.amazonaws.com
            Action: 'sts:AssumeRole'
      Tags:
        - Key: Name
          Value: VPC BPA Flow Logs Role

  VPCBPAFlowLogPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyName: VPC-BPA-FlowLogsPolicy
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Action:
              - 'logs:CreateLogGroup'
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
              - 'logs:DescribeLogGroups'
              - 'logs:DescribeLogStreams'
            Resource: '*'
      Roles:
        - !Ref VPCBPAFlowLogRole

  # Flow Logs
  VPCBPAFlowLog:
    Type: AWS::EC2::FlowLog
    Properties:
      ResourceId: !Ref VPCBPA
      ResourceType: VPC
      TrafficType: ALL
      LogDestinationType: cloud-watch-logs
      LogGroupName: /aws/vpc-flow-logs/VPC-BPA
      DeliverLogsPermissionArn: !GetAtt VPCBPAFlowLogRole.Arn
      LogFormat: '${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr}
 ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-
status} ${vpc-id} ${subnet-id} ${instance-id} ${tcp-flags} ${type} ${pkt-srcaddr}
 ${pkt-dstaddr} ${region} ${az-id} ${sublocation-type} ${sublocation-id} ${pkt-src-aws-
service} ${pkt-dst-aws-service} ${flow-direction} ${traffic-path} ${reject-reason}'
```

```
      Tags:
        - Key: Name
          Value: VPC BPA Flow Logs

  # EC2 Instance Connect Endpoint
  VPCBPAEC2InstanceConnectEndpoint:
    Type: AWS::EC2::InstanceConnectEndpoint
    Properties:
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      SubnetId: !Ref VPCBPAPublicSubnetB

Outputs:
  VPCBPAVPCId:
    Description: A reference to the created VPC
    Value: !Ref VPCBPA
    Export:
      Name: vpc-id

  VPCBPAPublicSubnetAId:
    Description: The ID of the public subnet A
    Value: !Ref VPCBPAPublicSubnetA

  VPCBPAPublicSubnetAName:
    Description: The name of the public subnet A
    Value: VPC BPA Public Subnet A

  VPCBPAPublicSubnetBId:
    Description: The ID of the public subnet B
    Value: !Ref VPCBPAPublicSubnetB

  VPCBPAPublicSubnetBName:
    Description: The name of the public subnet B
    Value: VPC BPA Public Subnet B

  VPCBPAPrivateSubnetCId:
    Description: The ID of the private subnet C
    Value: !Ref VPCBPAPrivateSubnetC

  VPCBPAPrivateSubnetCName:
    Description: The name of the private subnet C
    Value: VPC BPA Private Subnet C

  VPCBPAInstanceAId:
```

```
    Description: The ID of instance A
    Value: !Ref VPCBPAInstanceA

  VPCBPAInstanceBId:
    Description: The ID of instance B
    Value: !Ref VPCBPAInstanceB

  VPCBPAInstanceCId:
    Description: The ID of instance C
    Value: !Ref VPCBPAInstanceC

  VPCBPAInstanceDId:
    Description: The ID of instance D
    Value: !Ref VPCBPAInstanceD
```

AWS Management Console

1. Ouvrez la CloudFormation console à l'adressehttps://console.aws.amazon.com/cloudformation/.
2. Choisissez Créer une pile et téléchargez le fichier modèle .yaml.
3. Suivez les étapes pour lancer le modèle. Vous devrez saisir une ID d'image et un type d'instance (comme t2.micro). Vous devrez également autoriser la création CloudFormation d'un rôle IAM pour la création du journal de flux et l'autorisation de vous y connecter CloudWatch.
4. Une fois que vous avez lancé la pile, affichez l'onglet Événements pour voir la progression et assurez-vous que la pile est complète avant de continuer.

AWS CLI

1. Exécutez la commande suivante pour créer la CloudFormation pile :

```
aws cloudformation create-stack --stack-name VPC-BPA-stack --template-body
 file://sampletemplate.yaml --capabilities CAPABILITY_IAM --region us-east-2
```

Sortie :

```
{
    "StackId": "arn:aws:cloudformation:us-east-2:470889052923:stack/VPC-BPA-
stack/8a7a2cc0-8001-11ef-b196-06386a84b72f"
```

```
}
```

2. Affichez la progression et assurez-vous que la pile est complète avant de continuer :

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-east-2
```

Afficher l'impact de la fonctionnalité VPC BPA à l'aide de l'analyseur d'accès réseau

Dans cette section, vous allez utiliser l'analyseur d'accès réseau pour afficher les ressources de votre compte qui utilisent la passerelle Internet. Utilisez cette analyse pour comprendre l'impact de l'activation de la fonctionnalité VPC BPA sur votre compte et du blocage du trafic.

Pour plus d'informations sur la disponibilité régionale de l'analyseur d'accès réseau et de l'analyseur d'accessibilité, consultez les sections Restrictions dans le Guide de l'analyseur d'accès réseau.

AWS Management Console

1. Ouvrez la console AWS Network Insights à l'adressehttps://console.aws.amazon.com/networkinsights/.
2. Choisissez Analyseur d'accès réseau.
3. Choisissez Créer un périmètre Network Access.
4. Choisissez Évaluer l'impact de la fonctionnalité VPC Block Public Access, puis cliquez sur Suivant.
5. Le modèle est déjà configuré pour analyser le trafic à destination et en provenance des passerelles Internet de votre compte. Vous pouvez le consulter sous Source et Destination.
6. Choisissez Suivant.
7. Choisissez Créer un périmètre Network Access.
8. Choisissez le périmètre que vous venez de créer, puis sélectionnez Analyser.
9. Attendez que l'analyse se termine.
10. Affichez les résultats de l'analyse. Chaque ligne sous Résultats indique le chemin réseau qu'un paquet peut emprunter sur un réseau à destination ou en provenance d'une passerelle Internet de votre compte. Dans ce cas, si vous activez le BPA VPC et qu'aucun des sous-réseaux et/ou sous-réseaux qui apparaissent dans ces résultats n'est configuré comme une exclusion VPC BPA, le trafic vers ces réseaux VPCs et sous-réseaux sera restreint. VPCs

11. Analysez chaque résultat pour comprendre l'impact du BPA VPC sur les ressources de votre entreprise. VPCs

L'analyse de l'impact est terminée.

AWS CLI

1. Créez un périmètre d'accès au réseau :

```
aws ec2 create-network-insights-access-scope --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 --region us-east-2
```

Sortie :

```
{
  "NetworkInsightsAccessScope": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "NetworkInsightsAccessScopeArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope/nis-04cad3c4b3a1d5e3e",
    "CreatedDate": "2024-09-30T15:55:53.171000+00:00",
    "UpdatedDate": "2024-09-30T15:55:53.171000+00:00"
  },
  "NetworkInsightsAccessScopeContent": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "MatchPaths": [
      {
        "Source": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        }
      },
      {
        "Destination": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
```

```
          }
        }
      }
    ]
  }
}
```

2. Lancez l'analyse du périmètre :

```
aws ec2 start-network-insights-access-scope-analysis --network-insights-access-
scope-id nis-04cad3c4b3a1d5e3e --region us-east-2
```

Sortie :

```
{
  "NetworkInsightsAccessScopeAnalysis": {
    "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
    "NetworkInsightsAccessScopeAnalysisArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope-analysis/
nisa-0aa383a1938f94cd",
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "Status": "running",
    "StartDate": "2024-09-30T15:56:59.109000+00:00",
    "AnalyzedEniCount": 0
  }
}
```

3. Obtenez les résultats de l'analyse :

```
aws ec2 get-network-insights-access-scope-analysis-findings --network-insights-
access-scope-analysis-id nisa-0aa383a1938f94cd1 --region us-east-2 --max-items 1
```

Sortie :

```
{
  "AnalysisFindings": [
    {
      "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
      "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
      "FindingId": "AnalysisFinding-1",
      "FindingComponents": [
        {
```

```
          "SequenceNumber": 1,
          "Component": {
            "Id": "igw-04a5344b4e30486f1",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:internet-gateway/
igw-04a5344b4e30486f1",
            "Name": "VPC BPA Internet Gateway"
          },
          "OutboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ]
          },
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
              {
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
        },
        {
          "SequenceNumber": 2,
```

```
          "AclRule": {
            "Cidr": "0.0.0.0/0",
            "Egress": false,
            "Protocol": "all",
            "RuleAction": "allow",
            "RuleNumber": 100
          },
          "Component": {
            "Id": "acl-06194fc3a4a03040b",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-acl/
acl-06194fc3a4a03040b"
          }
        },
        {
          "SequenceNumber": 3,
          "Component": {
            "Id": "sg-093dde06415d03924",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:security-group/
sg-093dde06415d03924",
            "Name": "VPC BPA Instances Security Group"
          },
          "SecurityGroupRule": {
            "Cidr": "0.0.0.0/0",
            "Direction": "ingress",
            "PortRange": {
              "From": 22,
              "To": 22
            },
            "Protocol": "tcp"
          }
        },
        {
          "SequenceNumber": 4,
          "AttachedTo": {
            "Id": "i-058db34f9a0997895",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:instance/
i-058db34f9a0997895",
            "Name": "VPC BPA Instance A"
          },
          "Component": {
            "Id": "eni-0fa23f2766f03b286",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-interface/
eni-0fa23f2766f03b286"
          },
```

```
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
              {
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
          "Subnet": {
            "Id": "subnet-035d235a762eeed04",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:subnet/
subnet-035d235a762eeed04",
            "Name": "VPC BPA Public Subnet A"
          },
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
        }
      ]
    }
  ],
  "AnalysisStatus": "succeeded",
  "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
  "NextToken":
 "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ=="
```

```
}
```

Les résultats indiquent le trafic à destination et en provenance des passerelles Internet VPCs dans l'ensemble de votre compte. Les résultats sont organisés sous forme de « constatations ». FindingId« :" AnalysisFinding -1" indique qu'il s'agit du premier résultat de l'analyse. Notez qu'il existe plusieurs résultats et que chacun indique un flux de trafic affecté par l'activation de la fonctionnalité VPC BPA. La première constatation montrera que le trafic a commencé sur une passerelle Internet (» SequenceNumber « : 1), est passé à une NACL (» SequenceNumber « : 2) à un groupe de sécurité (» SequenceNumber « : 3) et s'est terminé sur une instance (» SequenceNumber « : 4).

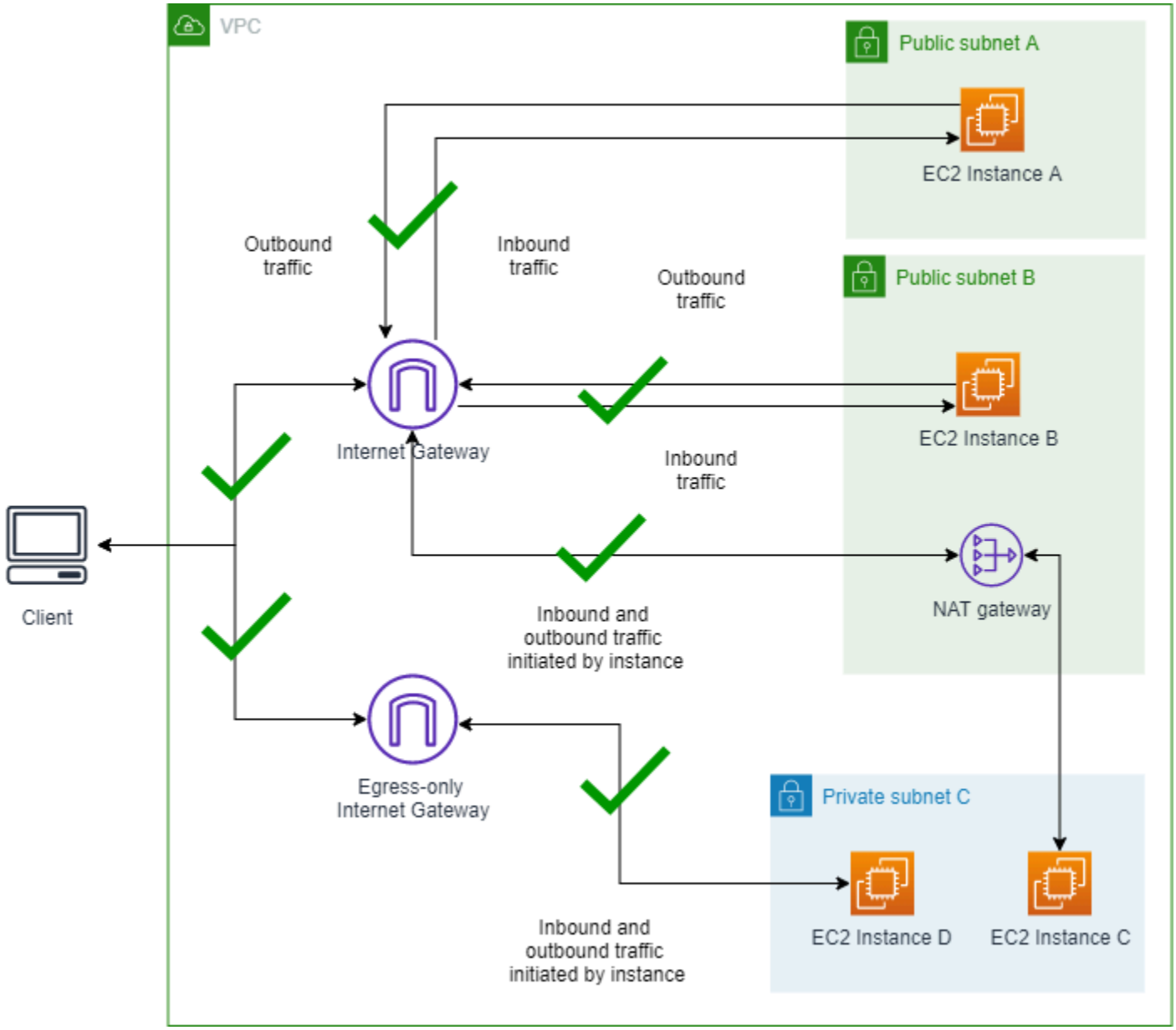
4. Analysez les résultats pour comprendre l'impact du BPA VPC sur les ressources de votre entreprise. VPCs

L'analyse de l'impact est terminée.

Scénario 1 : connexion à des instances sans que la fonctionnalité VPC BPA soit activée

Dans cette section, les instances EC2 des sous-réseaux publics A et B sont accessibles depuis Internet via la passerelle Internet, qui autorise le trafic entrant et sortant. Les instances C et D du sous-réseau privé peuvent envoyer le trafic sortant via la passerelle NAT ou la passerelle Internet de sortie uniquement, mais ne sont pas directement accessibles depuis Internet. Cette configuration permet d'accéder à certaines ressources via Internet tout en protégeant les autres ressources. Le but de cette configuration est de définir une base de référence et de vous assurer qu'avant d'activer la fonctionnalité VPC BPA, toutes les instances sont accessibles, en vous connectant à toutes les instances et en envoyant un ping à une adresse IP publique.

Schéma d'un VPC sans la fonctionnalité VPC BPA activée :



1.1 Se connecter à des instances

Terminez cette section pour vous connecter à vos instances lorsque la fonctionnalité VPC BPA est désactivée afin de pouvoir vous connecter sans problème. Toutes les instances créées avec le CloudFormation pour cet exemple portent des noms tels que « Instance VPC BPA A ».

AWS Management Console

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Ouvrez les détails de l'instance A.

3. Connectez-vous à l'instance A à l'aide de l'option EC2 Instance Connect > Se connecter à l'aide du point de terminaison EC2 Instance Connect.
4. Choisissez Se connecter. Une fois que vous avez réussi à vous connecter à l'instance, envoyez un ping à www.amazon.com pour vérifier que vous pouvez envoyer des demandes sortantes vers Internet.
5. Utilisez la même méthode que celle utilisée pour vous connecter à l'instance A pour vous connecter aux instances B, C et D. À partir de chaque instance, envoyez un ping à www.amazon.com pour vérifier que vous pouvez envoyer des demandes sortantes vers Internet.

AWS CLI

1. Envoyez un ping à l'instance A à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 18.225.8.244
```

Sortie :

```
Pinging 18.225.8.244 with 32 bytes of data:

Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

2. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
```

```
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 18:27:57 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING www-amazon-com.customer.fastly.net (18.65.233.187) 56(84) bytes of data.
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=15 ttl=58 time=2.06 ms
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=16 ttl=58 time=2.26 ms
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

3. Envoyez un ping à l'instance B à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 3.18.106.198
```

Sortie :

```
Pinging 3.18.106.198 with 32 bytes of data:
Reply from 3.18.106.198: bytes=32 time=83ms TTL=110
Reply from 3.18.106.198: bytes=32 time=54ms TTL=110
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

4. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
```

```
/m/'
Last login: Fri Sep 27 18:12:27 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.55 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.67 ms
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

5. Connectez-vous à l'instance C. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Thu Sep 19 20:31:26 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.75 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.97 ms
64 bytes from server-3-160-24-26.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=3 ttl=248 time=1.08 ms
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

6. Connectez-vous à l'instance D. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Sortie :

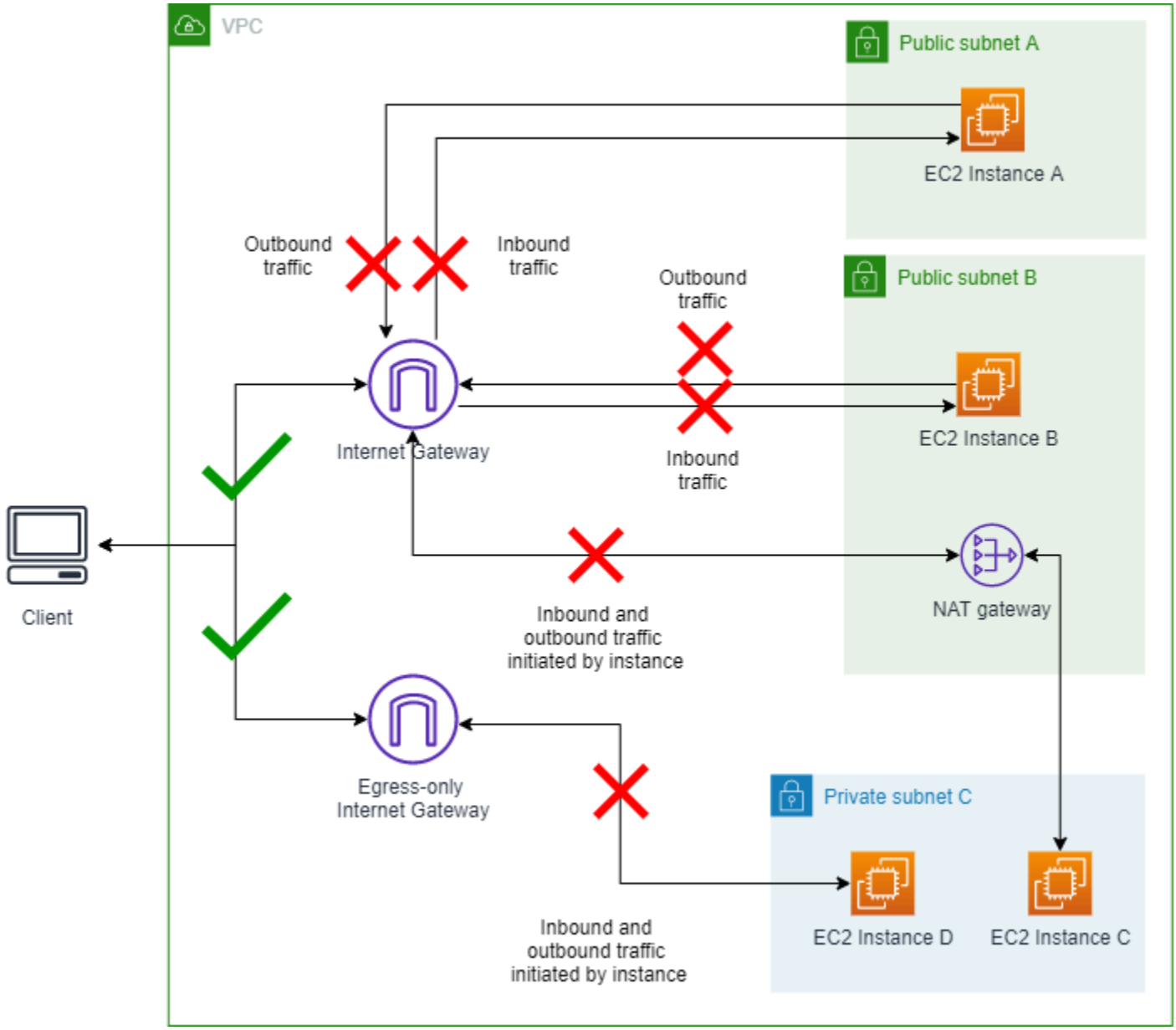
```
The authenticity of host '10.0.3.59 can't be established.
ECDSA key fingerprint is SHA256:c4naBCqbC61/cExDyccEproNU+1HHSpMSzl2J6cOtIZA8g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.59' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ _/
_/m/'
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.19 ms
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.38 ms
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

Scénario 2 : activation de la fonctionnalité VPC BPA en mode bidirectionnel

Dans cette section, vous allez activer la fonctionnalité VPC BPA et bloquer le trafic à destination et en provenance des passerelles Internet de votre compte.

Schéma illustrant le mode bidirectionnel VPC BPA activé :



2.1 Activation du mode bidirectionnel VPC BPA

Terminez cette section pour activer la fonctionnalité VPC BPA. Le mode bidirectionnel VPC BPA bloque tout le trafic à destination et en provenance des passerelles Internet et des passerelles Internet de sortie uniquement dans cette région (à l'exception des réseaux exclus et des sous-réseaux). VPCs

AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.

3. Choisissez Modifier les paramètres d'accès public.
4. Choisissez Activer le blocage d'accès public et Bidirectionnel, puis sélectionnez Enregistrer les modifications.
5. Attendez que l'état passe à Activé. Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour.

La fonctionnalité VPC BPA est désormais activée.

AWS CLI

1. Utilisez la commande modify-vpc-block-public -access-options pour activer le BPA VPC :

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-bidirectional
```

   Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour.
2. Affichez l'état de la fonctionnalité VPC BPA :

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

2.2 Se connecter à des instances

Terminez cette section pour vous connecter à vos instances.

AWS Management Console

1. Envoyez un ping à l' IPv4 adresse publique de l'instance A et de l'instance B comme vous l'avez fait dans le scénario 1. Notez que le trafic est bloqué.
2. Connectez-vous à l'instance A à l'aide de l'option EC2 Instance Connect > Se connecter à l'aide du point de terminaison EC2 Instance Connect comme vous l'avez fait dans le scénario 1. Assurez-vous d'utiliser l'option de point de terminaison.
3. Choisissez Se connecter. Une fois que vous avez réussi à vous connecter à l'instance, envoyez un ping à www.amazon.com. Notez que tout le trafic sortant est bloqué.
4. Utilisez la même méthode que celle utilisée pour vous connecter à l'instance A pour vous connecter aux instances B, C et D, puis testez les demandes sortantes vers Internet. Notez que tout le trafic sortant est bloqué.

AWS CLI

1. Envoyez un ping à l'instance A à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 18.225.8.244
```

Sortie :

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

Notez que le ping échoue et que le trafic est bloqué.

2. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Sortie :

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Notez que le ping échoue et que le trafic est bloqué.

3. Envoyez un ping à l'instance B à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 3.18.106.198
```

Sortie :

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Notez que le ping échoue et que le trafic est bloqué.

4. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Sortie :

```
The authenticity of host '10.0.2.98' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Notez que le ping échoue et que le trafic est bloqué.

5. Connectez-vous à l'instance C. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Tue Sep 24 15:17:56 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Notez que le ping échoue et que le trafic est bloqué.

6. Connectez-vous à l'instance D. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
```

```
~~..   _/
_/ _/
_/m/'
Last login: Fri Sep 27 16:42:01 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:8200:7:49a5:5fd4:b121
 (2600:9000:25f3:8200:7:49a5:5fd4:b121)) 56 data bytes
```

Notez que le ping échoue et que le trafic est bloqué.

2.3 Facultatif : vérifier que la connectivité est bloquée à l'aide de l'analyseur d'accessibilité

L'analyseur d'accessibilité VPC peut être utilisé pour comprendre si certains chemins d'accès réseau sont accessibles en fonction de la configuration de votre réseau, y compris les paramètres VPC BPA. Dans cet exemple, vous analyserez le même chemin réseau que celui qui a été tenté précédemment pour confirmer que la fonctionnalité VPC BPA est à l'origine de l'échec de la connectivité.

AWS Management Console

1. Accédez à la console Network Insights à l'adresse https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer.
2. Cliquez sur Créer et analyser le chemin.
3. Dans Type de source, choisissez Passerelles Internet et sélectionnez la passerelle Internet étiquetée Passerelle Internet VPC BPA dans le menu déroulant Source.
4. Dans Type de destination, choisissez Instances et sélectionnez l'instance étiquetée Instance A VPC BPA dans le menu déroulant Destination.
5. Cliquez sur Créer et analyser le chemin.
6. Attendez que l'analyse se termine. Cela peut prendre quelques minutes.
7. Une fois l'analyse terminée, vous devriez voir que l'État d'accessibilité est défini sur Non joignable et que les Détails du chemin indiquent que `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` en est la cause.

AWS CLI

1. Créez un chemin réseau à l'aide de l'ID de la passerelle Internet étiquetée Passerelle Internet VPC BPA et de l'ID de l'instance étiquetée Instance A VPC BPA :

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
destination instance-id --protocol TCP
```

2. Lancez une analyse sur le chemin réseau :

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

3. Récupérez les résultats de l'analyse :

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

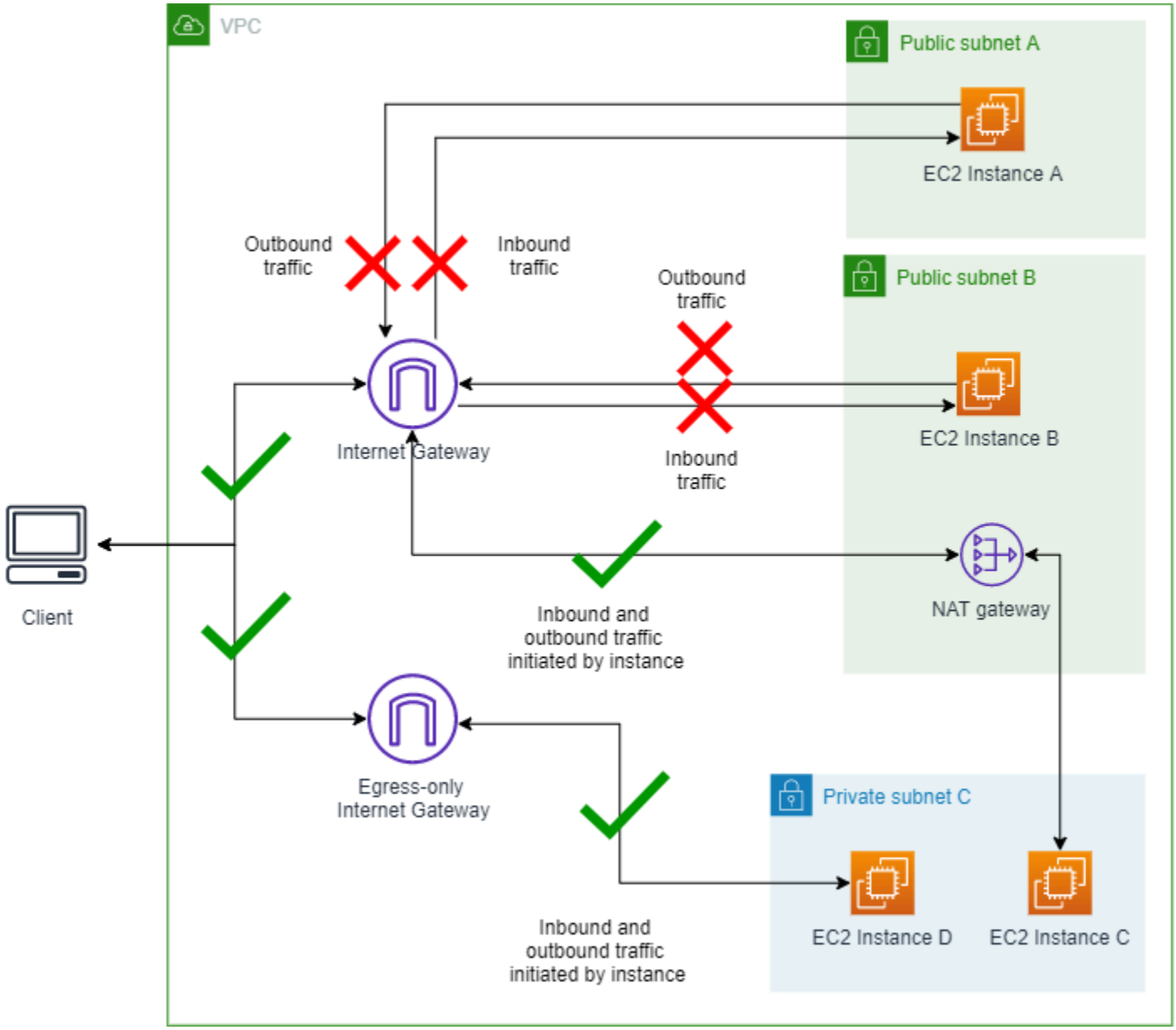
4. Vérifiez que `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` est le `ExplanationCode` du manque d'accessibilité.

Notez que vous pouvez également utiliser la section Surveillance de l'impact de la fonctionnalité VPC BPA à l'aide des journaux de flux.

Scénario 3 : modification du mode VPC BPA en mode d'entrée uniquement

Dans cette section, vous allez modifier la direction du trafic VPC BPA et n'autoriser que le trafic qui utilise une passerelle NAT ou une passerelle Internet de sortie uniquement. Les instances EC2 A et B des sous-réseaux publics seront injoignables depuis Internet du fait que la fonctionnalité BPA bloque le trafic entrant via la passerelle Internet. Les instances C et D du sous-réseau privé pourront toujours envoyer le trafic sortant via la passerelle NAT ou la passerelle Internet de sortie uniquement et pourront donc toujours accéder à Internet.

Schéma du mode VPC BPA d'entrée uniquement activé :



3.1 Changer le mode VPC BPA en mode d'entrée uniquement

Terminez cette section pour changer de mode.

AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Dans l'onglet Bloquer l'accès public, sélectionnez Modifier les paramètres d'accès public.

4. Modifiez les paramètres d'accès public dans la console VPC et réglez la direction sur Entrée uniquement.
5. Enregistrez les modifications et attendez que l'état soit mis à jour. Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour.

AWS CLI

1. Modifiez le mode VPC BPA :

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-ingress
```

   Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour.
2. Affichez l'état de la fonctionnalité VPC BPA :

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

3.2 Se connecter à des instances

Terminez cette section pour vous connecter aux instances.

AWS Management Console

1. Envoyez un ping à l' IPv4 adresse publique de l'instance A et de l'instance B comme vous l'avez fait dans le scénario 1. Notez que le trafic est bloqué.
2. Connectez-vous aux instances A et B à l'aide d'EC2 Instance Connect comme vous l'avez fait dans le scénario 1 et envoyez un ping à www.amazon.com à partir de ces instances. Notez que vous ne pouvez pas envoyer de ping à un site public sur Internet à partir de l'instance A ou B et que le trafic est bloqué.
3. Connectez-vous aux instances C et D à l'aide d'EC2 Instance Connect comme vous l'avez fait dans le scénario 1 et envoyez un ping à www.amazon.com à partir de ces instances. Notez que vous pouvez envoyer un ping à un site public sur Internet à partir de l'instance C ou D et que le trafic est autorisé.

AWS CLI

1. Envoyez un ping à l'instance A à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 18.225.8.244
```

Sortie :

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

Notez que le ping échoue et que le trafic est bloqué.

2. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Sortie :

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Notez que le ping échoue et que le trafic est bloqué.

3. Envoyez un ping à l'instance B à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 3.18.106.198
```

Sortie :

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Notez que le ping échoue et que le trafic est bloqué.

4. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Sortie :

```
The authenticity of host '10.0.2.98 ' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Notez que le ping échoue et que le trafic est bloqué.

5. Connectez-vous à l'instance C. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

6. Connectez-vous à l'instance D. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 16:48:38 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=14 ttl=58 time=1.47 ms
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=16 ttl=58 time=1.59 ms
```

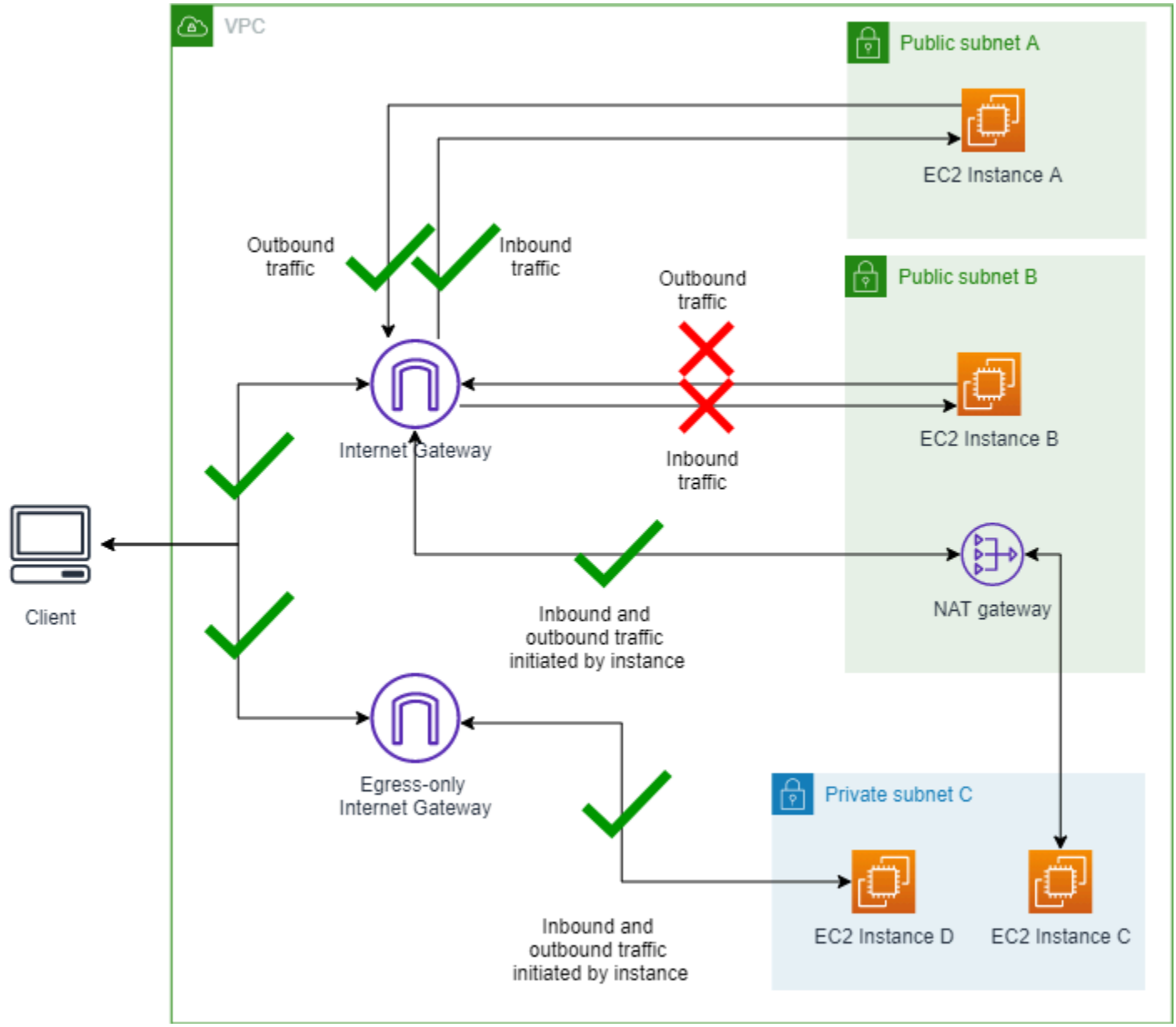
Notez que le ping est réussi et que le trafic n'est pas bloqué.

Scénario 4 : créer une exclusion

Dans cette section, vous allez créer une exclusion. La fonctionnalité VPC BPA bloquera alors uniquement le trafic sur les sous-réseaux sans exclusion. Une exclusion VPC BPA est un mode qui peut être appliqué à un seul VPC ou sous-réseau pour l'exempter du mode VPC BPA du compte et autoriser un accès bidirectionnel ou de sortie uniquement. Vous pouvez créer des exclusions VPC BPA pour les sous-réseaux VPCs et les sous-réseaux même lorsque le BPA VPC n'est pas activé sur le compte afin de garantir que le trafic des exclusions n'est pas perturbé lorsque le BPA VPC est activé.

Dans cet exemple, nous allons créer une exclusion pour le sous-réseau A afin de montrer comment le trafic vers les exclusions est impacté par la fonctionnalité VPC BPA.

Schéma du mode VPC BPA d'entrée uniquement activé et de l'exclusion du sous-réseau A avec mode bidirectionnel activé :



4.1 Créer une exclusion pour le sous-réseau A

Terminez cette section pour créer une exclusion. Une exclusion VPC BPA est un mode qui peut être appliqué à un seul VPC ou sous-réseau pour l'exempter du mode VPC BPA du compte et autoriser un accès bidirectionnel ou de sortie uniquement. Vous pouvez créer des exclusions VPC BPA pour les sous-réseaux VPCs et les sous-réseaux même lorsque le BPA VPC n'est pas activé sur le compte afin de garantir que le trafic des exclusions n'est pas perturbé lorsque le BPA VPC est activé.

AWS Management Console

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

2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Dans l'onglet Bloquer l'accès public, sous Exclusions, choisissez Créer des exclusions.
4. Choisissez Sous-réseau public A du VPC BPA, assurez-vous de sélectionnez l'option Bidirectionnel, puis choisissez Créer des exclusions.
5. Attendez que l'état d'exclusion passe à Actif. Vous devrez peut-être actualiser le tableau des exclusions pour voir la modification.

L'exclusion est créée.

AWS CLI

1. Modifiez le sens d'autorisation de l'exclusion :

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. La mise à jour de l'état d'exclusion peut prendre un certain temps. Pour afficher l'état de l'exclusion :

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

4.2 Se connecter à des instances

Terminez cette section pour vous connecter aux instances.

AWS Management Console

1. Envoyez un ping à l' IPv4 adresse publique de l'instance A. Notez que le trafic est autorisé.
2. Envoyez un ping à l' IPv4 adresse publique de l'instance B. Notez que le trafic est bloqué.
3. Connectez-vous à l'instance A à l'aide d'EC2 Instance Connect comme vous l'avez fait dans le scénario 1 et envoyez un ping à www.amazon.com. Notez que vous pouvez envoyer un ping à un site public sur Internet à partir de l'instance A. Le trafic est autorisé.
4. Connectez-vous à l'instances B à l'aide d'EC2 Instance Connect comme vous l'avez fait dans le scénario 1 et envoyez un ping à www.amazon.com à partir de cette instance. Notez que vous ne pouvez pas envoyer de ping à un site public sur Internet à partir de l'instance B. Le trafic est bloqué.

5. Connectez-vous aux instances C et D à l'aide d'EC2 Instance Connect comme vous l'avez fait dans le scénario 1 et envoyez un ping à www.amazon.com à partir de ces instances. Notez que vous pouvez envoyer un ping à un site public sur Internet à partir des instances C ou D. Le trafic est autorisé.

AWS CLI

1. Envoyez un ping à l'instance A à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 18.225.8.244
```

   Sortie :

```
Pinging 18.225.8.244 with 32 bytes of data:

Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
```

   Notez que le ping est réussi et que le trafic n'est pas bloqué.

2. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

   Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 17:58:12 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
```

```
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.03 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.72 ms
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

3. Envoyez un ping à l'instance B à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 3.18.106.198
```

Sortie :

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Notez que le ping échoue et que le trafic est bloqué.

4. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 18:12:03 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Notez que le ping échoue et que le trafic est bloqué.

5. Connectez-vous à l'instance C. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

6. Connectez-vous à l'instance D. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:00:52 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING
 www.amazon.com(g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologie
 (2600:141f:4000:59a::3bd4)) 56 data bytes
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=1 ttl=48 time=15.9 ms
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=2 ttl=48 time=15.8 ms
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

4.3 Facultatif : vérifier la connectivité l'aide de l'analyseur d'accessibilité

En utilisant le même chemin réseau que celui créé dans l'analyseur d'accessibilité dans le scénario 2, vous pouvez désormais exécuter une nouvelle analyse et confirmer que le chemin est accessible maintenant qu'une exclusion a été créée pour le sous-réseau public A.

Pour plus d'informations sur la disponibilité régionale de l'analyseur d'accessibilité, consultez Considérations dans le Guide de l'analyseur d'accessibilité.

AWS Management Console

1. À partir du chemin réseau que vous avez créé précédemment dans la console Network Insights, cliquez sur Exécuter à nouveau l'analyse.
2. Attendez que l'analyse se termine. Cette opération peut prendre plusieurs minutes.

3. Vérifiez que le chemin est désormais accessible.

AWS CLI

1. À l'aide de l'ID de chemin réseau créé précédemment, lancez une nouvelle analyse :

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-path-id nip-id
```

2. Récupérez les résultats de l'analyse :

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-insights-analysis-ids nia-id
```

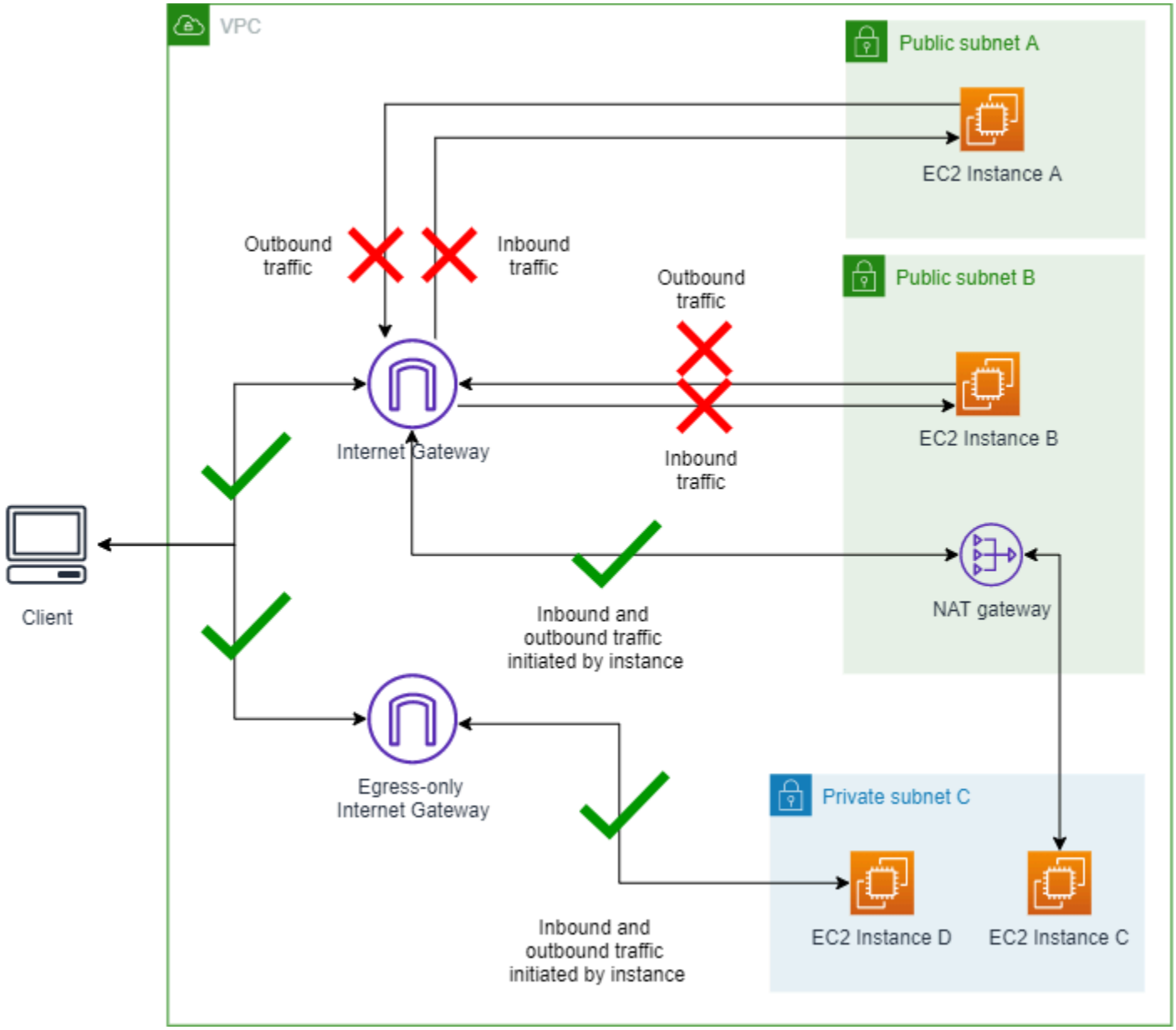
3. Vérifiez que le code d'explication `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` n'est plus présent.

Scénario 5 : modifier le mode d'exclusion

Dans cette section, vous allez modifier la direction du trafic autorisé lors de l'exclusion pour voir son impact sur la fonctionnalité VPC BPA.

> **Note**
>
> Dans ce scénario, vous allez modifier le mode d'exclusion en mode de sortie uniquement. Notez que dans ce cas, l'exclusion de sortie uniquement sur le sous-réseau A n'autorise pas le trafic sortant, ce qui est contraire à la logique, du fait qu'on pourrait s'attendre à ce qu'elle autorise le trafic sortant. Néanmoins, la fonctionnalité BPA au niveau du compte étant en mode d'entrée uniquement, les exclusions de sortie uniquement sont ignorées, et le routage du sous-réseau A vers une passerelle Internet est restreint par la fonctionnalité VPC BPA, bloquant ainsi le trafic sortant. Pour activer le trafic sortant sur le sous-réseau A, il faudrait basculer la fonctionnalité VPC BPA en mode bidirectionnel.

Schéma du mode VPC BPA d'entrée uniquement activé et de l'exclusion du sous-réseau A avec mode de sortie uniquement activé :



5.1 Modifier l'exclusion pour autoriser la direction vers la sortie uniquement

Terminez cette section pour modifier le sens de l'autorisation d'exclusion.

AWS Management Console

1. Modifiez l'exclusion que vous avez créée dans le scénario 4 et modifiez le sens d'autorisation en mode Sortie uniquement.
2. Sélectionnez Enregistrer les modifications.

3. Attendez que l'état d'exclusion passe à Actif. Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour. Vous devrez peut-être actualiser le tableau des exclusions pour voir la modification.

AWS CLI

1. Modifiez le sens d'autorisation de l'exclusion :

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-exclusion --exclusion-
id exclusion-id --internet-gateway-exclusion-mode allow-egress
```

   Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour.

2. La mise à jour de l'état d'exclusion peut prendre un certain temps. Pour afficher l'état de l'exclusion :

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusion
```

5.2 Se connecter à des instances

Terminez cette section pour vous connecter aux instances.

AWS Management Console

1. Envoyez un ping à l' IPv4 adresse publique des instances A et B. Notez que le trafic est bloqué.
2. Connectez-vous aux instances A et B à l'aide d'EC2 Instance Connect comme vous l'avez fait dans le scénario 1 et envoyez un ping à www.amazon.com. Notez que vous ne pouvez pas envoyer de ping à un site public sur Internet à partir des instances A ou B. Le trafic est bloqué.
3. Connectez-vous aux instances C et D à l'aide d'EC2 Instance Connect comme vous l'avez fait dans le scénario 1 et envoyez un ping à www.amazon.com à partir de ces instances. Notez que vous pouvez envoyer un ping à un site public sur Internet à partir des instances C ou D. Le trafic est autorisé.

AWS CLI

1. Envoyez un ping à l'instance A à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 18.225.8.244
```

Sortie :

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Notez que le ping échoue et que le trafic est bloqué.

2. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Notez que le ping échoue et que le trafic est bloqué.

3. Envoyez un ping à l'instance B à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 3.18.106.198
```

Sortie :

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Notez que le ping échoue et que le trafic est bloqué.

4. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Notez que le ping échoue et que le trafic est bloqué.

5. Connectez-vous à l'instance C. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
```

```
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:00:31 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.51 ms
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.49 ms
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

6. Connectez-vous à l'instance D. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:13:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2606:2cc0::374 (2606:2cc0::374)) 56 data bytes
```

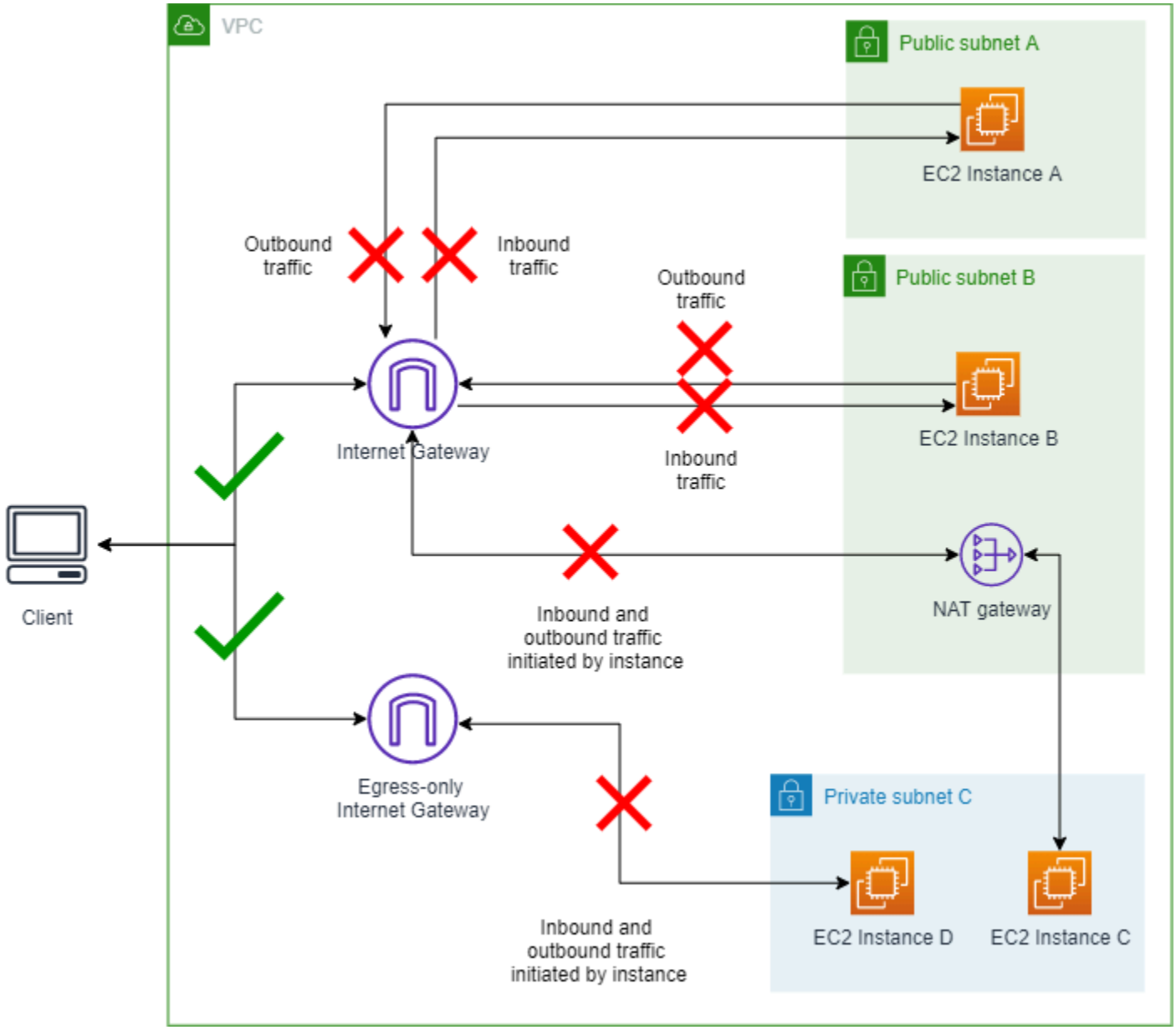
```
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=1 ttl=58 time=1.21 ms
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=2 ttl=58 time=1.51 ms
```

Notez que le ping est réussi et que le trafic n'est pas bloqué.

Scénario 6 : modification du mode de la fonctionnalité VPC BPA

Dans cette section, vous allez modifier la direction du blocage de la fonctionnalité VPC BPA pour voir son impact sur le trafic. Dans ce scénario, le VPC BPA activé en mode bidirectionnel bloque tout le trafic, comme dans le scénario 1. À moins qu'une exclusion ait accès à une passerelle NAT ou à une passerelle Internet de sortie uniquement, le trafic est bloqué.

Schéma du mode VPC BPA bidirectionnel activé et de l'exclusion du sous-réseau A avec mode de sortie uniquement activé :



6.1 Modifier le VPC BPA en mode bidirectionnel

Terminez cette section pour modifier le mode de la fonctionnalité VPC BPA.

AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Choisissez Modifier les paramètres d'accès public.
4. Changez le sens du blocage en Bidirectionnel, puis choisissez Enregistrer les modifications.

5. Attendez que l'état passe à Activé. Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour.

AWS CLI

1. Modifiez le sens de blocage de la fonctionnalité VPC BPA :

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
```

   Cela peut prendre quelques minutes avant que les paramètres VPC BPA prennent effet et que l'état soit mis à jour.
2. Affichez l'état de la fonctionnalité VPC BPA :

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

6.2 Se connecter à des instances

Terminez cette section pour vous connecter aux instances.

AWS Management Console

1. Envoyez un ping à l' IPv4 adresse publique des instances A et B. Notez que le trafic est bloqué.
2. Connectez-vous aux instances A et B à l'aide d'EC2 Instance Connect comme vous l'avez fait dans le scénario 1 et envoyez un ping à www.amazon.com. Notez que vous ne pouvez pas envoyer de ping à un site public sur Internet à partir des instances A ou B. Le trafic est bloqué.
3. Connectez-vous aux instances C et D à l'aide d'EC2 Instance Connect comme vous l'avez fait dans le scénario 1 et envoyez un ping à www.amazon.com à partir de ces instances. Notez que vous ne pouvez pas envoyer de ping à un site public sur Internet à partir des instances C ou D. Le trafic est bloqué.

AWS CLI

1. Envoyez un ping à l'instance A à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 18.225.8.244
```

Sortie :

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Notez que le ping échoue et que le trafic est bloqué.

2. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:17:44 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Notez que le ping échoue et que le trafic est bloqué.

3. Envoyez un ping à l'instance A à l'aide de IPv4 l'adresse publique pour vérifier le trafic entrant :

```
ping 3.18.106.198
```

Sortie :

```
Pinging 3.18.106.198 with 32 bytes of data:
```

```
Request timed out.
```

Notez que le ping échoue et que le trafic est bloqué.

4. Utilisez l' IPv4 adresse privée pour vous connecter et vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Notez que le ping échoue et que le trafic est bloqué.

5. Connectez-vous à l'instance C. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
```

```
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:19:45 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:6200:7:49a5:5fd4:b121
 (2600:9000:25f3:6200:7:49a5:5fd4:b121)) 56 data bytes
```

Notez que le ping échoue et que le trafic est bloqué.

6. Connectez-vous à l'instance D. Comme il n'existe aucune adresse IP publique à laquelle envoyer un ping, utilisez EC2 Instance Connect pour vous connecter, puis envoyez un ping à une adresse IP publique depuis l'instance pour vérifier le trafic sortant :

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Sortie :

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:20:58 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:b400:7:49a5:5fd4:b121
 (2600:9000:25f3:b400:7:49a5:5fd4:b121)) 56 data bytes
```

Notez que le ping échoue et que le trafic est bloqué.

Nettoyage

Dans cette section, vous allez supprimer toutes les ressources que vous avez créées pour cet exemple avancé. Il est important de nettoyer les ressources afin d'éviter des frais supplémentaires pour les ressources créées sur votre compte.

Supprimer les CloudFormation ressources

Complétez cette section pour supprimer les ressources que vous avez créées avec le CloudFormation modèle.

AWS Management Console

1. Ouvrez la CloudFormation console à l'adressehttps://console.aws.amazon.com/cloudformation/.
2. Choisissez la pile VPC BPA.
3. Sélectionnez Delete (Supprimer).
4. Une fois que vous avez commencé à supprimer la pile, affichez l'onglet Événements pour voir la progression et vous assurer que la pile est supprimée. Vous devrez peut-être forcer la suppression de la pile pour qu'elle soit complètement supprimée.

AWS CLI

1. Supprimez la CloudFormation pile. Vous devrez peut-être forcer la suppression de la pile pour qu'elle soit complètement supprimée.

```
aws cloudformation delete-stack --stack-name VPC-BPA-stack --region us-east-2
```

2. Affichez la progression et assurez-vous que la pile est supprimée.

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-east-2
```

Suivez la suppression des exclusions à l'aide de CloudTrail

Complétez cette section pour suivre la suppression des exclusions à l'aide de AWS CloudTrail. CloudTrail des entrées apparaissent lorsque vous supprimez une exclusion.

AWS Management Console

Vous pouvez consulter toutes les exclusions supprimées dans l'historique des CloudTrail événements en recherchant Type de ressource > AWS : :EC2 : : VPCBlock PublicAccessExclusion dans la AWS CloudTrail console à l'adresse. https://console.aws.amazon.com/cloudtrailv2/

AWS CLI

Vous pouvez utiliser la commande lookup-events pour afficher les événements liés à la suppression d'exclusions :

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

L'exemple avancé est terminé.

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.
- Utilisez des groupes de sécurité pour contrôler le trafic vers les instances EC2 dans vos sous-réseaux. Pour de plus amples informations, veuillez consulter Groupes de sécurité.
- Utilisez le réseau ACLs pour contrôler le trafic entrant et sortant au niveau du sous-réseau. Pour de plus amples informations, veuillez consulter Contrôler le trafic des sous-réseaux à l'aide de listes de contrôle d'accès réseau.
- Gérez l'accès aux AWS ressources de votre VPC à l'aide de la fédération d'identité Gestion des identités et des accès AWS (IAM), des utilisateurs et des rôles. Pour de plus amples informations, veuillez consulter 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 de plus amples informations, veuillez consulter Journaux de flux VPC.
- Utilisez l'analyseur d'accès réseau pour identifier les accès réseau involontaires aux ressources de notre. VPCs 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 les réponses aux questions fréquemment posées concernant la sécurité des VPC, consultez la section Sécurité et filtrage dans Amazon VPC. FAQs

Utilisez VPC d'Amazon avec d'autres Services AWS

Amazon Virtual Private Cloud (VPC) est un service AWS de base qui fournit un environnement réseau sécurisé et personnalisable pour votre infrastructure cloud. Au-delà de la création et de la gestion de votre propre VPC, vous pouvez tirer parti de l'intégration entre le VPC et d'autres services AWS pour créer des solutions complètes adaptées à vos besoins spécifiques.

Vous pouvez connecter votre VPC à différents services AWS à l'aide de AWS PrivateLink. Cela permet d'établir une connectivité privée entre votre VPC et vos services AWS pris en charge ou vos applications sur site, en maintenant le trafic réseau au sein du réseau AWS et en évitant l'exposition au réseau Internet public. Cela est particulièrement utile pour maintenir des limites de sécurité et des exigences de conformité strictes.

Pour renforcer davantage la sécurité de votre VPC, vous pouvez utiliser AWS Network Firewall. Ce service de pare-feu géré vous permet de définir et d'appliquer des politiques de sécurité au niveau du réseau, tout en filtrant le trafic nord-sud et est-ouest au sein de votre VPC. En associant Network Firewall à votre VPC, vous pouvez améliorer votre stratégie de défense et protéger vos ressources cloud contre les accès non autorisés ou les activités malveillantes.

En outre, vous pouvez filtrer le trafic DNS au sein de votre VPC à l'aide de Route 53 Resolver DNS Firewall. Cette fonctionnalité vous permet de créer des règles de filtrage DNS personnalisées pour contrôler les domaines que vos ressources VPC peuvent résoudre, fournissant ainsi un niveau supplémentaire de sécurité et de mise en conformité.

Si vous rencontrez des problèmes d'accessibilité entre les ressources de votre VPC ou connectées à votre VPC, vous pouvez utiliser l'analyseur d'accessibilité. L'analyseur d'accessibilité effectue des tests de connectivité virtuelle, fournit des informations détaillées sur le chemin saut par saut et identifie les composants bloquants. Cet outil de dépannage peut vous aider à identifier et à résoudre rapidement les problèmes de connectivité réseau.

En intégrant ces services AWS complémentaires à votre VPC, vous pouvez créer des solutions cloud puissantes, sécurisées et résilientes qui répondent à vos exigences commerciales et architecturales uniques.

Table des matières

- Filtrage du trafic DNS utilisant Route 53 Resolver DNS pare-feu
- Résoudre les problèmes d'accessibilité à l'aide de l'analyseur d'accessibilité

Connexion de votre VPC à des services avec AWS PrivateLink

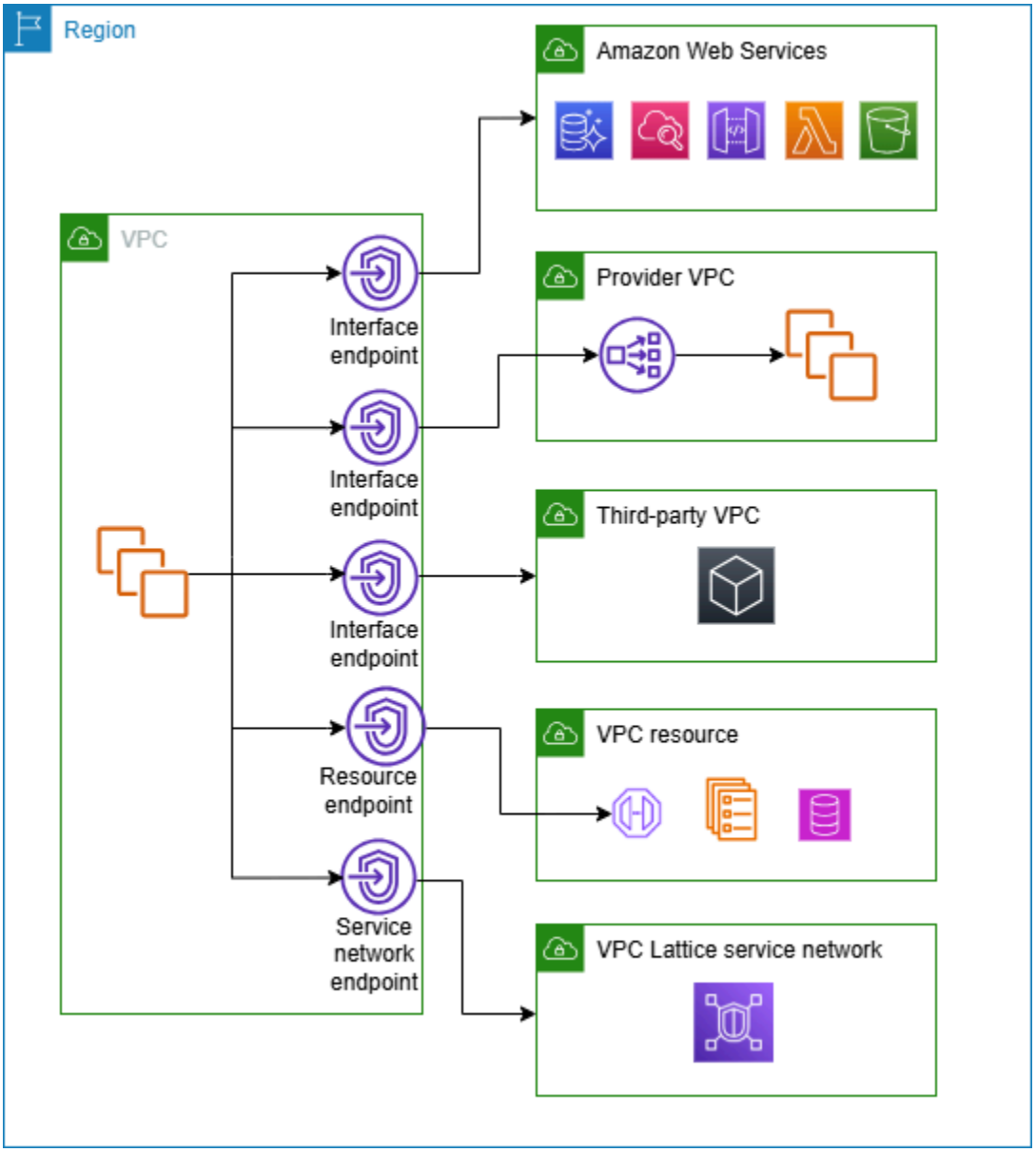
AWS PrivateLink établit une connectivité privée entre les clouds privés virtuels (VPC) et les services Services AWS pris en charge, les services hébergés par d'autres Comptes AWS, les services AWS Marketplace pris en charge et les ressources prises en charge. Pour communiquer avec le service ou la ressource, vous n'avez pas besoin de passerelle Internet, de périphérique NAT, de connexion de Direct Connect ou de connexion AWS Site-to-Site VPN.

Pour utiliser AWS PrivateLink, créez un point de terminaison de VPC dans tous les sous-réseaux à partir desquels vous devez accéder au service ou à la ressource. Cela crée dans les sous-réseaux spécifiés des interfaces réseau Elastic qui servent de points d'entrée au trafic destiné au service ou à la ressource.

Vous pouvez également créer votre propre service de point de terminaison d'un VPC, optimisé par la technologie AWS PrivateLink, et permettre à d'autres clients AWS d'accéder à votre service. PrivateLink permet de créer des points de terminaison d'API privée, permettant aux organisations de présenter leurs propres services en toute sécurité à d'autres clients AWS. Cela permet aux entreprises de monétiser leurs capacités internes, de favoriser les écosystèmes collaboratifs et de garder le contrôle sur la manière dont leurs services sont consultés et consommés.

L'un des principaux avantages de l'utilisation de AWS PrivateLink est la possibilité d'établir une connectivité privée et sécurisée sans avoir besoin de structures de mise en réseau traditionnelles telles que les passerelles Internet, les périphériques NAT ou les connexions VPN. Cela permet de simplifier l'architecture réseau, de réduire la surface d'attaque et d'améliorer la sécurité globale en limitant le trafic de données au sein du réseau AWS.

Le diagramme suivant illustre des cas d'utilisation courants pour AWS PrivateLink. Le VPC dispose de plusieurs instances EC2 dans un sous-réseau privé qui ont accès aux ressources via cinq points de terminaison de VPC : trois points de terminaison de VPC d'interface, un point de terminaison de VPC de ressource et un point de terminaison de VPC de réseau de services.



Pour de plus amples informations, consultez 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 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.

Ressource de pare-feu DNS	Description
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 l'analyseur d'accessibilité

L'analyseur d'accessibilité est un outil d'analyse de configuration statique. Utilisez l'analyseur d'accessibilité pour analyser et déboguer l'accessibilité réseau entre deux ressources dans votre VPC. L'analyseur d'accessibilité produit des détails saut par saut du chemin virtuel entre ces ressources lorsqu'elles sont accessibles, et identifie le composant bloquant dans le cas contraire.

Vous pouvez utiliser l'analyseur d'accessibilité 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

Amazon Virtual Private Cloud (VPC) est un élément fondamental de l'écosystème AWS, qui vous permet de mettre en service des réseaux virtuels isolés adaptés à vos besoins spécifiques. En créant et en gérant vos propres VPC, vous obtenez un contrôle total sur l'environnement réseau, y compris la possibilité de définir des plages d'adresses IP, des sous-réseaux, des tables de routage et des options de connectivité.

Cette section contient trois exemples de configuration de vos clouds privés virtuels (VPC), chacun étant conçu pour répondre à un ensemble d'exigences différent :

- VPC pour un environnement de test : cette configuration montre comment créer un VPC que vous pouvez utiliser comme environnement de développement ou de test.
- VPC pour les serveurs web et de base de données : cette configuration montre comment créer un VPC que vous pouvez utiliser pour une architecture résiliente dans un environnement de production.
- VPC avec serveurs dans des sous-réseaux privés et NAT : dans cette configuration plus avancée, toutes les instances EC2 sont provisionnées dans des sous-réseaux privés, avec une passerelle NAT facilitant un accès Internet sortant sécurisé. Il s'agit d'un exemple dans lequel vous devez limiter la connectivité Internet directe à vos ressources tout en permettant les communications sortantes nécessaires.

En fournissant ces exemples de configuration de VPC, nous espérons illustrer les options de flexibilité et de personnalisation disponibles lors de la conception de votre environnement réseau cloud. La configuration VPC spécifique que vous choisissez doit être basée sur l'architecture de votre application, vos exigences de sécurité et vos objectifs commerciaux généraux. Une planification minutieuse de votre infrastructure VPC peut vous aider à créer un réseau virtuel robuste, évolutif et sécurisé qui soutient la croissance et l'évolution de vos charges de travail basées sur le cloud.

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 Site-to-Site VPN scenarios dans le Guide d'utilisation d'AWS Site-to-Site VPN.
- Pour connecter vos VPC entre eux et à votre propre réseau, consultez Example transit gateway scenarios sur la page consacrée aux 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

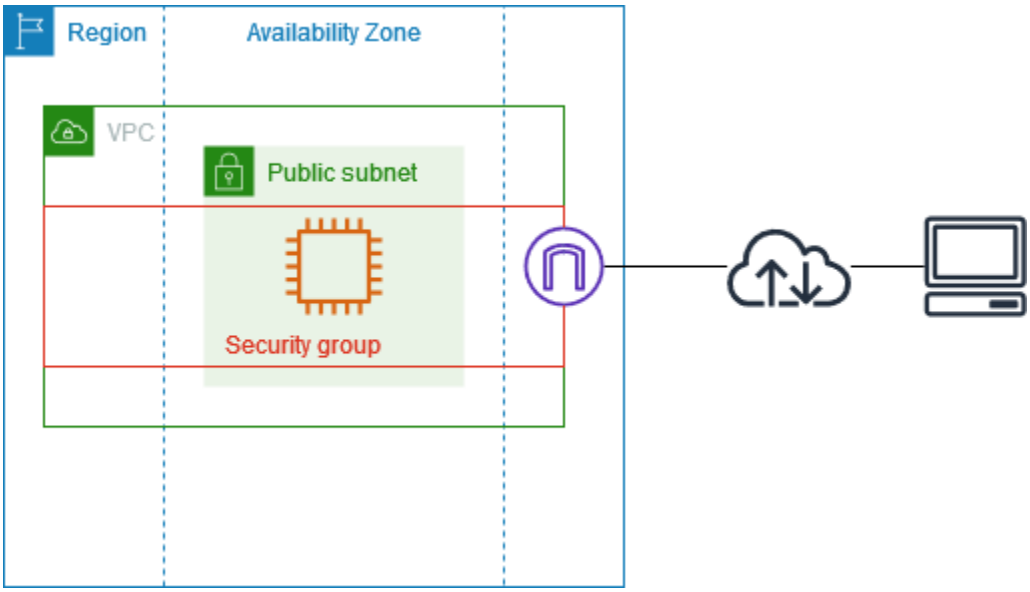
Cet exemple montre comment créer un VPC que vous pouvez utiliser comme environnement de développement ou de test. Ce VPC n'étant pas destiné à être utilisé en production, il n'est pas nécessaire de déployer vos serveurs dans plusieurs zones de disponibilité. Pour réduire les coûts et la complexité, vous pouvez déployer vos serveurs dans une seule zone de disponibilité.

Table des matières

Présentation de

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 itinéraires pour les deux IPv4 et IPv6. Si vous créez un sous-réseau IPv4 uniquement au lieu d'un sous-réseau à double pile, votre table de routage ne contient que les routes. IPv4

Destination	Target
10.0.0.0/16	local
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 les deux IPv4 et IPv6. Si vous créez des sous-réseaux IPv4 uniquement au lieu de sous-réseaux à double pile, vous n'avez besoin que des règles pour. IPv4

Source	Protocole	Plage de ports	Description
0.0.0.0/0	TCP	80	Autorise l'accès HTTP entrant à partir de toutes les adresses IPv4
::/0	TCP	80	Autorise l'accès HTTP entrant à partir de toutes les adresses IPv6
0.0.0.0/0	TCP	443	Autorise l'accès HTTPS entrant depuis toutes les adresses IPv4
::/0	TCP	443	Autorise l'accès HTTPS entrant depuis toutes les adresses IPv6
Public IPv4 address range of your network	TCP	22	(Facultatif) Autorise l'accès SSH entrant à partir des adresses IPv4 IP de votre réseau
IPv6 address range of your network	TCP	22	(Facultatif) Autorise l'accès SSH entrant à partir des adresses IPv6 IP de votre réseau
Public IPv4 address range of your network	TCP	3389	(Facultatif) Autorise l'accès RDP entrant à partir des adresses IPv4 IP de votre réseau
IPv6 address range of your network	TCP	3389	(Facultatif) Autorise l'accès RDP entrant à partir des adresses IPv6 IP de votre réseau

1. 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 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. Configurer le VPC
    a. Pour Name tag auto-generation (Génération automatique de balises de nom), saisissez un nom pour le VPC.
    b. Pour le bloc d'adresse IPv4 CIDR, 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' IPv6 adresses, choisissez le bloc IPv6 CIDR, le bloc CIDR fourni par Amazon IPv6 .
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 bien vous pouvez développer Personnaliser AZs 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).

2. 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, consultez Create an AMI dans le Guide d'utilisation d'Amazon EC2. Vous pouvez également utiliser EC2 Image Builder pour créer et gérer votre Amazon Machine Image (AMI).

3. 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.

4. 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”.

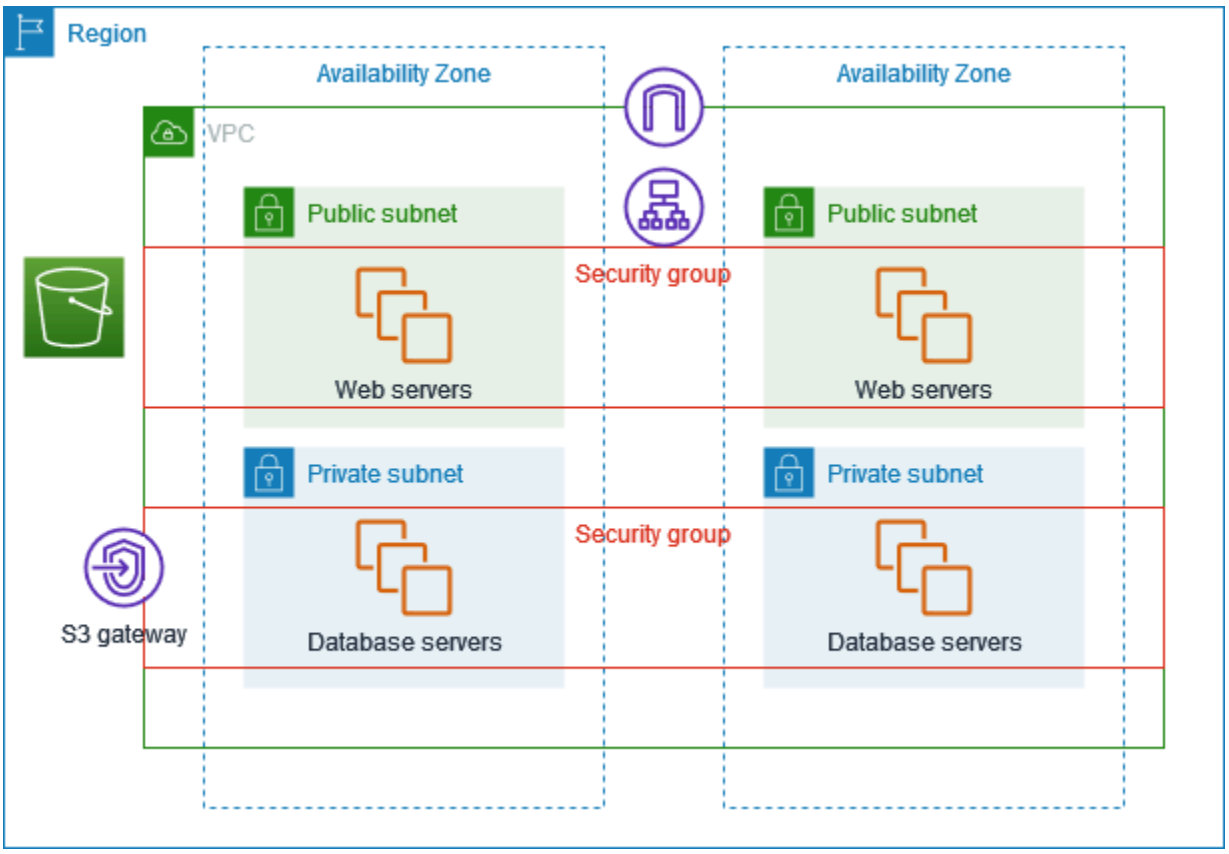
Exemple : VPC pour serveurs web et de base de données

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 de

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 itinéraires pour les deux IPv4 et IPv6. Si vous créez des sous-réseaux IPv4 uniquement au lieu de sous-réseaux à double pile, votre table de routage ne contient que les routes. IPv4

Destination	Target
10.0.0.0/16	local
2001:db8:1234:1a00::/56	locale
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Voici un exemple de table de routage pour les sous-réseaux privés, avec des itinéraires locaux pour les deux IPv4 et IPv6. Si vous avez créé des sous-réseaux IPv4 réservés, votre table de routage contient uniquement l' IPv4 itinéraire. La dernière route envoie le trafic destiné à Amazon S3 vers le point de terminaison d'un VPC de la passerelle.

Destination	Target
10.0.0.0/16	local
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.

Source	Protocole	Plage de ports	Description
ID of the security group for the load balancer	TCP	80	Autorise l'accès HTTP entrant depuis l'équilibreur de charge
ID of the security group for the load balancer	TCP	443	Autorise l'accès HTTPS entrant depuis l'équilibreur de charge
Public IPv4 address range of your network	TCP	22	(Facultatif) Autorise l'accès SSH entrant à partir des adresses IPv4 IP de votre réseau
IPv6 address range of your network	TCP	22	(Facultatif) Autorise l'accès SSH entrant à partir des adresses IPv6 IP de votre réseau

Source	Protocole	Plage de ports	Description
Public IPv4 address range of your network	TCP	3389	(Facultatif) Autorise l'accès RDP entrant à partir des adresses IPv4 IP de votre réseau
IPv6 address range of your network	TCP	3389	(Facultatif) Autorise l'accès RDP entrant à partir des adresses IPv6 IP de votre réseau

Destination	Protocole	Plage de ports	Description
ID of the security group for instances running Microsoft SQL Server	TCP	1433	Autorise l'accès Microsoft SQL Server sortant aux serveurs de base de données
ID of the security group for instances running 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.

Source	Protocole	Plage de ports	Commentaires
ID of the web server security group	TCP	1433	Autorise l'accès entrant Microsoft SQL Server depuis les serveurs web

Source	Protocole	Plage de ports	Commentaires
ID of the web server security group	TCP	3306	Autorise l'accès entrant MySQL Server depuis les serveurs web

Destination	Protocole	Plage de ports	Commentaires
0.0.0.0/0	TCP	80	Autorise l'accès HTTP sortant à Internet via IPv4
0.0.0.0/0	TCP	443	Autorise l'accès HTTPS sortant à Internet via 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.

1. 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 l'option Génération automatique de balise 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 le bloc d'adresse IPv4 CIDR, 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' IPv6 adresses, choisissez le bloc IPv6 CIDR, le bloc CIDR fourni par Amazon IPv6 .

d. Choisissez une option de location. Cette option définit si EC2 les instances que vous lancez dans le VPC s'exécuteront sur du matériel partagé avec d'autres Comptes AWS ou sur du matériel dédié à votre usage uniquement. Si vous choisissez la location du VPC EC2 , les instances lancées dans ce VPC utiliseront l'attribut de location spécifié lors du lancement de l'instance. `Default` Pour plus d'informations, consultez Lancer une instance à l'aide de paramètres définis dans le guide de EC2 l'utilisateur Amazon. 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 publics ou développer Personnaliser les blocs CIDR des sous-réseaux 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 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).

2. 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 EC2 des instances pour vos serveurs Web. Il existe différentes manières de déployer des EC2 instances. Par exemple :

- Assistant de EC2 lancement d'instance Amazon
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Pour 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 EC2 des instances pour vos serveurs de base de données ou l'un de nos types de bases de données spécialement conçus. Pour plus d'informations, voir Bases de données sur AWS : Comment choisir.

3. 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.

4. 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 de plus amples informations, veuillez consulter the section called “Supprimer votre VPC”.

Exemple : VPC avec des serveurs dans des sous-réseaux privés et NAT

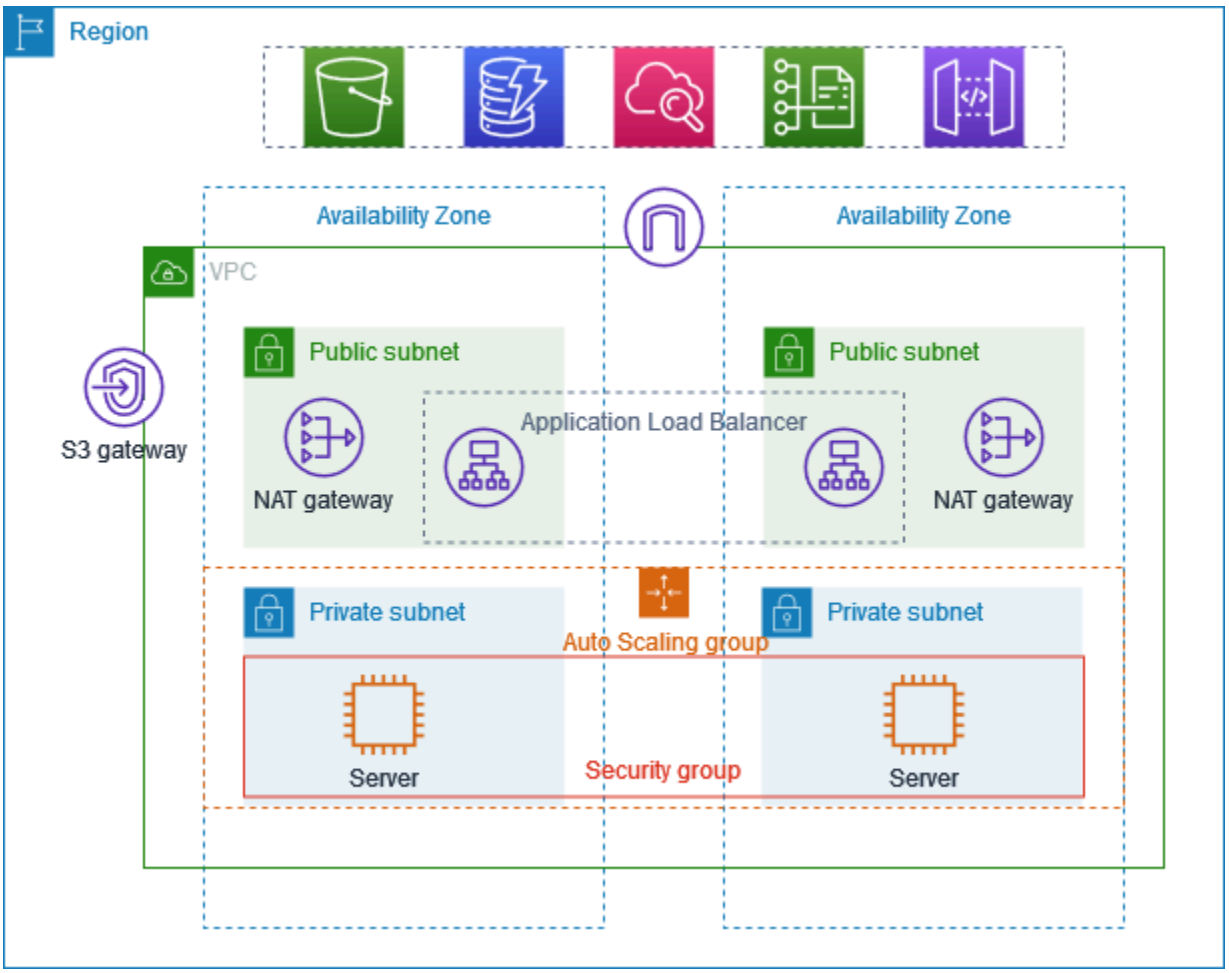
Cet exemple montre comment créer un VPC que vous pouvez utiliser pour les serveurs d'un environnement de production. Pour améliorer la résilience, vous déployez les serveurs dans

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 de

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 itinéraires pour les deux IPv4 et IPv6. Si vous créez des sous-réseaux IPv4 uniquement au lieu de sous-réseaux à double pile, votre table de routage inclut uniquement les itinéraires. IPv4

Destination	Target
10.0.0.0/16	local

Destination	Target
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 itinéraires pour les deux sous-réseaux IPv4 et IPv6. Si vous avez créé des sous-réseaux IPv4 réservés, la table de routage inclut uniquement les IPv4 itinéraires. La dernière route envoie le trafic destiné à Amazon S3 vers le point de terminaison d'un VPC de la passerelle.

Destination	Target
10.0.0.0/16	local
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.

Source	Protocole	Plage de ports	Commentaires
ID of the load balancer security group	*listener protocol*	*listener port*	Autorise tout le trafic entrant depuis l'équilibreur de charge sur le port d'écoute

Source	Protocole	Plage de ports	Commentaires
ID of the load balancer security group	*health check protocol*	*health check port*	Autorise le trafic de surveillance de l'état entrant depuis l'équilibreur de charge

1. 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 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. Configurer le VPC
    a. Pour Name tag auto-generation (Génération automatique de balises de nom), saisissez un nom pour le VPC.
    b. Pour le bloc d'adresse IPv4 CIDR, 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' IPv6 adresses, choisissez le bloc IPv6CIDR, le bloc CIDR fourni par Amazon IPv6 .
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' IPv6 adresses, pour la passerelle Internet de sortie uniquement, sélectionnez 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).

2. 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 EC2 instances à l'aide d'Amazon EC2 Auto Scaling. Pour obtenir des step-by-step instructions, consultez la section Créer un modèle de lancement pour votre groupe Auto Scaling dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.
2. Créez un groupe Auto Scaling, qui est un ensemble d' EC2 instances avec une taille minimale, maximale et souhaitée. Pour obtenir des step-by-step instructions, consultez Create an Auto Scaling group using a launch template (Créer un groupe Auto Scaling à l'aide d'un modèle de lancement) 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 d'Elastic Load Balancing et utilisez Elastic Load Balancing dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

3. 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.

4. 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”.

Didacticiels de VPC

Le cloud privé virtuel (VPC) Amazon constitue la base de votre infrastructure réseau dans AWS. La console de gestion AWS fournit une interface conviviale, tandis que l'interface de ligne de commande (CLI) AWS offre une plus grande flexibilité et des fonctionnalités d'automatisation pour la création et la gestion de vos ressources VPC.

Ce guide présente deux scénarios essentiels de déploiement de VPC :

- Une configuration VPC de base avec un sous-réseau public, idéale pour les applications web simples
- Une configuration VPC avancée avec des sous-réseaux privés et publics utilisant des passerelles NAT, adaptée aux applications multiniveaux

Ces tutoriels vous apprendront à effectuer les opérations suivantes :

- Créer des VPC avec différentes configurations de sous-réseaux
- Configurer des passerelles Internet et NAT
- Configurer des tables de routage et des groupes de sécurité
- Gérer votre infrastructure réseau à l'aide des commandes de l'AWS CLI
- Mettre en œuvre les bonnes pratiques AWS en matière de mise en réseau

Vous allez commencer par créer votre infrastructure réseau AWS à l'aide de la ligne de commande.

Didacticiels

- Commencer à utiliser Amazon VPC à l'aide de la CLI AWS
- Création d'un VPC avec des sous-réseaux privés et des passerelles NAT à l'aide de l'AWS CLI

Commencer à utiliser Amazon VPC à l'aide de la CLI AWS

Ce didacticiel vous explique comment créer un Virtual Private Cloud (VPC) à l'aide de l'interface de ligne de AWS commande ().AWS CLI Vous apprendrez à configurer un VPC avec des sous-réseaux publics et privés, à configurer la connectivité Internet et à déployer des EC2 instances pour démontrer une architecture d'application Web commune.

Conditions préalables

Avant de démarrer ce tutoriel, assurez-vous de disposer des éléments suivants :

1. Le AWS CLI. Si vous devez l'installer, suivez les instructions du Guide d'installation de l'AWS CLI.
2. Vous avez configuré AWS CLI avec les informations d'identification appropriées. Si vous n'avez pas encore configuré vos informations d'identification, exécutez la commande `aws configure`.
3. Des connaissances de base sur les concepts de mise en réseau.
4. Identity and Access Management pour Amazon VPCpour créer et gérer les ressources VPC de votre AWS compte.

Considérations de coût

Ce didacticiel crée AWS des ressources susceptibles d'entraîner des coûts sur votre compte. Le coût principal provient de la passerelle NAT (0,045$ de l'heure plus les frais de traitement des données) et des EC2 instances (t2.micro, environ 0,0116$ de l'heure chacune). Si vous exécutez le tutoriel en une heure et que vous nettoyez ensuite toutes les ressources, le coût total s'élèvera à environ 0,07 USD. Pour optimiser les coûts dans les environnements de développement, vous pouvez utiliser une instance NAT plutôt qu'une passerelle NAT. Cela peut réduire considérablement les coûts.

Vérifions-nous que le vôtre AWS CLI est correctement configuré avant de continuer.

```
aws configure list
```

Vous devriez voir votre clé AWS d'accès, votre clé secrète et votre région par défaut. Vérifiez également que vous disposez des autorisations requises pour créer des ressources VPC.

```
aws sts get-caller-identity
```

Cette commande affiche votre identifiant de AWS compte, votre identifiant utilisateur et votre ARN pour confirmer que vos informations d'identification sont valides.

Création d'un VPC

Un Virtual Private Cloud (VPC) est un réseau virtuel dédié à votre compte. AWS Dans cette section, vous allez créer un VPC avec le bloc CIDR 10.0.0.0/16, qui fournit jusqu'à 65 536 adresses IP.

Création du VPC

La commande suivante crée un VPC et lui attribue une balise de nom.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=MyVPC}]'
```

Notez l'ID de VPC indiqué dans la sortie. Vous en aurez besoin pour les commandes suivantes. Ce tutoriel utilise l'ID de VPC « vpc-0123456789abcdef0 » comme exemple. Remplacez-le par votre ID de VPC réel dans toutes les commandes.

Activation de la prise en charge du DNS et des noms d'hôte

Par défaut, la résolution DNS et les noms d'hôte DNS sont désactivés dans un nouveau VPC. Activez ces fonctionnalités pour permettre aux instances de votre VPC de résoudre les noms de domaine.

```
aws ec2 modify-vpc-attribute --vpc-id vpc-0123456789abcdef0 --enable-dns-support
aws ec2 modify-vpc-attribute --vpc-id vpc-0123456789abcdef0 --enable-dns-hostnames
```

Ces commandes ne génèrent aucune sortie lorsqu'elles aboutissent. La prise en charge du DNS et la résolution des noms d'hôte sont désormais activées pour votre VPC.

Création de sous-réseaux

Les sous-réseaux sont des segments d'une plage d'adresses IP d'un VPC dans lesquels vous pouvez placer des groupes de ressources isolées. Dans cette section, vous allez créer des sous-réseaux publics et privés dans deux zones de disponibilité pour assurer un haut niveau de disponibilité.

Accès aux zones de disponibilité disponibles

Commencez par récupérer les zones de disponibilité disponibles dans votre région.

```
aws ec2 describe-availability-zones
```

Dans ce tutoriel, vous utiliserez les deux premières zones de disponibilité. Notez leurs noms dans la sortie (par exemple, « us-east-1a » et « us-east-1b »).

Création de sous-réseaux publics

Les sous-réseaux publics sont utilisés pour les ressources qui doivent être accessibles depuis Internet, telles que les serveurs web.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-AZ1}]'
```

Notez l'ID de sous-réseau indiqué dans la sortie. Ce tutoriel utilise « subnet-0123456789abcdef0 » comme exemple pour le premier sous-réseau public.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.1.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-AZ2}]'
```

Notez l'ID de sous-réseau indiqué dans la sortie. Ce tutoriel utilise « subnet-0123456789abcdef1 » comme exemple pour le deuxième sous-réseau public.

Créer des sous-réseaux privés

Les sous-réseaux privés sont utilisés pour les ressources qui n'ont pas besoin d'être accessibles directement depuis Internet, comme les bases de données.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.2.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-AZ1}]'
```

Notez l'ID de sous-réseau indiqué dans la sortie. Ce tutoriel utilise « subnet-0123456789abcdef2 » comme exemple pour le premier sous-réseau privé.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.3.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-AZ2}]'
```

Notez l'ID de sous-réseau indiqué dans la sortie. Ce tutoriel utilise « subnet-0123456789abcdef3 » comme exemple pour le deuxième sous-réseau privé.

Vous disposez désormais de quatre sous-réseaux, deux publics et deux privés, répartis sur deux zones de disponibilité.

Conseil : lorsque vous planifiez vos blocs CIDR, assurez-vous qu'ils ne chevauchent pas vos réseaux existants. Pour les environnements de production, allouez suffisamment d'adresses IP pour anticiper la croissance future tout en conservant des sous-réseaux de taille raisonnable pour des questions de sécurité et de gestion.

Configuration de la connectivité Internet

Pour permettre aux ressources de votre VPC de communiquer avec Internet, vous devez créer et attacher une passerelle Internet. Dans cette section, vous allez configurer la connectivité Internet pour votre VPC.

Création d'une passerelle Internet

Une passerelle Internet permet la communication entre votre VPC et Internet.

```
aws ec2 create-internet-gateway \
  --tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name,Value=MyIGW}]'
```

Notez l'ID de passerelle Internet indiqué dans la sortie. Ce tutoriel utilise « igw-0123456789abcdef0 » comme exemple.

Attachement de la passerelle Internet à votre VPC

Après avoir créé la passerelle Internet, vous devez l'attacher à votre VPC.

```
aws ec2 attach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0
```

Création et configuration de tables de routage

Les tables de routage contiennent des règles (routes) qui déterminent où le trafic réseau est dirigé. Commencez par créer une table de routage pour vos sous-réseaux publics.

```
aws ec2 create-route-table \
  --vpc-id vpc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Public-RT}]'
```

Notez l'ID de table de routage indiqué dans la sortie. Ce tutoriel utilise « rtb-0123456789abcdef0 » comme exemple pour la table de routage publique.

Ajoutez à la table de routage publique une route vers la passerelle Internet.

```
aws ec2 create-route --route-table-id rtb-0123456789abcdef0 --destination-cidr-block
 0.0.0.0/0 --gateway-id igw-0123456789abcdef0
```

Associez les sous-réseaux publics à la table de routage publique.

```
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef0 --subnet-id
 subnet-0123456789abcdef0
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef0 --subnet-id
 subnet-0123456789abcdef1
```

Créez à présent une table de routage pour vos sous-réseaux privés.

```
aws ec2 create-route-table \
  --vpc-id vpc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Private-RT}]'
```

Notez l'ID de table de routage indiqué dans la sortie. Ce tutoriel utilise « rtb-0123456789abcdef1 » comme exemple pour la table de routage privée.

Associez les sous-réseaux privés à la table de routage privée.

```
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef1 --subnet-id
 subnet-0123456789abcdef2
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef1 --subnet-id
 subnet-0123456789abcdef3
```

Création d'une passerelle NAT

Une passerelle NAT permet aux instances des sous-réseaux privés d'envoyer le trafic sortant vers Internet tout en bloquant le trafic entrant en provenance d'Internet. Son rôle est essentiel pour les instances qui doivent télécharger des mises à jour ou accéder à des services externes.

Allocation d'une adresse IP Elastic

Commencez par allouer une adresse IP Elastic à votre passerelle NAT.

```
aws ec2 allocate-address --domain vpc
```

Notez l'ID d'allocation indiqué dans la sortie. Ce tutoriel utilise « eipalloc-0123456789abcdef0 » comme exemple.

Création de la passerelle NAT

Créez une passerelle NAT dans l'un de vos sous-réseaux publics à l'aide de l'adresse IP Elastic allouée.

```
aws ec2 create-nat-gateway \
  --subnet-id subnet-0123456789abcdef0 \
  --allocation-id eipalloc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=MyNATGateway}]'
```

Notez l'ID de passerelle NAT indiqué dans la sortie. Ce tutoriel utilise « nat-0123456789abcdef0 » comme exemple.

Attendez que la passerelle NAT soit disponible pour poursuivre.

```
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-0123456789abcdef0
```

Ajout d'une route vers la passerelle NAT

Ajoutez à la table de routage privée une route vers la passerelle NAT pour permettre aux instances des sous-réseaux privés d'accéder à Internet.

```
aws ec2 create-route --route-table-id rtb-0123456789abcdef1 --destination-cidr-block
 0.0.0.0/0 --nat-gateway-id nat-0123456789abcdef0
```

Remarque : dans les environnements de production, il peut être utile de créer une passerelle NAT dans chaque zone de disponibilité comprenant des sous-réseaux privés pour éliminer les points de défaillance uniques.

Configuration des paramètres des sous-réseaux

Configurez vos sous-réseaux publics pour qu'ils attribuent automatiquement des adresses IP publiques aux instances qui y sont lancées.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-0123456789abcdef0 --map-public-ip-
on-launch
aws ec2 modify-subnet-attribute --subnet-id subnet-0123456789abcdef1 --map-public-ip-
on-launch
```

Vous aurez ainsi la garantie que les instances lancées dans vos sous-réseaux publics reçoivent une adresse IP publique par défaut qui les rend accessibles depuis Internet.

Création de groupes de sécurité

Les groupes de sécurité agissent comme des pare-feu virtuels pour vos instances afin de contrôler le trafic entrant et sortant. Dans cette section, vous allez créer des groupes de sécurité pour les serveurs web et les serveurs de base de données.

Création d'un groupe de sécurité pour les serveurs web

```
aws ec2 create-security-group \
  --group-name WebServerSG \
  --description "Security group for web servers" \
  --vpc-id vpc-0123456789abcdef0
```

Notez l'ID de groupe de sécurité indiqué dans la sortie. Ce tutoriel utilise « sg-0123456789abcdef0 » comme exemple pour le groupe de sécurité des serveurs web.

Autorisez le trafic HTTP et HTTPS vers vos serveurs web.

```
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef0 --protocol tcp
 --port 80 --cidr 0.0.0.0/0
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef0 --protocol tcp
 --port 443 --cidr 0.0.0.0/0
```

Remarque : dans les environnements de production, limitez le trafic entrant à des plages d'adresses IP spécifiques au lieu d'autoriser le trafic provenant de 0.0.0.0/0 (n'importe quelle adresse IP).

Création d'un groupe de sécurité pour les serveurs de base de données

```
aws ec2 create-security-group \
  --group-name DBServerSG \
```

```
  --description "Security group for database servers" \
  --vpc-id vpc-0123456789abcdef0
```

Notez l'ID de groupe de sécurité indiqué dans la sortie. Ce tutoriel utilise « sg-0123456789abcdef1 » comme exemple pour le groupe de sécurité des serveurs de base de données.

Autoriser MySQL/Aurora le trafic provenant des serveurs Web uniquement.

```
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef1 --protocol tcp
 --port 3306 --source-group sg-0123456789abcdef0
```

Cette configuration garantit que seules les instances du groupe de sécurité des serveurs web peuvent se connecter à vos serveurs de base de données sur le port 3306, conformément au principe du moindre privilège.

Vérification de votre configuration VPC

Après avoir créé tous les composants nécessaires, vérifiez que la configuration de votre VPC est correcte.

Vérification de votre VPC

```
aws ec2 describe-vpcs --vpc-id vpc-0123456789abcdef0
```

Vérification de vos sous-réseaux

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Vérification de vos tables de routage

```
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Vérification de votre passerelle Internet

```
aws ec2 describe-internet-gateways --filters "Name=attachment.vpc-
id,Values=vpc-0123456789abcdef0"
```

Vérification de votre passerelle NAT

```
aws ec2 describe-nat-gateways --filter "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Vérification de vos groupes de sécurité

```
aws ec2 describe-security-groups --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Ces commandes fournissent des informations détaillées sur chaque composant de votre VPC pour vous permettre de vérifier que tout est correctement configuré.

Déployer EC2 des instances

Maintenant que vous avez créé votre infrastructure VPC, vous pouvez déployer des EC2 instances pour démontrer le fonctionnement de l'architecture. Vous allez lancer un serveur web dans un sous-réseau public et un serveur de base de données dans un sous-réseau privé.

Création d'une paire de clés pour l'accès SSH

Commencez par créer une paire de clés pour vous connecter en toute sécurité à vos instances :

```
aws ec2 create-key-pair --key-name vpc-tutorial-key --query 'KeyMaterial' --output text
 > vpc-tutorial-key.pem
chmod 400 vpc-tutorial-key.pem
```

Cette commande crée une paire de clés et enregistre la clé privée dans un fichier sur lequel les autorisations sont restreintes.

Recherche de l'AMI Amazon Linux 2 la plus récente

Recherchez l'AMI Amazon Linux 2 la plus récente à utiliser pour vos instances :

```
aws ec2 describe-images --owners amazon \
  --filters "Name=name,Values=amzn2-ami-hvm-*-x86_64-gp2" "Name=state,Values=available"
 \
  --query "sort_by(Images, &CreationDate)[-1].ImageId" --output text
```

Notez l'ID d'AMI indiqué dans la sortie. Ce tutoriel utilise « ami-0123456789abcdef0 » comme exemple.

Lancement d'un serveur web dans le sous-réseau public

Maintenant, lancez une EC2 instance dans le sous-réseau public pour qu'elle serve de serveur Web :

```
aws ec2 run-instances \
  --image-id ami-0123456789abcdef0 \
  --count 1 \
  --instance-type t2.micro \
  --key-name vpc-tutorial-key \
  --security-group-ids sg-0123456789abcdef0 \
  --subnet-id subnet-0123456789abcdef0 \
  --associate-public-ip-address \
  --user-data '#!/bin/bash
               yum update -y
               yum install -y httpd
               systemctl start httpd
               systemctl enable httpd
               echo "<h1>Hello from $(hostname -f)</h1>" > /var/www/html/index.html' \
  --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=WebServer}]'
```

Notez l'ID d'instance indiqué dans la sortie. Ce tutoriel utilise « i-0123456789abcdef0 » comme exemple pour l'instance de serveur web.

Lancement d'un serveur de base de données dans le sous-réseau privé

Ensuite, lancez une EC2 instance dans le sous-réseau privé pour servir de serveur de base de données :

```
aws ec2 run-instances \
  --image-id ami-0123456789abcdef0 \
  --count 1 \
  --instance-type t2.micro \
  --key-name vpc-tutorial-key \
  --security-group-ids sg-0123456789abcdef1 \
  --subnet-id subnet-0123456789abcdef2 \
  --user-data '#!/bin/bash
               yum update -y
               yum install -y mariadb-server
               systemctl start mariadb
               systemctl enable mariadb' \
  --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=DBServer}]'
```

Notez l'ID d'instance indiqué dans la sortie. Ce tutoriel utilise « i-0123456789abcdef1 » comme exemple pour l'instance de serveur de base de données.

Accès à votre serveur web

Une fois que votre instance de serveur web est en cours d'exécution, vous pouvez y accéder à l'aide de son adresse IP publique :

```
aws ec2 describe-instances \
  --instance-ids i-0123456789abcdef0 \
  --query 'Reservations[0].Instances[0].PublicIpAddress' \
  --output text
```

Cette commande renvoie l'adresse IP publique de votre serveur web. Ce tutoriel utilise « 203.0.113.10 » comme exemple.

Vous pouvez désormais ouvrir cette URL dans votre navigateur web : http://203.0.113.10

Connexion à vos instances à l'aide de SSH

Pour vous connecter à votre serveur web :

```
ssh -i vpc-tutorial-key.pem ec2-user@203.0.113.10
```

Pour vous connecter à votre serveur de base de données, vous devez d'abord vous connecter en SSH à votre serveur web, puis à votre serveur de base de données :

```
# Get the private IP of the database server
aws ec2 describe-instances \
  --instance-ids i-0123456789abcdef1 \
  --query 'Reservations[0].Instances[0].PrivateIpAddress' \
  --output text
```

Cette commande renvoie l'adresse IP privée de votre serveur de base de données. Ce tutoriel utilise « 10.0.2.10 » comme exemple.

```
# First SSH to web server, then to database server
ssh -i vpc-tutorial-key.pem -A ec2-user@203.0.113.10
ssh ec2-user@10.0.2.10
```

Dans l'architecture réseau que vous avez créée, le serveur web est accessible publiquement tandis que le serveur de base de données n'est accessible que depuis le VPC.

Résolution des problèmes

Cette section présente des problèmes courants que vous pouvez rencontrer lors de la création d'un VPC et les solutions appropriées :

Chevauchements de blocs CIDR

Si vous recevez un message d'erreur concernant le chevauchement des blocs d'adresse CIDR, assurez-vous que les blocs d'adresse CIDR de votre VPC et de vos sous-réseaux ne se chevauchent pas avec les sous-réseaux existants VPCs ou les sous-réseaux de votre compte.

Erreurs d'autorisation

Si vous rencontrez des erreurs d'autorisation, vérifiez que votre utilisateur ou votre rôle IAM dispose des autorisations requises pour créer et gérer des ressources VPC. Vous devrez peut-être attacher la politique `AmazonVPCFullAccess` ou créer une politique personnalisée avec les autorisations requises.

Limites de ressources

AWS les comptes ont des limites par défaut quant au nombre de VPCs, de sous-réseaux et d'autres ressources que vous pouvez créer. Si vous atteignez ces limites, vous pouvez demander une augmentation par le biais du AWS Support Center.

Erreurs de dépendance pendant le nettoyage

Lors du nettoyage des ressources, vous risquez de rencontrer des erreurs de dépendance si vous ne supprimez pas les ressources dans l'ordre approprié. Supprimez toujours les ressources dans l'ordre inverse à celui de leur création, en commençant par les plus dépendantes.

nettoyer des ressources ;

Lorsque vous n'avez plus besoin de votre VPC, vous pouvez nettoyer les ressources pour éviter les frais associés. Supprimez-les dans l'ordre inverse à celui de leur création pour gérer correctement les dépendances.

Mettre fin à EC2 des instances

```
aws ec2 terminate-instances --instance-ids i-0123456789abcdef0 i-0123456789abcdef1
```

```
aws ec2 wait instance-terminated --instance-ids i-0123456789abcdef0 i-0123456789abcdef1
```

Suppression de la paire de clés

```
aws ec2 delete-key-pair --key-name vpc-tutorial-key
rm vpc-tutorial-key.pem
```

Suppression de la passerelle NAT

```
aws ec2 delete-nat-gateway --nat-gateway-id nat-0123456789abcdef0
aws ec2 wait nat-gateway-deleted --nat-gateway-ids nat-0123456789abcdef0
```

Libération de l'adresse IP Elastic

```
aws ec2 release-address --allocation-id eipalloc-0123456789abcdef0
```

Suppression des groupes de sécurité

```
aws ec2 delete-security-group --group-id sg-0123456789abcdef1
aws ec2 delete-security-group --group-id sg-0123456789abcdef0
```

Suppression des tables de routage

Tout d'abord, recherchez l'association de la table de routage IDs :

```
aws ec2 describe-route-tables --route-table-id rtb-0123456789abcdef0
aws ec2 describe-route-tables --route-table-id rtb-0123456789abcdef1
```

Dissociez ensuite les tables de routage des sous-réseaux (remplacez l'association IDs par celles de votre sortie) :

```
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef0
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef1
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef2
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef3
```

Pour terminer, supprimez les tables de routage :

```
aws ec2 delete-route-table --route-table-id rtb-0123456789abcdef1
```

```
aws ec2 delete-route-table --route-table-id rtb-0123456789abcdef0
```

Détachement et suppression de la passerelle Internet

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0
aws ec2 delete-internet-gateway --internet-gateway-id igw-0123456789abcdef0
```

Suppression des sous-réseaux

```
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef0
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef1
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef2
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef3
```

Suppression du VPC

```
aws ec2 delete-vpc --vpc-id vpc-0123456789abcdef0
```

Passage en production

Ce tutoriel vous explique comment créer un VPC à l'aide de l' AWS CLI. Dans un environnement de production, respectez les bonnes pratiques de sécurité et d'architecture suivantes :

1. Règles des groupes de sécurité : limitez le trafic entrant à des plages d'adresses IP spécifiques au lieu d'autoriser le trafic provenant de 0.0.0.0/0.
2. Haute disponibilité : déployez des passerelles NAT dans chaque zone de disponibilité comprenant des sous-réseaux privés pour éliminer les points de défaillance uniques.
3. Réseau ACLs : implémentez ACLs le réseau comme couche de sécurité supplémentaire au-delà des groupes de sécurité.
4. Journaux de flux VPC : activez les journaux de flux VPC pour surveiller et analyser les modèles de trafic réseau.
5. Balisage des ressources : mettez en œuvre une stratégie de balisage complète pour une meilleure gestion des ressources.

Pour plus d'informations sur la création d'architectures prêtes pour la production, consultez AWS Well-Architected Framework et AWS Security Best Practices.

Étapes suivantes

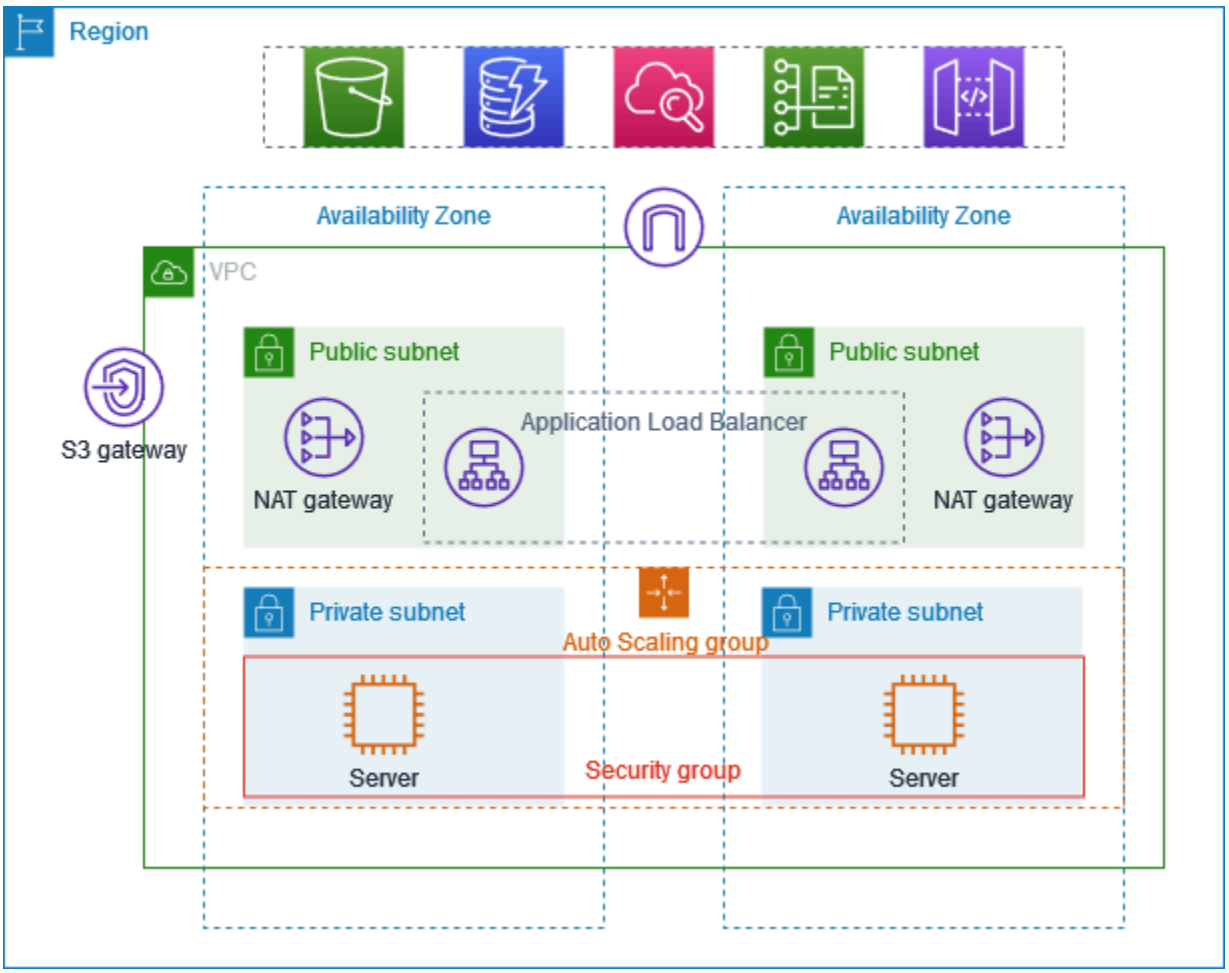
Maintenant que vous avez créé un VPC avec des sous-réseaux publics et privés, vous pouvez effectuer les opérations suivantes :

1. Lancez EC2 des instances dans vos sous-réseaux publics ou privés.
2. Déployer des équilibreurs de charge pour répartir le trafic sur plusieurs instances
3. Configurer des groupes Auto Scaling pour bénéficier d'un niveau de disponibilité et d'une capacité de mise à l'échelle élevés
4. Configurer des bases de données RDS dans vos sous-réseaux privés
5. Implémentez le peering VPC pour vous connecter aux autres. VPCs
6. Configurer des connexions VPN pour connecter votre VPC à votre réseau sur site

Création d'un VPC avec des sous-réseaux privés et des passerelles NAT à l'aide de l'AWS CLI

Ce tutoriel vous explique comment créer un VPC que vous pouvez utiliser pour les serveurs d'un environnement de production à l'aide de l'AWS CLI. Pour améliorer la résilience, vous allez déployer les serveurs dans deux zones de disponibilité à l'aide d'un groupe Auto Scaling et d'un équilibreur de charge Application Load Balancer. Pour plus de sécurité, vous allez déployer les serveurs dans des sous-réseaux privés. Les serveurs recevront les demandes via l'équilibreur de charge et pourront se connecter à Internet à l'aide de passerelles NAT. Vous déploierez une passerelle NAT dans chaque zone de disponibilité pour assurer une meilleure résilience.

Le schéma suivant donne une vue d'ensemble des ressources comprises 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.



Prérequis

Avant de démarrer ce tutoriel, assurez-vous de disposer des éléments suivants :

- L'AWS CLI installée et configurée avec les autorisations requises pour créer des ressources VPC, des instances EC2, des équilibreurs de charge et des groupes Auto Scaling. Pour plus d'informations sur l'installation d'AWS CLI, consultez la section Installation ou mise à jour de la version la plus récente de AWS CLI.
- Des connaissances de base sur les concepts VPC, notamment les sous-réseaux, les tables de routage et les passerelles Internet.
- Le processeur JSON en ligne de commande `jq` pour analyser la sortie des commandes AWS CLI. Pour plus d'informations sur l'installation de jq, consultez Download jq.
- Des quotas de service suffisants pour les ressources que vous allez créer, notamment :
- Au moins deux adresses IP Elastic disponibles
- Au moins deux passerelles NAT

- Au moins un VPC
- Au moins quatre sous-réseaux
- Au moins un équilibreur de charge Application Load Balancer

Coût estimé : les ressources créées lors de ce tutoriel seront facturées comme suit sur votre compte AWS : passerelles NAT : environ 0,045 USD/h, plus des frais de traitement des données, adresses IP Elastic : gratuites lorsqu'elles sont associées à des instances en cours d'exécution, 0,005 USD/h dans les autres cas, instances EC2 : variable selon le type d'instance (t3.micro dans ce tutoriel), Application Load Balancer : environ 0,0225 USD/h, plus des frais de traitement des données.

Création du VPC et des sous-réseaux

Commencez par créer un VPC avec le bloc CIDR 10.0.0.0/16, qui fournit jusqu'à 65 536 adresses IP privées.

```
# Create a VPC with CIDR block 10.0.0.0/16
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=ProductionVPC}]'
```

La commande renvoie un résultat semblable à ce qui suit :

```
{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-abcd1234",
        "State": "pending",
        "VpcId": "vpc-abcd1234",
        "OwnerId": "123456789012",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-abcd1234",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false,
```

```
        "Tags": [
            {
                "Key": "Name",
                "Value": "ProductionVPC"
            }
        ]
    }
}
```

Notez l'ID de VPC indiqué dans la sortie (par exemple, `vpc-abcd1234`). Vous l'utiliserez dans les commandes suivantes.

Identifiez ensuite deux zones de disponibilité dans votre région pour créer une architecture résiliente.

```
# Get available Availability Zones
aws ec2 describe-availability-zones --query 'AvailabilityZones[0:2].ZoneName' --output
 text
```

La commande renvoie un résultat semblable à ce qui suit :

```
us-east-1a us-east-1b
```

Créez à présent quatre sous-réseaux : deux publics pour l'équilibreur de charge et les passerelles NAT et deux privés pour vos serveurs d'applications. Remplacez `vpc-abcd1234` par votre ID de VPC réel et `us-east-1a` et `us-east-1b` par vos zones de disponibilité réelles.

```
# Create public subnet in first AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet1}]'

# Create private subnet in first AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.1.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet1}]'

# Create public subnet in second AZ
```

```
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.2.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet2}]'

# Create private subnet in second AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.3.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet2}]'
```

Chaque commande renvoie une sortie contenant l'ID de sous-réseau. Notez ces ID, car vous les utiliserez dans les commandes suivantes :

- Sous-réseau public 1 : `subnet-abcd1234`
- Sous-réseau privé 1 : `subnet-abcd5678`
- Sous-réseau public 2 : `subnet-efgh1234`
- Sous-réseau privé 2 : `subnet-efgh5678`

Création et configuration de la connectivité Internet

Dans cette section, vous allez créer une passerelle Internet permettant la communication entre votre VPC et Internet que vous attacherez à votre VPC.

```
# Create an Internet Gateway
aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-
gateway,Tags=[{Key=Name,Value=ProductionIGW}]'
```

La commande renvoie une sortie contenant l'ID de passerelle Internet. Notez cet ID (par exemple, `igw-abcd1234`).

Attachez la passerelle Internet à votre VPC. Remplacez `igw-abcd1234` par votre ID de passerelle Internet réel et `vpc-abcd1234` par votre ID de VPC réel.

```
# Attach the Internet Gateway to the VPC
aws ec2 attach-internet-gateway --internet-gateway-id igw-abcd1234 --vpc-id vpc-
abcd1234
```

Créez ensuite des tables de routage pour vos sous-réseaux publics et privés. Remplacez `vpc-abcd1234` par votre ID de VPC réel.

```
# Create a route table for public subnets
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PublicRouteTable}]'

# Create route table for private subnet in first AZ
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable1}]'

# Create route table for private subnet in second AZ
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable2}]'
```

Chaque commande renvoie une sortie contenant l'ID de table de routage. Notez ces ID :

- Table de routage publique : `rtb-abcd1234`
- Table de routage privée 1 : `rtb-efgh1234`
- Table de routage privée 2 : `rtb-ijkl1234`

Ajoutez à la table de routage publique une route vers la passerelle Internet pour permettre l'accès à Internet. Remplacez `rtb-abcd1234` par votre ID de table de routage publique réel et `igw-abcd1234` par votre ID de passerelle Internet réel.

```
# Add a route to the Internet Gateway
aws ec2 create-route --route-table-id rtb-abcd1234 --destination-cidr-block 0.0.0.0/0
 --gateway-id igw-abcd1234
```

Associez les sous-réseaux à leurs tables de routage respectives. Remplacez les ID de table de routage et de sous-réseau par vos ID réels.

```
# Associate public subnets with the public route table
aws ec2 associate-route-table --route-table-id rtb-abcd1234 --subnet-id subnet-abcd1234
aws ec2 associate-route-table --route-table-id rtb-abcd1234 --subnet-id subnet-efgh1234

# Associate private subnets with their respective route tables
aws ec2 associate-route-table --route-table-id rtb-efgh1234 --subnet-id subnet-abcd5678
aws ec2 associate-route-table --route-table-id rtb-ijkl1234 --subnet-id subnet-efgh5678
```

Création de passerelles NAT

Les passerelles NAT permettent aux instances des sous-réseaux privés de se connecter à Internet ou à d'autres services AWS tout en empêchant l'établissement de connexions avec ces instances depuis Internet. Commencez par allouer une adresse IP Elastic à vos passerelles NAT.

```
# Allocate Elastic IP for NAT Gateway in first AZ
aws ec2 allocate-address --domain vpc --tag-specifications 'ResourceType=elastic-
ip,Tags=[{Key=Name,Value=NAT1-EIP}]'

# Allocate Elastic IP for NAT Gateway in second AZ
aws ec2 allocate-address --domain vpc --tag-specifications 'ResourceType=elastic-
ip,Tags=[{Key=Name,Value=NAT2-EIP}]'
```

Chaque commande renvoie une sortie contenant l'ID d'allocation. Notez ces ID :

- ID d'allocation EIP 1 : `eipalloc-abcd1234`
- ID d'allocation EIP 2 : `eipalloc-efgh1234`

Créez des passerelles NAT dans chaque sous-réseau public. Remplacez les ID de sous-réseau et d'allocation par vos ID réels.

```
# Create NAT Gateway in public subnet of first AZ
aws ec2 create-nat-gateway \
  --subnet-id subnet-abcd1234 \
  --allocation-id eipalloc-abcd1234 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway1}]'

# Create NAT Gateway in public subnet of second AZ
aws ec2 create-nat-gateway \
  --subnet-id subnet-efgh1234 \
  --allocation-id eipalloc-efgh1234 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway2}]'
```

Chaque commande renvoie une sortie contenant l'ID de passerelle NAT. Notez ces ID :

- Passerelle NAT 1 : `nat-abcd1234`
- Passerelle NAT 2 : `nat-efgh1234`

Le provisionnement des passerelles NAT prend quelques minutes. Attendez qu'elles soient disponibles pour poursuivre. Remplacez les ID de passerelle NAT par vos ID réels.

```
# Wait for NAT Gateways to be available
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-abcd1234
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-efgh1234
```

Ajoutez aux tables de routage privées des routes vers les passerelles NAT pour permettre aux instances des sous-réseaux privés d'accéder à Internet. Remplacez les ID de table de routage et de passerelle NAT par vos ID réels.

```
# Add route to NAT Gateway 1 in private route table 1
aws ec2 create-route \
  --route-table-id rtb-efgh1234 \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id nat-abcd1234

# Add route to NAT Gateway 2 in private route table 2
aws ec2 create-route \
  --route-table-id rtb-ijkl1234 \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id nat-efgh1234
```

Création d'un point de terminaison de VPC pour Amazon S3

Un point de terminaison de VPC pour Amazon S3 permet aux instances de vos sous-réseaux privés d'accéder à S3 sans passer par la passerelle NAT, ce qui réduit les coûts de transfert de données et améliore les performances du réseau. Remplacez `vpc-abcd1234` par votre ID de VPC réel et les ID de table de routage par vos ID réels.

```
# Get the prefix list ID for S3 in your region
S3_PREFIX_LIST_ID=$(aws ec2 describe-prefix-lists --filters "Name=prefix-
list-name,Values=com.amazonaws.$(aws configure get region).s3" --query
 'PrefixLists[0].PrefixListId' --output text)

# Create the VPC endpoint for S3
aws ec2 create-vpc-endpoint \
  --vpc-id vpc-abcd1234 \
  --service-name com.amazonaws.$(aws configure get region).s3 \
  --route-table-ids rtb-efgh1234 rtb-ijkl1234 \
  --tag-specifications 'ResourceType=vpc-endpoint,Tags=[{Key=Name,Value=S3-Endpoint}]'
```

La commande renvoie une sortie contenant l'ID de point de terminaison de VPC. Notez cet ID (par exemple, `vpce-abcd1234`).

Configurer des groupes de sécurité

Les groupes de sécurité agissent comme des pare-feu virtuels pour vos instances afin de contrôler le trafic entrant et sortant. Créez pour l'équilibreur de charge un groupe de sécurité qui autorise le trafic HTTP entrant quelle que soit son origine. Remplacez `vpc-abcd1234` par votre ID de VPC réel.

```
# Create security group for the load balancer
aws ec2 create-security-group \
  --group-name LoadBalancerSG \
  --description "Security group for the load balancer" \
  --vpc-id vpc-abcd1234 \
  --tag-specifications 'ResourceType=security-
group,Tags=[{Key=Name,Value=LoadBalancerSG}]'
```

La commande renvoie une sortie contenant l'ID de groupe de sécurité. Notez cet ID (par exemple, `sg-abcd1234`).

Autorisez le trafic HTTP entrant vers l'équilibreur de charge. Remplacez `sg-abcd1234` par l'ID de groupe de sécurité réel de votre équilibreur de charge.

```
# Allow inbound HTTP traffic from anywhere
aws ec2 authorize-security-group-ingress \
  --group-id sg-abcd1234 \
  --protocol tcp \
  --port 80 \
  --cidr 0.0.0.0/0
```

Créez pour les serveurs d'applications un groupe de sécurité qui autorise uniquement le trafic entrant en provenance de l'équilibreur de charge. Remplacez `vpc-abcd1234` par votre ID de VPC réel.

```
# Create security group for the application servers
aws ec2 create-security-group \
  --group-name AppServerSG \
  --description "Security group for the application servers" \
  --vpc-id vpc-abcd1234 \
  --tag-specifications 'ResourceType=security-
group,Tags=[{Key=Name,Value=AppServerSG}]'
```

La commande renvoie une sortie contenant l'ID de groupe de sécurité. Notez cet ID (par exemple, `sg-efgh1234`).

Autorisez le trafic HTTP entrant du groupe de sécurité de l'équilibreur de charge vers les serveurs d'applications. Remplacez `sg-efgh1234` par l'ID de groupe de sécurité réel de votre serveur d'applications et `sg-abcd1234` par l'ID de groupe de sécurité réel de votre équilibreur de charge.

```
# Allow inbound HTTP traffic from the load balancer security group
aws ec2 authorize-security-group-ingress \
  --group-id sg-efgh1234 \
  --protocol tcp \
  --port 80 \
  --source-group sg-abcd1234
```

Création d'un modèle de lancement pour les instances EC2

Un modèle de lancement contient les informations de configuration pour le lancement d'une instance, notamment l'ID d'AMI, le type d'instance et les groupes de sécurité. Commencez par créer un script de données utilisateur qui sera exécuté au lancement de l'instance.

```
cat > user-data.sh << 'EOF'
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "<h1>Hello from $(hostname -f) in $(curl -s http://169.254.169.254/latest/meta-
data/placement/availability-zone)</h1>" > /var/www/html/index.html
EOF
```

Codez le script de données utilisateur en base64.

```
USER_DATA=$(base64 -w 0 user-data.sh)
```

Recherchez l'ID de l'AMI Amazon Linux 2 la plus récente.

```
# Get the latest Amazon Linux 2 AMI ID
aws ec2 describe-images --owners amazon --filters "Name=name,Values=amzn2-ami-hvm-
*-x86_64-gp2" "Name=state,Values=available" --query 'sort_by(Images, &CreationDate)
[-1].ImageId' --output text
```

Créez un modèle de lancement avec l'ID d'AMI, le type d'instance, le groupe de sécurité et les données utilisateur. Remplacez `sg-efgh1234` par l'ID de groupe de sécurité réel de votre serveur d'applications, et `$AMI_ID` et `$USER_DATA` par les valeurs issues des commandes précédentes.

```
# Create a launch template
aws ec2 create-launch-template \
  --launch-template-name AppServerTemplate \
  --version-description "Initial version" \
  --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=Name,Value=AppServerTemplate}]' \
  --launch-template-data '{
    "NetworkInterfaces": [{
      "DeviceIndex": 0,
      "Groups": ["sg-efgh1234"],
      "DeleteOnTermination": true
    }],
    "ImageId": "ami-abcd1234",
    "InstanceType": "t3.micro",
    "UserData":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQp5dW0gaW5zdGFsbCAteSBodHRwZApzeXN0ZW1jdGwgc3RhcnQgaHR0cGQKc
+SGVsbG8gZnJvbSAkKGhvc3RuYW1lIC1mKSBpbiAkKGN1cmwgLXMgaHR0cDovLzE2OS4yNTQuMTY5LjI1NC9sYXRlc3QvbW
    "TagSpecifications": [{
      "ResourceType": "instance",
      "Tags": [{
        "Key": "Name",
        "Value": "AppServer"
      }]
    }]
  }'
```

Création d'un équilibreur de charge et d'un groupe cible

Un groupe cible achemine les demandes vers les cibles enregistrées (des instances EC2, par exemple) à l'aide du protocole et du numéro de port que vous spécifiez. Créez un groupe cible pour vos serveurs d'applications. Remplacez `vpc-abcd1234` par votre ID de VPC réel.

```
# Create a target group
aws elbv2 create-target-group \
  --name AppTargetGroup \
  --protocol HTTP \
  --port 80 \
  --vpc-id vpc-abcd1234 \
```

```
  --target-type instance \
  --health-check-protocol HTTP \
  --health-check-path / \
  --health-check-port traffic-port
```

La commande renvoie une sortie contenant l'ARN du groupe cible. Notez cet ARN (par exemple, `arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/AppTargetGroup/abcd1234`).

Créez un équilibreur de charge Application Load Balancer dans les sous-réseaux publics. Remplacez les ID de sous-réseau et de groupe de sécurité par vos ID réels.

```
# Create a load balancer
aws elbv2 create-load-balancer \
  --name AppLoadBalancer \
  --subnets subnet-abcd1234 subnet-efgh1234 \
  --security-groups sg-abcd1234 \
  --tags Key=Name,Value=AppLoadBalancer
```

La commande renvoie une sortie contenant l'ARN de l'équilibreur de charge. Notez cet ARN (par exemple, `arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234`).

Attendez que l'équilibreur de charge soit actif pour poursuivre. Remplacez `arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234` par l'ARN réel de votre équilibreur de charge.

```
# Wait for load balancer to be active
aws elbv2 wait load-balancer-available \
  --load-balancer-arns arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234
```

Créez un écouteur pour l'équilibreur de charge qui transfère le trafic HTTP au groupe cible. Remplacez les ARN de l'équilibreur de charge et du groupe cible par vos ARN réels.

```
# Create a listener
aws elbv2 create-listener \
  --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/
app/AppLoadBalancer/abcd1234 \
  --protocol HTTP \
  --port 80 \
```

```
  --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-
east-1:123456789012:targetgroup/AppTargetGroup/abcd1234
```

Créer un groupe Auto Scaling

Un groupe Auto Scaling contient un ensemble d'instances EC2 traitées comme un regroupement logique, aux fins de mise à l'échelle et de gestion automatique. Créez un groupe Auto Scaling qui utilise le modèle de lancement et place les instances dans les sous-réseaux privés. Remplacez les ID de sous-réseau et l'ARN du groupe cible par vos ID et ARN réels.

```
# Create an Auto Scaling group
aws autoscaling create-auto-scaling-group \
  --auto-scaling-group-name AppAutoScalingGroup \
  --launch-template LaunchTemplateName=AppServerTemplate,Version='$Latest' \
  --min-size 2 \
  --max-size 4 \
  --desired-capacity 2 \
  --vpc-zone-identifier "subnet-abcd5678,subnet-efgh5678" \
  --target-group-arns arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/
AppTargetGroup/abcd1234 \
  --health-check-type ELB \
  --health-check-grace-period 300 \
  --tags Key=Name,Value=AppServer,PropagateAtLaunch=true
```

Tester votre configuration

Une fois que le groupe Auto Scaling a lancé des instances et que le résultat de la surveillance de l'état de ces instances est positif, vous pouvez tester votre équilibreur de charge. Obtenez le nom DNS de l'équilibreur de charge. Remplacez l'ARN de l'équilibreur de charge par votre ARN réel.

```
# Get the DNS name of the load balancer
aws elbv2 describe-load-balancers \
  --load-balancer-arns arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234 \
  --query "LoadBalancers[0].DNSName" \
  --output text
```

Utilisez la commande curl pour tester l'application avec le nom de l'équilibreur de charge.

```
curl http://LoadBalancerName
```

En actualisant la page à plusieurs reprises, vous accéderez aux réponses provenant de différentes instances de différentes zones de disponibilité.

Nettoyage des ressources

Une fois que vous avez terminé ce tutoriel, supprimez toutes les ressources pour éviter les coûts associés. Remplacez tous les ID par vos ID de ressource réels.

```
# Delete the Auto Scaling group
aws autoscaling delete-auto-scaling-group \
  --auto-scaling-group-name AppAutoScalingGroup \
  --force-delete

# Wait for the Auto Scaling group to be deleted
sleep 60

# Delete the load balancer
aws elbv2 delete-load-balancer \
  --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/
app/AppLoadBalancer/abcd1234

# Wait for the load balancer to be deleted
sleep 30

# Delete the target group
aws elbv2 delete-target-group \
  --target-group-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/
AppTargetGroup/abcd1234

# Delete the launch template
aws ec2 delete-launch-template \
  --launch-template-name AppServerTemplate

# Delete the NAT Gateways
aws ec2 delete-nat-gateway --nat-gateway-id nat-abcd1234
aws ec2 delete-nat-gateway --nat-gateway-id nat-efgh1234

# Wait for the NAT Gateways to be deleted
sleep 90

# Release the Elastic IPs
aws ec2 release-address --allocation-id eipalloc-abcd1234
aws ec2 release-address --allocation-id eipalloc-efgh1234
```

```
# Delete the VPC endpoint
aws ec2 delete-vpc-endpoints --vpc-endpoint-ids vpce-abcd1234

# Wait for security group dependencies to clear
sleep 30

# Delete the security groups
aws ec2 delete-security-group --group-id sg-efgh1234
aws ec2 delete-security-group --group-id sg-abcd1234

# Detach the Internet Gateway
aws ec2 detach-internet-gateway --internet-gateway-id igw-abcd1234 --vpc-id vpc-
abcd1234

# Delete the Internet Gateway
aws ec2 delete-internet-gateway --internet-gateway-id igw-abcd1234

# Delete the route tables
aws ec2 delete-route-table --route-table-id rtb-efgh1234
aws ec2 delete-route-table --route-table-id rtb-ijkl1234
aws ec2 delete-route-table --route-table-id rtb-abcd1234

# Delete the subnets
aws ec2 delete-subnet --subnet-id subnet-abcd1234
aws ec2 delete-subnet --subnet-id subnet-efgh1234
aws ec2 delete-subnet --subnet-id subnet-abcd5678
aws ec2 delete-subnet --subnet-id subnet-efgh5678

# Delete the VPC
aws ec2 delete-vpc --vpc-id vpc-abcd1234
```

Étapes suivantes

Maintenant que vous avez créé un VPC avec des sous-réseaux privés et des passerelles NAT, vous pouvez explorer les sujets connexes suivants :

- Bonnes pratiques de sécurité pour votre VPC
- Journalisation du trafic IP à l'aide des journaux de flux VPC
- Politiques de mise à l'échelle des groupes Auto Scaling
- Surveillance de l'état des groupes cibles de l'équilibreur de charge

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
VPCs 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'en avoir des centaines VPCs par région.
Sous-réseaux par VPC	200	Oui	
IPv4 Blocs CIDR 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.
IPv6 Blocs CIDR par VPC	5	Oui (jusqu'à 50)	Le nombre CIDRs que vous pouvez allouer à un seul VPC.
Exclusions VPC Block Public Access par compte et par région	50	Oui. Pour demander une augmentation de	Nombre d'exclusions VPC BPA que vous pouvez créer dans un compte.

Nom	Par défaut	Ajustable	Commentaires
		quota, consultez Request a service quota increase dans le Guide d'utilisation d'AWS Support.	

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 élastiques

Nom	Par défaut	Ajustable	Commentaires
Adresses IP Elastic par région	5	Oui	Ce quota s'applique aux personnes individuelles Compte AWS VPCs et partagées VPCs.
Adresses IP Elastic par passerelle NAT publique	2	Oui	Vous pouvez demander une augmentat ion de quota jusqu'à 8.

Passerelles

Nom	Par défaut	Ajustable	Commentaires
Passerelles Internet de sortie uniquement par région	5	Oui	Pour augmenter ce quota, augmentez le VPCs quota pour chaque 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	Pour augmenter ce quota, augmentez le VPCs quota pour chaque 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`.
Quota d'adresses IP privées par passerelle NAT	8	Oui	
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 de support. Consultez Request a service quota increase dans le Guide d'utilisation d'AWS Support.

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 de plus amples informations, veuillez consulter 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 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	10 000	Oui	Ce quota s'applique par type de ressource pouvant référencer une liste de préfixes. Par exemple, vous pouvez avoir 10 000 références à une liste de préfixes sur l'ensemble de vos groupes de sécurité et 10 000 références à une liste de préfixes sur l'ensemble de vos tables de routage de sous-réseau. Si vous partagez une liste de préfixes avec

Nom	Par défaut	Ajustable	Commentaires
			d'autres AWS comptes, les référence s des autres comptes à votre liste de préfixes sont prises en compte dans votre quota.

Réseau ACLs

Nom	Par défaut	Ajustable	Commentaires
Réseau ACLs 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 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'instanc e	Non	Pour plus d'informations, veuillez consulter Interfaces réseau par type d'instance.

Nom	Par défaut	Ajustable	Commentaires
Interfaces réseau par région	5 000	Oui	Ce quota s'applique aux personnes individuelles Compte AWS VPCs et partagées VPCs. Cette limite est appliquée par zone de disponibilité (AZ). Si, par exemple, les interfaces réseau sont en trois AZs, chaque AZ 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, 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)	500	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 IPv4 itinéraires et IPv6 les itinéraires.

Nom	Par défaut	Ajustable	Commentaires
			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 acheminement par défaut.

Serveurs de routage

Nom	Par défaut	Ajustable	Commentaires
Serveurs de routage par VPC	5	Oui. Pour demander une augmentation de quota, consultez Request a service quota increase dans le Guide d'utilisation d'AWS Support.	

Nom	Par défaut	Ajustable	Commentaires
Points de terminaison de serveur de routage par serveur de routage	10	Oui. Pour demander une augmentation de quota, consultez Request a service quota increase dans le Guide d'utilisation d'AWS Support.	

Nom	Par défaut	Ajustable	Commentaires
Sessions d'appairage par interface réseau	20	Oui. Pour demander une augmentation de quota, consultez Request a service quota increase dans le Guide d'utilisation d'AWS Support.	
Points de terminaison de serveur de routage par serveur de routage et sous-réseau	2	Non	Vous ne pouvez créer que deux points de terminaison dans le même sous-rése au pour le même serveur de routage à des fins de redondance.
Routes par pair de serveur de routage	100	Non	Il s'agit du nombre de routes pouvant être publiées dynamiquement via un pair de serveur de routage.
Routes par serveur de routage	100	Non	Il s'agit du nombre de routes pouvant être installées dans la base d'informations de transfert (FIB) d'un serveur de routage.

Groupes de sécurité

Nom	Par défaut	Ajustable	Commentaires
Groupes de sécurité VPC par région	2 500	Oui	Ce quota s'applique aux personnes individuelles Compte AWS VPCs et partagées VPCs. 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 IPv4 règles et IPv6 les règles. Pour un compte dont le quota par défaut est de 60 règles, un groupe de sécurité peut avoir 60 règles entrantes pour le IPv4 trafic et 60 règles entrantes pour IPv6 le trafic entrant. Pour de plus amples informati ons, veuillez consulter 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.

Nom	Par défaut	Ajustable	Commentaires
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. Pour définir un quota de groupes de sécurité par interface réseau inférieur à cinq (valeur par défaut), consultez Request a service quota increase dans le Guide d'utilisation d'AWS Support. Suivez la même procédure que pour une demande d'augmentation de quota.

Partage de sous-réseaux VPC

Tous les quotas de VPC standard s'appliquent aux sous-réseaux VPC partagés.

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 (NAU) comprend les adresses IP, les interfaces réseau et les listes CIDRs 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 de plus amples informations, veuillez consulter 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)	Le nombre maximum d'unités NAU pour un VPC et l'ensemble de ses homologue s intra-régionaux. VPCs VPCs qui sont comparés entre différentes régions ne contribuent pas à ce chiffre.

Limitation de l'API Amazon EC2

Pour plus d'informations sur la limitation Amazon EC2, consultez Request throttling dans le Guide de développement d'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 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
- Site-to-Site Quotas VPN dans le guide de AWS Site-to-Site VPN l'utilisateur
- 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
Contrôles de chiffrement VPC	Vous pouvez désormais appliquer le chiffrement en transit pour le trafic réseau au sein de votre VPC à l'aide des contrôles de chiffrement VPC. Cette fonctionnalité fournit des fonctionnalités centralisées d'application et de surveillance des politiques de chiffrement.	21 novembre 2025
Passerelles NAT régionales pour une extension multi-AZ automatique	Vous pouvez désormais utiliser des passerelles NAT régionales qui s'étendent automatiquement entre les zones de disponibilité en fonction de votre charge de travail. Les passerelles NAT régionales fournissent une configuration simplifiée, une sécurité renforcée et une haute disponibilité automatiq ue sans intervention manuelle.	19 novembre 2025
Acheminement du trafic VPC entrant vers des adresses IP publiques	Vous pouvez désormais configurer des règles de routage avancées pour diriger le trafic entrant d’Internet vers des adresses IP publiques spécifiques au sein de votre VPC. Cela vous permet	13 août 2025

	d'exercer un contrôle plus précis sur le flux de trafic et les décisions de routage pour les scénarios d'entrée.	
Routage dynamique dans votre VPC à l'aide du serveur de routage Amazon VPC	Le serveur de routage Amazon VPC simplifie le routage du trafic entre les charges de travail déployées au sein d'un VPC et passerelles Internet. Grâce à cette fonctionnalité, le serveur de routage VPC met à jour de manière dynamique les tables de routage VPC et de passerelle avec vos IPv6 itinéraires IPv4 ou itinéraires préférés afin de garantir la tolérance aux pannes de routage pour ces charges de travail. Cela vous permet de rediriger automatiquement le trafic au sein d'un VPC, ce qui facilite la gestion du routage VPC et améliore l'interopérabilité avec des charges de travail tierces.	31 mars 2025
AWS mise à jour des politiques gérée	Amazon VPC a mis à jour les politiques gérées AmazonVPCFullAccess et AmazonVPCReadOnlyAccess.	9 décembre 2024

Prise en charge de la politique déclarative pour le VPC BPA	Si vous utilisez AWS Organizations pour gérer les comptes de votre organisation, vous pouvez utiliser une politique déclarative pour appliquer le BPA VPC aux comptes de l'organisation.	1er décembre 2024
VPC Block Public Access (BPA)	L'accès public par blocage VPC (BPA) vous permet d'empêcher les ressources VPCs et les sous-réseaux que vous possédez dans une région d'atteindre ou d'être accessibles depuis Internet via des passerelles Internet et des passerelles Internet de sortie uniquement.	19 novembre 2024
Groupes de sécurité partagés	Cette fonctionnalité vous permet de partager un groupe de sécurité avec d'autres comptes AWS Organizations.	30 octobre 2024
Associations de VPC et de groupes de sécurité	Cette fonctionnalité vous permet d'associer un groupe de sécurité à plusieurs VPCs dans la même région.	30 octobre 2024
MTU prise en charge par les passerelles NAT	Les passerelles NAT prennent en charge le trafic avec une unité de transmission maximale (MTU) de 8 500.	10 septembre 2024

IPv6 Adressage privé	Des informations sur l' IPv6 adressage privé ont été ajoutées. Les IPv6 adresses privées ne sont disponibl es que dans le gestionnaire d'adresses IP Amazon VPC.	8 août 2024
IPv6 durée de location préférée	Vous pouvez désormais choisir la fréquence à laquelle une instance en cours d'exécution à laquelle un a IPv6 été attribué DHCPv6 doit être renouvelée.	20 février 2024
Révision et améliorations de la structure du guide	La structure du guide a été révisée et des améliorat ions ont été apportées pour améliorer l'expérience client liée à la recherche d'informa tions pour des scénarios spécifiques.	20 février 2024
AWS mise à jour des politique s gérée	Amazon VPC a mis à jour les politiques gérées AmazonVPC FullAccess et AmazonVPC ReadOnlyAccess.	8 février 2024
AWS mise à jour des politique s gérée	Amazon VPC a mis à jour la politique gérée AmazonVPC CrossAccountNetworkInterfac eOperations.	25 septembre 2023

EC2-Classic est obsolète	Avec EC2 -Classic, EC2 les instances s'exécutaient sur un réseau unique et plat 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
Ajouter des IPv4 adresses secondaires aux passerelles NAT	Vous pouvez ajouter des IPv4 adresses privées secondaires aux passerelles NAT publiques et privées. Les IPv4 adresses secondaires augmentent le nombre de ports disponibles et, par conséquent, elles augmentent 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
IPv6 configuration du routeur passerelle par défaut	Trois IPv6 adresses sont désormais réservées pour être utilisées 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 vers Amazon Data Firehose	Vous pouvez spécifier un flux de diffusion Amazon Data Firehose en tant que 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
IPv6 Blocs CIDR multiples	Vous pouvez associer jusqu'à cinq blocs IPv6 CIDR 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
IPv6-sous-réseaux uniquement dans VPCs	Vous pouvez créer des sous-réseaux IPv6 uniquement dans lesquels vous pouvez lancer IPv6 des instances uniquement. EC2	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

Vue EC2 globale d'Amazon	Amazon EC2 Global View vous permet de visualiser les sous-réseaux VPCs, les instances, les groupes de sécurité et les volumes dans plusieurs AWS régions dans 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 un dispositif middlebox. Vous pouvez définir la destination d'une route pour qu'elle corresponde à un bloc entier IPv4 ou à un bloc IPv6 CIDR d'un sous-réseau de votre VPC.	30 août 2021
Support des ressources IDs et du balisage pour les règles des 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 les communications privées uniquement sortantes entre VPCs 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 disponibl es, 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 vous VPCs depuis la console Amazon VPC.	22 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 IPv4 CIDR secondaires pour votre VPC	Vous pouvez ajouter plusieurs blocs IPv4 CIDR 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
IPv6 soutien	Vous pouvez associer un bloc IPv6 CIDR à votre VPC et IPv6 attribuer des adresses aux ressources de votre VPC.	1er 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, permettant ainsi la communication entre votre instance EC2-Classic et les 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 du VPC dans cinq AWS régions, VPCs dans plusieurs zones de disponibilité, plusieurs VPCs par AWS compte et plusieurs connexions VPN par VPC.	3 août 2011
Instances dédiées	Les instances dédiées sont des EC2 instances Amazon lancées au sein de votre VPC qui exécutent du 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.