Appairage de VPC

Amazon Virtual Private Cloud

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Virtual Private Cloud: Appairage de VPC

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d’une manière susceptible d’entraîner une confusion chez les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

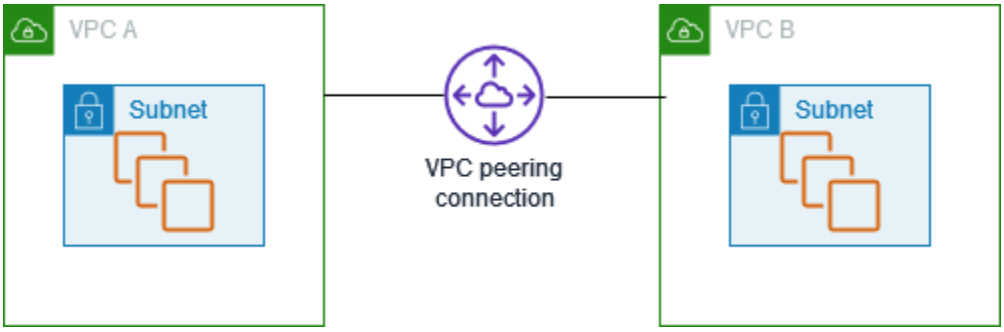
Qu'est-ce que l'appairage de VPC ? ... 1
Tarification d'une connexion d'appairage de VPC ... 2
Comment fonctionnent les connexions de peering ... 3
Cycle de vie d'une connexion d'appairage de VPC ... 3
Connexions d'appairage de plusieurs VPC ... 5
Limitations des appairages de VPC ... 6
Connexions d'appairage ... 9
Création ... 10
Prérequis ... 10
Création d'une connexion d'appairage à l'aide de la console ... 10
Créez une connexion d'appairage à l'aide de la ligne de commande ... 11
Accepter ou rejeter ... 11
Mise à jour des tables de routage ... 13
Référence des groupes de sécurité pairs ... 16
Identification de vos groupes de sécurité référencés ... 18
Afficher et supprimer des règles du groupe de sécurité obsolètes ... 19
Activation de la résolution DNS pour une connexion d'appairage de VPC ... 20
Suppression ... 22
Dépannage ... 23
Configurations communes d’appairage de VPC ... 24
Route vers un bloc d'adresse CIDR VPC ... 24
Deux se sont VPCs regardés ensemble ... 25
Un VPC jumelé à deux VPCs ... 27
Trois ont VPCs regardé ensemble ... 31
Plusieurs VPCs comparés ensemble ... 33
Route vers des adresses spécifiques ... 43
Deux VPCs qui accèdent à des sous-réseaux spécifiques dans un VPC ... 43
Deux VPCs qui accèdent à des blocs CIDR spécifiques dans un VPC ... 46
Un VPC qui accède à des sous-réseaux spécifiques en deux VPCs ... 47
Instances d'un VPC qui accèdent à des instances spécifiques dans deux VPCs ... 50
Un VPC qui accède à deux en VPCs utilisant les plus longues correspondances de préfixes ... 52
Configurations de plusieurs VPC ... 53
Scénarios d'appairage de VPC ... 57

En appairer deux ou plus VPCs pour fournir un accès complet aux ressources 57
Appairage à un VPC pour accéder à des ressources centralisées 58
Gestion des identités et des accès 59
Créer une connexion d'appairage de VPC 59
Accepter une connexion d'appairage de VPC 61
Supprimer une connexion d'appairage de VPC 62
Utiliser dans un compte spécifique 62
Gérer les connexions d'appairage de VPC dans la console 64
Quotas 66
Historique de la documentation 67
..... lxix

Qu'est-ce que l'appairage de VPC ?

Un cloud privé virtuel (VPC) est un réseau virtuel dédié à votre Compte AWS. Il est logiquement isolé des autres réseaux virtuels du AWS Cloud. Vous pouvez lancer AWS des ressources, telles que des EC2 instances Amazon, dans votre 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 ou d' IPv4 adresses privées. IPv6 Les instances des deux VPC peuvent communiquer entre elles comme si elles se trouvaient dans le même réseau. Vous pouvez créer une connexion d'appairage VPC entre les vôtres VPCs ou avec un VPC d'un autre compte. AWS Ils VPCs peuvent se trouver dans différentes régions (également connue sous le nom de connexion d'appairage VPC inter-régions).



AWS utilise l'infrastructure existante d'un VPC pour créer une connexion d'appairage VPC ; il ne s'agit ni d'une passerelle ni d'une connexion VPN, et ne repose pas sur un matériel physique distinct. Il n'y a donc pas de point unique de défaillance pour la communication, ni de goulet d'étranglement en termes de bande passante.

Une connexion d'appairage de VPC vous aide à faciliter le transfert des données. Par exemple, si vous avez plusieurs AWS comptes, vous pouvez les VPCs comparer entre eux pour créer un réseau de partage de fichiers. Vous pouvez également utiliser une connexion d'appairage VPC pour permettre à d'autres personnes d'accéder VPCs aux ressources que vous avez dans l'un de vos. VPCs

Lorsque vous établissez des relations d'appairage entre différentes VPCs AWS régions, les ressources VPCs (par exemple, les EC2 instances et les fonctions Lambda) des AWS différentes régions peuvent communiquer entre elles à l'aide d'adresses IP privées, sans utiliser de passerelle, de connexion VPN ou d'appliance réseau. Le trafic reste dans l’espace adresse IP privé. Tout le trafic inter-région est chiffré sans point de défaillance unique ni goulet d'étranglement. Le trafic reste toujours sur l' AWS épine dorsale mondiale et ne traverse jamais l'Internet public, ce qui réduit les

menaces, telles que les exploits courants et les attaques DDo S. L’appairage de VPC interrégion fournit un moyen simple et rentable pour le partage de ressources entre régions ou la réplication de données pour une redondance géographique.

Tarification d'une connexion d'appairage de VPC

Il n'y a pas de frais pour créer une connexion d'appairage de VPC. Tous les transferts de données via une connexion de peering VPC qui reste dans une zone de disponibilité sont gratuits, même s'ils se font entre différents comptes. Des frais s'appliquent pour le transfert de données via des connexions d'appairage VPC qui traversent des zones de disponibilité et des régions. Pour plus d'informations, consultez Amazon EC2 Pricing .

Comment fonctionnent les connexions d'appairage VPC

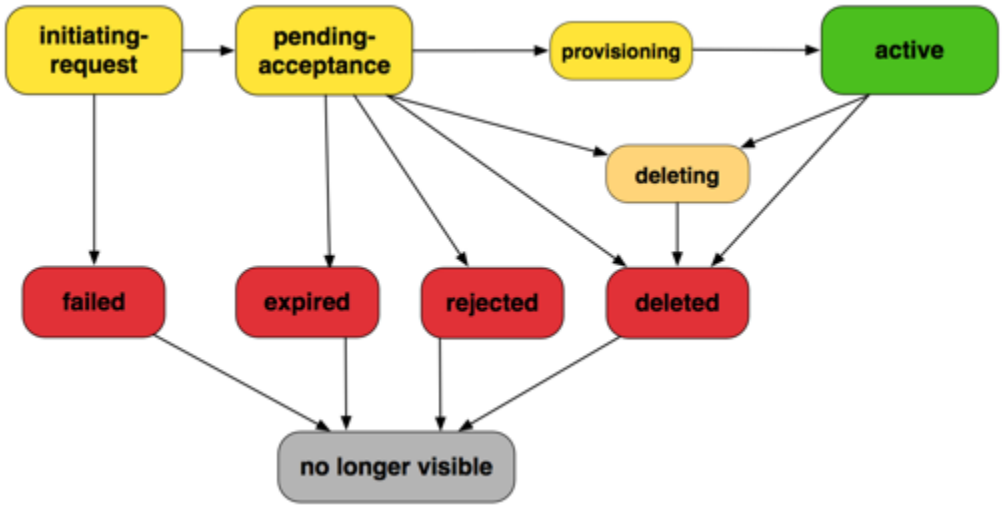
Les étapes suivantes décrivent le processus de peering VPC :

1. Le propriétaire du VPC demandeur envoie une demande au propriétaire du VPC accepteur pour créer une connexion d'appairage de VPC. Le VPC accepteur peut être votre propriété ou celle d'un autre AWS compte, et ne peut pas avoir de bloc d'adresse CIDR superposé au bloc d'adresse CIDR du VPC demandeur.
2. Le propriétaire du VPC accepteur accepte la demande de connexion d'appairage VPC pour activer la connexion d'appairage VPC.
3. Pour permettre le flux de trafic entre les adresses IP privées VPCs utilisatrices, le propriétaire de chaque VPC dans la connexion d'appairage VPC doit ajouter manuellement une route vers une ou plusieurs de ses tables de routage VPC qui pointe vers la plage d'adresses IP de l'autre VPC (le VPC homologue).
4. Si nécessaire, mettez à jour les règles du groupe de sécurité associées à votre EC2 instance pour garantir que le trafic à destination et en provenance du VPC homologue n'est pas restreint. Si les deux VPCs se trouvent dans la même région, vous pouvez faire référence à un groupe de sécurité issu du VPC homologue en tant que source ou destination pour les règles entrantes ou sortantes de votre groupe de sécurité.
5. Avec les options de connexion d'appairage VPC par défaut, si les EC2 instances situées de part et d'autre d'une connexion d'appairage VPC s'adressent mutuellement en utilisant un nom d'hôte DNS public, le nom d'hôte est remplacé par l'adresse IP publique de l'instance. EC2 Pour modifier ce comportement, activez la résolution de nom d'hôte DNS pour votre connexion VPC. Après avoir activé la résolution du nom d'hôte DNS, si les EC2 instances situées de part et d'autre de la connexion d'appairage du VPC s'adressent mutuellement en utilisant un nom d'hôte DNS public, le nom d'hôte est converti en adresse IP privée de l'instance. EC2

Pour de plus amples informations, veuillez consulter Connexions d’appairage de VPC.

Cycle de vie d'une connexion d'appairage de VPC

Une connexion d'appairage de VPC passe par plusieurs étapes à partir du moment où la demande a été initiée. Vous pouvez être amené à effectuer des actions lors de chaque étape. A la fin de son cycle de vie, la connexion d'appairage de VPC reste visible dans la console Amazon VPC; et dans l'API ou la sortie de la ligne de commande pendant une période de temps déterminée.



- Initiating-request : une demande de connexion d'appairage de VPC a été initiée. À ce stade, la connexion d'appairage peut échouer ou passer à l'état `pending-acceptance`.
- Failed : la demande de connexion d'appairage de VPC a échoué. À ce stade, elle ne peut pas être acceptée, refusée ou supprimée. La connexion d'appairage de VPC ayant échoué reste visible pour le demandeur pendant 2 heures.
- Pending-acceptance : La demande de connexion d'appairage de VPC attend d'être acceptée par le propriétaire du VPC accepteur. À ce stade, le propriétaire du VPC demandeur peut supprimer la demande, et le propriétaire du VPC accepteur peut accepter ou refuser la demande. Si aucune mesure n'est prise concernant la demande, elle expire au bout de 7 jours.
- Expired : la demande de connexion d'appairage de VPC est arrivée à expiration et elle ne peut faire l'objet d'aucune action de la part des deux propriétaires des VPC. La connexion d'appairage de VPC arrivée à expiration reste visible pour les deux propriétaires de VPC pendant 2 jours.
- Rejected : le propriétaire du VPC accepteur a rejeté une demande de connexion d'appairage de VPC `pending-acceptance`. À ce stade, la demande ne peut pas être acceptée. La connexion d'appairage de VPC refusée reste visible pendant 2 jours pour le propriétaire du VPC demandeur et pendant 2 heures pour le propriétaire du VPC accepteur. Si la demande a été créée dans le même AWS compte, la demande rejetée reste visible pendant 2 heures.
- Provisioning : la demande de connexion d'appairage de VPC a été acceptée et sera bientôt associée à l'état `active`.
- Active : la connexion d'appairage VPC est active et le trafic peut circuler entre les VPCs (à condition que vos groupes de sécurité et tables de routage autorisent le flux de trafic). À ce stade, les deux propriétaires de VPC peuvent supprimer la connexion d'appairage de VPC, mais ils ne peuvent pas la refuser.

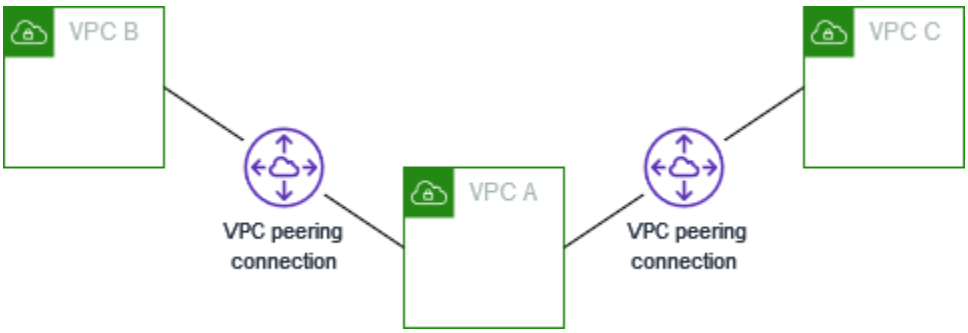
> **Note**
>
> Si un événement d'une région dans laquelle un VPC réside empêche le flux du trafic, le statut de la connexion d'appairage de VPC demeure `Active`.

- Deleting (Suppression) : s'applique à une connexion d'appairage de VPC inter-région qui se trouve en cours de suppression. Le propriétaire de l'un des VPC a envoyé une demande pour supprimer une connexion d'appairage de VPC `active` ou le propriétaire du VPC demandeur a envoyé une demande pour supprimer une demande de connexion d'appairage de VPC `pending-acceptance`.
- Deleted : une connexion d'appairage de VPC `active` a été supprimée par l'un des propriétaires de VPC, ou une connexion d'appairage de VPC `pending-acceptance` a été supprimée par le propriétaire du VPC demandeur. À ce stade, la connexion d'appairage de VPC ne peut pas être acceptée ni refusée. La connexion d'appairage de VPC reste visible pendant 2 heures pour la personne qui l'a supprimée et pendant 2 jours pour l'autre. Si la connexion d'appairage de VPC a été créée dans le même compte AWS , la demande supprimée reste visible pendant 2 heures.

Connexions d'appairage de plusieurs VPC

Une connexion d'appairage VPC est une relation un à un entre deux. VPCs Vous pouvez créer plusieurs connexions d'appairage de VPC pour chaque VPC que vous détenez, mais les relations d'appairage transitives ne sont pas prises en charge. Vous n'avez aucune relation d'appairage avec VPCs laquelle votre VPC n'est pas directement apparenté.

Le schéma suivant est un exemple d'un VPC apparenté à deux VPC différents. VPCs Dans cet exemple, il y a deux connexions d'appairage de VPC : VPC A est appairé à VPC B et VPC C. VPC B et VPC C ne sont pas appairés, et vous ne pouvez pas utiliser VPC A comme point de transit pour l'appairage entre VPC B et VPC C. Si vous souhaitez activer le routage du trafic entre VPC B et VPC C, vous devez créer une connexion d'appairage de VPC unique entre eux.



Limitations des appairages de VPC

Tenez compte des limites suivantes pour les connexions d'appairage de VPC. Dans certains cas, vous pouvez utiliser un attachement de la passerelle de transit au lieu de la connexion d'appairage de VPC. Pour plus d'informations, consultez Exemples de scénarios de passerelle de transit dans Amazon VPC Transit Gateways.

Connexions

- Il existe un quota pour le nombre de connexions d'appairage de VPC actives et en attente par VPC. Pour de plus amples informations, veuillez consulter Quotas.
- Vous ne pouvez pas avoir plus d'une connexion d'appairage VPC entre deux connexions en même VPCs temps.
- Les balises que vous créez pour la connexion d'appairage de votre VPC ne s'appliquent qu'au compte ou à la région dans lequel ou laquelle vous les créez.
- Vous ne pouvez pas vous connecter au serveur Amazon DNS ou l'interroger dans un appairage de VPC.
- Si le bloc IPv4 CIDR d'un VPC dans une connexion d'appairage VPC se situe en dehors des plages d'adresses IPv4 privées spécifiées par la RFC 1918, les noms d'hôtes DNS privés pour ce VPC ne peuvent pas être résolus en adresses IP privées. Pour résoudre des noms d'hôtes DNS privés en adresses IP privées, vous pouvez activer la prise en charge de la résolution DNS pour la connexion d'appairage de VPC. Pour de plus amples informations, veuillez consulter Activation de la résolution DNS pour une connexion d'appairage de VPC.
- Vous pouvez activer les ressources situées de part et d'autre d'une connexion d'appairage VPC pour qu'elles puissent communiquer. IPv6 Vous devez associer un bloc IPv6 CIDR à chaque VPC, activer les instances dans le VPC IPv6 pour la communication et IPv6 acheminer VPCs le trafic destiné au VPC homologue vers la connexion d'appairage du VPC.
- La recherche par chemin inverse Unicast dans les connexions d'appairage de VPC n'est pas prise en charge. Pour de plus amples informations, veuillez consulter Routage pour le trafic de la réponse.

Blocs d'adresse CIDR se chevauchant

- Vous ne pouvez pas créer de connexion d'appairage VPC entre des blocs CIDR ou des blocs CIDR correspondants, VPCs qui se chevauchent ou qui se chevauchent IPv4 . IPv6

- Si vous avez plusieurs blocs d'adresse IPv4 CIDR, vous ne pouvez pas créer de connexion d'appairage VPC si l'un des blocs d'adresse CIDR se chevauche, même si vous avez l'intention d'utiliser uniquement les blocs d'adresse CIDR qui ne se chevauchent pas ou uniquement des blocs d'adresse CIDR. IPv6

Appairage transitif

- L'appairage de VPC ne prend pas en charge les relations d'appairage transitives. Par exemple, s'il existe des connexions d'appairage de VPC entre le VPC A et le VPC B, et entre le VPC A et le VPC C, vous ne pouvez pas acheminer le trafic du VPC B vers le VPC C via le VPC A. Pour acheminer le trafic entre le VPC B et le VPC C, vous devez créer une connexion d'appairage de VPC entre eux. Pour de plus amples informations, veuillez consulter Trois ont VPCs regardé ensemble.

Routage d'un bout à l'autre via une passerelle ou une connexion privée

- Si le VPC A possède une passerelle Internet, les ressources du VPC B ne peuvent pas utiliser la passerelle Internet du VPC A pour accéder à Internet.
- Si le VPC A possède un périphérique NAT qui offre un accès Internet aux sous-réseaux privés du VPC A, les ressources du VPC B ne peuvent pas utiliser le périphérique NAT dans le VPC A pour accéder à Internet.
- Si le VPC A dispose d'une connexion VPN à un réseau d'entreprise, les ressources du VPC B ne peuvent pas utiliser la connexion VPN pour communiquer avec le réseau d'entreprise.
- Si le VPC A dispose d'une AWS Direct Connect connexion à un réseau d'entreprise, les ressources du VPC B ne peuvent pas utiliser cette AWS Direct Connect connexion pour communiquer avec le réseau d'entreprise.
- Si le VPC A possède un point de terminaison de passerelle qui fournit une connectivité à Amazon S3 aux sous-réseaux privés du VPC A, les ressources du VPC B ne peuvent pas utiliser le point de terminaison de passerelle pour accéder à Amazon S3.

Connexions d'appairage de VPC entre régions

- Pour les trames jumbo, l'unité de transmission maximale (MTU) entre les connexions d'appairage VPC au sein d'une même région est de 9001 octets. Le MTU pour les connexions d'appairage VPC inter-régions est de 8 500 octets. Pour plus d'informations sur les cadres Jumbo, consultez la section Cadres Jumbo (9001 MTU) dans le Guide de l'utilisateur Amazon EC2 .

- Vous devez activer la prise en charge de la résolution DNS pour la connexion d'appairage VPC afin de convertir les noms d'hôtes DNS privés du VPC appairé en adresses IP privées, même si le CIDR du VPC se situe dans les plages IPv4 d'adresses privées spécifiées par la RFC 1918. IPv4

Partagé VPCs et sous-réseaux

- Seuls les propriétaires de VPC peuvent utiliser (décrire, créer, accepter, rejeter, modifier ou supprimer) les connexions d'appairage. Les participants ne peuvent pas utiliser les connexions d'appairage. Pour de plus amples informations, veuillez consulter Partager votre VPC avec d'autres comptes dans le Guide de l'utilisateur Amazon VPC.

Connexions d’appairage de VPC

Le peering VPC vous permet d'en connecter deux VPCs dans la même région ou dans des régions différentes. AWS Cela permet aux instances d’un VPC de communiquer avec les instances de l’autre VPC comme si elles faisaient toutes partie du même réseau.

Le peering VPC crée une route réseau directe entre les deux à l' VPCs aide d'adresses ou d' IPv4 adresses privées. IPv6 Le trafic envoyé entre les personnes connectées VPCs ne passe pas par Internet, par une connexion VPN ou par une connexion AWS Direct Connect. Cela fait de l’appairage de VPC un moyen sécurisé de partager des ressources, telles que des bases de données ou des serveurs web, au-delà des limites du VPC.

Pour établir une connexion d'appairage VPC, vous créez une demande de connexion d'appairage à partir d'un VPC et le propriétaire de l'autre VPC accepte la demande. Une fois la connexion établie, vous pouvez mettre à jour vos tables de routage pour acheminer le trafic entre les VPCs. Cela permet aux instances d’un VPC d’accéder aux ressources de l’autre VPC.

L’appairage de VPC est un outil important pour créer des architectures multi-VPC et partager des ressources au-delà des limites organisationnelles d’ AWS. Il fournit un moyen simple et à faible latence de se connecter VPCs sans la complexité de la configuration d'un VPN ou d'un autre service réseau.

Utilisez les procédures suivantes pour créer et utiliser des connexions d'appairage de VPC.

Tâches

- Créer une connexion d'appairage de VPC
- Accepter ou rejeter une connexion d’appairage de VPC
- Mise à jour de vos tables de routage pour une connexion d'appairage de VPC
- Mise à jour de vos groupes de sécurité pour référencer des groupes de sécurité pairs
- Activation de la résolution DNS pour une connexion d'appairage de VPC
- Suppression d'une connexion d'appairage de VPC
- Dépannage d'une connexion d'appairage de VPC

Créer une connexion d'appairage de VPC

Pour créer une connexion d'appairage de VPC, créez d'abord une demande d'appairage avec un autre VPC. Pour activer la demande, le propriétaire du VPC accepteur doit accepter la demande. Les connexions d'appairage suivantes sont prises en charge :

- Entre VPCs le même compte et la même région
- Entre VPCs un même compte et différentes régions
- Entre différents comptes et VPCs dans la même région
- Entre VPCs différents comptes et régions

Pour une connexion d'appairage VPC inter-régions, la demande doit être faite depuis la région du VPC demandeur, et la demande doit être acceptée depuis la région du VPC accepteur. Pour de plus amples informations, veuillez consulter the section called “Accepter ou rejeter”.

Tâches

- Prérequis
- Création d'une connexion d'appairage à l'aide de la console
- Créez une connexion d'appairage à l'aide de la ligne de commande

Prérequis

- Passez en revue les limites des connexions d'appairage VPC.
- Assurez-vous que les blocs IPv4 CIDR VPCs ne se chevauchent pas. Si c'est le cas, le statut de la connexion d'appairage de VPC devient immédiatement `failed`. Cette limitation s'applique même s' VPCs ils ont des blocs IPv6 CIDR uniques.

Création d'une connexion d'appairage à l'aide de la console

Utilisez la procédure suivante pour créer une connexion d'appairage VPC.

Pour créer une connexion d'appairage 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 Peering connections (Connexions d'appairage).

3. Choisissez Create peering connection (Créer une connexion d'appairage).
4. (Facultatif) Dans Nom, spécifiez le nom de la connexion d'appairage VPC. Cela crée une balise avec une clé de Name et la valeur que vous spécifiez.
5. Pour l'ID VPC (demandeur), sélectionnez un VPC dans le compte actuel.
6. Sous Sélectionnez un autre VPC avec lequel établir un pair, procédez comme suit :
   a. Dans Compte, pour établir un pair avec un VPC dans un autre compte, choisissez Un autre compte et entrez l'ID du compte. Sinon, conservez Mon compte.
   b. Pour Region, pour établir un pair avec un VPC dans une autre région, choisissez Another Region, puis choisissez la Region. Sinon, conservez cette région.
   c. Pour l'ID VPC (Accepteur), sélectionnez un VPC dans le compte et la région spécifiés.
7. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
8. Choisissez Create peering connection (Créer une connexion d'appairage).
9. Le propriétaire du compte accepteur doit accepter la connexion d'appairage. Pour de plus amples informations, veuillez consulter the section called “Accepter ou rejeter”.
10. Mettez à jour les tables de routage pour les deux VPCs afin de permettre la communication entre eux. Pour de plus amples informations, veuillez consulter the section called “Mise à jour des tables de routage”.

Créez une connexion d'appairage à l'aide de la ligne de commande

Vous pouvez créer une connexion d'appairage de VPC à l'aide des commandes suivantes :

- create-vpc-peering-connection (AWS CLI)
- New-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Accepter ou rejeter une connexion d’appairage de VPC

Une connexion d'appairage de VPC en état `pending-acceptance` doit être acceptée par le propriétaire du VPC accepteur pour être activée. Pour plus d'informations sur l'état de la connexion d'appairage `Deleted`, consultez Cycle de vie d'une connexion d'appairage de VPC. Vous ne pouvez pas accepter une demande de connexion d'appairage VPC que vous avez envoyée à un autre compte. AWS Pour créer une connexion d'appairage VPC entre VPCs deux AWS comptes, vous pouvez créer et accepter vous-même la demande.

Vous pouvez rejeter toute demande de connexion d'appairage de VPC que vous avez reçue en état `pending-acceptance`. Vous ne devez accepter que les connexions d'appairage VPC Comptes AWS que celles que vous connaissez et auxquelles vous faites confiance ; vous pouvez rejeter toute demande indésirable. Pour plus d'informations sur l'état de la connexion d'appairage `Rejected`, consultez Cycle de vie d'une connexion d'appairage de VPC.

> **Important**
>
> N'acceptez pas les connexions d'appairage VPC provenant de comptes inconnus. AWS Un utilisateur malveillant peut vous avoir envoyé une demande de connexion d'appairage de VPC pour obtenir un accès réseau non autorisé à votre VPC. Cette méthode est appelée « peer phishing » ou hameçonnage de pairs. Vous pouvez rejeter en toute sécurité les demandes de connexion d'appairage VPC indésirables sans risquer que le demandeur ait accès à des informations concernant votre compte AWS ou votre VPC. Pour de plus amples informations, veuillez consulter Accepter ou rejeter une connexion d'appairage de VPC. Vous pouvez également ignorer la demande et la laisser expirer ; par défaut, les demandes expirent après 7 jours.

Pour accepter ou rejeter une connexion de peering à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Utilisez le sélecteur de région pour choisir la région du VPC accepteur.
3. Dans le volet de navigation, choisissez Peering connections (Connexions d'appairage).
4. Pour rejeter une connexion d'appairage, sélectionnez la connexion d'appairage de VPC, puis choisissez Actions, Rejeter la demande. Lorsque vous êtes invité à confirmer l'opération, choisissez Rejeter la demande.
5. Pour accepter une connexion d'appairage, sélectionnez la connexion d'appairage de VPC en attente (état `pending-acceptance`), puis choisissez Actions, Accepter la demande. Pour plus d'informations sur les états du cycle de vie d'une connexion d'appairage, consultez Cycle de vie d'une connexion d'appairage de VPC.

   S'il n'y a aucune connexion d'appairage VPC en attente, vérifiez que vous avez sélectionné la région du VPC accepteur.
6. Lorsque vous êtes invité à confirmer l'opération, choisissez Accepter la demande.
7. Choisissez Modifier mes tables de routage maintenant pour ajouter une route à la table de routage de VPC et pouvoir envoyer et recevoir du trafic via la connexion d'appairage. Pour

de plus amples informations, veuillez consulter Mise à jour de vos tables de routage pour une connexion d'appairage de VPC.

Pour accepter une connexion d'appairage à l'aide de la ligne de commande

- accept-vpc-peering-connection (AWS CLI)
- Approve-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Pour rejeter une connexion d'appairage à l'aide de la ligne de commande

- reject-vpc-peering-connection (AWS CLI)
- Deny-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Mise à jour de vos tables de routage pour une connexion d'appairage de VPC

Pour activer le IPv4 trafic privé entre les instances dans Peered VPCs, vous devez ajouter une route vers les tables de routage associées aux sous-réseaux des deux instances. La destination du routage est le bloc d'adresse CIDR (ou une partie du bloc d'adresse CIDR) du VPC pair et la cible est l'ID de la connexion d'appairage de VPC. Pour plus d'informations, consultez Configuration des tables de routage dans le Guide de l'utilisateur d'Amazon VPC.

Voici un exemple de tables de routage qui permettent la communication entre les instances de deux VPC homologues VPCs, le VPC A et le VPC B. Chaque table possède une route locale et une route qui envoie le trafic du VPC homologue à la connexion d'appairage du VPC.

Table de routage	Destination	Cible
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx- *11112222*
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx- *11112222*

De même, si la connexion d'appairage intégrée VPCs au VPC est associée à des blocs IPv6 CIDR, vous pouvez ajouter des routes qui permettent la communication avec le VPC homologue. IPv6

Pour plus d'informations sur les configurations de tables de routages prises en charge pour les connexions d'appairage de VPC, consultez la page Configurations courantes de connexion d'appairage de VPC.

Considérations

- Si vous avez un VPC apparenté avec plusieurs blocs IPv4 CIDR VPCs qui se chevauchent ou correspondent, assurez-vous que vos tables de routage sont configurées de manière à éviter d'envoyer le trafic de réponse de votre VPC vers le mauvais VPC. AWS ne prend actuellement pas en charge le transfert de chemin inversé monodiffusion dans les connexions d'appairage VPC qui vérifient l'adresse IP source des paquets et acheminent les paquets de réponse vers la source. Pour de plus amples informations, veuillez consulter Routage pour le trafic de la réponse.
- Votre compte a un quota sur le nombre d'entrées que vous pouvez ajouter par table de routage. Si le nombre de connexions d'appairage de VPC dans votre VPC dépasse le quota d'entrée de la table de routage pour une même table de routage, pensez à utiliser plusieurs sous-réseaux qui sont chacun associés à une table de routage personnalisée.
- Vous pouvez ajouter une route pour une connexion d'appairage de VPC présentant l'état `pending-acceptance`. Cependant, l'acheminement a un état de `blackhole`, et n'a aucun effet tant que la connexion d'appairage de VPC n'est pas dans l'état `active`.

Pour ajouter une IPv4 route pour une connexion d'appairage VPC

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 case à cocher à côté de la table de routage associée au sous-réseau dans lequel votre instance réside.

   Si vous n'avez pas de table de routage explicitement associée à ce sous-réseau, la table de routage principale du VPC lui est implicitement associée.
4. Choisissez Actions, Modifier les routes.
5. Choisissez Ajouter une route.
6. Pour Destination, entrez la plage d' IPv4 adresses vers laquelle le trafic réseau de la connexion d'appairage VPC doit être dirigé. Vous pouvez spécifier l'intégralité du bloc IPv4 CIDR du VPC

homologue, une plage spécifique ou une adresse IPv4 individuelle, telle que l'adresse IP de l'instance avec laquelle communiquer. Par exemple, si le bloc d'adresse CIDR du VPC pair est `10.0.0.0/16`, vous pouvez spécifier une partie `10.0.0.0/24` ou une adresse IP spécifique `10.0.0.7/32`.

7. Pour Cible, sélectionnez la connexion d'appairage de VPC.
8. Sélectionnez Enregistrer les modifications.

Le propriétaire du VPC pair doit également effectuer ces étapes pour ajouter une route pour rediriger le trafic vers votre VPC via la connexion d'appairage de VPC.

Si vous avez des ressources dans différentes AWS régions qui utilisent IPv6 des adresses, vous pouvez créer une connexion d'appairage interrégionale. Vous pouvez ensuite ajouter un IPv6 itinéraire de communication entre les ressources.

Pour ajouter une IPv6 route pour une connexion d'appairage VPC

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 case à cocher à côté de la table de routage associée au sous-réseau dans lequel votre instance réside.

> **Note**
>
> Si vous n'avez pas de table de routage associée à ce sous-réseau, sélectionnez la table de routage principale pour le VPC, puisque le sous-réseau utilise ensuite cette table de routage par défaut.

4. Choisissez Actions, Modifier les routes.
5. Choisissez Ajouter une route.
6. Pour Destination, entrez la plage d' IPv6 adresses du VPC homologue. Vous pouvez spécifier l'intégralité du bloc IPv6 CIDR du VPC homologue, une plage spécifique ou une IPv6 adresse individuelle. Par exemple, si le bloc d'adresse CIDR du VPC pair est `2001:db8:1234:1a00::/56`, vous pouvez spécifier une partie `2001:db8:1234:1a00::/64` ou une adresse IP spécifique `2001:db8:1234:1a00::123/128`.
7. Pour Cible, sélectionnez la connexion d'appairage de VPC.
8. Sélectionnez Enregistrer les modifications.

Pour plus d'informations, consultez Tables de routage dans le Guide de l'utilisateur Amazon VPC.

Pour ajouter ou remplacer un itinéraire à l'aide de la ligne de commande

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

Mise à jour de vos groupes de sécurité pour référencer des groupes de sécurité pairs

Vous pouvez mettre à jour les règles entrantes ou sortantes de vos groupes de sécurité VPC afin de référencer les groupes de sécurité pour les pairs. VPCs Cette étape autorise le trafic vers et depuis les instances associées au groupe de sécurité référencé dans le VPC appairé.

> **Note**
>
> Les groupes de sécurité d'un VPC pair ne s'affichent pas dans la console pour que vous puissiez les sélectionner.

Prérequis

- Pour référencer un groupe de sécurité dans un VPC pair, la connexion d'appairage de VPC doit être à l'état `active`.
- Le VPC homologue peut être un VPC de votre compte ou un VPC d'un autre compte. AWS Pour référencer un groupe de sécurité qui se trouve dans un autre AWS compte mais dans la même région, incluez le numéro de compte avec l'ID du groupe de sécurité. Par exemple, `123456789012/sg-1a2b3c4d`.
- Vous ne pouvez pas faire référence au groupe de sécurité d'un VPC pair qui se trouve dans une autre région. À la place, utilisez le bloc CIDR du VPC pair.
- Si vous configurez des acheminements pour transférer le trafic entre deux instances de sous-réseaux différents via une appliance middlebox, vous devez vous assurer que les groupes de sécurité des deux instances autorisent le trafic à transiter entre les instances. Le groupe de sécurité de chaque instance doit référencer l'adresse IP privée de l'autre instance ou la plage d'adresses CIDR du sous-réseau qui contient l'autre instance en tant que source. Si vous référencez le groupe de sécurité de l'autre instance en tant que source, cela n'autorise pas le trafic à transiter entre les instances.

Pour mettre à jour les règles de votre 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 et effectuez l'une des actions suivantes :
   - Pour modifier les règles entrantes, sélectionnez Actions, Modifier les règles entrantes.
   - Pour modifier les règles sortantes, sélectionnez Actions, Modifier les règles sortantes.
4. Pour ajouter une règle, choisissez Ajouter une règle et spécifiez le type, le protocole et la plage de ports. Pour Source (règle entrante) ou Destination (règle sortante), effectuez l'une des opérations suivantes :
   - Pour un VPC pair dans le même compte et dans la même région, saisissez l'ID du groupe de sécurité.
   - Pour un VPC pair situé dans un compte différent mais dans la même région, saisissez l'ID du compte et l'ID du groupe de sécurité, séparés par une barre oblique (par exemple, `123456789012/sg-1a2b3c4d`).
   - Pour un VPC pair dans une autre région, saisissez le bloc d'adresse CIDR du VPC pair.
5. Pour modifier une règle existante, modifiez ses valeurs (par exemple, la source ou la description).
6. Pour supprimer une règle, cliquez sur Supprimer à côté de la règle.
7. Sélectionnez Enregistrer les règles.

Pour mettre à jour les règles entrantes à l'aide de la ligne de commande

- authorize-security-group-ingress et revoke-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress et Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

Par exemple, pour mettre à jour votre groupe de sécurité `sg-aaaa1111` pour autoriser un accès entrant sur HTTP depuis `sg-bbbb2222` pour un VPC pair, utilisez la commande d'interface de ligne de commande qui suit. Si le VPC homologue se trouve dans la même région mais sur un compte différent, ajoutez-le. `--group-owner` *`aws-account-id`*

```
aws ec2 authorize-security-group-ingress --group-id sg-aaaa1111 --protocol tcp --
port 80 --source-group sg-bbbb2222
```

Pour mettre à jour les règles sortantes à l'aide de la ligne de commande

- authorize-security-group-egress et revoke-security-group-egress (AWS CLI)
- Grant-EC2SecurityGroupEgress et Revoke-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Après avoir mis à jour les règles du groupe de sécurité, utilisez la describe-security-groupscommande pour afficher le groupe de sécurité référencé dans les règles de votre groupe de sécurité.

Identification de vos groupes de sécurité référencés

Pour déterminer si votre groupe de sécurité est référencé dans les règles d'un groupe de sécurité dans un VPC pair, vous pouvez utiliser l'une des commandes suivantes pour un ou pour plusieurs groupes de sécurité dans votre compte.

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)

Dans l'exemple suivant, la réponse indique que le groupe de sécurité `sg-bbbb2222` est référencé par un groupe de sécurité dans le VPC `vpc-aaaaaaaa` :

```
aws ec2 describe-security-group-references --group-id sg-bbbb2222
```

```
{
  "SecurityGroupsReferenceSet": [
    {
      "ReferencingVpcId": "vpc-aaaaaaaa",
      "GroupId": "sg-bbbb2222",
      "VpcPeeringConnectionId": "pcx-b04deed9"
    }
  ]
}
```

Si la connexion d'appairage de VPC est supprimée, ou si le propriétaire du VPC pair supprime le groupe de sécurité référencé, la règle du groupe de sécurité devient caduque.

Afficher et supprimer des règles du groupe de sécurité obsolètes

Une règle de groupe de sécurité obsolète est une règle qui référence un groupe de sécurité supprimé dans le même VPC ou dans un VPC pair, ou qui référence un groupe de sécurité dans un VPC pair pour lequel la connexion d'appairage de VPC a été supprimée. Lorsqu'une règle du groupe de sécurité devient obsolète, elle n'est pas automatiquement supprimée de votre groupe de sécurité et vous devez la supprimer manuellement. Si une règle de groupe de sécurité est obsolète parce que la connexion d'appairage VPC a été supprimée, elle ne sera plus marquée comme obsolète si vous créez une nouvelle connexion d'appairage VPC avec la même règle. VPCs

Vous pouvez afficher et supprimer les règles du groupe de sécurité obsolètes pour un VPC à l'aide de la console Amazon VPC.

Pour afficher et supprimer des règles du groupe de sécurité obsolètes

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. Choisissez Actions (Actions), Manage stale rules (Gestion les règles obsolètes).
4. PourVPC, choisissez le VPC dont les règles sont obsolètes.
5. Choisissez Modifier.
6. Choisissez le bouton Supprimer à la droite de la règle à supprimer. Choisissez Prévisualiser les modifications, Enregistrer les règles.

Pour décrire les règles de votre groupe de sécurité périmées à l'aide de la ligne de commande

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)

Dans l'exemple suivant, le VPC A (`vpc-aaaaaaaa`) et le VPC B étaient appairés, et la connexion d'appairage de VPC a été supprimée. Votre groupe de sécurité `sg-aaaa1111` dans le VPC A référence `sg-bbbb2222` dans le VPC B. Quand vous exécutez la commande `describe-stale-security-groups` pour votre VPC, la réponse indique que le groupe de sécurité `sg-aaaa1111` possède une règle SSH obsolète qui référence `sg-bbbb2222`.

```
aws ec2 describe-stale-security-groups --vpc-id vpc-aaaaaaaa
```

```
{
    "StaleSecurityGroupSet": [
        {
            "VpcId": "vpc-aaaaaaaa",
            "StaleIpPermissionsEgress": [],
            "GroupName": "Access1",
            "StaleIpPermissions": [
                {
                    "ToPort": 22,
                    "FromPort": 22,
                    "UserIdGroupPairs": [
                        {
                            "VpcId": "vpc-bbbbbbbb",
                            "PeeringStatus": "deleted",
                            "UserId": "123456789101",
                            "GroupName": "Prod1",
                            "VpcPeeringConnectionId": "pcx-b04deed9",
                            "GroupId": "sg-bbbb2222"
                        }
                    ],
                    "IpProtocol": "tcp"
                }
            ],
            "GroupId": "sg-aaaa1111",
            "Description": "Reference remote SG"
        }
    ]
}
```

Après avoir identifié les règles du groupe de sécurité périmées, vous pouvez les supprimer à l'aide des revoke-security-group-egresscommandes revoke-security-group-ingressor.

Activation de la résolution DNS pour une connexion d'appairage de VPC

Les paramètres DNS d'une connexion d'appairage VPC déterminent la manière dont les noms d'hôtes DNS publics sont résolus pour les demandes qui transitent par la connexion d'appairage VPC. Si une EC2 instance d'un côté d'une connexion d'appairage VPC envoie une demande à une EC2 instance de l'autre côté en utilisant le nom d'hôte IPv4 DNS public de l'instance, le nom d'hôte DNS est résolu comme suit.

Résolution DNS désactivée (par défaut)

Le nom d'hôte IPv4 DNS public est résolu en IPv4 adresse publique de l'instance.

Résolution DNS activée

Le nom d'hôte IPv4 DNS public est remplacé par l' IPv4 adresse privée de l'instance.

Prérequis

- Les deux VPCs doivent être activés pour les noms d'hôte DNS et la résolution DNS. Pour plus d'informations, consultez DNS attributes for your VPC (Attributs DNS pour votre VPC) dans le Guide de l'utilisateur d'Amazon VPC.
- La connexion d'appairage doit être en bon `active` état. Vous ne pouvez pas activer la résolution DNS lorsque vous créez une connexion de peering.
- Le propriétaire du VPC demandeur doit modifier les options d'appairage du VPC demandeur, et le propriétaire du VPC accepteur doit modifier les options d'appairage du VPC accepteur. S' VPCs ils appartiennent au même compte et à la même région, vous pouvez activer la résolution DNS pour le demandeur et l'accepteur VPCs en même temps.

Pour activer la résolution DNS pour une connexion de peering 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 Peering connections (Connexions d'appairage).
3. Sélectionnez la connexion d'appairage de VPC.
4. Choisissez Actions, puis Modifier les paramètres DNS.
5. Pour activer la résolution DNS pour les demandes provenant du VPC demandeur, sélectionnez Résolution DNS du demandeur, puis Autoriser le VPC accepteur à résoudre le DNS du VPC demandeur.
6. Pour garantir la résolution DNS des demandes provenant du VPC accepteur, sélectionnez Accepter la résolution DNS, Autoriser le VPC demandeur à résoudre le DNS du VPC accepteur.
7. Sélectionnez Enregistrer les modifications.

Pour activer la résolution DNS à l'aide de la ligne de commande

- modify-vpc-peering-connection-options ()AWS CLI

- Edit-EC2VpcPeeringConnectionOption (AWS Tools for Windows PowerShell)

Pour décrire les options de connexion par peering VPC à l'aide de la ligne de commande

- describe-vpc-peering-connections (AWS CLI)
- Get-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Suppression d'une connexion d'appairage de VPC

Chaque propriétaire d'un VPC dans une connexion d'appairage peut supprimer la connexion d'appairage de VPC à tout moment. Vous pouvez également supprimer une connexion d'appairage de VPC que vous avez demandée et qui est toujours en état `pending-acceptance`.

Vous ne pouvez pas supprimer la connexion d'appairage de VPC lorsque la connexion d'appairage de VPC est dans l'état `rejected`. Nous supprimons automatiquement la connexion pour vous.

La suppression d'un VPC de la console Amazon VPC; qui fait partie d'une connexion d'appairage de VPC active, supprime également la connexion d'appairage de VPC. Si vous avez demandé une connexion d'appairage de VPC avec un VPC dans un autre compte et que vous supprimez votre VPC avant que l'autre partie ait accepté la demande, la connexion d'appairage de VPC est également supprimée. Vous ne pouvez pas supprimer un VPC pour lequel vous avez une demande `pending-acceptance` d'un VPC dans un autre compte. Vous devez d'abord rejeter la demande de connexion d'appairage de VPC.

Lorsque vous supprimez une connexion d'appairage, l'état est défini sur `Deleting`, puis sur `Deleted`. Une fois que vous avez supprimé une connexion, elle ne peut être ni acceptée, ni refusée, ni modifiée. Pour plus d'informations sur la durée de visibilité de la connexion d'appairage, consultez Cycle de vie d'une connexion d'appairage de VPC.

Supprimer une connexion d'appairage de VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Peering connections (Connexions d'appairage).
3. Sélectionnez la connexion d'appairage de VPC.
4. Choisissez Actions, Delete peering connection (Supprimer la connexion d'appairage).
5. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

Pour supprimer une connexion d'appairage VPC à l'aide de la ligne de commande

- delete-vpc-peering-connection (AWS CLI)
- Remove-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Dépannage d'une connexion d'appairage de VPC

Si vous rencontrez des difficultés pour vous connecter à une ressource dans un VPC à partir d'une ressource dans un VPC pair, procédez comme suit :

- Pour chaque ressource dans chaque VPC, vérifiez que la table de routage de son sous-réseau contient un acheminement qui envoie le trafic destiné au VPC pair vers la connexion d'appairage de VPC. Cela garantit que le trafic réseau peut circuler correctement entre les deux VPCs. Pour de plus amples informations, veuillez consulter Mise à jour des tables de routage.
- Pour toutes les EC2 instances impliquées, vérifiez que les groupes de sécurité de ces instances autorisent le trafic entrant et sortant depuis le VPC homologue. Les règles des groupes de sécurité contrôlent le trafic autorisé à accéder à vos EC2 instances. Pour de plus amples informations, veuillez consulter Référence des groupes de sécurité pairs.
- Vérifiez que le réseau ACLs des sous-réseaux contenant vos ressources autorise le trafic nécessaire en provenance du VPC homologue. Le réseau ACLs constitue une couche de sécurité supplémentaire qui filtre le trafic au niveau du sous-réseau.

Si le problème persiste, vous pouvez utiliser l’analyseur d’accessibilité. Reachability Analyzer peut aider à identifier le composant spécifique (qu'il s'agisse d'une table de routage, d'un groupe de sécurité ou d'une ACL réseau) à l'origine du problème de connectivité entre les deux. VPCs Pour plus d'informations, reportez-vous au Guide de l'Analyseur d'accessibilité.

Il est essentiel de vérifier minutieusement les configurations réseau de votre VPC pour résoudre les problèmes de connexion d’appairage de VPC que vous pourriez rencontrer.

Configurations courantes de connexion d’appairage de VPC

Cette section décrit deux types courants de configurations d’appairage de VPC que vous pouvez implémenter :

- Configurations d’appairage de VPC avec des itinéraires vers un VPC entier : dans cette configuration, vous créez un acheminement dans la table de routage de chaque VPC qui envoie tout le trafic destiné au VPC pair vers la connexion d’appairage de VPC. Cela permet à n’importe quelle ressource d’un VPC de communiquer avec n’importe quelle ressource du VPC homologue, simplifiant ainsi la gestion. Cependant, cela signifie également que tout le trafic entre eux VPCs passera par la connexion de peering, ce qui pourrait devenir un goulot d'étranglement si le volume de trafic est élevé.
- Configurations d’appairage de VPC avec des itinéraires spécifiques : vous pouvez également créer des itinéraires plus granulaires dans la table de routage de chaque VPC qui envoient du trafic uniquement vers des sous-réseaux ou des ressources spécifiques du VPC homologue. Cela vous permet de limiter le trafic passant par la connexion d’appairage au strict nécessaire, ce qui peut être plus efficace. Cependant, cela nécessite également plus de maintenance, car vous devrez mettre à jour les tables de routage chaque fois que vous ajoutez de nouvelles ressources dans le VPC homologue devant communiquer.

La meilleure approche dépend de facteurs tels que la taille et la complexité de votre architecture VPC, le volume de trafic attendu entre les et les VPCs besoins de votre organisation en matière de sécurité et d'accès aux ressources. De nombreuses entreprises utilisent une approche hybride, avec des itinéraires larges pour les modèles de trafic courants et des itinéraires spécifiques pour les cas d’utilisation plus sensibles ou gourmands en bande passante.

Configurations

- Configurations d'appairage de VPC avec routes vers un VPC complet
- Configurations d'appairage de VPC avec des routes spécifiques

Configurations d'appairage de VPC avec routes vers un VPC complet

Vous pouvez configurer les connexions d'appairage de VPC afin que vos tables de routage accèdent à l'ensemble du bloc d'adresse CIDR du VPC pair. Pour plus d'informations sur les scénarios dans

lesquels vous pouvez avoir besoin d'une configuration de connexion d'appairage de VPC spécifique, consultez la section Scénarios de mise en réseau de connexions d'appairage de VPC. Pour en savoir plus sur la création et l'utilisation de connexions d'appairage de VPC, consultez Connexions d'appairage de VPC.

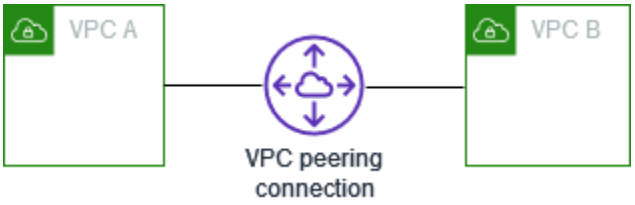
Pour en savoir plus sur la mise à jour de vos tables de routage, consultez la page Mise à jour de vos tables de routage pour une connexion d'appairage de VPC.

Configurations

- Deux se sont VPCs regardés ensemble
- Un VPC jumelé à deux VPCs
- Trois ont VPCs regardé ensemble
- Plusieurs VPCs comparés ensemble

Deux se sont VPCs regardés ensemble

Dans cette configuration, il existe une connexion d'appairage entre le VPC A et le VPC B (`pcx-11112222`). Ils VPCs sont identiques Compte AWS et leurs blocs CIDR ne se chevauchent pas.



Vous pouvez utiliser cette configuration lorsque vous en avez deux VPCs qui ont besoin d'accéder aux ressources de l'autre. Par exemple, vous créez un VPC A pour vos enregistrements comptables, et un VPC B pour vos enregistrements financiers, et chaque VPC doit accéder aux ressources de l'autre VPC, sans aucune restriction.

CIDR VPC unique

Mettez à jour la table de routage de chaque VPC avec une route qui envoie le trafic pour le bloc d'adresse CIDR du VPC pair vers la connexion d'appairage de VPC.

Table de routage	Destination	Cible
VPC A	*`VPC A CIDR`*	Local

Table de routage	Destination	Cible
	VPC B CIDR	pcx-11112222
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-11112222

IPv4 VPC multiples CIDRs

Si plusieurs blocs d'adresse IPv4 CIDR sont associés au VPC A et au VPC B, vous pouvez mettre à jour la table de routage pour chaque VPC avec des itinéraires pour certains ou pour tous les blocs d'adresse CIDR IPv4 du VPC homologue.

Table de routage	Destination	Cible
VPC A	*VPC A CIDR 1*	Local
	VPC A CIDR 2	Local
	VPC B CIDR 1	pcx-11112222
	VPC B CIDR 2	pcx-11112222
VPC B	*VPC B CIDR 1*	Local
	VPC B CIDR 2	Local
	VPC A CIDR 1	pcx-11112222
	VPC A CIDR 2	pcx-11112222

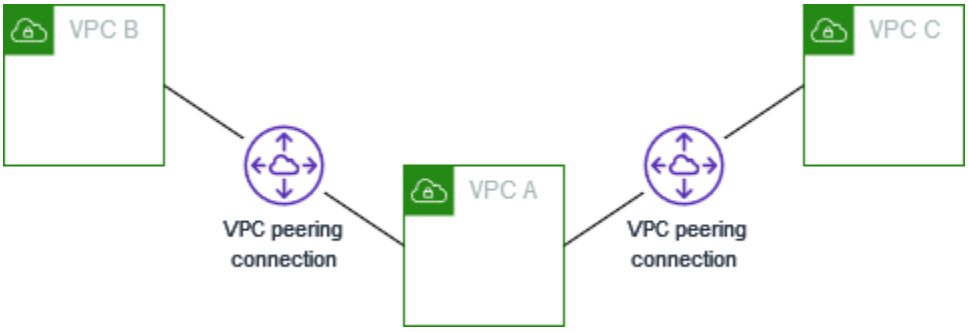
IPv4 et IPv6 VPC CIDRs

Si des blocs d'adresse IPv6 CIDR sont associés au VPC A et au VPC B, vous pouvez mettre à jour la table de routage de chaque VPC avec des itinéraires pour les blocs d'adresse CIDR et pour le bloc d'adresse IPv4 CIDR IPv6 du VPC homologue.

Table de routage	Destination	Cible
VPC A	*VPC A IPv4 CIDR*	Local
	VPC A IPv6 CIDR	Local
	VPC B IPv4 CIDR	pcx-11112222
	VPC B IPv6 CIDR	pcx-11112222
VPC B	*VPC B IPv4 CIDR*	Local
	VPC B IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-11112222
	VPC A IPv6 CIDR	pcx-11112222

Un VPC jumelé à deux VPCs

Dans cette configuration, il existe un VPC central (VPC A), une connexion d'appairage entre le VPC A et le VPC B (`pcx-12121212`) et une connexion d'appairage entre le VPC A et le VPC C (`pcx-23232323`). Les trois VPCs sont identiques Compte AWS et leurs blocs CIDR ne se chevauchent pas.



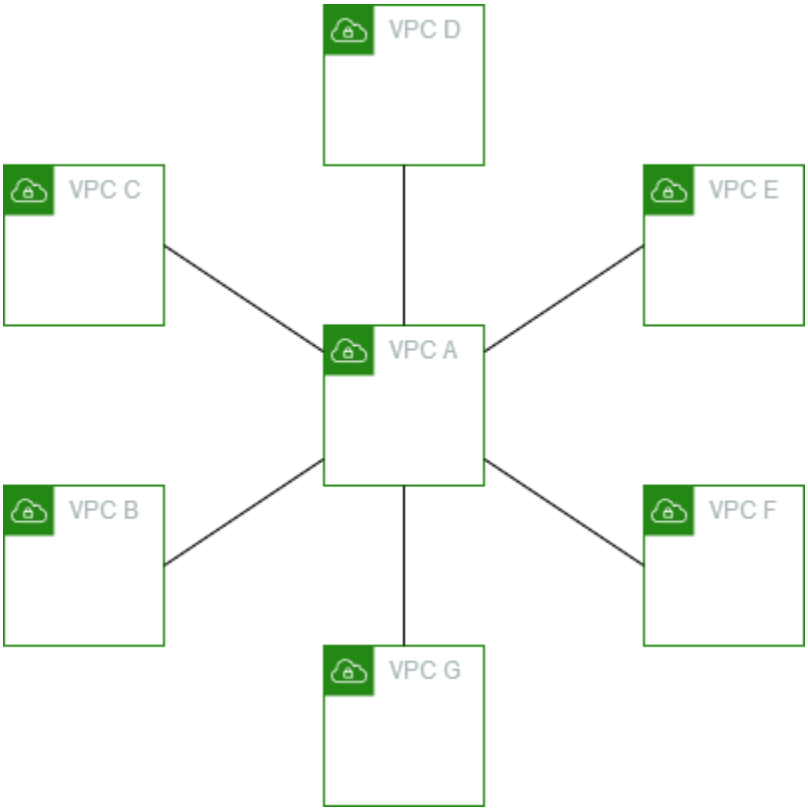
Le VPC B et le VPC C ne peuvent pas envoyer de trafic directement via un VPC A, car l'appairage de VPC ne prend pas en charge les relations d'appairage transitives. Vous pouvez créer une connexion d'appairage de VPC entre le VPC B et le VPC C, comme indiqué dans Trois ont VPCs regardé ensemble. Pour plus d'informations sur les scénarios d'appairage non pris en charge, consultez la section the section called “Limitations des appairages de VPC”.

Vous pouvez utiliser cette configuration lorsque vous disposez de ressources sur un VPC central, telles qu'un référentiel de services, auxquelles d'autres utilisateurs VPCs ont besoin d'accéder. Les autres VPCs n'ont pas besoin d'accéder aux ressources des autres ; ils doivent uniquement accéder aux ressources du VPC central.

Mettez à jour la table de routage pour chaque VPC comme suit pour implémenter cette configuration à l'aide d'un bloc CIDR par VPC.

Table de routage	Destination	Cible
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-12121212
	VPC C CIDR	pcx-23232323
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-12121212
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-23232323

Vous pouvez étendre cette configuration à d'autres VPCs. Par exemple, le VPC A est apparié au VPC B via le VPC G en utilisant les deux, mais IPv4 les deux autres ne sont pas IPv6 CIDRs appariés l'un à l' VPCs autre. Dans ce diagramme, les lignes représentent les connexions d'appairage de VPC.



Mettez à jour la table de routage comme suit.

Table de routage	Destination	Cible
VPC A	*VPC A IPv4 CIDR*	Local
	VPC A IPv6 CIDR	Local
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
	VPC C IPv6 CIDR	pcx-aaaacccc
	VPC D IPv4 CIDR	pcx-aaaadddd
	VPC D IPv6 CIDR	pcx-aaaadddd
	VPC E IPv4 CIDR	pcx-aaaaeeee

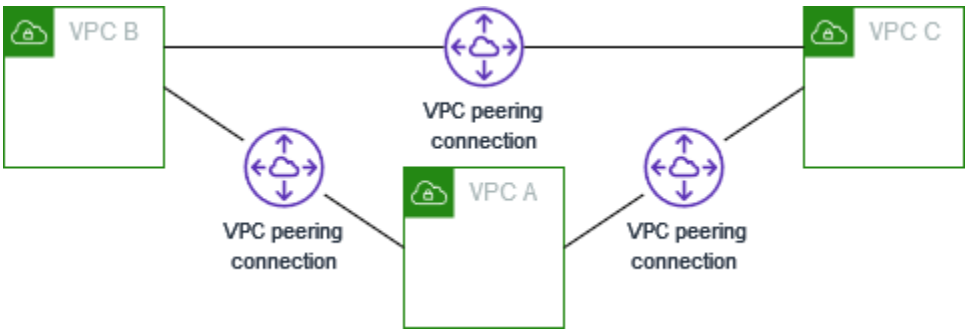
Table de routage	Destination	Cible
	VPC E IPv6 CIDR	pcx-aaaaeeee
	VPC F IPv4 CIDR	pcx-aaaaffff
	VPC F IPv6 CIDR	pcx-aaaaffff
	VPC G IPv4 CIDR	pcx-aaaagggg
	VPC G IPv6 CIDR	pcx-aaaagggg
VPC B	*VPC B IPv4 CIDR*	Local
	VPC B IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
VPC C	*VPC C IPv4 CIDR*	Local
	VPC C IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC A IPv6 CIDR	pcx-aaaacccc
VPC D	*VPC D IPv4 CIDR*	Local
	VPC D IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaadddd
	VPC A IPv6 CIDR	pcx-aaaadddd
VPC E	*VPC E IPv4 CIDR*	Local
	VPC E IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaaeeee

Table de routage	Destination	Cible
	VPC A IPv6 CIDR	pcx-aaaaeeee
VPC F	*VPC F IPv4 CIDR*	Local
	VPC F IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaaffff
	VPC A IPv6 CIDR	pcx-aaaaffff
VPC G	*VPC G IPv4 CIDR*	Local
	VPC G IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaagggg
	VPC A IPv6 CIDR	pcx-aaaagggg

Trois ont VPCs regardé ensemble

Dans cette configuration, il VPCs en existe trois identiques Compte AWS avec des blocs CIDR qui ne se chevauchent pas. Ils VPCs sont examinés dans un maillage complet comme suit :

- Le VPC A est appairé au VPC B via une connexion d'appairage de VPC `pcx-aaaabbbb`
- Le VPC A est appairé au VPC C via une connexion d'appairage de VPC `pcx-aaaacccc`
- Le VPC B est appairé au VPC C via une connexion d'appairage de VPC `pcx-bbbbcccc`



Vous pouvez utiliser cette configuration lorsque vous avez VPCs besoin de partager des ressources entre vous sans restriction. Par exemple, en tant que système de partage de fichiers.

Mettez à jour la table de routage pour chaque VPC comme suit pour implémenter cette configuration.

Table de routage	Destination	Cible
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-bbbbcccc
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc

Si le VPC A et le VPC B possèdent à la fois des IPv6 blocs d'adresse CIDR IPv4 et que le VPC C ne possède pas de bloc d'adresse IPv6 CIDR, mettez à jour les tables de routage comme suit. Les ressources du VPC A et du VPC B peuvent communiquer via la connexion d'appairage IPv6 du VPC. Cependant, le VPC C ne peut pas communiquer avec le VPC A ou le VPC B en utilisant. IPv6

Tables de routage	Destination	Cible
VPC A	*VPC A IPv4 CIDR*	Local
	VPC A IPv6 CIDR	Local
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb

Tables de routage	Destination	Cible
	VPC C IPv4 CIDR	pcx-aaaacccc
VPC B	*VPC B IPv4 CIDR*	Local
	VPC B IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-bbbbcccc
VPC C	*VPC C IPv4 CIDR*	Local
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC B IPv4 CIDR	pcx-bbbbcccc

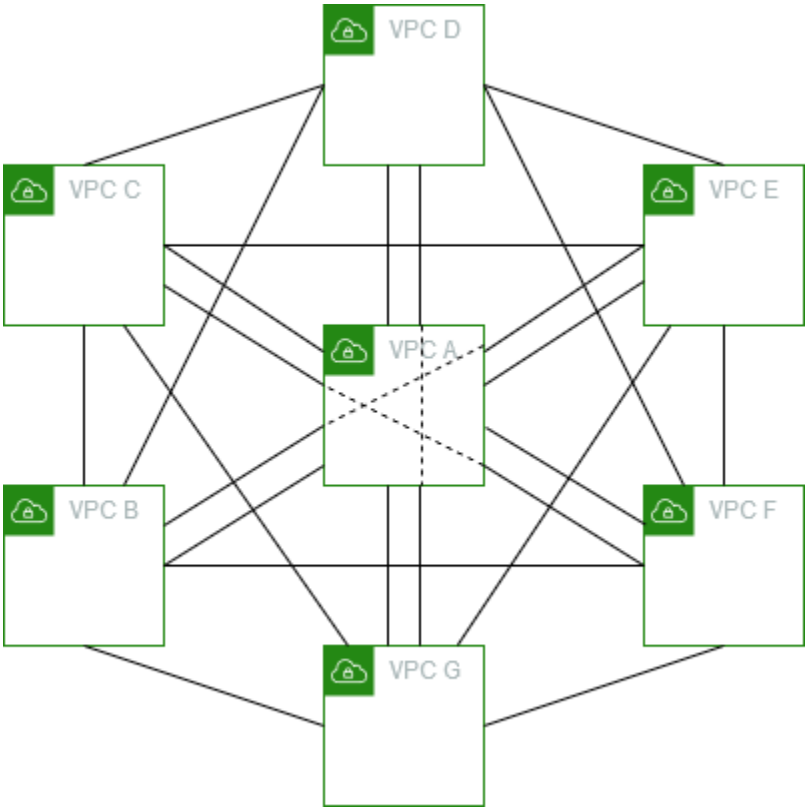
Plusieurs VPCs comparés ensemble

Dans cette configuration, il y en a sept VPCs pairs dans une configuration à maillage complet. Ils VPCs sont identiques Compte AWS et leurs blocs CIDR ne se chevauchent pas.

VPC	VPC	Connexion d'appairage de VPC
A	B	pcx-aaaabbbb
A	C	pcx-aaaacccc
A	D	pcx-aaaadddd
A	E	pcx-aaaaeeee
A	F	pcx-aaaaffff
A	G	pcx-aaaagggg
B	C	pcx-bbbbcccc

VPC	VPC	Connexion d’appairage de VPC
B	D	pcx-bbbbdddd
B	E	pcx-bbbbeeee
B	F	pcx-bbbbffff
B	G	pcx-bbbbgggg
C	D	pcx-ccccdddd
C	E	pcx-ccccceeee
C	F	pcx-ccccffff
C	G	pcx-ccccgggg
D	E	pcx-ddddeeee
D	F	pcx-ddddffff
D	G	pcx-ddddgggg
E	F	pcx-eeeeffff
E	G	pcx-eeeegggg
F	G	pcx-ffffgggg

Vous pouvez utiliser cette configuration lorsque vous en avez plusieurs VPCs qui doivent pouvoir accéder aux ressources des autres sans restriction. Par exemple, en tant que réseau de partage de fichiers. Dans ce diagramme, les lignes représentent les connexions d'appairage de VPC.



Mettez à jour la table de routage pour chaque VPC comme suit pour implémenter cette configuration.

Table de routage	Destination	Cible
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
	VPC D CIDR	pcx-aaaadddd
	VPC E CIDR	pcx-aaaaeeee
	VPC F CIDR	pcx-aaaaffff
	VPC G CIDR	pcx-aaaagggg
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-aaaabbbb

Table de routage	Destination	Cible
	VPC C CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-bbbbdddd
	VPC E CIDR	pcx-bbbbeeee
	VPC F CIDR	pcx-bbbbffff
	VPC G CIDR	pcx-bbbbgggg
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-ccccdddd
	VPC E CIDR	pcx-cccceeee
	VPC F CIDR	pcx-ccccffff
	VPC G CIDR	pcx-ccccgggg
VPC D	*VPC D CIDR*	Local
	VPC A CIDR	pcx-aaaadddd
	VPC B CIDR	pcx-bbbbdddd
	VPC C CIDR	pcx-ccccdddd
	VPC E CIDR	pcx-ddddeeee
	VPC F CIDR	pcx-ddddffff
	VPC G CIDR	pcx-ddddgggg
VPC E	*VPC E CIDR*	Local

Table de routage	Destination	Cible
	VPC A CIDR	pcx-aaaaeeee
	VPC B CIDR	pcx-bbbbeeee
	VPC C CIDR	pcx-cccceeee
	VPC D CIDR	pcx-ddddeeee
	VPC F CIDR	pcx-eeeeffff
	VPC G CIDR	pcx-eeeegggg
VPC F	*VPC F CIDR*	Local
	VPC A CIDR	pcx-aaaaffff
	VPC B CIDR	pcx-bbbbffff
	VPC C CIDR	pcx-ccccffff
	VPC D CIDR	pcx-ddddffff
	VPC E CIDR	pcx-eeeeffff
	VPC G CIDR	pcx-ffffgggg
VPC G	*VPC G CIDR*	Local
	VPC A CIDR	pcx-aaaagggg
	VPC B CIDR	pcx-bbbbgggg
	VPC C CIDR	pcx-ccccgggg
	VPC D CIDR	pcx-ddddgggg
	VPC E CIDR	pcx-eeeegggg
	VPC F CIDR	pcx-ffffgggg

Si tous VPCs sont associés à des blocs IPv6 CIDR, mettez à jour les tables de routage comme suit.

Table de routage	Destination	Cible
VPC A	*VPC A IPv4 CIDR*	Local
	VPC A IPv6 CIDR	Local
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
	VPC C IPv6 CIDR	pcx-aaaacccc
	VPC D IPv4 CIDR	pcx-aaaadddd
	VPC D IPv6 CIDR	pcx-aaaadddd
	VPC E IPv4 CIDR	pcx-aaaaeeee
	VPC E IPv6 CIDR	pcx-aaaaeeee
	VPC F IPv4 CIDR	pcx-aaaaffff
	VPC F IPv6 CIDR	pcx-aaaaffff
	VPC G IPv4 CIDR	pcx-aaaagggg
	VPC G IPv6 CIDR	pcx-aaaagggg
VPC B	*VPC B IPv4 CIDR*	Local
	VPC B IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-bbbbcccc

Table de routage	Destination	Cible
	VPC C IPv6 CIDR	pcx-bbbbcccc
	VPC D IPv4 CIDR	pcx-bbbbdddd
	VPC D IPv6 CIDR	pcx-bbbbdddd
	VPC E IPv4 CIDR	pcx-bbbbeeee
	VPC E IPv6 CIDR	pcx-bbbbeeee
	VPC F IPv4 CIDR	pcx-bbbbffff
	VPC F IPv6 CIDR	pcx-bbbbffff
	VPC G IPv4 CIDR	pcx-bbbbgggg
	VPC G IPv6 CIDR	pcx-bbbbgggg
VPC C	*VPC C IPv4 CIDR*	Local
	VPC C IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC A IPv6 CIDR	pcx-aaaacccc
	VPC B IPv4 CIDR	pcx-bbbbcccc
	VPC B IPv6 CIDR	pcx-bbbbcccc
	VPC D IPv4 CIDR	pcx-ccccdddd
	VPC D IPv6 CIDR	pcx-ccccdddd
	VPC E IPv4 CIDR	pcx-cccceeee
	VPC E IPv6 CIDR	pcx-cccceeee
	VPC F IPv4 CIDR	pcx-ccccffff

Table de routage	Destination	Cible
	VPC F IPv6 CIDR	pcx-ccccffff
	VPC G IPv4 CIDR	pcx-ccccgggg
	VPC G IPv6 CIDR	pcx-ccccgggg
VPC D	*VPC D IPv4 CIDR*	Local
	VPC D IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaadddd
	VPC A IPv6 CIDR	pcx-aaaadddd
	VPC B IPv4 CIDR	pcx-bbbbdddd
	VPC B IPv6 CIDR	pcx-bbbbdddd
	VPC C IPv4 CIDR	pcx-ccccdddd
	VPC C IPv6 CIDR	pcx-ccccdddd
	VPC E IPv4 CIDR	pcx-ddddeeee
	VPC E IPv6 CIDR	pcx-ddddeeee
	VPC F IPv4 CIDR	pcx-ddddffff
	VPC F IPv6 CIDR	pcx-ddddffff
	VPC G IPv4 CIDR	pcx-ddddgggg
	VPC G IPv6 CIDR	pcx-ddddgggg
VPC E	*VPC E IPv4 CIDR*	Local
	VPC E IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaaeeee

Table de routage	Destination	Cible
	VPC A IPv6 CIDR	pcx-aaaaeeee
	VPC B IPv4 CIDR	pcx-bbbbeeee
	VPC B IPv6 CIDR	pcx-bbbbeeee
	VPC C IPv4 CIDR	pcx-ccccceeee
	VPC C IPv6 CIDR	pcx-ccccceeee
	VPC D IPv4 CIDR	pcx-ddddeeee
	VPC D IPv6 CIDR	pcx-ddddeeee
	VPC F IPv4 CIDR	pcx-eeeeffff
	VPC F IPv6 CIDR	pcx-eeeeffff
	VPC G IPv4 CIDR	pcx-eeeegggg
	VPC G IPv6 CIDR	pcx-eeeegggg
VPC F	*VPC F IPv4 CIDR*	Local
	VPC F IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaaffff
	VPC A IPv6 CIDR	pcx-aaaaffff
	VPC B IPv4 CIDR	pcx-bbbbffff
	VPC B IPv6 CIDR	pcx-bbbbffff
	VPC C IPv4 CIDR	pcx-ccccffff
	VPC C IPv6 CIDR	pcx-ccccffff
	VPC D IPv4 CIDR	pcx-ddddffff

Table de routage	Destination	Cible
	VPC D IPv6 CIDR	pcx-ddddffff
	VPC E IPv4 CIDR	pcx-eeeeffff
	VPC E IPv6 CIDR	pcx-eeeeffff
	VPC G IPv4 CIDR	pcx-ffffgggg
	VPC G IPv6 CIDR	pcx-ffffgggg
VPC G	*VPC G IPv4 CIDR*	Local
	VPC G IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaagggg
	VPC A IPv6 CIDR	pcx-aaaagggg
	VPC B IPv4 CIDR	pcx-bbbbgggg
	VPC B IPv6 CIDR	pcx-bbbbgggg
	VPC C IPv4 CIDR	pcx-ccccgggg
	VPC C IPv6 CIDR	pcx-ccccgggg
	VPC D IPv4 CIDR	pcx-ddddgggg
	VPC D IPv6 CIDR	pcx-ddddgggg
	VPC E IPv4 CIDR	pcx-eeeegggg
	VPC E IPv6 CIDR	pcx-eeeegggg
	VPC F IPv4 CIDR	pcx-ffffgggg
	VPC F IPv6 CIDR	pcx-ffffgggg

Configurations d'appairage de VPC avec des routes spécifiques

Vous pouvez configurer des tables de routage pour une connexion d'appairage de VPC afin de restreindre l'accès à un bloc d'adresse CIDR de sous-réseau, à un bloc d'adresse CIDR spécifique (si le VPC comporte plusieurs blocs d'adresse CIDR) ou à une ressource spécifique dans le VPC appairé. Dans ces exemples, un VPC central est apparenté à au moins deux VPCs dont les blocs CIDR se chevauchent.

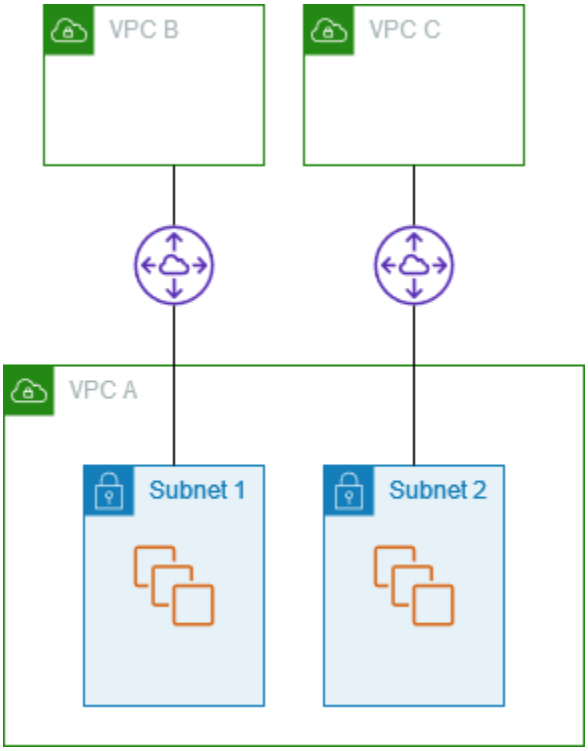
Pour des exemples de scénarios dans lesquels vous pouvez avoir besoin d'une configuration de connexion d'appairage de VPC spécifique, consultez Scénarios de mise en réseau de connexions d'appairage de VPC. Pour en savoir plus sur l'utilisation de connexions d'appairage de VPC, consultez Connexions d'appairage de VPC. Pour en savoir plus sur la mise à jour de vos tables de routage, consultez la page Mise à jour de vos tables de routage pour une connexion d'appairage de VPC.

Configurations

- Deux VPCs qui accèdent à des sous-réseaux spécifiques dans un VPC
- Deux VPCs qui accèdent à des blocs CIDR spécifiques dans un VPC
- Un VPC qui accède à des sous-réseaux spécifiques en deux VPCs
- Instances d'un VPC qui accèdent à des instances spécifiques dans deux VPCs
- Un VPC qui accède à deux en VPCs utilisant les plus longues correspondances de préfixes
- Configurations de plusieurs VPC

Deux VPCs qui accèdent à des sous-réseaux spécifiques dans un VPC

Dans cette configuration, il existe un VPC central avec deux sous-réseaux (VPC A), une connexion d'appairage entre le VPC A et le VPC B (`pcx-aaaabbbb`) et une connexion d'appairage entre le VPC A et le VPC C (`pcx-aaaacccc`). Chaque VPC a besoin d'accéder aux ressources d'un seul des sous-réseaux du VPC A.



La table de routage pour le sous-réseau 1 utilise la connexion d'appairage de VPC `pcx-aaaabbbb` pour accéder à l'ensemble du bloc d'adresse CIDR du VPC B. La table de routage du VPC B utilise `pcx-aaaabbbb` pour accéder au bloc d'adresse CIDR du sous-réseau 1 du VPC A. La table de routage pour le sous-réseau 2 utilise la connexion d'appairage de VPC `pcx-aaaacccc` pour accéder à l'ensemble du bloc d'adresse CIDR du VPC C. La table de routage du VPC C utilise `pcx-aaaacccc` pour accéder au bloc d'adresse CIDR du sous-réseau 2 du VPC A.

Table de routage	Destination	Cible
Sous-réseau 1 (VPC A)	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb
Sous-réseau 2 (VPC A)	*VPC A CIDR*	Local
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local
	Subnet 1 CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local

Table de routage	Destination	Cible
	Subnet 2 CIDR	pcx-aaaacccc

Vous pouvez appliquer cette configuration à plusieurs blocs CIDR. Supposons que le VPC A et le VPC B possèdent à la fois des blocs d'adresse IPv6 CIDR IPv4 et que le sous-réseau 1 possède un bloc d'adresse CIDR associé. IPv6 Vous pouvez permettre au VPC B de communiquer avec le sous-réseau 1 du VPC A via la connexion d'appairage IPv6 du VPC. Pour ce faire, ajoutez une route à la table de routage pour le VPC A avec une destination du bloc IPv6 CIDR pour le VPC B, et une route vers la table de routage pour le VPC B avec une destination du CIDR IPv6 du sous-réseau 1 dans le VPC A.

Table de routage	Destination	Target	Remarques
Sous-réseau 1 du VPC A	*VPC A IPv4 CIDR*	Local	
	VPC A IPv6 CIDR	Local	Route locale ajoutée automatiquement pour la IPv6 communication au sein du VPC.
	VPC B IPv4 CIDR	pcx-aaaabbbb	
	VPC B IPv6 CIDR	pcx-aaaabbbb	Route vers le bloc IPv6 CIDR du VPC B.
Sous-réseau 2 du VPC A	*VPC A IPv4 CIDR*	Local	
	VPC A IPv6 CIDR	Local	Route locale ajoutée automatiquement pour la IPv6 communication au sein du VPC.
	VPC C IPv4 CIDR	pcx-aaaacccc	
VPC B	*VPC B IPv4 CIDR*	Local	

Table de routage	Destination	Target	Remarques
	VPC B IPv6 CIDR	Local	Route locale ajoutée automatiq uement pour la IPv6 communication au sein du VPC.
	Subnet 1 IPv4 CIDR	pcx-aaaabbbb	
	Subnet 1 IPv6 CIDR	pcx-aaaabbbb	Route vers le bloc IPv6 CIDR du VPC A.
VPC C	*VPC C IPv4 CIDR*	Local	
	Subnet 2 IPv4 CIDR	pcx-aaaacccc	

Deux VPCs qui accèdent à des blocs CIDR spécifiques dans un VPC

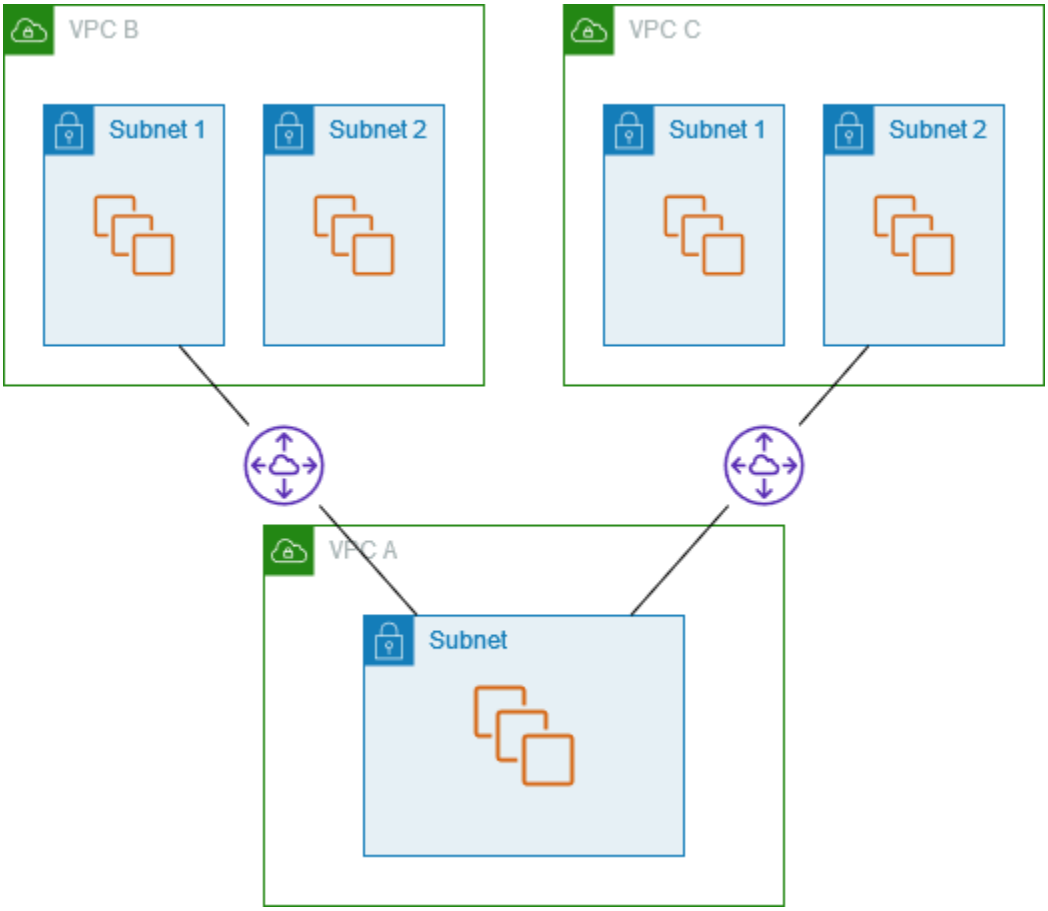
Dans cette configuration, il existe un VPC central (VPC A), une connexion d'appairage entre le VPC A et le VPC B (`pcx-aaaabbbb`) et une connexion d'appairage entre le VPC A et le VPC C (`pcx-aaaacccc`). Le VPC A a un bloc d'adresse CIDR pour chaque connexion d'appairage.

Table de routage	Destination	Cible
VPC A	*VPC A CIDR 1*	Local
	VPC A CIDR 2	Local
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local
	VPC A CIDR 1	pcx-aaaabbbb

Table de routage	Destination	Cible
VPC C	*VPC C CIDR*	Local
	VPC A CIDR 2	pcx-aaaacccc

Un VPC qui accède à des sous-réseaux spécifiques en deux VPCs

Dans cette configuration, il existe un VPC central (VPC A) avec un sous-réseau, une connexion d'appairage entre le VPC A et le VPC B (`pcx-aaaabbbb`) et une connexion d'appairage entre le VPC A et le VPC C (`pcx-aaaacccc`). Le VPC B et le VPC C ont chacun deux sous-réseaux. La connexion d'appairage entre le VPC A et le VPC B utilise uniquement l'un des sous-réseaux du VPC B. La connexion d'appairage entre le VPC A et le VPC C utilise uniquement l'un des sous-réseaux du VPC C.



Utilisez cette configuration lorsque vous disposez d'un VPC central doté d'un ensemble unique de ressources, telles que les services Active Directory, auxquelles les autres utilisateurs VPCs ont

besoin d'accéder. Le VPC central n'a pas besoin d'un accès complet à VPCs celui avec lequel il est apparenté.

La table de routage du VPC A utilise les connexions d'appairage pour accéder uniquement à des sous-réseaux spécifiques du VPC apparenté. VPCs La table de routage du sous-réseau 1 utilise la connexion d'appairage avec le VPC A pour accéder au sous-réseau du VPC A. La table de routage du sous-réseau 2 utilise la connexion d'appairage avec le VPC A pour accéder au sous-réseau du VPC A.

Table de routage	Destination	Cible
VPC A	*VPC A CIDR*	Local
	Subnet 1 CIDR	pcx-aaaabbbb
	Subnet 2 CIDR	pcx-aaaacccc
Sous-réseau 1 (VPC B)	*VPC B CIDR*	Local
	Subnet in VPC A CIDR	pcx-aaaabbbb
Sous-réseau 2 (VPC C)	*VPC C CIDR*	Local
	Subnet in VPC A CIDR	pcx-aaaacccc

Routage pour le trafic de la réponse

Si vous avez un VPC apparenté avec plusieurs blocs CIDR VPCs qui se chevauchent ou correspondent, assurez-vous que vos tables de routage sont configurées de manière à éviter d'envoyer le trafic de réponse de votre VPC vers le mauvais VPC. AWS ne prend pas en charge le transfert de chemin inversé monodiffusion dans les connexions d'appairage VPC qui vérifient l'adresse IP source des paquets et acheminent les paquets de réponse vers la source.

Par exemple, le VPC A est appairé au VPC B et au VPC C. Les VPC B et VPC C ont des blocs d'adresse CIDR identiques, tout comme leurs sous-réseaux. La table de routage pour le sous-réseau 2 dans le VPC B pointe vers la connexion d'appairage de VPC `pcx-aaaabbbb` pour accéder au sous-réseau du VPC A. La table de routage du VPC A est configurée pour envoyer le trafic destiné au CIDR VPC vers la connexion d'appairage `pcx-aaaaccccc`.

Table de routage	Destination	Cible
Sous-réseau 2 (VPC B)	*VPC B CIDR*	Local
	Subnet in VPC A CIDR	pcx-aaaabbbb
VPC A	*VPC A CIDR*	Local
	VPC C CIDR	pcx-aaaacccc

Supposons qu'une instance du sous-réseau 2 du VPC B envoie du trafic au serveur Active Directory du VPC A en utilisant la connexion d'appairage de VPC `pcx-aaaabbbb`. Le VPC A envoie le trafic de réponse au serveur Active Directory. Toutefois, la table de routage du VPC A est configurée pour envoyer tout le trafic de la plage CIDR VPC à la connexion d'appairage de VPC `pcx-aaaacccc`. Si le sous-réseau 2 du VPC C possède une instance avec la même adresse IP que l'instance du sous-réseau 2 du VPC B, elle reçoit le trafic de réponse du VPC A. L'instance du sous-réseau 2 du VPC B ne reçoit pas de réponse à sa demande au VPC A.

Pour éviter ce problème, vous pouvez ajouter une route spécifique à la table de routage de VPC A avec le CIDR du sous-réseau 2 de VPC B comme destination et comme cible `pcx-aaaabbbb`. La nouvelle route est plus spécifique. Par conséquent, le trafic destiné au CIDR du sous-réseau 2 est acheminé vers la connexion d'appairage de VPC `pcx-aaaabbbb`

Sinon, dans l'exemple suivant, la table de routage du VPC A comporte une route pour chaque sous-réseau pour chaque connexion d'appairage de VPC. Le VPC A peut communiquer avec le sous-réseau 2 du VPC B et avec le sous-réseau 1 du VPC C. Ce scénario est utile si vous devez ajouter une autre connexion d'appairage VPC avec un autre sous-réseau situé dans la même plage d'adresses que le VPC B et le VPC C. Vous pouvez simplement ajouter une autre route pour ce sous-réseau spécifique.

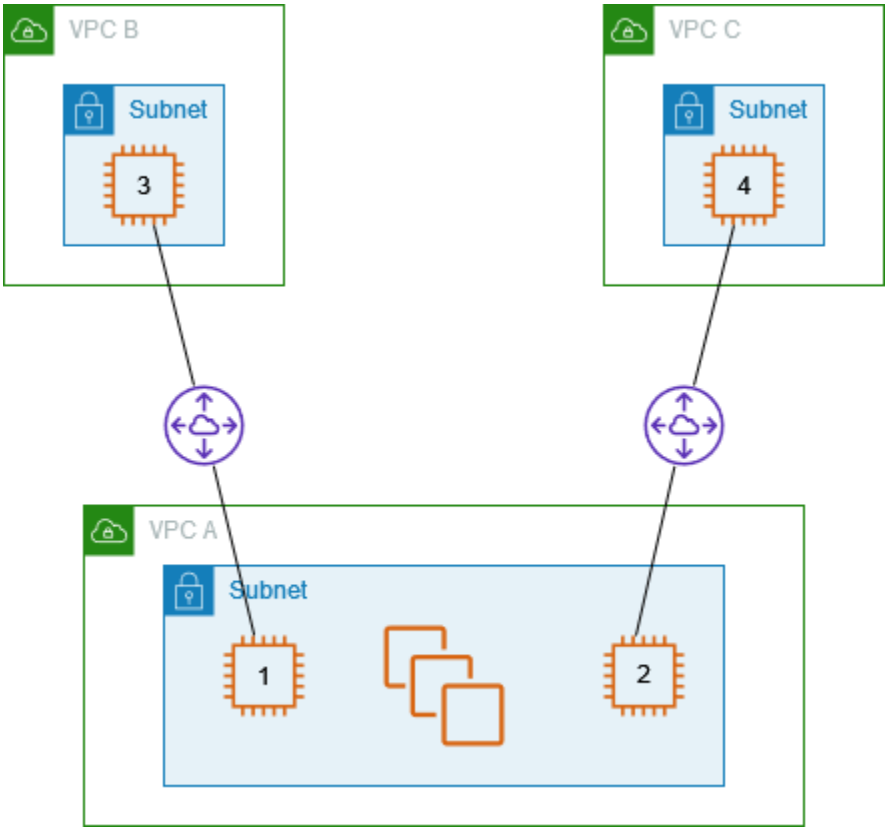
Destination	Target
VPC A CIDR	Local
Subnet 2 CIDR	pcx-aaaabbbb
Subnet 1 CIDR	pcx-aaaacccc

Sinon, en fonction de votre cas d'utilisation, vous pouvez créer une route vers une adresse IP spécifique du VPC B afin de garantir que le trafic sera acheminé vers le serveur approprié (la table de routage utilise la correspondance de préfixe le plus long pour hiérarchiser les routes) :

Destination	Target
VPC A CIDR	Local
Specific IP address in subnet 2	pcx-aaaabbbb
VPC B CIDR	pcx-aaaacccc

Instances d'un VPC qui accèdent à des instances spécifiques dans deux VPCs

Dans cette configuration, il existe un VPC central (VPC A) avec un sous-réseau, une connexion d'appairage entre le VPC A et le VPC B (`pcx-aaaabbbb`) et une connexion d'appairage entre le VPC A et le VPC C (`pcx-aaaacccc`). Le VPC A possède un sous-réseau avec une instance pour chaque connexion d'appairage. Vous pouvez utiliser cette configuration pour limiter le trafic d'appairage à des instances spécifiques.

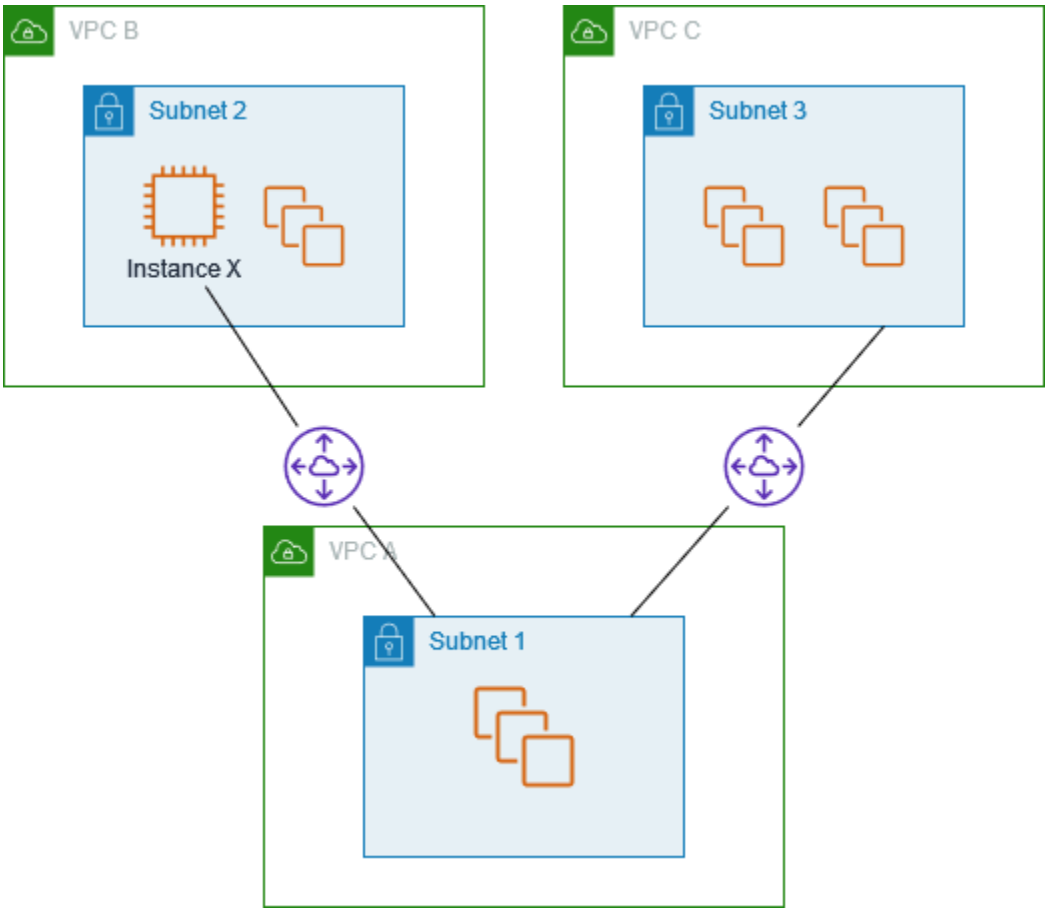


Chaque table de routage de VPC pointe vers la connexion d'appairage de VPC appropriée pour accéder à une seule adresse IP (et donc à une instance spécifique) dans le VPC pair.

Table de routage	Destination	Cible
VPC A	*VPC A CIDR*	Local
	Instance 3 IP address	pcx-aaaabbbb
	Instance 4 IP address	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local
	Instance 1 IP address	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local
	Instance 2 IP address	pcx-aaaacccc

Un VPC qui accède à deux en VPCs utilisant les plus longues correspondances de préfixes

Dans cette configuration, il existe un VPC central (VPC A) avec un sous-réseau, une connexion d'appairage entre le VPC A et le VPC B (`pcx-aaaabbbb`) et une connexion d'appairage entre le VPC A et le VPC C (`pcx-aaaacccc`). Le VPC B et le VPC C ont des blocs d'adresse CIDR identiques. Vous utilisez une connexion d'appairage de VPC `pcx-aaaabbbb` pour acheminer le trafic entre le VPC A et une instance spécifique du VPC B. Le reste du trafic destiné à la plage d'adresses CIDR partagée entre le VPC A et le VPC C est acheminé vers le VPC C via `pcx-aaaacccc`.



Les tables de routage de VPC utilisent la correspondance de préfixe le plus long pour sélectionner la route la plus spécifique sur la connexion d'appairage de VPC désignée. Le reste du trafic est acheminé via la prochaine route adéquate ; dans ce cas, sur la connexion d'appairage de VPC `pcx-aaaacccc`.

Table de routage	Destination	Cible
VPC A	*VPC A CIDR block*	Local
	Instance X IP address	pcx-aaaabbbb
	VPC C CIDR block	pcx-aaaacccc
VPC B	*VPC B CIDR block*	Local
	VPC A CIDR block	pcx-aaaabbbb
VPC C	*VPC C CIDR block*	Local
	VPC A CIDR block	pcx-aaaacccc

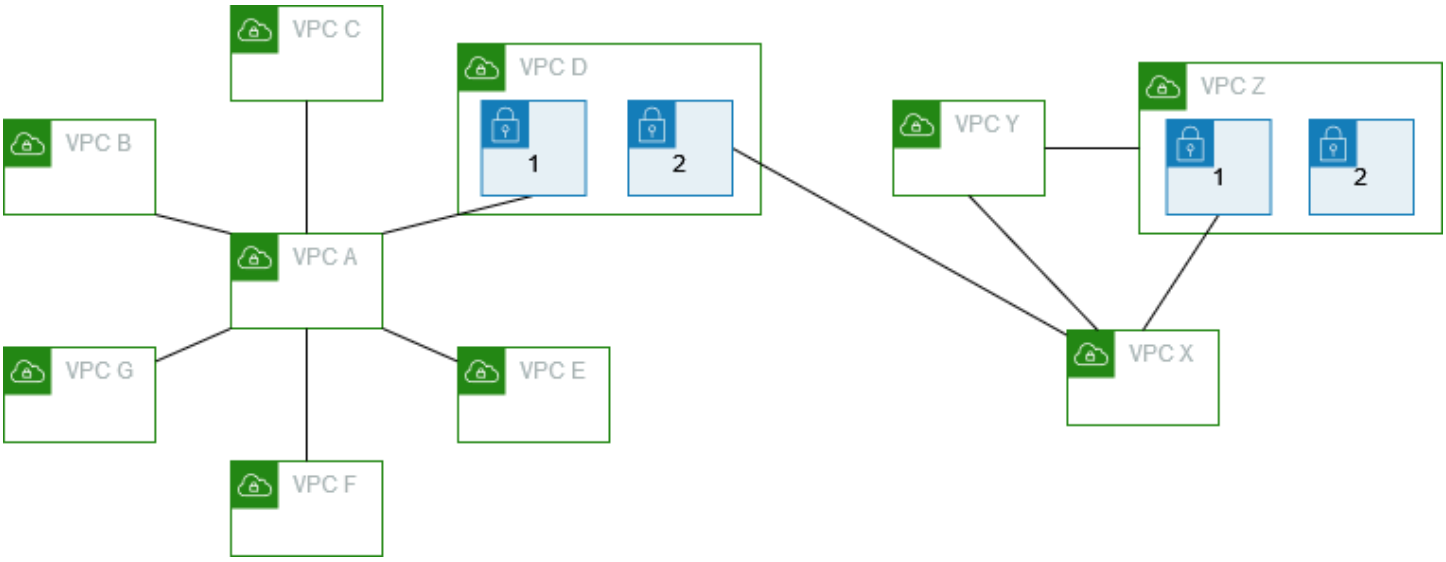
> **Important**
>
> Si une instance autre que l'instance X du VPC B envoie du trafic vers le VPC A, le trafic de réponse peut être acheminé vers le VPC C au lieu du VPC B. Pour plus d'informations, consultez Routage pour le trafic de la réponse.

Configurations de plusieurs VPC

Dans cette configuration, un VPC central (VPC A) est associé à plusieurs VPCs dans une configuration en rayons. Vous en avez également trois VPCs (VPCs X, Y et Z) homologues dans une configuration de maillage complet.

Le VPC D possède également une connexion d'appairage de VPC avec le VPC X (`pcx-ddddxxxx`). Le VPC A et le VPC X ont des blocs d'adresse CIDR se chevauchant. Cela signifie que le trafic de peering entre le VPC A et le VPC D est limité à un sous-réseau spécifique (sous-réseau 1) du VPC D. Cela permet de garantir que si le VPC D reçoit une demande du VPC A ou du VPC X, il envoie le trafic de réponse au VPC approprié. AWS ne prend pas en charge le transfert de chemin inversé monodiffusion dans les connexions d'appairage VPC qui vérifient l'adresse IP source des paquets et acheminent les paquets de réponse vers la source. Pour de plus amples informations, veuillez consulter Routage pour le trafic de la réponse.

De même, le VPC D et le VPC Z ont des blocs d'adresse CIDR se chevauchant. Le trafic d'appairage entre le VPC D et le VPC X est limité au sous-réseau 2 dans le VPC D, et le trafic d'appairage entre le VPC X et le VPC Z est limité au sous-réseau 1 dans le VPC Z. Il s'agit d'assurer que le VPC X renvoie le trafic de réponse au bon VPC s'il reçoit du trafic d'appairage du VPC D ou du VPC Z.



Les tables de routage pour VPCs B, C, E, F et G pointent vers les connexions d'appairage pertinentes pour accéder au bloc CIDR complet pour le VPC A, et la table de routage du VPC A pointe vers les connexions d'appairage pertinentes pour VPCs B, C, E, F et G pour accéder à leurs blocs CIDR complets. Pour la connexion d'appairage `pcx-aaaadddd`, la table de routage du VPC A achemine uniquement le trafic vers le sous-réseau 1 du VPC D, et la table de routage du sous-réseau 1 du VPC D pointe vers l'ensemble du bloc d'adresse CIDR du VPC A.

La table de routage du VPC Y pointe vers les connexions d'appairage appropriées pour accéder à l'ensemble des blocs d'adresse CIDR du VPC X et du VPC Z, et la table de routage du VPC Z pointe vers la connexion d'appairage appropriée pour accéder à l'ensemble du bloc d'adresse CIDR du VPC Y. La table de routage du sous-réseau 1 dans le VPC Z pointe vers la connexion d'appairage appropriée pour accéder à l'ensemble du bloc d'adresse CIDR du VPC Y. La table de routage du VPC X pointe vers la connexion d'appairage appropriée pour accéder au sous-réseau 2 dans le VPC D et au sous-réseau 1 dans le VPC Z.

Table de routage	Destination	Cible
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb

Table de routage	Destination	Cible
	VPC C CIDR	pcx-aaaacccc
	Subnet 1 CIDR in VPC D	pcx-aaaadddd
	VPC E CIDR	pcx-aaaaeeee
	VPC F CIDR	pcx-aaaaffff
	VPC G CIDR	pcx-aaaagggg
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-aaaacccc
Sous-réseau 1 du VPC D	*VPC D CIDR*	Local
	VPC A CIDR	pcx-aaaadddd
Sous-réseau 2 du VPC D	*VPC D CIDR*	Local
	VPC X CIDR	pcx-ddddxxxx
VPC E	*VPC E CIDR*	Local
	VPC A CIDR	pcx-aaaaeeee
VPC F	*VPC F CIDR*	Local
	VPC A CIDR	pcx-aaaaaffff
VPC G	*VPC G CIDR*	Local
	VPC A CIDR	pcx-aaaagggg
VPC X	*VPC X CIDR*	Local

Table de routage	Destination	Cible
	Subnet 2 CIDR in VPC D	pcx-ddddxxxx
	VPC Y CIDR	pcx-xxxxyyyy
	Subnet 1 CIDR in VPC Z	pcx-xxxxzzzz
VPC Y	*VPC Y CIDR*	Local
	VPC X CIDR	pcx-xxxxyyyy
	VPC Z CIDR	pcx-yyyyzzzz
VPC Z	*VPC Z CIDR*	Local
	VPC Y CIDR	pcx-yyyyzzzz
	VPC X CIDR	pcx-xxxxzzzz

Scénarios de mise en réseau de connexions d’appairage de VPC

Il existe un certain nombre de raisons pour lesquelles vous pourriez avoir besoin de configurer une connexion d'appairage VPC entre votre VPCs VPC ou entre un VPC dont vous êtes le propriétaire et un VPC d'un autre compte. AWS Les scénarios suivants peuvent vous aider à identifier la configuration la mieux adaptée à vos besoins en matière de mise en réseau.

Scénarios

- En appairer deux ou plus VPCs pour fournir un accès complet aux ressources
- Appairage à un VPC pour accéder à des ressources centralisées

En appairer deux ou plus VPCs pour fournir un accès complet aux ressources

Dans ce scénario, vous souhaitez associer deux ou plusieurs VPCs ressources pour permettre le partage complet des ressources entre tous VPCs. Voici quelques exemples :

- Votre entreprise dispose d'un VPC pour son service financier et d'un autre pour le service comptabilité. Le service financier a besoin d'un accès à toutes les ressources du service comptabilité, et vice versa.
- Votre entreprise compte plusieurs services informatiques, qui possèdent chacun leur propre VPC. Certains se VPCs trouvent dans le même AWS compte, tandis que d'autres se trouvent dans un AWS compte différent. Vous devez tous les comparer VPCs pour permettre aux services informatiques d'avoir un accès complet aux ressources des uns et des autres.

Pour plus d'informations sur la façon de configurer la connexion d'appairage de VPC et les tables de routage pour ce scénario, consultez la documentation suivante :

- Deux se sont VPCs regardés ensemble
- Trois ont VPCs regardé ensemble
- Plusieurs VPCs comparés ensemble

Pour en savoir plus sur la création et l'utilisation de connexions d'appairage de VPC dans la console Amazon VPC, consultez Connexions d’appairage de VPC.

Appairage à un VPC pour accéder à des ressources centralisées

Dans ce scénario, vous disposez d'un VPC central qui contient des ressources que vous souhaitez partager avec d'autres personnes. VPCs Votre VPC central peut avoir besoin d'un accès total ou partiel à l'homologue VPCs, et de même, le pair VPCs peut avoir besoin d'un accès complet ou partiel au VPC central. Voici quelques exemples :

- Le service informatique de votre entreprise possède un VPC pour le partage des fichiers. Vous souhaitez établir un pair avec ce VPC central, mais vous ne voulez pas que l'autre VPCs envoie du trafic entre eux. VPCs
- Votre entreprise possède un VPC que vous souhaitez partager avec vos clients. Chaque client peut créer une connexion d'appairage VPC avec votre VPC, mais vos clients ne peuvent pas acheminer le trafic vers d'autres clients VPCs qui sont associés au vôtre, et ils ne connaissent pas non plus les itinéraires des autres clients.
- Vous disposez d'un VPC central, utilisé pour les services Active Directory. Les instances spécifiques des homologues VPCs envoient des demandes aux serveurs Active Directory et nécessitent un accès complet au VPC central. Le VPC central n'a pas besoin d'un accès complet à l'homologue VPCs ; il doit uniquement acheminer le trafic de réponse vers les instances spécifiques.

Pour en savoir plus sur la création et l'utilisation de connexions d'appairage de VPC dans la console Amazon VPC, consultez Connexions d’appairage de VPC.

IAM (Identity and Access Management) pour appairage de VPC

Par défaut, les utilisateurs d' ne peuvent pas créer ou modifier de connexions d'appairage de VPC. Pour accorder l'accès aux ressources d'appairage de VPC, attachez une politique IAM à une identité IAM, telle qu'un rôle.

Exemples

- Exemple : créer une connexion d'appairage de VPC
- Exemple : accepter une connexion d'appairage de VPC
- Exemple : supprimer une connexion d'appairage de VPC
- Exemple : utiliser dans un compte spécifique
- Exemple : gérer les connexions d'appairage de VPC à l'aide de la console

Pour obtenir la liste des actions Amazon VPC, ainsi que les ressources prises en charge et les clés de conditions pour chaque action, consultez la section Actions, ressources et clés de condition pour Amazon EC2 dans la référence d'autorisation de service.

Exemple : créer une connexion d'appairage de VPC

La politique suivante autorise les utilisateurs à créer des demandes de connexion d'appairage VPC à l'aide de celles VPCs étiquetées avec. `Purpose=Peering` La première instruction applique une clé de condition (`ec2:ResourceTag`) à la ressource du VPC. Notez que la ressource du VPC pour l'action `CreateVpcPeeringConnection` est toujours le VPC demandeur.

La deuxième instruction autorise les utilisateurs à créer les ressources de connexion d'appairage de VPC et utilise donc le caractère générique * au lieu d'un ID de ressource spécifique.

JSON

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
```

```
      "Resource": "arn:aws:ec2:region:account-id:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc-peering-connection/*"
    }
  ]
}
```

La politique suivante accorde aux utilisateurs du AWS compte spécifié l'autorisation de créer des connexions d'appairage VPC en utilisant n'importe quel VPC de la région spécifiée, mais uniquement si le VPC qui accepte la connexion d'appairage est un VPC spécifique dans un compte spécifique.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:region:account-id-2:vpc/vpc-id"
        }
      }
    }
  ]
}
```

Exemple : accepter une connexion d'appairage de VPC

La politique suivante autorise les utilisateurs à accepter les demandes de connexion d'appairage VPC provenant d'un compte spécifique. AWS Elle permet d'empêcher les utilisateurs d'accepter des demandes de connexion d'appairage de VPC depuis des comptes inconnus. L'instruction utilise la clé de condition `ec2:RequesterVpc` pour la faire appliquer.

JSON

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:RequesterVpc": "arn:aws:ec2:region:account-id-2:vpc/*"
        }
      }
    }
  ]
}
```

La politique suivante octroie aux utilisateurs l'autorisation accepter des demandes d'appairage de VPC si le VPC a l'identification `Purpose=Peering`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect": "Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc/*",
      "Condition": {
        "StringEquals": {
```

```
            "ec2:ResourceTag/Purpose": "Peering"
          }
        }
      }
    ]
}
```

Exemple : supprimer une connexion d'appairage de VPC

La stratégie suivante octroie aux utilisateurs l'autorisation du compte spécifié de supprimer toute connexion d'appairage de VPC, sauf celles qui utilisent le VPC spécifié, qui est dans le même compte. La stratégie spécifie les deux clés de condition `ec2:AccepterVpc` et `ec2:RequesterVpc`, puisque le VPC a peut-être été le VPC demandeur ou le VPC pair dans la demande de connexion d'appairage de VPC d'origine.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": "ec2:DeleteVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc-peering-connection/*",
      "Condition": {
        "ArnNotEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:region:account-id:vpc/vpc-id",
          "ec2:RequesterVpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
        }
      }
    }
  ]
}
```

Exemple : utiliser dans un compte spécifique

La stratégie suivante octroie aux utilisateurs l'autorisation d'utiliser des connexions d'appairage de VPC dans un compte spécifique. Les utilisateurs peuvent consulter, créer, accepter, rejeter et

supprimer des connexions d'appairage VPC, à condition qu'elles soient toutes associées au même compte. AWS

La première instruction octroie aux utilisateurs l'autorisation de voir toutes les connexions d'appairage de VPC. L'élément `Resource` exige un caractère générique * dans ce cas, puisque cette action d'API (`DescribeVpcPeeringConnections`) ne prend pas en charge de permissions au niveau des ressources pour le moment.

La deuxième déclaration autorise les utilisateurs à créer des connexions d'appairage VPC et à accéder VPCs à toutes les connexions du compte spécifié pour ce faire.

La troisième instruction utilise un caractère générique * dans le cadre de l'élément `Action` pour octroyer l'autorisation de toutes les actions de connexion d'appairage de VPC. Les clés de condition garantissent que les actions ne peuvent être effectuées que sur les connexions d'appairage VPC VPCs associées au compte. Par exemple, un utilisateur ne peut pas supprimer une connexion d'appairage de VPC si le VPC demandeur ou accepteur est dans un compte différent. Un utilisateur ne peut pas créer de connexion d'appairage de VPC avec un VPC dans un compte différent.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeVpcPeeringConnections",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action":
 ["ec2:CreateVpcPeeringConnection","ec2:AcceptVpcPeeringConnection"],
      "Resource": "arn:aws:ec2:*:account-id:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:*VpcPeeringConnection",
      "Resource": "arn:aws:ec2:*:account-id:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:*:account-id:vpc/*",
```

```
            "ec2:RequesterVpc": "arn:aws:ec2:*:account-id:vpc/*"
          }
        }
      }
    ]
}
```

Exemple : gérer les connexions d'appairage de VPC à l'aide de la console

Pour voir les connexions d'appairage de VPC dans la console Amazon VPC, les utilisateurs doivent être autorisés à utiliser l'action `ec2:DescribeVpcPeeringConnections`. Pour utiliser la page Créer une connexion d'appairage, les utilisateurs doivent être autorisés à utiliser l'action `ec2:DescribeVpcs`. Cela leur permet de consulter et de sélectionner un VPC. Vous pouvez appliquer des permissions au niveau des ressources à toutes les actions `ec2:*PeeringConnection`, sauf `ec2:DescribeVpcPeeringConnections`.

La stratégie suivante octroie aux utilisateurs l'autorisation de visualiser des connexions d'appairage de VPC et d'utiliser la boîte de dialogue Create VPC Peering Connection (Créer une connexion d'appairage de VPC) pour créer une connexion d'appairage en utilisant uniquement un VPC demandeur spécifique. Si les utilisateurs essayent de créer une connexion d'appairage de VPC avec un VPC demandeur différent, la demande échoue.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeVpcPeeringConnections", "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": [
```

```
        "arn:aws:ec2:*:*:vpc/vpc-id",
        "arn:aws:ec2:*:*:vpc-peering-connection/*"
      ]
    }
  ]
}
```

Quotas d’une connexion d’appairage de VPC pour un compte

Le peering VPC vous permet d'en connecter deux. VPCs Cela permet aux ressources d’un VPC de communiquer avec les ressources de l’autre VPC comme si elles se trouvaient sur le même réseau. Le peering VPC est une fonctionnalité utile pour vous connecter VPCs, qu'ils se trouvent dans la même AWS région ou dans des régions différentes. Cette section décrit les quotas que vous devez connaître lorsque vous travaillez avec des connexions d’appairage de VPC.

Le tableau suivant répertorie les quotas, anciennement appelés limites, pour les connexions de peering VPC pour votre compte. AWS Sauf indication contraire, vous pouvez demander une augmentation pour ces quotas.

Si vous constatez que vos exigences actuelles en matière de connexion d’appairage de VPC dépassent les quotas par défaut, nous vous encourageons à soumettre une demande d’augmentation de limite de service. Nous examinerons votre cas d’utilisation et travaillerons avec vous pour ajuster les quotas en conséquence, afin de garantir que votre environnement VPC réponde aux besoins croissants de votre entreprise.

Nom	Par défaut	Ajustable
Connexions d'appairage de VPC actives par VPC	50	Oui (jusqu'à 125)
Demandes de connexion d'appairage de VPC en attente	25	Oui
Date d'expiration d'une demande de connexion d'appairage de VPC non acceptée	1 semaine (168 heures)	Non

Pour plus d'informations sur les règles d'utilisation des connexions d'appairage de VPC, consultez Limitations des appairages de VPC. Pour plus d’informations sur les quotas pour Amazon VPC, voir Quotas Amazon VPC dans le Guide de l’utilisateur Amazon VPC.

Historique de document du Guide d'appairage Amazon VPC

Le tableau suivant décrit les versions de documentation du Guide d'appairage Amazon VPC.

Modification	Description	Date
Identifier à la création	Vous pouvez ajouter des balises lorsque vous créez une connexion d'appairage VPC et une table de routage.	20 juillet 2020
Appairage inter-région	La résolution des noms d'hôte DNS est compatible avec les connexions d'appairage VPC inter-région de la région Asie-Pacifique (Hong Kong).	26 août 2019
Appairage inter-région	Vous pouvez créer une connexion d'appairage VPC entre différentes VPCs régions. AWS	29 novembre 2017
Prise en charge de la résolution DNS pour l'appairage de VPC	Vous pouvez activer un VPC local pour résoudre les noms d'hôte DNS publics en adresses IP privées lorsqu'il est interrogé à partir d'instances du VPC pair.	28 juillet 2016
Règles du groupe de sécurité obsolètes	Vous pouvez déterminer si votre groupe de sécurité est référencé dans les règles d'un groupe de sécurité d'un VPC pair, de même qu'identifier les règles du groupe de sécurité obsolètes.	12 mai 2016

Utilisation ClassicLink via une connexion d'appairage VPC	Vous pouvez modifier votre connexion d'appairage VPC pour permettre aux instances locales liées EC2 -Classic de communiquer avec les instances d'un VPC homologue, ou vice versa.	26 avril 2016
Appairage de VPC	Vous pouvez créer une connexion d'appairage VPC entre deux instances VPCs, ce qui permet aux instances de l'un ou l'autre VPC de communiquer entre elles à l'aide d'adresses IP privées	24 mars 2014

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.