Appairage de VPC

Amazon Virtual Private Cloud

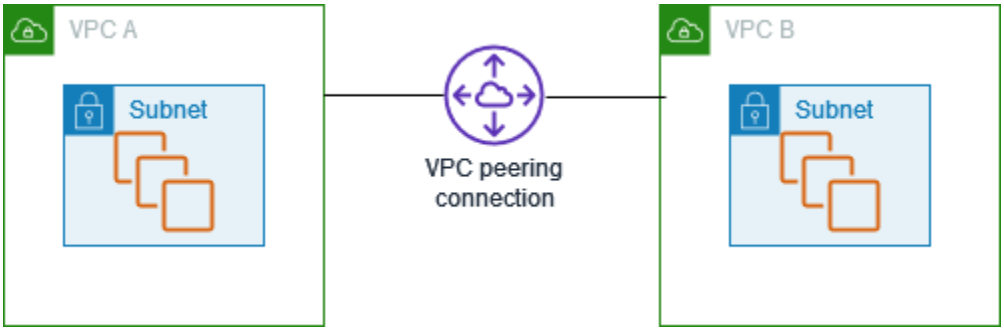
Amazon Virtual Private Cloud: Appairage de VPC

Table of Contents

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 instances Amazon EC2, dans votre VPC.

Une connexion d'appairage de VPC est une connexion de mise en réseau entre deux VPC qui permet d'acheminer le trafic entre ces derniers à l'aide d'adresses IPv4 privées ou d'adresses 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 de VPC entre vos propres VPC, ou avec un VPC situé dans un autre compte AWS . Les VPC se trouvent dans différentes régions (concept aussi appelé « connexion d'appairage de VPC inter-région »).



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 comparer les VPC de ces comptes pour créer un réseau de partage de fichiers. Vous pouvez également utiliser une connexion d'appairage de VPC pour permettre à d'autres VPC d'accéder aux ressources dont vous disposez dans l'un de vos VPC.

Lorsque vous établissez des relations d'appairage entre des VPC de différentes AWS régions, les ressources des VPC (par exemple, les instances EC2 et les fonctions Lambda) des différentes AWS 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 d'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 DDoS. Le peering VPC interrégional

constitue un moyen simple et rentable de partager des ressources entre les régions ou de répliquer des données à des fins de 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. Tout transfert de données via une connexion d'appairage VPC qui reste dans une zone de disponibilité (même s'il s'agit d'un transfert entre différents comptes) est gratuit. Des frais s'appliquent aux transferts de données via des connexions d'appairage de VPC entre zones de disponibilité ou régions différentes. Pour en savoir plus, consultez Tarification Amazon EC2.

Principes de base de l'appairage de VPC

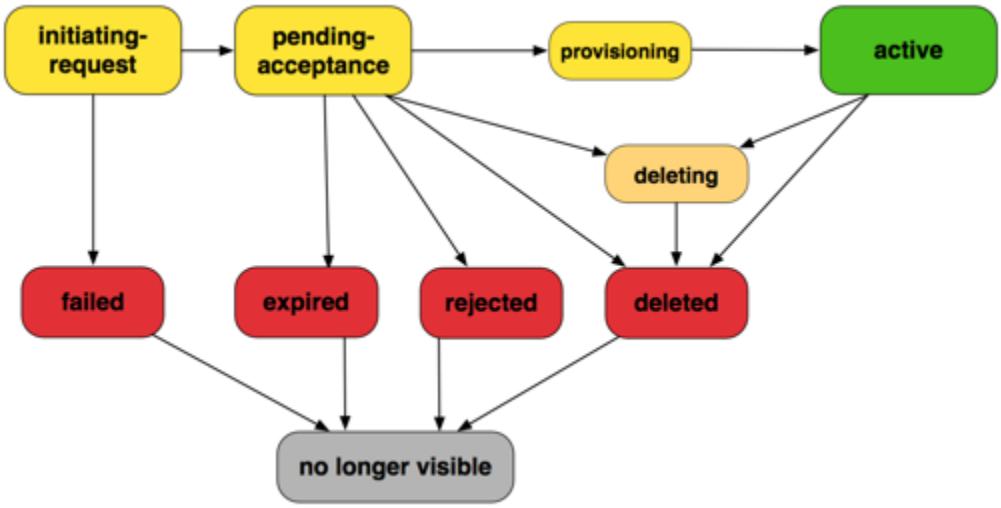
Pour établir une connexion d'appairage de VPC, vous effectuez les opérations suivantes :

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 de VPC pour activer cette connexion.
3. Pour activer le flux du trafic entre les VPC à l'aide d'adresses IP privées, le propriétaire de chaque VPC de la connexion d'appairage de VPC doit manuellement ajouter un itinéraire vers une ou plusieurs des tables de routage de son VPC qui pointe vers la plage d'adresses IP de l'autre VPC (le VPC pair).
4. Si nécessaire, mettez à jour les règles du groupe de sécurité associées à votre instance EC2 pour garantir que le trafic à destination et en provenance du VPC homologue n'est pas restreint. Si les deux VPC se trouvent dans la même région, vous pouvez faire référence à un groupe de sécurité issu du VPC homologue comme 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 instances EC2 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 instances EC2 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 résolu en adresse IP privée de l'instance EC2.

Pour plus d’informations, consultez Utilisation de 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 de VPC est active et le trafic peut circuler entre les VPC (sous réserve que vos groupes de sécurité et tables de routage permettent le flux du trafic). À ce stade, les deux propriétaires de VPC peuvent supprimer la connexion d'appairage de VPC, mais ils ne peuvent pas la refuser.

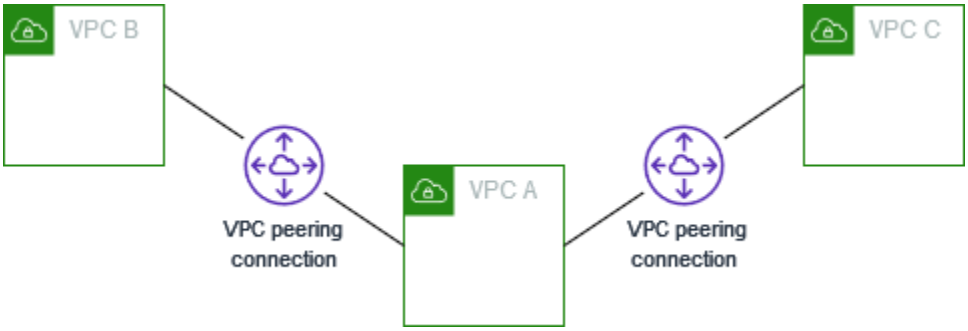
> **Note**
>
> Si un événement dans une région dans laquelle réside un VPC empêche le flux de trafic, l'état de la connexion d'appairage du VPC est conservé. `Active`

- 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 VPC a été créée dans le même AWS compte, la demande supprimée reste visible pendant 2 heures.

Connexions d'appairage de plusieurs VPC

Une connexion d'appairage de VPC est une relation un-à-un entre deux VPC. 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 les VPC avec lesquels votre VPC n'est pas directement appairé.

Le schéma suivant illustre un VPC appairé à deux VPC distincts. 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 de plus amples informations, veuillez consulter Exemples dans Passerelles de transit Amazon VPC.

Connexions

- Il existe un quota pour le nombre de connexions d'appairage de VPC actives et en attente par VPC. Pour plus d'informations, consultez Quotas.
- Vous ne pouvez pas avoir simultanément plusieurs connexions d'appairage de VPC entre deux VPC.
- 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 d'adresse CIDR IPv4 d'un VPC dans une connexion d'appairage de VPC se trouve en dehors des plages d'adresses IPv4 privées spécifiées par 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 plus d'informations, consultez Activation de la résolution DNS pour une connexion d'appairage de VPC.
- Vous pouvez permettre aux ressources de chaque côté d'une connexion d'appairage de VPC de communiquer sur IPv6. Vous devez associer un bloc d'adresse CIDR IPv6 à chaque VPC, activer les instances dans les VPC pour les communications IPv6 et acheminer le trafic IPv6 destiné au VPC pair vers la connexion d'appairage de VPC.
- La recherche par chemin inverse Unicast dans les connexions d'appairage de VPC n'est pas prise en charge. Pour plus d'informations, consultez Routage pour le trafic de la réponse.

Blocs d'adresse CIDR se chevauchant

- Vous ne pouvez pas créer de connexion d'appairage de VPC entre des VPC dont les blocs d'adresse CIDR IPv4 ou IPv6 sont identiques ou se chevauchent.
- Si vous avez plusieurs blocs d'adresse CIDR IPv4, vous ne pouvez pas créer de connexion d'appairage de VPC si certains blocs d'adresse CIDR se chevauchent, même si vous avez

l'intention d'utiliser uniquement les blocs 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 plus d'informations, consultez Appairage de trois VPC.

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

- La valeur Unité de transmission maximale (MTU) dans une connexion d'appairage de VPC est de 1 500 octets entre régions. Les trames jumbo (MTU jusqu'à 9 001 octets) ne sont pas prises en charge pour les connexions d'appairage de VPC entre régions. Elles sont toutefois prises en charge pour les connexions d'appairage de VPC dans la même région. 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 le support de résolution DNS pour la connexion d'appairage de VPC pour résoudre les noms d'hôtes DNS privés du VPC appairé en adresses IP privées, même si le bloc CIDR IPv4 du VPC se trouve dans les plages d'adresses IPv4 privées spécifiées par RFC 1918.

VPC et sous-réseaux partagés

- 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.

Utilisation de connexions d'appairage de VPC

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

Tâches

- Créer une connexion d'appairage de VPC
- Accepter une connexion d'appairage de VPC
- Rejet d'une connexion d'appairage de VPC
- Affichage de vos connexions 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
- Modification des options de 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. Vous pouvez demander une connexion d'appairage de VPC avec un autre VPC dans votre compte, ou avec un VPC situé dans un autre compte AWS. Pour une connexion d'appairage VPC inter-région où les VPC se trouvent dans différentes régions, la demande doit être effectuée à partir de la région du VPC demandeur.

Pour activer la demande, le propriétaire du VPC accepteur doit accepter la demande. Pour une connexion d'appairage VPC inter-région, la demande doit être acceptée dans la région du VPC qui accepte. Pour de plus amples informations, veuillez consulter the section called “Accept”. Pour plus d'informations sur l'état de la connexion d'appairage `Pending acceptance`, consultez Cycle de vie d'une connexion d'appairage de VPC.

Tâches

- Prérequis
- Créer avec des VPC du même compte et de la même région
- Créer avec des VPC dans le même compte et dans des régions différentes

- Créez avec des VPC dans des comptes différents et dans la même région
- Créez avec des VPC dans des comptes différents et dans des régions différentes
- Créer une connexion d'appairage de VPC à l'aide de la ligne de commande

Prérequis

- Consultez les limites et règles des connexions d'appairage de VPC.
- Assurez-vous qu'aucun bloc d'adresse CIDR IPv4 de vos VPC ne se chevauche. Si c'est le cas, le statut de la connexion d'appairage de VPC devient immédiatement `failed`. Cette limitation s'applique même si les VPC disposent de blocs d'adresses CIDR IPv6 uniques.

Créer avec des VPC du même compte et de la même région

Pour créer une connexion d'appairage de VPC avec des VPC du même compte et de la même région

1. Ouvrez la console Amazon VPC sur 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. Configurez les informations suivantes et choisissez Créer une connexion d'appairage une fois que vous avez terminé :
   - Nom : si vous le souhaitez, vous pouvez nommer votre connexion d'appairage de VPC.
   - ID de VPC (Demandeur) : sélectionnez le VPC dans votre compte avec lequel vous souhaitez créer la connexion d'appairage de VPC.
   - Pour Sélectionner un autre VPC auquel s'appairer : choisissez Mon compte et sélectionnez un autre de vos VPC.
   - (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
5. Choisissez Actions, Accepter la demande.
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.

Créer avec des VPC dans le même compte et dans des régions différentes

Pour créer une connexion d'appairage de VPC avec des VPC du même compte et dans des régions différentes

1. Ouvrez la console Amazon VPC sur 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. Configurez les informations suivantes et choisissez Créer une connexion d'appairage une fois que vous avez terminé :
   - Nom : si vous le souhaitez, vous pouvez nommer votre connexion d'appairage de VPC. Une identification est alors créée avec la clé `Name` et la valeur que vous spécifiez.
   - ID de VPC (Demandeur) : sélectionnez le VPC demandeur de votre compte pour lequel vous demandez la connexion d'appairage de VPC.
   - Compte : choisissez Mon compte.
   - Région : choisissez Une autre région et sélectionnez la région correspondant au VPC accepteur.
   - ID de VPC (Accepteur) : sélectionnez le VPC accepteur.
5. Dans le sélecteur de région, sélectionnez la région du VPC accepteur.
6. Dans le volet de navigation, choisissez Peering connections (Connexions d'appairage). Sélectionnez la connexion d'appairage de VPC que vous avez créée, puis choisissez Actions, Accepter la demande.
7. Lorsque vous êtes invité à confirmer l'opération, choisissez Accepter la demande.
8. 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.

Créez avec des VPC dans des comptes différents et dans la même région

Pour demander une connexion d'appairage de VPC à un VPC dans des comptes différents et dans la même région

1. Ouvrez la console Amazon VPC sur 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. Configurez les informations comme suit et choisissez Créer une connexion d'appairage une fois que vous avez terminé :

   - Nom : si vous le souhaitez, vous pouvez nommer votre connexion d'appairage de VPC. Cette étape crée une balise avec une clé de `Name` et une valeur que vous spécifiez. Cette balise est uniquement visible par vous ; le propriétaire du VPC pair peut créer ses propres balises pour la connexion d'appairage de VPC.
   - ID de VPC (Demandeur) : sélectionnez le VPC dans votre compte avec lequel vous souhaitez créer la connexion d'appairage de VPC.
   - Compte : choisissez Un autre compte.
   - ID de compte : entrez l'ID du Compte AWS propriétaire du VPC accepteur.
   - ID de VPC (Accepteur) : entrez l'ID du VPC de votre compte avec lequel vous souhaitez créer la connexion d'appairage de VPC.

Créez avec des VPC dans des comptes différents et dans des régions différentes

Pour demander une connexion d'appairage de VPC à des VPC dans des comptes différents et des régions différentes

1. Ouvrez la console Amazon VPC sur 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. Configurez les informations comme suit et choisissez Créer une connexion d'appairage une fois que vous avez terminé :

   - Nom : si vous le souhaitez, vous pouvez nommer votre connexion d'appairage de VPC. Cette étape crée une balise avec une clé de `Name` et une valeur que vous spécifiez. Cette balise est uniquement visible par vous ; le propriétaire du VPC pair peut créer ses propres balises pour la connexion d'appairage de VPC.
   - ID de VPC (Demandeur) : sélectionnez le VPC dans votre compte avec lequel vous souhaitez créer la connexion d'appairage de VPC.
   - Compte : choisissez Un autre compte.

- ID de compte : entrez l'ID du Compte AWS propriétaire du VPC accepteur.
- Région : choisissez Une autre région et sélectionnez la région dans laquelle le VPC accepteur réside.
- ID de VPC (Accepteur) : entrez l'ID du VPC de votre compte avec lequel vous souhaitez créer la connexion d'appairage de VPC.

Créer une connexion d'appairage de VPC 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 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 de VPC que vous avez envoyée dans un autre compte AWS. Si vous créez une connexion d'appairage de VPC dans le même compte AWS, vous devez créer et accepter la demande vous-même.

Si les VPC se trouvent dans des régions différentes, la demande doit être acceptée dans la région du VPC accepteur.

> **Important**
>
> N'acceptez pas de connexions d'appairage de VPC de comptes AWS que vous ne connaissez pas. 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 sans problème rejeter les demandes de connexion d'appairage de VPC indésirables sans courir le risque que le demandeur puisse accéder aux informations sur votre compte AWS ou votre VPC. Pour plus d'informations, consultez Rejet d'une connexion d'appairage de VPC. Vous pouvez également ignorer la demande et la laisser expirer ; par défaut, les demandes expirent après 7 jours.

Après avoir accepté la connexion d'appairage de VPC, vous devez ajouter une entrée dans les tables de routage pour activer le trafic entre les VPC appairés. Pour de plus amples informations, veuillez consulter Mise à jour de vos tables de routage pour une connexion d'appairage de VPC.

Accepter une connexion d'appairage de VPC

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. 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.

   > **Tip**
   >
   > Si vous ne pouvez pas voir la connexion d'appairage de VPC en attente, vérifiez la région. Une demande d'appairage inter-région doit être acceptée dans la région du VPC accepteur.

5. Lorsque vous êtes invité à confirmer l'opération, choisissez Accepter la demande.
6. 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 de VPC à l'aide de la ligne de commande ou d'une API

- accept-vpc-peering-connection (AWS CLI)
- Approve-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)
- AcceptVpcPeeringConnection (API de requête Amazon EC2)

Rejet d'une connexion d'appairage de VPC

Vous pouvez rejeter toute demande de connexion d'appairage de VPC que vous avez reçue en état `pending-acceptance`. Vous devriez uniquement accepter les connexions d'appairage de VPC de Comptes AWS que vous connaissez et auxquels 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.

Rejeter 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, puis choisissez Actions, Rejeter la demande.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Rejeter la demande.

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

- reject-vpc-peering-connection (AWS CLI)
- Deny-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)
- RejectVpcPeeringConnection (API de requête Amazon EC2)

Affichage de vos connexions d'appairage de VPC

Vous pouvez voir toutes vos connexions d'appairage de VPC dans la console Amazon VPC. Par défaut, la console affiche toutes les connexions d'appairage de VPC dans différents états, y compris celles qui peuvent avoir été supprimées ou rejetées récemment. Pour plus d'informations sur le cycle de vie d'une connexion d'appairage de VPC, consultez Cycle de vie d'une connexion d'appairage de VPC.

Voir vos connexions 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. Toutes vos connexions d'appairage de VPC sont répertoriées. Utilisez la barre de recherche de filtres pour affiner vos résultats.

Pour décrire une connexion d'appairage de VPC à l'aide de la ligne de commande ou d'une API

- describe-vpc-peering-connections (AWS CLI)
- Get-EC2VpcPeeringConnections (AWS Tools for Windows PowerShell)
- DescribeVpcPeeringConnections (API de requête Amazon EC2)

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

Pour permettre le trafic IPv4 privé entre des instances dans des VPC appairés, vous devez ajouter un acheminement aux 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 des tables de routage qui permettent la communication entre les instances de deux VPC pairs, VPC A et VPC B. Chaque table comporte un acheminement local et un acheminement qui envoie le trafic du VPC pair à la connexion d'appairage de VPC.

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

De même, si les VPC de la connexion d'appairage de VPC disposent de blocs d'adresse CIDR IPv6 associés, vous pouvez ajouter des routages qui permettent de communiquer avec le VPC pair via 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 d'appairage de VPC.

Considérations

- Si vous avez un VPC appairé à plusieurs VPC qui ont des blocs d'adresse CIDR IPv4 se chevauchant ou identiques, assurez-vous que vos tables de routage sont configurées pour éviter d'envoyer le trafic de réponse sortant de votre VPC vers le mauvais VPC. Pour le moment, AWS ne prend pas en charge de recherche par chemin inverse Unicast dans les connexions d'appairage de VPC qui vérifie l'adresse IP source des paquets et qui renvoie 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 route IPv4 pour 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 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. Dans le champ Destination, entrez la plage d'adresses IPv4 vers laquelle le trafic réseau de la connexion d'appairage de VPC doit être dirigé. Vous pouvez spécifier l'ensemble du bloc d'adresse CIDR IPv4 du VPC pair, 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 Save Changes (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 disposez de ressources dans différentes régions AWS qui utilisent des adresses IPv6, vous pouvez créer une connexion d'appairage entre régions. Vous pouvez ensuite ajouter une route IPv6 pour communiquer entre les ressources.

Pour ajouter une route IPv6 pour 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 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. Dans le champ Destination, entrez la plage d'adresses IPv6 du VPC pair. Vous pouvez spécifier l'ensemble du bloc d'adresse CIDR IPv6 du VPC pair, une plage spécifique ou une adresse IPv6 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 Save Changes (Enregistrer les modifications).

Pour de plus amples informations, veuillez consulter Tables de routage dans le Guide de l'utilisateur Amazon VPC.

Pour ajouter ou remplacer une route à l'aide de la ligne de commande ou d'une API

- create-route (AWS CLI)
- New-EC2Route (AWS Tools for Windows PowerShell)
- CreateRoute (API de requête Amazon EC2)
- replace-route (AWS CLI)
- Set-EC2Route (AWS Tools for Windows PowerShell)
- ReplaceRoute (API de requête Amazon EC2)

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 pour les groupes de sécurité de votre VPC pour référencer des groupes de sécurité dans le VPC appairé. Cette étape autorise le trafic vers et depuis les instances associées au groupe de sécurité référencé dans le VPC appairé.

Prérequis

- Le VPC pair peut être un VPC dans votre compte ou un VPC dans un autre compte AWS. Pour faire référence à un groupe de sécurité dans un autre compte AWS, incluez le numéro de compte dans Source ou Destination ; 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.
- Pour référencer un groupe de sécurité dans un VPC pair, la connexion d'appairage de VPC doit être à l'état `active`.
- 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 choisissez Actions, Modifier les règles entrantes pour modifier les règles entrantes ou Actions, Modifier les règles sortantes pour 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), saisissez l'ID du groupe de sécurité dans le VPC pair s'il se trouve dans la même région ou le bloc d'adresse CIDR du VPC pair s'il se trouve dans une région différente.

> **Note**
>
> Les groupes de sécurité d'un VPC pair ne s'affichent pas automatiquement.

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

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

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

Par exemple, pour mettre à jour votre groupe de sécurité `sg-aaaa1111` pour autoriser un accès entrant sur HTTP depuis `sg-bbbb2222` qui est dans un VPC pair, vous pouvez utiliser la commande AWS CLI suivante :

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

Après avoir mis à jour les règles du groupe de sécurité, utilisez la commande describe-security-groups pour afficher le groupe de sécurité référencé dans vos règles de 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)
- DescribeSecurityGroupReferences (API de requête Amazon EC2)

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.

Utilisation de règles de groupes 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 du groupe de sécurité est obsolète parce que la connexion d'appairage de VPC a été supprimée, elle ne sera plus marquée comme obsolète si vous créez une connexion d'appairage de VPC avec les mêmes VPC.

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 Security groups (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 Edit (Modifier).
6. Choisissez le bouton Supprimer à la droite de la règle à supprimer. Choisissez Prévisualiser les modifications, Enregistrer les règles.

Pour décrire vos règles de groupe de sécurité obsolètes à l'aide de la ligne de commande ou d'une API

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)
- DescribeStaleSecurityGroups (API de requête Amazon EC2)

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"
        }
    ]
}
```

Une fois que vous avez identifié les règles du groupe de sécurité obsolètes, vous pouvez les supprimer à l'aide des commandes revoke-security-group-ingress ou revoke-security-group-egress.

Modification des options de connexion d'appairage de VPC

Vous pouvez modifier une connexion d'appairage de VPC pour effectuer les opérations suivantes :

- Activez un VPC pour résoudre les noms d'hôte DNS IPv4 publics en adresses IPv4 privées lorsqu'il est interrogé à partir d'instances de VPC pair. Pour de plus amples informations, veuillez consulter Activation de la résolution DNS pour une connexion d'appairage de VPC.

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

Pour permettre à un VPC de résoudre les noms d'hôte DNS IPv4 publics en adresses IPv4 privées lorsqu'il est interrogé à partir d'instances de VPC pair, vous devez modifier la connexion d'appairage existante.

Les deux VPC doit être activés pour les noms d'hôte DNS et la résolution DNS.

Vous ne pouvez pas activer la prise en charge de la résolution DNS lorsque vous créez une nouvelle connexion d'appairage. Vous pouvez activer la prise en charge de la résolution DNS pour une connexion d'appairage existante qui a l'état `active`.

Pour activer la résolution DNS pour la connexion d'appairage

1. Ouvrez la console Amazon VPC sur 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, puis choisissez Actions, Modifier les paramètres DNS.
4. Pour veiller à ce que les requêtes du VPC pair soient résolues en adresses IP privées dans votre VPC local, sélectionnez l'option permettant d'activer la résolution DNS pour les requêtes à partir du VPC pair. Cette option est Requester DNS resolution (Résolution DNS du demandeur) ou Accepter DNS resolution (Résolution DNS de l'accepteur), selon que le VPC est le demandeur ou l'accepteur.
5. Si le VPC pair se trouve dans le même Compte AWS, vous pouvez activer la résolution DNS pour les deux VPC dans la connexion d'appairage.
6. Sélectionnez Save Changes (Enregistrer les modifications).
7. Si le VPC pair se trouve dans un autre compte ou une autre région AWS, le propriétaire du VPC pair doit se connecter à la console VPC, effectuer les étapes 2 à 4, puis choisir Enregistrer les modifications.

Pour activer la résolution DNS à l'aide de la ligne de commande ou d'une API

- modify-vpc-peering-connection-options (AWS CLI)
- Edit-EC2VpcPeeringConnectionOption (AWS Tools for Windows PowerShell)
- ModifyVpcPeeringConnectionOptions (API de requête Amazon EC2)

Vous devez modifier les options d'appairage du VPC demandeur si vous êtes le demandeur de la connexion d'appairage de VPC et vous devez modifier les options d'appairage du VPC accepteur si vous êtes l'accepteur de la connexion d'appairage de VPC. Vous pouvez utiliser les commandes describe-vpc-peering-connections ou Get-EC2VpcPeeringConnections pour vérifier quel VPC est l'accepteur et lequel est le demandeur de la connexion d'appairage de VPC. Pour les connexions d'appairage inter-région, vous devez utiliser la région pour le VPC demandeur afin de modifier les

options d'appairage du VPC demandeur et la région du VPC accepteur pour modifier les options d'appairage du VPC accepteur.

Dans cet exemple, vous êtes le demandeur de la connexion d'appairage de VPC, vous devez donc modifier les options de connexion d'appairage à l'aide de l'AWS CLI de la façon suivante :

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-aaaabbbb
 --requester-peering-connection-options AllowDnsResolutionFromRemoteVpc=true
```

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 de VPC à l'aide de la ligne de commande ou d'une API

- delete-vpc-peering-connection (AWS CLI)
- Remove-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)
- DeleteVpcPeeringConnection (API de requête Amazon EC2)

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. Pour de plus amples informations, veuillez consulter Mise à jour des tables de routage.
- Pour les instances EC2, vérifiez que les groupes de sécurité des instances EC2 autorisent le trafic provenant du VPC pair. Pour de plus amples informations, veuillez consulter Référence des groupes de sécurité pairs.
- Pour chaque ressource dans chaque VPC, vérifiez que l'ACL réseau de son sous-réseau autorise le trafic provenant du VPC pair.

Vous pouvez également utiliser l'Analyseur d'accessibilité pour identifier le composant présentant un problème de configuration, tel qu'une table de routage, un groupe de sécurité ou une liste ACL réseau. Pour plus d'informations, reportez-vous au Guide de l'Analyseur d'accessibilité.

Configurations d'appairage de VPC

La documentation suivante décrit les différents types de configurations d'appairage de VPC.

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 d'appairage de VPC. Pour en savoir plus sur la création et l'utilisation de connexions d'appairage de VPC, consultez Utilisation de connexions d'appairage de VPC.

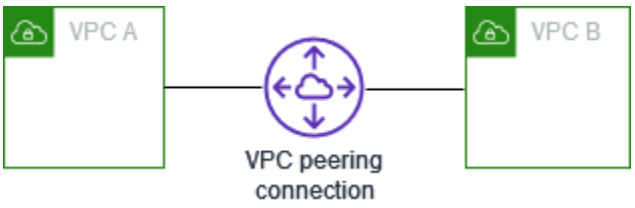
Pour en savoir plus sur la mise à jour de vos tables de routage, consultez la page Mise à jour de vos tables de routage pour une connexion d'appairage de VPC.

Configurations

- Appairage de deux VPC
- Un VPC appairé à deux VPC
- Appairage de trois VPC
- Appairage conjoint de plusieurs VPC

Appairage de deux VPC

Dans cette configuration, il existe une connexion d'appairage entre le VPC A et le VPC B (`pcx-11112222`). Les VPC se trouvent dans le même Compte AWS et leurs blocs d'adresse CIDR ne se chevauchent pas.



Vous avez la possibilité d'utiliser cette configuration quand vous avez deux VPC qui ont besoin d'accéder aux ressources les uns des autres. 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	*CIDR VPC A*	Local
	CIDR VPC B	pcx-11112222
VPC B	*CIDR VPC B*	Local
	CIDR VPC A	pcx-11112222

CIDR VPC IPv4 multiples

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

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

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

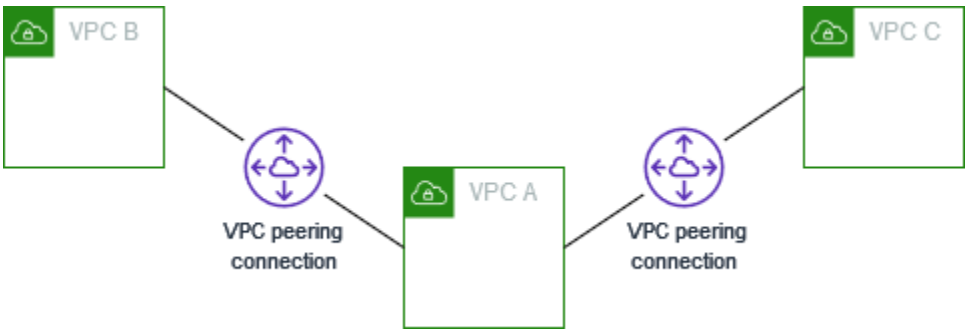
CIDR VPC IPv4 et IPv6

Si le VPC A et le VPC B possèdent plusieurs blocs d'adresse CIDR IPv6 associés, vous pouvez mettre à jour la table de routage de chaque VPC avec des routes pour les blocs d'adresse CIDR IPv4 et IPv6 du VPC pair.

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

Un VPC appairé à deux VPC

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 VPC se trouvent dans le même Compte AWS et leurs blocs d'adresse 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 Appairage de trois VPC. Pour plus d'informations sur les scénarios d'appairage non pris en charge, consultez la section the section called “Limitations des appairages de VPC”.

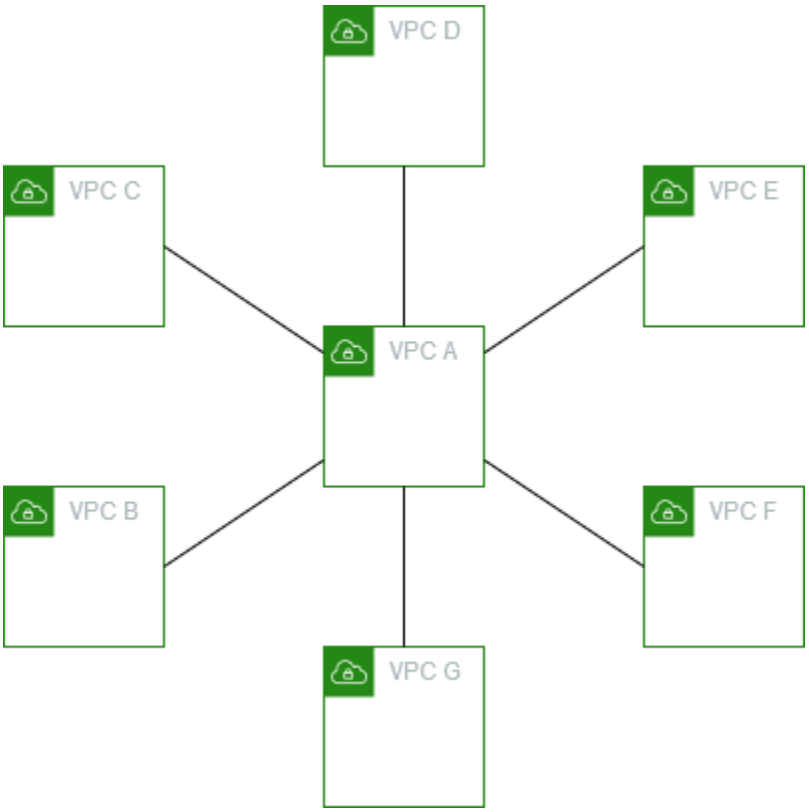
Vous avez la possibilité d'utiliser cette configuration quand vous avez des ressources sur un VPC central, comme un référentiel de services, auquel les autres VPC ont besoin d'accéder. Les autres VPC n'ont pas besoin d'accéder aux ressources les uns des autres, ils ont simplement besoin d'accéder aux ressources dans le 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	*CIDR VPC A*	Local
	CIDR VPC B	pcx-12121212
	CIDR VPC C	pcx-23232323
VPC B	*CIDR VPC B*	Local
	CIDR VPC A	pcx-12121212

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

Vous pouvez appliquer cette configuration à d'autres VPC. Par exemple, le VPC A est appairé avec le VPC B via le VPC G en utilisant des CIDR IPv4 et IPv6, mais les autres VPC ne sont pas appairés entre eux. 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	*CIDR IPv4 VPC A*	Local
	CIDR IPv6 VPC A	Local
	CIDR IPv4 VPC B	pcx-aaaabbbb

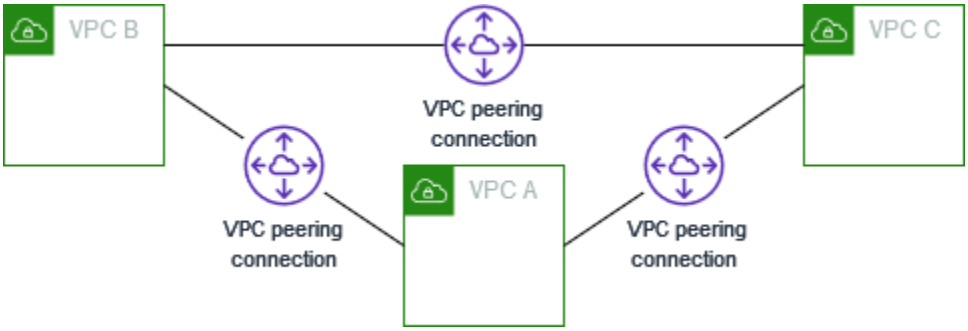
Table de routage	Destination	Cible
	CIDR IPv6 VPC B	pcx-aaaabbbb
	CIDR IPv4 VPC C	pcx-aaaacccc
	CIDR IPv6 VPC C	pcx-aaaacccc
	CIDR IPv4 VPC D	pcx-aaaadddd
	CIDR IPv6 VPC D	pcx-aaaadddd
	CIDR IPv4 VPC E	pcx-aaaaeeee
	CIDR IPv6 VPC E	pcx-aaaaeeee
	CIDR IPv4 VPC F	pcx-aaaaffff
	CIDR IPv6 VPC F	pcx-aaaaffff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

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

Appairage de trois VPC

Dans cette configuration, il existe trois VPC dans le même Compte AWS avec des blocs CIDR qui ne se chevauchent pas. Les VPC sont appairés 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 des VPC qui doivent partager des ressources entre eux 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	*CIDR VPC A*	Local
	CIDR VPC B	pcx-aaaabbbb
	CIDR VPC C	pcx-aaaacccc
VPC B	*CIDR VPC B*	Local
	CIDR VPC A	pcx-aaaabbbb
	CIDR VPC C	pcx-bbbbcccc
VPC C	*CIDR VPC C*	Local
	CIDR VPC A	pcx-aaaacccc
	CIDR VPC B	pcx-bbbbcccc

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

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

Appairage conjoint de plusieurs VPC

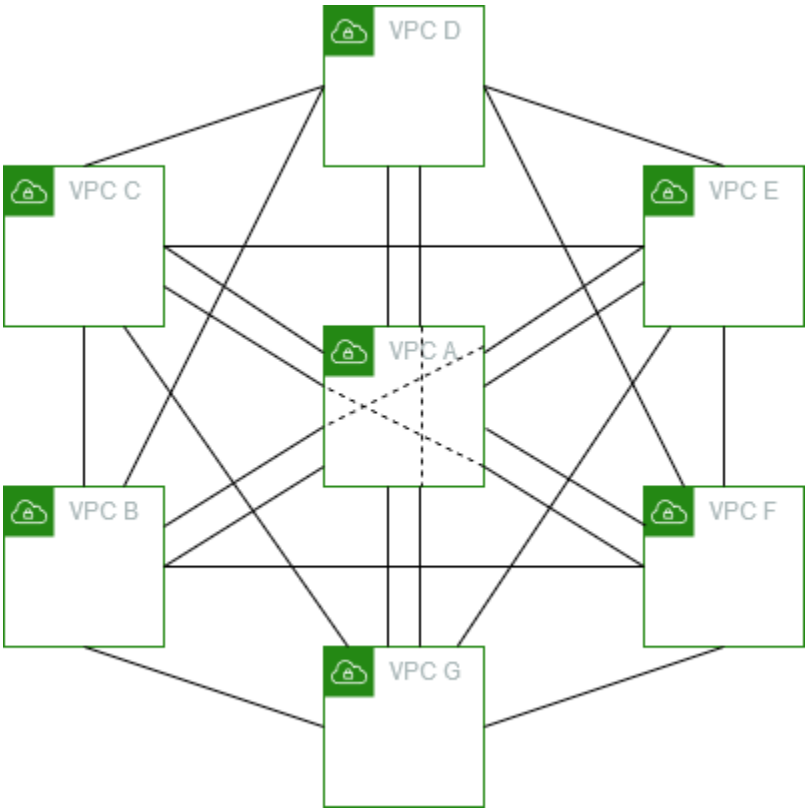
Cette configuration comporte sept VPC appairés dans une configuration de maillage complet. Les VPC se trouvent dans le même Compte AWS et leurs blocs d'adresse CIDR ne se chevauchent pas.

VPC	VPC	Connexion d'appairage de VPC
A	B	pcx-aaaabbbb
A	C	pcx-aaaacccc
A	D	pcx-aaaadddd

VPC	VPC	Connexion d'appairage de VPC
A	E	pcx-aaaaeeee
A	F	pcx-aaaaffff
A	G	pcx-aaaagggg
B	C	pcx-bbbbcccc
B	D	pcx-bbbbdddd
B	E	pcx-bbbbeeee
B	F	pcx-bbbbffff
B	G	pcx-bbbbgggg
C	D	pcx-ccccdddd
C	E	pcx-cccceeee
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 avez la possibilité d'utiliser cette configuration quand vous avez plusieurs VPC qui ont besoin de pouvoir accéder aux ressources les uns 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	*CIDR VPC A*	Local
	CIDR VPC B	pcx-aaaabbbb
	CIDR VPC C	pcx-aaaacccc
	CIDR VPC D	pcx-aaaadddd
	CIDR VPC E	pcx-aaaaeeee
	CIDR VPC F	pcx-aaaaffff
	CIDR VPC G	pcx-aaaagggg
VPC B	*CIDR VPC B*	Local

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

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

Table de routage	Destination	Cible
	CIDR VPC F	pcx-ffffgggg

Si tous les VPC ont des blocs d'adresse CIDR IPv6 associés, mettez à jour les tables de routage comme suit.

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

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

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

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

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

Table de routage	Destination	Cible
	CIDR IPv4 VPC F	pcx-ffffgggg
	CIDR IPv6 VPC F	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 appairé à au moins deux VPC qui ont des blocs d'adresse CIDR se chevauchant.

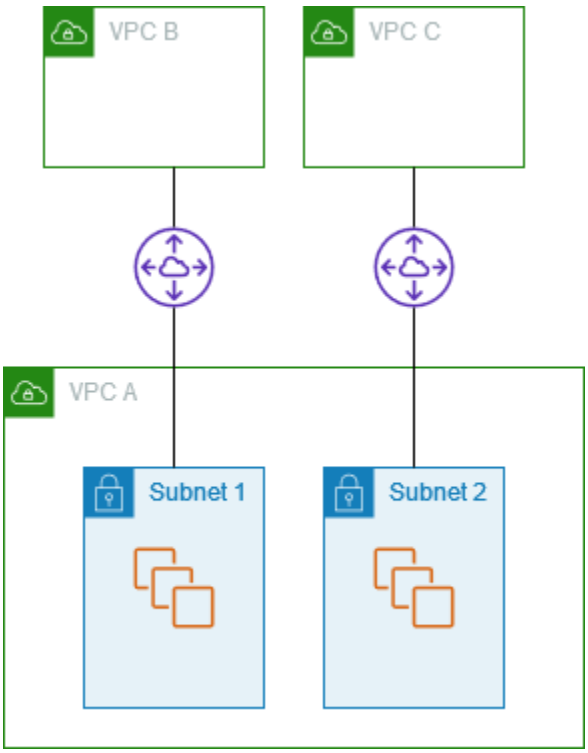
Pour des exemples de scénarios dans lesquels vous pouvez avoir besoin d'une configuration de connexion d'appairage de VPC spécifique, consultez Scénarios d'appairage de VPC. Pour en savoir plus sur l'utilisation de connexions d'appairage de VPC, consultez Utilisation de connexions d'appairage de VPC. 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 VPC qui ont accès à des sous-réseaux spécifiques dans un VPC
- Deux VPC qui ont accès à des blocs d'adresse CIDR spécifiques dans un seul VPC
- Un seul VPC qui a accès à des sous-réseaux spécifiques dans deux VPC
- Instances dans un seul VPC qui ont accès à des instances spécifiques dans deux VPC
- Un VPC qui a accès à deux VPC à l'aide des correspondances de préfixe les plus longues
- Configurations de plusieurs VPC

Deux VPC qui ont accès 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)	*CIDR VPC A*	Local
	CIDR VPC B	pcx-aaaabbbb
Sous-réseau 2 (VPC A)	*CIDR VPC A*	Local
	CIDR VPC C	pcx-aaaacccc
VPC B	*CIDR VPC B*	Local
	CIDR du sous-réseau 1	pcx-aaaabbbb
VPC C	*CIDR VPC C*	Local

Table de routage	Destination	Cible
	CIDR du sous-réseau 2	pcx-aaaacccc

Vous pouvez appliquer cette configuration à plusieurs blocs CIDR. Supposons que le VPC A et le VPC B comportent des blocs CIDR IPv4 et IPv6, et que le sous-réseau 1 ait un bloc CIDR IPv6 associé. Vous pouvez activer VPC B pour communiquer avec le sous-réseau 1 du VPC A via IPv6 à l'aide de la connexion d'appairage de VPC. Pour ce faire, ajoutez une route vers la table de routage pour le VPC A avec une destination du bloc d'adresse CIDR IPv6 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	*CIDR IPv4 VPC A*	Local	
	CIDR IPv6 VPC A	Local	Route locale qui est ajoutée automatiq uement pour toute communication IPv6 dans le VPC.
	CIDR IPv4 VPC B	pcx-aaaabbbb	
	CIDR IPv6 VPC B	pcx-aaaabbbb	Route vers le bloc d'adresse CIDR IPv6 du VPC B.
Sous-réseau 2 du VPC A	*CIDR IPv4 VPC A*	Local	
	CIDR IPv6 VPC A	Local	Route locale qui est ajoutée automatiq uement pour toute communication IPv6 dans le VPC.
	CIDR IPv4 VPC C	pcx-aaaacccc	
VPC B	*CIDR IPv4 VPC B*	Local	

Table de routage	Destination	Target	Remarques
	CIDR IPv6 VPC B	Local	Route locale qui est ajoutée automatiq uement pour toute communication IPv6 dans le VPC.
	CIDR IPv4 du sous-réseau 1	pcx-aaaabbbb	
	CIDR IPv4 du sous-réseau 2	pcx-aaaabbbb	Route vers le bloc d'adresse CIDR IPv6 du VPC A.
VPC C	*CIDR IPv4 VPC C*	Local	
	CIDR IPv4 du sous-réseau 2	pcx-aaaacccc	

Deux VPC qui ont accès à des blocs d'adresse CIDR spécifiques dans un seul VPC

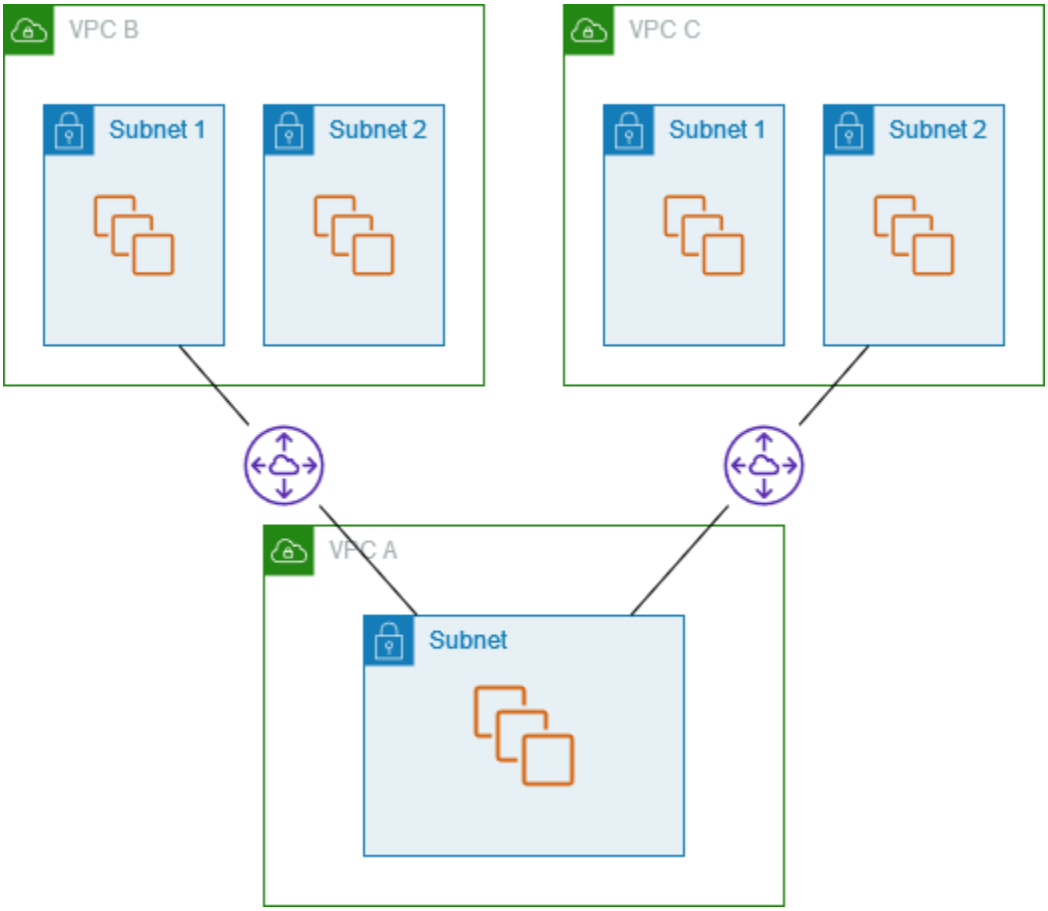
Dans cette configuration, il existe un VPC central (VPC A), une connexion d'appairage entre le VPC A et le VPC B (`pcx-aaaabbbb`) et une connexion d'appairage entre le VPC A et le VPC C (`pcx-aaaacccc`). Le VPC A a un bloc d'adresse CIDR pour chaque connexion d'appairage.

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

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

Un seul VPC qui a accès à des sous-réseaux spécifiques dans deux VPC

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 quand vous avez un VPC central avec un seul jeu ressources, comme les services Active Directory, auquel les autres VPC ont besoin d'accéder. Le VPC central n'a pas besoin d'un accès total aux VPC auxquels il est appairé.

La table de routage du VPC A utilise les connexions d'appairage pour accéder uniquement à des sous-réseaux spécifiques dans les VPC appairés. 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	*CIDR VPC A*	Local
	CIDR du sous-réseau 1	pcx-aaaabbbb
	CIDR du sous-réseau 2	pcx-aaaacccc
Sous-réseau 1 (VPC B)	*CIDR VPC B*	Local
	Sous-réseau dans le CIDR du VPC A	pcx-aaaabbbb
Sous-réseau 2 (VPC C)	*CIDR VPC C*	Local
	Sous-réseau dans le CIDR du VPC A	pcx-aaaacccc

Routage pour le trafic de la réponse

Si vous avez un VPC appairé à plusieurs VPC qui ont des blocs d'adresse CIDR se chevauchant ou identiques, assurez-vous que vos tables de routage sont configurées pour éviter d'envoyer le trafic de réponse sortant de votre VPC vers le mauvais VPC. AWS ne prend pas en charge de recherche par chemin inverse Unicast dans les connexions d'appairage de VPC qui vérifie l'adresse IP source des paquets et qui renvoie 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)	*CIDR VPC B*	Local
	Sous-réseau dans le CIDR du VPC A	pcx-aaaabbbb
VPC A	*CIDR VPC A*	Local
	CIDR VPC C	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 B dans le VPC B et le sous-réseau A dans le VPC C. Ce scénario est utile si vous devez ajouter une autre connexion d'appairage de VPC avec un autre sous-réseau faisant partie de la même plage d'adresses que les VPC B et C ; vous pouvez simplement ajouter une autre route pour ce sous-réseau spécifique.

Destination	Target
CIDR VPC A	Local

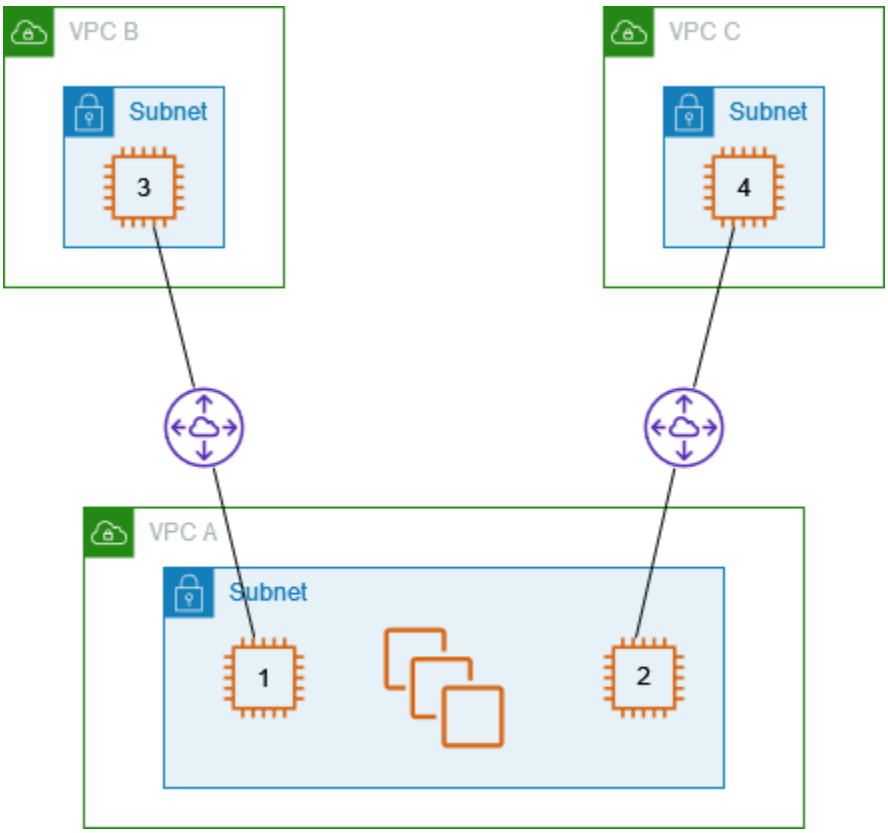
Destination	Target
CIDR du sous-réseau 2	pcx-aaaabbbb
CIDR du sous-réseau 1	pcx-aaaacccc

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
CIDR VPC A	Local
Adresse IP spécifique dans le sous-réseau 2	pcx-aaaabbbb
CIDR VPC B	pcx-aaaacccc

Instances dans un seul VPC qui ont accès à des instances spécifiques dans deux VPC

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.



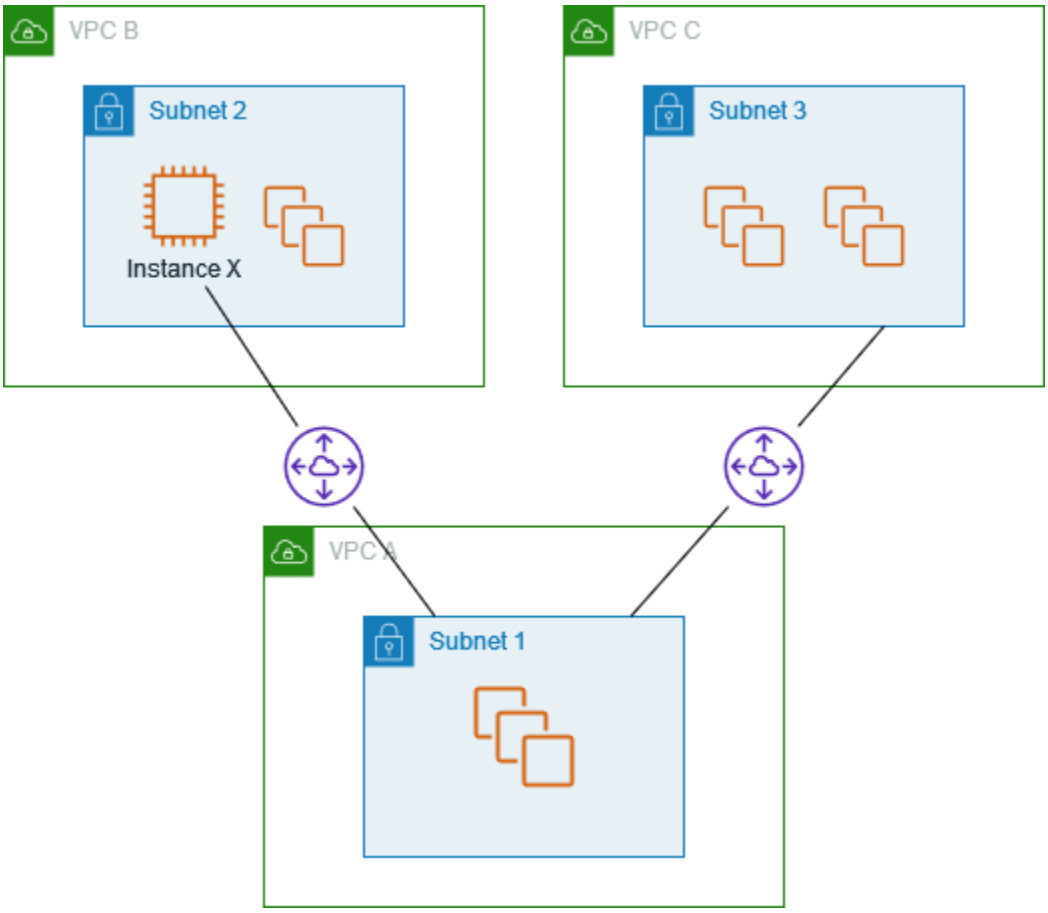
Chaque table de routage de VPC pointe vers la connexion d'appairage de VPC appropriée pour accéder à une seule adresse IP (et donc à une instance spécifique) dans le VPC pair.

Table de routage	Destination	Cible
VPC A	*CIDR VPC A*	Local
	Adresse IP de l'instance 3	pcx-aaaabbbb
	Adresse IP de l'instance 4	pcx-aaaacccc
VPC B	*CIDR VPC B*	Local
	Adresse IP de l'instance 1	pcx-aaaabbbb
VPC C	*CIDR VPC C*	Local

Table de routage	Destination	Cible
	Adresse IP de l'instance 2	pcx-aaaacccc

Un VPC qui a accès à deux VPC à l'aide des correspondances de préfixe les plus longues

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	*Bloc CIDR VPC A*	Local
	Adresse IP de l'instance X	pcx-aaaabbbb
	Bloc CIDR VPC C	pcx-aaaacccc
VPC B	*Bloc CIDR VPC B*	Local
	Bloc CIDR VPC A	pcx-aaaabbbb
VPC C	*Bloc CIDR VPC C*	Local
	Bloc CIDR VPC A	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.

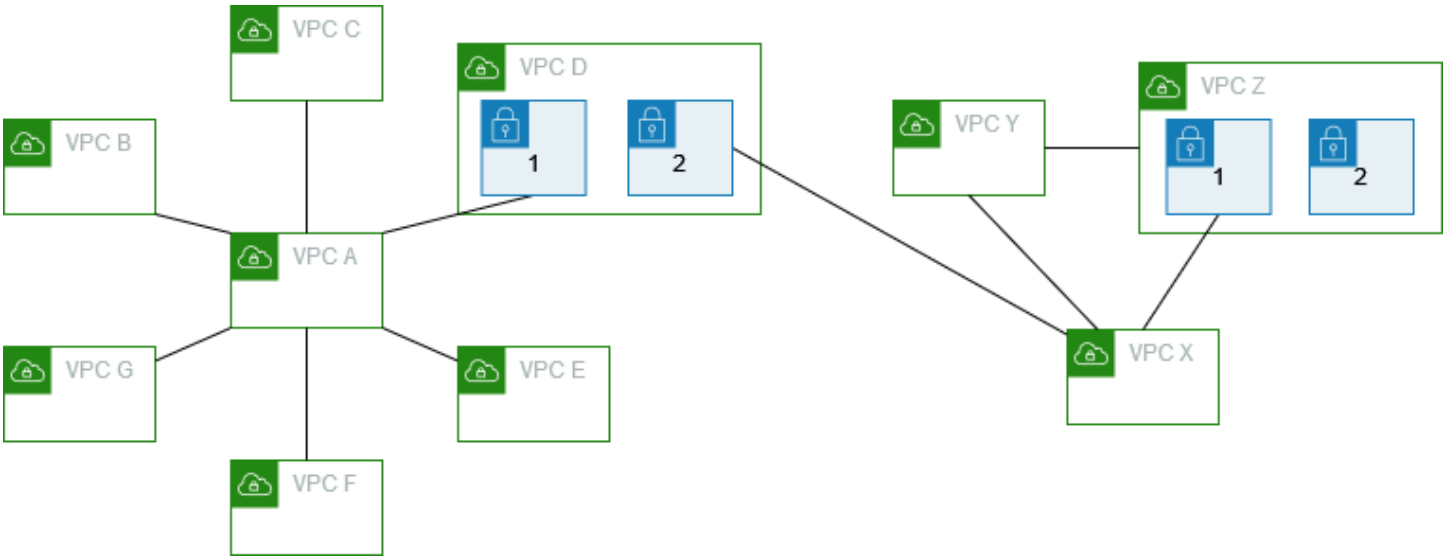
Configurations de plusieurs VPC

Dans cette configuration, un VPC central (VPC A) est appairé à plusieurs VPC dans une configuration en étoile. Vous avez également trois VPC (VPC X, Y et Z) appairés 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. AWSne 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 plus d'informations, consultez 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 les VPC B, C, E, F et G pointent vers les connexions d'appairage appropriées pour accéder à l'ensemble du bloc d'adresse CIDR pour le VPC A, et la table de routage du VPC A pointe vers les connexions d'appairage appropriées des VPC B, C, E, F et G pour accéder à l'ensemble de leurs blocs d'adresse CIDR. 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	*CIDR VPC A*	Local
	CIDR VPC B	pcx-aaaabbbb
	CIDR VPC C	pcx-aaaacccc
	CIDR sous-réseau 1 dans le VPC D	pcx-aaaadddd
	CIDR VPC E	pcx-aaaaeeee
	CIDR VPC F	pcx-aaaaffff
	CIDR VPC G	pcx-aaaagggg
VPC B	*CIDR VPC B*	Local
	CIDR VPC A	pcx-aaaabbbb
VPC C	*CIDR VPC C*	Local
	CIDR VPC A	pcx-aaaacccc
Sous-réseau 1 du VPC D	*CIDR VPC D*	Local
	CIDR VPC A	pcx-aaaadddd
Sous-réseau 2 du VPC D	*CIDR VPC D*	Local
	CIDR VPC X	pcx-ddddxxxx
VPC E	*CIDR VPC E*	Local
	CIDR VPC A	pcx-aaaaeeee
VPC F	*CIDR VPC F*	Local
	CIDR VPC A	pcx-aaaaffff

Table de routage	Destination	Cible
VPC G	*CIDR VPC G*	Local
	CIDR VPC A	pcx-aaaagggg
VPC X	*CIDR VPC X*	Local
	CIDR sous-réseau 2 dans le VPC D	pcx-ddddxxxx
	CIDR VPC Y	pcx-xxxxyyyy
	CIDR sous-réseau 1 dans le VPC Z	pcx-xxxxzzzz
VPC Y	*CIDR VPC Y*	Local
	CIDR VPC X	pcx-xxxxyyyy
	CIDR VPC Z	pcx-yyyyzzzz
VPC Z	*CIDR VPC Z*	Local
	CIDR VPC Y	pcx-yyyyzzzz
	CIDR VPC X	pcx-xxxxzzzz

Scénarios d'appairage de VPC

Vous pouvez avoir besoin de configurer une connexion d'appairage entre vos VPC, ou entre l'un de vos VPC et un VPC appartenant à un autre compte AWS, et ce pour différentes raisons. Les scénarios suivants peuvent vous aider à identifier la configuration la mieux adaptée à vos besoins en matière de mise en réseau.

Scénarios

- Appairage de deux VPC ou plus afin d'offrir un accès complet aux ressources
- Appairage à un VPC pour accéder à des ressources centralisées

Appairage de deux VPC ou plus afin d'offrir un accès complet aux ressources

Dans ce scénario, vous disposez d'au moins deux VPC que vous souhaitez appairer afin d'activer le partage complet des ressources entre tous les VPC. 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 VPC appartiennent au même compte AWS tandis que d'autres sont inclus dans un autre compte AWS. Vous souhaitez appairer tous les VPC ensemble pour permettre aux services informatiques de bénéficier d'un accès complet aux ressources 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 :

- Appairage de deux VPC
- Appairage de trois VPC
- Appairage conjoint de plusieurs VPC

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

Appairage à un VPC pour accéder à des ressources centralisées

Dans ce scénario, vous disposez d'un VPC central contenant des ressources que vous souhaitez partager avec d'autres VPC. Votre VPC central peut avoir besoin d'un accès total ou partiel aux VPC pairs, et vice versa. Voici quelques exemples :

- Le service informatique de votre entreprise possède un VPC pour le partage des fichiers. Vous souhaitez appairer d'autres VPC à ce VPC central, mais vous ne voulez pas que les autres VPC s'envoient du trafic entre eux.
- Votre entreprise possède un VPC que vous souhaitez partager avec vos clients. Chaque client peut créer une connexion d'appairage avec votre VPC. Toutefois, vos clients ne peuvent pas acheminer du trafic vers les autres VPC qui sont appairés à votre VPC et ils ne connaissent pas les routes des autres clients.
- Vous disposez d'un VPC central, utilisé pour les services Active Directory. Des instances spécifiques des VPC pairs envoient des demandes aux serveurs Active Directory et ont besoin d'un accès complet au VPC central. Le VPC central n'a pas besoin d'un accès complet aux VPC pairs, mais seulement d'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 Utilisation de 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, et connaître les ressources et les clés de conditions prises en charge pour chaque action, consultez Actions, ressources et clés de condition pour Amazon EC2 dans le Guide de l'utilisateur IAM.

Exemple : créer une connexion d'appairage de VPC

La stratégie suivante octroie aux utilisateurs l'autorisation de créer des demandes de connexion d'appairage de VPC en utilisant des VPC dont la balise est `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.

```
{
  "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 stratégie suivante octroie aux utilisateurs du compte AWS spécifié l'autorisation de créer des connexions d'appairage de VPC grâce à n'importe quel VPC dans la région spécifiée, mais uniquement si celui qui accepte la connexion d'appairage est un VPC spécifique dans un compte spécifique.

```
{
  "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 stratégie suivante octroie aux utilisateurs l'autorisation d'accepter des demandes de connexion d'appairage de VPC depuis un compte AWS spécifique. 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.

```
{
  "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`.

```
{
  "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.

```
{
  "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 afficher, créer, accepter, rejeter et supprimer des connexions d'appairage de VPC, à condition qu'elles soient toutes dans le 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 instruction octroie aux utilisateurs l'autorisation de créer des connexions d'appairage de VPC et, dans ce but, d'accéder à tous les VPC dans le compte spécifié.

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 peuvent uniquement être effectuées sur des connexions d'appairage de VPC avec des VPC qui font partie du 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.

```
{
  "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.

```
{
  "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

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

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 obtenir des quotas supplémentaires pour Amazon VPC, consultez 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 de VPC entre des VPC qui se trouvent dans des régions AWS différentes.	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 de ClassicLink sur une connexion d'appairage de VPC	Vous pouvez modifier votre connexion d'appairage de VPC pour autoriser les instances EC2-Classic liées locales à communiquer avec des instances dans un VPC pair ou vice versa.	26 avril 2016
Appairage de VPC	Vous pouvez créer une connexion d'appairage VPC entre deux VPC, permettant ainsi aux instances situées dans chaque 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.