aws

VPC Peering

Amazon Virtual Private Cloud

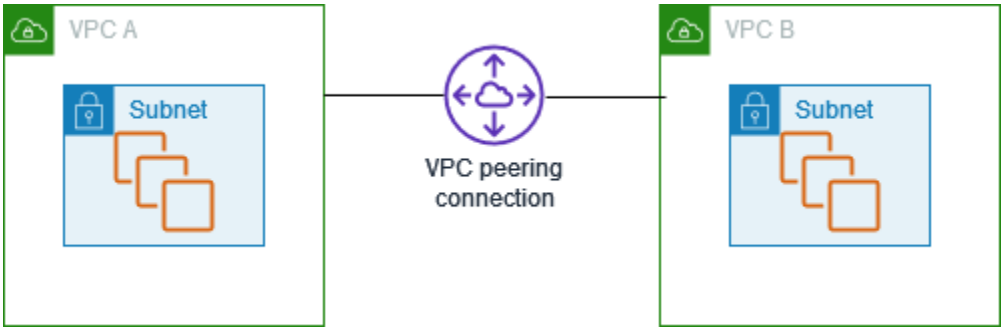
Amazon Virtual Private Cloud: VPC Peering

Table of Contents

Was ist VPC Peering?

Eine Virtual Private Cloud (VPC – virtuelle private Cloud) ist ein virtuelles Netzwerk für Ihren AWS-Konto. Es ist logisch von anderen virtuellen Netzwerken in der AWS Cloud isoliert. Sie können AWS Ressourcen wie Amazon EC2 EC2-Instances in Ihrer VPC starten.

Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs. Sie ermöglicht die Weiterleitung des Datenverkehrs zwischen den VPCs mithilfe privater IPv4- oder IPv6-Adressen. Instances in jeder der VPCs können so miteinander kommunizieren, als befänden sie sich im selben Netzwerk. Sie können eine VPC-Peering-Verbindung zwischen Ihren eigenen VPCs oder mit einer VPC in einem anderen AWS -Konto herstellen. Die VPCs können sich in unterschiedlichen Regionen befinden (auch als regionsübergreifende VPC-Peering-Verbindung bezeichnet).



AWS verwendet die bestehende Infrastruktur einer VPC, um eine VPC-Peering-Verbindung herzustellen. Sie ist weder ein Gateway noch eine VPN-Verbindung und benötigt keine separate physische Hardware. Es gibt keine einzelne Fehlerstelle für die Kommunikation und keinen Bandbreiten-Engpass.

Eine VPC-Peering-Verbindung hilft Ihnen, die Datenübertragung zu erleichtern. Wenn Sie beispielsweise mehr als ein AWS Konto haben, können Sie die VPCs über diese Konten miteinander verbinden, um ein Filesharing-Netzwerk einzurichten. Sie können auch eine VPC-Peering-Verbindung verwenden, um anderen VPCs den Zugriff auf Ressourcen zu gewähren, die Sie in einer Ihrer VPCs haben.

Wenn Sie Peering-Beziehungen zwischen VPCs in verschiedenen AWS Regionen einrichten, können Ressourcen in den VPCs (z. B. EC2-Instances und Lambda-Funktionen) in verschiedenen AWS Regionen über private IP-Adressen miteinander kommunizieren, ohne ein Gateway, eine VPN-Verbindung oder eine Netzwerk-Appliance zu verwenden. Der Datenverkehr verbleibt im privaten IP-Adressraum. Der gesamte regionsübergreifende Datenverkehr wird ohne single point of failure (einzelner Fehlerpunkt) oder Engpässen bei der Bandbreite verschlüsselt. Der Datenverkehr bleibt

immer auf dem globalen AWS Backbone und durchquert niemals das öffentliche Internet, wodurch Bedrohungen wie häufige Exploits und DDoS-Angriffe reduziert werden. Regionsübergreifendes VPC-Peering bietet eine einfache und kostengünstige Möglichkeit, Ressourcen zwischen Regionen gemeinsam zu nutzen oder Daten für geografische Redundanz zu replizieren.

Preisgestaltung für eine VPC-Peering-Verbindung

Das Erstellen einer VPC-Peering-Verbindung ist kostenlos. Jegliche Datenübertragung über eine VPC-Peering-Verbindung, die innerhalb einer Availability Zone bleibt (auch wenn sie zwischen verschiedenen Konten stattfindet), ist kostenlos. Für die Datenübertragung über VPC-Peering-Verbindungen, die Availability Zones und Regionen überschreiten, fallen Gebühren an. Weitere Informationen finden Sie unter Amazon-EC2-Preise.

VPC Peering-Grundlagen

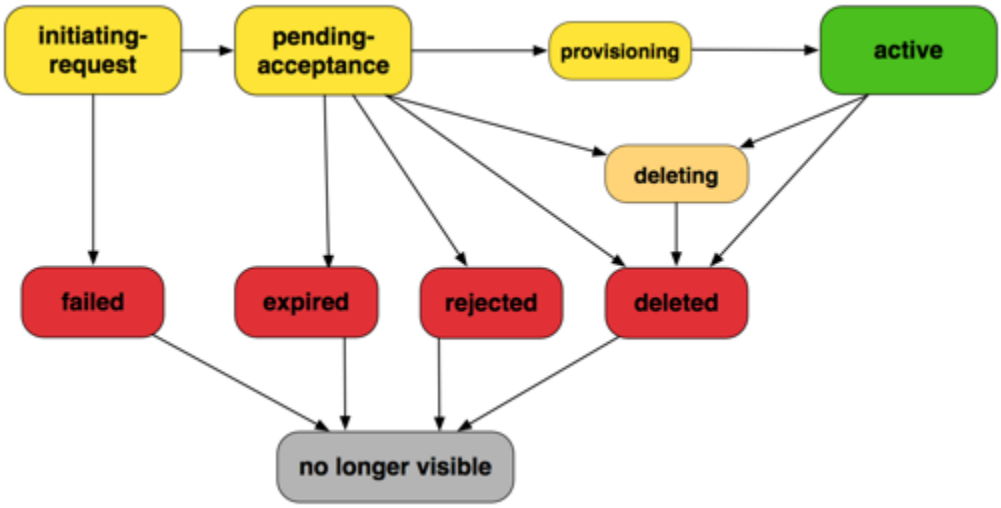
Beachten Sie beim Herstellen einer VPC-Peering-Verbindung Folgendes:

1. Der Eigentümer der anfordernden VPC sendet eine Anforderung zur Herstellung der VPC-Peering-Verbindung an den Eigentümer der annehmenden VPC. Die akzeptierende VPC kann Ihnen oder einem anderen AWS Konto gehören und darf keinen CIDR-Block haben, der sich mit dem CIDR-Block der anfordernden VPC überschneidet.
2. Der Eigentümer der annehmenden VPC akzeptiert die Anforderung für die VPC-Peering-Verbindung, um die VPC-Peering-Verbindung zu aktivieren.
3. Um den Datenverkehr zwischen den Peer-VPCs unter Verwendung privater IP-Adressen zu ermöglichen, muss der Eigentümer von jeder einzelnen VPC der VPC-Peering-Verbindung eine Route zu einer oder mehreren Routing-Tabellen seiner VPCs manuell hinzufügen, die auf den IP-Adressbereich der anderen VPC (der Peer-VPC) verweist.
4. Aktualisieren Sie bei Bedarf die Sicherheitsgruppenregeln, die Ihrer EC2-Instance zugeordnet sind, um sicherzustellen, dass der Verkehr zur und von der Peer-VPC nicht eingeschränkt wird. Wenn sich beide VPCs in derselben Region befinden, können Sie auf eine Sicherheitsgruppe von der Peer-VPC als Quelle oder Ziel für eingehende oder ausgehende Regeln in Ihrer Sicherheitsgruppe verweisen.
5. Bei den standardmäßigen VPC-Peering-Verbindungsoptionen wird der Hostname in die öffentliche IP-Adresse der EC2-Instance aufgelöst, wenn sich EC2-Instances auf beiden Seiten einer VPC-Peering-Verbindung gegenseitig mit einem öffentlichen DNS-Hostnamen adressieren. Um dieses Verhalten zu ändern, aktivieren Sie die Auflösung des DNS-Hostnamens für Ihren VPC-Verbindung. Wenn sich EC2-Instances auf beiden Seiten der VPC-Peering-Verbindung gegenseitig mit einem öffentlichen DNS-Hostnamen adressieren, wird der Hostname nach der Aktivierung der DNS-Hostnamenauflösung in die private IP-Adresse der EC2-Instance aufgelöst.

Weitere Informationen finden Sie unter Arbeiten mit VPC-Peering-Verbindungen.

Lebenszyklus einer VPC-Peering-Verbindung

Eine VPC-Peering-Verbindung durchläuft verschiedene Phasen, die mit der Einleitung der Anforderung beginnen. In jeder Phase kann es Aktionen geben, die Sie einleiten können. Am Ende Ihres Lebenszyklus bleibt die VPC-Peering-Verbindung in der Amazon VPC-Konsole und -API oder in der Befehlszeilenausgabe eine Zeit lang sichtbar.



- Auslösungsanforderung: Eine Anforderung für eine VPC-Peering-Verbindung ist ausgelöst worden. In dieser Phase kann eine Peering-Verbindung fehlschlagen oder nach `pending-acceptance` verschoben werden.
- Fehlgeschlagen: Die Anforderung für die VPC-Peering-Verbindung ist fehlgeschlagen. In dieser Phase kann sie nicht angenommen, abgewiesen oder gelöscht werden. Die fehlgeschlagene VPC-Peering-Verbindung bleibt für den Auftraggeber zwei Stunden lang sichtbar.
- In Annahme: Die VPC-Peering-Verbindungsanforderung befindet sich in Erwartung der Annahme des Eigentümers der annehmenden VPC. Während dieser Phase kann der Eigentümer der anfordernden VPC die Anforderung löschen und der Eigentümer der annehmenden VPC kann die Anforderung annehmen oder ablehnen. Falls keine Aktionen bezüglich der Anforderung eingeleitet werden, läuft diese in 7 Tagen ab.
- Abgelaufen: Die VPC-Peering-Verbindungsanforderung ist abgelaufen. Keine Aktionen wurden diesbezüglich seitens der VPC-Eigentümer vorgenommen. Die abgelaufene VPC-Peering-Verbindung bleibt für beide VPC-Eigentümer 2 Tage lang sichtbar.
- Abgelehnt: Der Eigentümer der annehmenden VPC hat eine VPC-Peering-Verbindungsanforderung, die sich im Status `pending-acceptance` befindet, abgelehnt. In dieser Phase kann die Anforderung nicht akzeptiert werden. Die abgelehnte VPC-Peering-Verbindung bleibt für den Eigentümer der anfordernden VPC 2 Tage und für den Eigentümer der annehmenden VPC 2 Stunden lang sichtbar. Wenn die Anfrage innerhalb desselben AWS Kontos erstellt wurde, bleibt die abgelehnte Anfrage 2 Stunden lang sichtbar.
- Bereitstellung: Die VPC-Peering-Verbindungsanforderung ist akzeptiert worden und wird sich bald im Status `active` befinden.

- Aktiv: Die VPC-Peering-Verbindung ist aktiv und Datenverkehr kann zwischen den VPCs fließen (vorausgesetzt, Ihre Sicherheitsgruppen und Routingtabellen lassen den Datenverkehr zu). In diesem Status können beide VPC-Eigentümer die VPC-Peering-Verbindung löschen, aber nicht ablehnen.

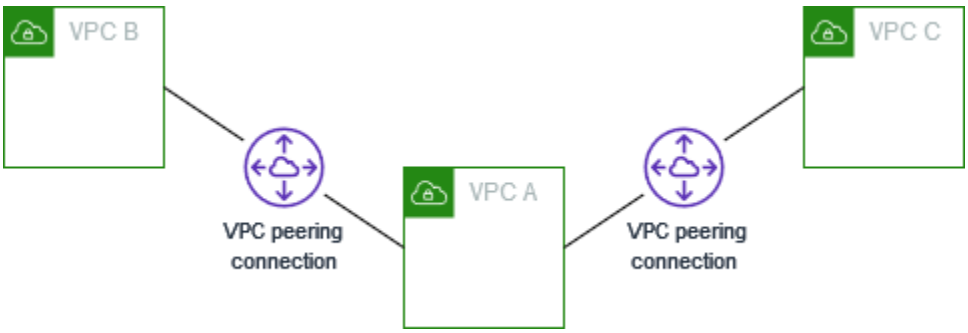
> **Note**
>
> Wenn ein Ereignis in einer Region, in der sich eine VPC befindet, den Verkehrsfluss verhindert, bleibt der Status der VPC-Peering-Verbindung bestehen. `Active`

- Löschen: Bezieht sich auf eine regionsübergreifende VPC-Peering-Verbindung, die gerade gelöscht wird. Der Eigentümer einer VPC hat eine Anfrage gestellt, eine `active` VPC-Peering-Verbindung zu löschen, oder der Eigentümer der anfordernden VPC hat eine Anfrage gestellt, eine `pending-acceptance`VPC-Peering-Verbindungsanfrage zu löschen.
- Gelöscht: Eine VPC-Peering-Verbindung im Status `active` wurde von beiden VPC-Eigentümern gelöscht oder eine VPC-Peering-Verbindungsanforderung im Status `pending-acceptance` wurde von dem Eigentümer der anfordernden VPC gelöscht. In dieser Phase kann die VPC-Peering-Verbindung nicht angenommen oder abgelehnt werden. Die VPC-Peering-Verbindung bleibt für die Partei, die sie gelöscht hat, 2 Stunden und für die andere Partei 2 Tage lang sichtbar. Wenn die VPC-Peering-Verbindung innerhalb desselben AWS Kontos erstellt wurde, bleibt die gelöschte Anfrage 2 Stunden lang sichtbar.

Multiple VPC-Peering-Verbindungen

Eine VPC-Peering-Verbindung ist eine Eins-zu-eins-Beziehung zwischen zwei VPCs. Sie können mehrere VPC Peering-Verbindungen für jede VPC, deren Eigentümer Sie sind, erstellen. Es werden aber keine transitiven Peering-Beziehungen unterstützt. Es werden keine Peering-Beziehungen mit VPCs bestehen, zu denen Ihre VPC kein direkter Peer ist.

Das folgende Diagramm ist ein Beispiel für eine VPC, die mit zwei verschiedenen VPCs durch Peering verbunden ist. Es gibt zwei VPC-Peering-Verbindungen: VPC A ist sowohl mit VPC B als auch VPC C durch Peering verbunden. VPC B und VPC C sind nicht durch Peering verbunden. Sie können VPC A nicht als Transitpunkt für das Peering zwischen VPC B und VPC C verwenden. Falls Sie einen Verkehrsbetrieb zwischen VPC B und VPC C ermöglichen möchten, müssen Sie eine eigene VPC-Peering-Verbindung zwischen den beiden erstellen.



VPC Peering-Einschränkungen

Beachten Sie die folgenden Einschränkungen für VPC-Peering-Verbindungen. In einigen Fällen können Sie anstelle der VPC-Peering-Verbindung einen Transit-Gateway-Anhang verwenden. Weitere Informationen finden Sie unter Beispiele in Amazon VPC Transit Gateways.

Verbindungen

- Es gibt eine Quote für die Anzahl der aktiven und ausstehenden VPC-Peering-Verbindungen pro VPC. Weitere Informationen finden Sie unter Kontingente.
- Sie können nicht mehr als eine VPC-Peering-Verbindung zwischen denselben beiden VPCs gleichzeitig haben.
- Alle Tags, die Sie für Ihre VPC-Peering-Verbindung erstellen, werden nur für das Konto oder die Region angewendet, in dem bzw. der Sie sie erstellt haben.
- Sie können in einer Peer-VPC keine Verbindung zum Amazon DNS Server herstellen oder diesen abfragen.
- Wenn der IPv4-CIDR-Block einer VPC in einer VPC-Peering-Verbindung außerhalb der von RFC 1918 vorgegebenen IPv4-Adressbereiche liegt, können private DNS-Hostnamen für diese VPC nicht in private IP-Adressen aufgelöst werden. Um private DNS-Hostnamen in private IP-Adressen aufzulösen, können Sie eine Unterstützung der DNS-Auflösung für die VPC-Peering-Verbindung aktivieren. Weitere Informationen finden Sie unter Aktivieren einer DNS-Auflösungsunterstützung für eine VPC-Peering-Verbindung.
- Sie können Ressourcen auf beiden Seiten einer VPC-Peering-Verbindung aktivieren, um über IPv6 zu kommunizieren. Sie müssen einen IPv6-CIDR-Block mit jeder VPC verbinden, die Instances für die IPv6-Kommunikation in den VPCs aktivieren und Routen zu Ihren Routing-Tabellen hinzufügen, die IPv6-Verkehrsdaten senden, welche für Peer-VPC zur VPC-Peering-Verbindung vorgesehen sind.

- Unicast Reverse Path Forwarding wird für VPC-Peering-Verbindungen nicht unterstützt. Weitere Informationen finden Sie unter Routing für Antwortdatenverkehr.

Überlappende CIDR-Blöcke

- Sie können keine VPC-Peering-Verbindung zwischen VPCs erstellen, deren IPv4- oder IPv6-CIDR-Blöcke identisch sind oder sich überschneiden.
- Wenn Sie mehrere IPv4-CIDR-Blöcke haben, können Sie keine VPC-Peering-Verbindung einrichten, wenn sich CIDR-Blöcke überlappen, selbst wenn Sie nur die nicht überlappenden CIDR-Blöcke oder nur IPv6-CIDR-Blöcke verwenden wollen.

Transitives Peering

- Das VPC-Peering unterstützt keine transitiven Peering-Beziehungen. Wenn beispielsweise VPC-Peering-Verbindungen zwischen VPC A und VPC B sowie zwischen VPC A und VPC C bestehen, können Sie den Datenverkehr nicht über VPC A von VPC B zu VPC C weiterleiten. Um den Datenverkehr zwischen VPC B und VPC C weiterzuleiten, müssen Sie eine VPC-Peering-Verbindung zwischen ihnen einrichten. Weitere Informationen finden Sie unter Drei durch Peering verbundene VPCs.

Edge-to-Edge-Routing mithilfe eines Gateways oder einer privaten Verbindung

- Wenn VPC A über ein Internet-Gateway verfügt, können Ressourcen in VPC B das Internet-Gateway in VPC A nicht für den Zugriff auf das Internet verwenden.
- Wenn VPC A über ein NAT-Gerät verfügt, das Internet-Zugang zu Subnetzen in VPC A bietet, können Ressourcen in VPC B das NAT-Gerät in VPC A nicht verwenden, um auf das Internet zuzugreifen.
- Wenn VPC A über eine VPN-Verbindung zu einem Unternehmensnetzwerk verfügt, können Ressourcen in VPC B die VPN-Verbindung nicht für die Kommunikation mit dem Unternehmensnetzwerk verwenden.
- Wenn VPC A eine AWS Direct Connect Verbindung zu einem Unternehmensnetzwerk hat, können Ressourcen in VPC B die AWS Direct Connect Verbindung nicht für die Kommunikation mit dem Unternehmensnetzwerk verwenden.

- Wenn VPC A über einen Gateway-Endpunkt verfügt, der Verbindungen zu Amazon S3 zu privaten Subnetzen in VPC A bereitstellt, können Ressourcen in VPC B den Gateway-Endpunkt nicht für den Zugriff auf Amazon S3 verwenden.

VPC-Peering-Verbindungen zwischen Regionen

- Die Maximum Transmission Unit (MTU – maximale Übertragungseinheit) über die VPC-Peering-Verbindung über Regionen beträgt 1 500 Byte. Jumbo-Frames (MTUs bis zu 9 001 Byte) werden für regionsübergreifende VPC-Peering-Verbindungen nicht unterstützt. Sie werden jedoch für VPC-Peering-Verbindungen in derselben Region unterstützt. Weitere Informationen zu Jumbo Frames finden Sie unter Jumbo Frames (9001 MTU) im Amazon EC2 EC2-Benutzerhandbuch.
- Sie müssen den Support für DNS-Auflösung für die VPC-Peering-Verbindung aktivieren, um private DNS-Hostnamen der gleichrangingen VPC in private IP-Adressen aufzulösen, auch wenn die IPv4 CIDR für die VPC in den durch RFC 1918 festgelegten privaten IPv4-Adressebereichen liegen.

Gemeinsam genutzte VPCs und Subnetze

- Nur VPC-Besitzer können mit Peering-Verbindungen arbeiten (beschreiben, erstellen, akzeptieren, ablehnen, ändern oder löschen). Teilnehmer können nicht mit Peering-Verbindungen arbeiten. Weitere Informationen finden Sie unter Gemeinsames Verwenden Ihrer VPC mit anderen Konten im Amazon-VPC-Benutzerhandbuch.

Arbeiten mit VPC-Peering-Verbindungen

Nutzen Sie die folgenden Schritte zum Erstellen und Arbeiten mit VPC-Peering-Verbindungen.

Aufgaben

- Erstellen einer VPC-Peering-Verbindung
- Akzeptieren einer VPC-Peering-Verbindung
- Sie lehnen eine VPC-Peering-Verbindung ab
- So zeigen Sie Ihre VPC-Peering-Verbindungen an
- Aktualisieren Sie ihre Routing-Tabellen für eine VPC-Peering-Verbindung
- Aktualisieren Ihrer Sicherheitsgruppen, um auf Peer-Sicherheitsgruppen zu verweisen
- Ändern der Optionen für VPC-Peering-Verbindungen
- Sie löschen eine VPC-Peering-Verbindung
- Fehlerbehebung bei einer VPC-Peering-Verbindung

Erstellen einer VPC-Peering-Verbindung

Zum Erstellen einer VPC-Peering-Verbindung erstellen Sie zuerst eine Anforderung für ein Peering mit einer anderen VPC. Sie können eine VPC-Peering-Verbindung zu einer anderen VPC in Ihrem Konto anfordern oder zu einer VPC in einem anderen AWS-Konto. Für eine interregionale VPC-Peering-Verbindung, wobei sich die VPCs in unterschiedlichen Regionen befinden, müssen die Anfragen von der Region oder der VPC des Anforderers erfolgen.

Zur Aktivierung der Anforderung muss der Eigentümer der annehmenden VPC die Anforderung akzeptieren. Für eine interregionale VPC-Peering-Verbindung muss die Anfrage in der Region des VPC des Anforderers akzeptiert werden. Weitere Informationen finden Sie unter the section called “Accept”. Weitere Informationen zum `Pending acceptance`-Peering-Verbindungsstatus finden Sie unter Lebenszyklus einer VPC-Peering-Verbindung.

Aufgaben

- Voraussetzungen
- Mit VPCs in demselben Konto und derselben Region erstellen
- Erstellen mit VPCs in demselben Konto und unterschiedlichen Regionen
- Erstellen mit VPCs in unterschiedlichen Konten und derselben Region

- Erstellen mit VPCs in verschiedenen Konten und Regionen
- Erstellen einer VPC-Peering-Verbindung über die Befehlszeile

Voraussetzungen

- Überprüfen Sie die Einschränkungen und Regeln für VPC-Peering-Verbindungen.
- Achten Sie darauf, dass die VPCs keine sich überschneidenden IPv4-CIDR-Blöcke haben. Wenn sie sich überlappen, ändert sich der Status der VPC-Peering-Verbindung direkt in `failed`. Diese Einschränkung trifft auch dann zu, wenn die VPCs eindeutige IPv6 CIDR-Blöcke haben.

Mit VPCs in demselben Konto und derselben Region erstellen

So erstellen Sie eine VPC-Peering-Verbindung zu einer VPC in einem anderen Konto in derselben Region

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Peering connections (Peering-Verbindungen) aus.
3. Wählen Sie Create peering connection (Peering-Verbindung erstellen).
4. Konfigurieren Sie die folgenden Informationen und wählen Sie Peering-Verbindung erstellen aus, wenn Sie fertig sind:
   - Name: Sie können Ihrer VPC-Peering-Verbindung optional einen Namen geben.
   - VPC-ID (Anforderer):Wählen Sie die VPC in Ihrem Konto aus, mit der Sie eine VPC-Peering-Verbindung erstellen möchten.
   - Unter Wählen Sie eine weitere VPC für das Peering aus: Stellen Sie sicher, dass Mein Konto ausgewählt ist, und wählen Sie eine andere Ihrer VPCs aus.
   - (Optional) Um ein Tag hinzuzufügen, wählen Sie Add new tag (Neuen Tag hinzufügen) aus und geben Sie den Schlüssel und den Wert für den Tag ein.
5. Wählen Sie Aktionen, Anfrage akzeptieren.
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Akzeptieren aus.
7. Wählen Sie Meine Routing-Tabellen jetzt ändern, um der VPC-Routing-Tabelle eine Route hinzuzufügen, sodass Sie Traffic über die Peering-Verbindung senden und empfangen können. Weitere Informationen finden Sie unter Aktualisieren Sie ihre Routing-Tabellen für eine VPC-Peering-Verbindung.

Erstellen mit VPCs in demselben Konto und unterschiedlichen Regionen

Wie Sie eine VPC-Peering-Verbindung zu einer VPC im gleichen Konto in einer anderen Region erstellen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Peering connections (Peering-Verbindungen) aus.
3. Wählen Sie Create peering connection (Peering-Verbindung erstellen).
4. Konfigurieren Sie die folgenden Informationen und wählen Sie Peering-Verbindung erstellen aus, wenn Sie fertig sind:
   - Name: Sie können Ihrer VPC-Peering-Verbindung optional einen Namen geben. Auf diese Weise wird ein Tag mit dem Schlüssel `Name` und dem von Ihnen angegebenen Wert erstellt.
   - VPC-ID (Anforderer):Wählen Sie die VPC des Anforderers in Ihrem Konto aus, mit dem Sie die VPC-Peering-Verbindung anfordern.
   - Konto: Wählen Sie Mein Konto.
   - Region: Wählen Sie Andere Region und wählen Sie die Region für die akzeptierende VPC.
   - VPC ID (Akzeptierer): Wählen Sie die Akzeptierer-VPC aus.
5. Wählen Sie in der Regionsauswahl die Region der VPC des Annehmers aus.
6. Wählen Sie im Navigationsbereich Peering connections (Peering-Verbindungen) aus. Wählen Sie erst die VPC-Peering-Verbindung aus, die Sie erstellt haben, und dann Aktionen und Anforderung akzeptieren.
7. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Akzeptieren aus.
8. Wählen Sie Meine Routing-Tabellen jetzt ändern, um der VPC-Routing-Tabelle eine Route hinzuzufügen, sodass Sie Traffic über die Peering-Verbindung senden und empfangen können. Weitere Informationen finden Sie unter Aktualisieren Sie ihre Routing-Tabellen für eine VPC-Peering-Verbindung.

Erstellen mit VPCs in unterschiedlichen Konten und derselben Region

Wie Sie eine VPC-Peering-Verbindung zu einer VPC in unterschiedlichen Konten in der gleichen Region erstellen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Peering connections (Peering-Verbindungen) aus.

3. Wählen Sie Create peering connection (Peering-Verbindung erstellen).
4. Konfigurieren Sie die Informationen wie folgt und wählen Sie Peering-Verbindung erstellen aus, wenn Sie fertig sind:

   - Name: Sie können Ihrer VPC-Peering-Verbindung optional einen Namen geben. Auf diese Weise wird eine Markierung mit dem Schlüssel für `Name` und einem von Ihnen angegebenen Wert erstellt. Diese Markierung ist nur für Sie sichtbar; der Eigentümer der Peer-VPC kann seine eigenen Markierungen für die VPC-Peering-Verbindung erstellen.
   - VPC (Anforderer): Wählen Sie die VPC in Ihrem Konto aus, mit der Sie eine VPC-Peering-Verbindung erstellen möchten.
   - Account: Wählen Sie Another account.
   - Konto-ID: Geben Sie die ID des AWS-Konto des Eigentümers der VPC des Akzeptierers an.
   - VPC-ID (Akzeptierer): Geben Sie die ID der VPC ein, zu der Sie eine VPC-Peering-Verbindung erstellen möchten.

Erstellen mit VPCs in verschiedenen Konten und Regionen

Wie Sie eine VPC-Peering-Verbindung zu einer VPC in unterschiedlichen Konten in unterschiedlichen Regionen erstellen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Peering connections (Peering-Verbindungen) aus.
3. Wählen Sie Create peering connection (Peering-Verbindung erstellen).
4. Konfigurieren Sie die Informationen wie folgt und wählen Sie Peering-Verbindung erstellen aus, wenn Sie fertig sind:

   - Name: Sie können Ihrer VPC-Peering-Verbindung optional einen Namen geben. Auf diese Weise wird eine Markierung mit dem Schlüssel für `Name` und einem von Ihnen angegebenen Wert erstellt. Diese Markierung ist nur für Sie sichtbar; der Eigentümer der Peer-VPC kann seine eigenen Markierungen für die VPC-Peering-Verbindung erstellen.
   - VPC (Anforderer): Wählen Sie die VPC in Ihrem Konto aus, mit der Sie eine VPC-Peering-Verbindung erstellen möchten.
   - Account: Wählen Sie Another account.
   - Konto-ID: Geben Sie die ID des AWS-Konto des Eigentümers der VPC des Akzeptierers an.

- Region: Wählen Sie Andere Region und wählen Sie die Region, in der sich die VPC des Akzeptierers befindet.
- VPC-ID (Akzeptierer): Geben Sie die ID der VPC ein, zu der Sie eine VPC-Peering-Verbindung erstellen möchten.

Erstellen einer VPC-Peering-Verbindung über die Befehlszeile

Sie können eine VPC Peering-Verbindung erstellen, indem Sie die folgenden Befehle verwenden:

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

Akzeptieren einer VPC-Peering-Verbindung

Eine VPC-Peering-Verbindung, die den Status `pending-acceptance` hat, muss vom Eigentümer der annehmenden VPC akzeptiert werden, um aktiviert werden zu können. Weitere Informationen zum `Deleted`-Peering-Verbindungsstatus finden Sie unter Lebenszyklus einer VPC-Peering-Verbindung. Sie können keine Anforderung für eine VPC-Peering-Verbindung akzeptieren, die Sie an ein anderes AWS-Konto geschickt haben. Wenn Sie eine VPC-Peering-Verbindung im selben AWS-Konto erstellen, müssen Sie diese Anforderung selbst erstellen und akzeptieren.

Wenn sich die VPCs in unterschiedlichen Regionen befinden, muss die Anfrage in der Region des VPC des Anforderers akzeptiert werden.

> **Important**
>
> Akzeptieren Sie keine VPC-Peering-Verbindungen von unbekannten AWS-Konten. Ein böswilliger Benutzer hat Ihnen möglicherweise eine Anforderung für eine VPC-Peering-Verbindung geschickt, um auf diese Weise unberechtigten Netzwerkzugriff auf Ihre VPC zu erhalten. Dies wird als Peer-Phishing bezeichnet. Sie können unerwünschte Anforderungen für VPC-Peering-Verbindungen unbesorgt ablehnen, ohne befürchten zu müssen, dass der Anforderer Zugriff auf Informationen zu Ihrem AWS-Konto oder zu Ihrer VPC erhält. Weitere Informationen finden Sie unter Sie lehnen eine VPC-Peering-Verbindung ab. Sie können eine solche Anforderung auch ignorieren und sie verfallen lassen; standardmäßig verfallen Anforderungen nach sieben Tagen.

Nachdem Sie die VPC-Peering-Verbindung akzeptiert haben, müssen Sie einen Eintrag zu Ihren Routing-Tabellen hinzufügen, um den Verkehr zwischen den über Peering verbundenen VPCs zu ermöglichen. Weitere Informationen finden Sie unter Aktualisieren Sie ihre Routing-Tabellen für eine VPC-Peering-Verbindung.

So akzeptieren Sie eine VPC-Peering-Verbindung

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie in der Regionsauswahl die Region der VPC des Annehmers aus.
3. Wählen Sie im Navigationsbereich Peering connections (Peering-Verbindungen) aus.
4. Wählen Sie erst die ausstehende VPC-Peering-Verbindung (der Status lautet `pending-acceptance`) und dann Aktionen und Anforderung akzeptieren aus. Weitere Informationen zum Lebenszyklusstatus von Peering-Verbindungen finden Sie unter Lebenszyklus einer VPC-Peering-Verbindung.

   > **Tip**
   >
   > Wenn Sie die ausstehende VPC-Peering-Verbindung nicht sehen, überprüfen Sie die Region. Eine interregionale VPC-Peering-Anfrage muss in der Region des VPC des Anforderers akzeptiert werden.

5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Akzeptieren aus.
6. Wählen Sie Meine Routing-Tabellen jetzt ändern, um der VPC-Routing-Tabelle eine Route hinzuzufügen, sodass Sie Traffic über die Peering-Verbindung senden und empfangen können. Weitere Informationen finden Sie unter Aktualisieren Sie ihre Routing-Tabellen für eine VPC-Peering-Verbindung.

Akzeptieren einer VPC-Peering-Verbindung über die Befehlszeile oder eine API

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

Sie lehnen eine VPC-Peering-Verbindung ab

Sie können jede Anforderung für eine VPC-Peering-Verbindung ablehnen, die Sie erhalten haben, wenn diese sich im Status `pending-acceptance` befindet. Sie sollten nur VPC-Peering-Verbindungen von AWS-Konten akzeptieren, die Sie kennen und denen Sie vertrauen; Sie können jede unerwünschte Anforderungen ablehnen. Weitere Informationen zum `Rejected`-Peering-Verbindungsstatus finden Sie unter Lebenszyklus einer VPC-Peering-Verbindung.

So lehnen Sie eine VPC-Peering-Verbindung ab

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Peering connections (Peering-Verbindungen) aus.
3. Wählen Sie die VPC-Peering-Verbindung aus und klicken Sie auf Aktionen und Anforderung ablehnen.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Anforderung ablehnen aus.

Ablehnen einer VPC-Peering-Verbindung über die Befehlszeile oder eine API

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

So zeigen Sie Ihre VPC-Peering-Verbindungen an

Sie können Ihre gesamten VPC-Peering-Verbindungen in der Amazon VPC-Konsole anzeigen. Standardmäßig zeigt die Konsole alle VPC-Peering-Verbindungen in unterschiedlichen Status an, einschließlich derjenigen, die kürzlich gelöscht oder abgelehnt wurden. Weitere Informationen zum Lebenszyklus einer VPC-Peering-Verbindung finden Sie unter Lebenszyklus einer VPC-Peering-Verbindung.

So zeigen Sie Ihre VPC-Peering-Verbindungen an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Peering connections (Peering-Verbindungen) aus.
3. Alle Ihre VPC-Peering-Verbindungen werden aufgelistet. Grenzen Sie die Ergebnisse mithilfe der Filtersuchleiste ein.

Beschreiben einer VPC-Peering-Verbindung über die Befehlszeile oder eine API

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

Aktualisieren Sie ihre Routing-Tabellen für eine VPC-Peering-Verbindung

Um privaten IPv4-Verkehr zwischen Instances in Peer-VPCs zu ermöglichen, müssen Sie eine Route zu den Routing-Tabellen hinzufügen, die mit den Subnetzen für beide Instances verbunden sind. Das Ziel der Route ist der CIDR-Block (oder ein Teil des CIDR-Blocks) des Peer-VPC und das Ziel ist die ID der VPC-Peering-Verbindung. Weitere Informationen finden Sie unter Konfigurieren von Routing-Tabellen im Benutzerhandbuch zu Amazon VPC.

Im Folgenden finden Sie ein Beispiel für die Routing-Tabellen, die die Kommunikation zwischen Instances in zwei Peer-VPCs, VPC A und VPC B, ermöglichen. Jede Tabelle enthält eine lokale Route und eine Route, die den Datenverkehr für die Peer-VPC an die VPC-Peering-Verbindung sendet.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-*11112222*
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-*11112222*

Ebenso können Sie, wenn den VPCs in der VPC-Peering-Verbindung IPv6-CIDR-Blöcke zugewiesen sind, Routen hinzufügen, die die Kommunikation mit dem Peer-VPC über IPv6 ermöglichen.

Weitere Informationen zu den unterstützten Routing-Tabellen-Konfigurationen für VPC-Peering-Verbindungen finden Sie unter VPC-Peering-Konfigurationen.

Überlegungen

- Wenn Sie eine VPC über ein Peering mit mehreren VPCs verbinden, die sich überschneidende oder sich entsprechende IPv4-CIDR-Blöcke haben, achten Sie darauf, dass Ihre Routing-Tabellen so konfiguriert sind, dass kein Antwortdatenverkehr von Ihrer VPC an die falsche VPC gesendet wird. AWS unterstützt derzeit kein Unicast Reverse Path Forwarding in VPC-Peering-Verbindungen, das die Quell-IP von Paketen prüft und Antwortpakete zurück zur Quelle leitet. Weitere Informationen finden Sie unter Routing für Antwortdatenverkehr.
- Ihr Konto verfügt über ein Kontingent für die Anzahl der Einträge, die Sie pro Routing-Tabelle hinzufügen können. Wenn die Anzahl der VPC-Peering-Verbindungen in Ihrer VPC das Eintragskontingent für eine einzelne Routing-Tabelle überschreitet, sollten Sie in Betracht ziehen, mehrere Subnetze zu verwenden, die jeweils einer benutzerdefinierten Routing-Tabelle zugewiesen sind.
- Sie können eine Route für eine VPC-Peering-Verbindung hinzufügen, die sich im Status `pending-acceptance` befindet. Die Route hat jedoch den Status `blackhole` und wird erst wirksam, wenn die VPC-Peering-Verbindung den Status `active` erhält.

So fügen Sie einer VPC-Peering-Verbindung eine IPv4-Route hinzu

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Wählen Sie das Kontrollkästchen neben der Routing-Tabelle aus, die dem Subnetz zugewiesen ist, in dem sich Ihre Instance befindet.

   Sofern Sie einem Subnetz nicht explizit eine bestimmte Routing-Tabelle zuordnen, wird die Haupt-Routing-Tabelle für die VPC implizit mit dem Subnetz verknüpft.
4. Wählen Sie Actions (Aktionen) und dann Edit routes (Routen bearbeiten).
5. Wählen Sie Add Route (Route hinzufügen) aus.
6. Geben Sie bei Destination den IPv4-Adressbereich ein, an den der Netzwerkdatenverkehr in der VPC-Peering-Verbindung weitergeleitet werden soll. Sie können den gesamten IPv4-CIDR-Block der Peer-VPC angeben, einen spezifischen Bereich oder eine individuelle IPv4-Adresse, wie die IP-Adresse der Instance, mit der die Kommunikation erfolgen soll. Wenn z. B. der CIDR-Block der Peer-VPC `10.0.0.0/16` ist, können Sie einen Teilbereich `10.0.0.0/24` oder eine konkrete IP-Adresse `10.0.0.7/32` angeben.
7. Wählen Sie als Ziel die VPC-Peering-Verbindung aus.

8. Wählen Sie Save Changes.

Der Besitzer der Peer-VPC muss diese Schritte auch ausführen, um eine Route für die Zurückleitung des Datenverkehrs über die VPC-Peering-Verbindung hinzuzufügen.

Wenn Sie Ressourcen in verschiedenen AWS-Regionen haben, die IPv6-Adressen verwenden, können Sie eine Peering-Verbindung zwischen den Regionen erstellen. Sie können dann eine IPv6-Route für die Kommunikation zwischen den Ressourcen hinzufügen.

So fügen Sie einer VPC-Peering-Verbindung eine IPv6-Route hinzu

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Wählen Sie das Kontrollkästchen neben der Routing-Tabelle aus, die dem Subnetz zugewiesen ist, in dem sich Ihre Instance befindet.

   > **Note**
   >
   > Wenn diesem Subnetz keine Routing-Tabelle zugewiesen ist, wählen Sie die Haupt-Routing-Tabelle für die VPC aus, da das Subnetz diese Routing-Tabelle dann standardmäßig verwendet.

4. Wählen Sie Actions (Aktionen) und dann Edit routes (Routen bearbeiten).
5. Wählen Sie Add Route (Route hinzufügen) aus.
6. Geben Sie unter Destination den IPv6-Adressbereich für die Peer-VPC ein. Sie können den gesamten IPv6 CIDR-Block der Peer-VPC angeben, einen konkreten Bereich oder eine individuelle IPv6-Adresse. Wenn z. B. der CIDR-Block der Peer-VPC `2001:db8:1234:1a00::/56` ist, können Sie einen Teilbereich `2001:db8:1234:1a00::/64` oder eine konkrete IP-Adresse `2001:db8:1234:1a00::123/128` angeben.
7. Wählen Sie als Ziel die VPC-Peering-Verbindung aus.
8. Wählen Sie Save Changes.

Weitere Informationen finden Sie unter Routing-Tabellen im Amazon VPC-Benutzerhandbuch.

Löschen oder Ersetzen einer Route über die Befehlszeile oder eine API

- create-route (AWS CLI)

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

Aktualisieren Ihrer Sicherheitsgruppen, um auf Peer-Sicherheitsgruppen zu verweisen

Sie können die eingehenden oder ausgehenden Regeln für die VPC-Sicherheitsgruppen aktualisieren, um auf Sicherheitsgruppen in der über Peering verbundenen VPC zu verweisen. Danach kann der Datenverkehr von und zu den Instances fließen, die der referenzierten Sicherheitsgruppe in der über Peering verbundenen VPC zugewiesen sind.

Voraussetzungen

- Die Peer-VPC kann eine VPC in Ihrem Konto oder in einem anderen AWS-Konto sein. Um auf eine Sicherheitsgruppe in einem anderen AWS-Konto zu verweisen, schließen Sie im Feld Source (Quelle) oder Destination (Ziel) die Kontonummer ein, z. B. `123456789012/sg-1a2b3c4d`.
- Sie können nicht auf die Sicherheitsgruppe einer Peer-VPC in einer anderen Region verweisen. Verwenden Sie stattdessen den CIDR-Block der Peer-VPC.
- Um auf eine Sicherheitsgruppe in einer Peer-VPC zu verweisen, muss die VPC-Peering-Verbindung den Status `active` haben.
- Wenn Sie Routen konfigurieren, um den Datenverkehr zwischen zwei Instances in unterschiedlichen Subnetzen über eine Middlebox-Appliance weiterzuleiten, müssen Sie sicherstellen, dass die Sicherheitsgruppen für beide Instances den Datenverkehr zwischen den Instances zulassen. Die Sicherheitsgruppe für jede Instance muss die private IP-Adresse der anderen Instance oder den CIDR-Bereich des Subnetzes, das die andere Instance enthält, als Quelle referenzieren. Wenn Sie die Sicherheitsgruppe der anderen Instance als Quelle referenzieren, wird dadurch kein Datenverkehr zwischen den Instances möglich.

So aktualisieren Sie Ihre Sicherheitsgruppenregeln mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.

3. Markieren Sie die Sicherheitsgruppe und wählen Sie Aktionen, Eingehende Regeln bearbeiten, um die eingehenden Regeln zu ändern, oder wählen Sie Aktionen, Ausgehende Regeln bearbeiten, um die ausgehenden Regeln zu ändern.
4. Um eine Regel hinzuzufügen, wählen Sie Regel hinzufügen und geben Sie bei Bedarf den Typ, das Protokoll und den Portbereich an. Geben Sie für Quelle (eingehende Regel) oder Ziel (ausgehende Regel) die ID der Sicherheitsgruppe in der Peer-VPC ein, falls sie sich in derselben Region befindet, oder den CIDR-Block der Peer-VPC, falls sie sich in einer anderen Region befindet.

   > **Note**
   >
   > Sicherheitsgruppen in einer Peer-VPC werden nicht automatisch angezeigt.

5. Um eine bestehende Regel zu bearbeiten, ändern Sie ihre Werte (z. B. die Quelle oder die Beschreibung).
6. Um eine Regel zu löschen, wählen Sie die Schaltfläche Löschen neben der Regel.
7. Wählen Sie Save rules (Regeln speichern) aus.

So aktualisieren Sie Regeln für eingehenden Datenverkehr über die Befehlszeile

- 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)

So aktualisieren Sie Regeln für ausgehenden Datenverkehr über die Befehlszeile

- 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)

Sie können beispielsweise den folgenden `sg-aaaa1111`-Befehl verwenden, um Ihre Sicherheitsgruppe `sg-bbbb2222` zu aktualisieren, damit sie eingehenden Datenverkehr über HTTP von AWS CLI aus einer Peer-VPC zulässt:

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

Verwenden Sie nach dem Aktualisieren der Sicherheitsgruppe den Befehl describe-security-groups, um die referenzierte Sicherheitsgruppe in Ihren Sicherheitsgruppenregeln anzuzeigen.

Identifizieren der referenzierten Sicherheitsgruppen

Verwenden Sie einen der folgenden Befehle für eine oder mehrere Sicherheitsgruppen in Ihrem Konto, um festzustellen, ob in den Sicherheitsgruppenregeln in einer Peer-VPC auf Ihre Sicherheitsgruppe verwiesen wird.

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)
- DescribeSecurityGroupReferences (Amazon EC2-Abfrage-API)

Im folgenden Beispiel zeigt die Antwort, dass von einer Sicherheitsgruppe in der VPC `sg-bbbb2222` auf die Sicherheitsgruppe `vpc-aaaaaaaa` verwiesen wird:

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

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

Wenn die VPC-Peering-Verbindung gelöscht wird oder der Eigentümer der Peer-VPC die referenzierte Sicherheitsgruppe löscht, ist die Sicherheitsgruppenregel veraltet.

Arbeiten mit veralteten Sicherheitsgruppenregeln

Eine veraltete Sicherheitsgruppenregel ist eine Regel, die auf eine gelöschte Sicherheitsgruppe in derselben VPC oder in einer Peer-VPC oder auf eine Sicherheitsgruppe in einer Peer-VPC verweist,

für die die VPC-Peering-Verbindung gelöscht wurde. Wenn eine Sicherheitsgruppenregel veraltet ist, wird sie nicht automatisch aus der Sicherheitsgruppe entfernt – Sie müssen Sie manuell entfernen. Wenn eine Sicherheitsgruppenregel veraltet ist, weil die VPC-Peering-Verbindung gelöscht wurde, wird diese Regel dann nicht mehr als veraltet gekennzeichnet, wenn Sie eine neue VPC-Peering-Verbindung mit denselben VPCs erstellen.

Sie können die veralteten Sicherheitsgruppenregeln einer VPC mit der Amazon VPC-Konsole anzeigen und löschen.

So zeigen Sie veraltete Sicherheitsgruppenregeln an und löschen sie

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Security groups (Sicherheitsgruppen) aus.
3. Klicken Sie auf Actions (Aktionen), Manage stale rules (Verwalten veraltter Regeln).
4. Wählen Sie unter VPC die VPC mit den veraltbaren Regeln aus.
5. Wählen Sie Edit (Bearbeiten) aus.
6. Wählen Sie die Schaltfläche Löschen neben der Regel, die Sie löschen möchten. Wählen Sie Preview changes (Änderungen überprüfen), Save rules (Regeln speichern).

Beschreiben veralteter Sicherheitsgruppenregeln über die Befehlszeile oder eine API

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

Im folgenden Beispiel wurden VPC A (`vpc-aaaaaaaa`) und VPC B durch Peering verbunden und die VPC-Peering-Verbindung wurde gelöscht. Die Sicherheitsgruppe `sg-aaaa1111` in VPC A verweist auf `sg-bbbb2222` in VPC B. Wenn Sie den Befehl `describe-stale-security-groups` für Ihre VPC ausführen, weist die Antwort darauf hin, dass die Sicherheitsgruppe `sg-aaaa1111` eine veraltete SSH-Regel aufweist, die auf `sg-bbbb2222` verweist.

```
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"
        }
    ]
}
```

Wenn Sie die veralteten Sicherheitsgruppenregeln identifiziert haben, können Sie diese mithilfe des Befehls revoke-security-group-ingress oder revoke-security-group-egress löschen.

Ändern der Optionen für VPC-Peering-Verbindungen

Sie können eine VPC-Peering-Verbindung so ändern, dass Sie folgende Aktionen ausführt:

- Aktivieren Sie eine VPC, um die öffentlichen IPv4 DNS-Hostnamen in private IPv4-Adressen aufzulösen, wenn dies von Instances in der Peer-VPC angefordert wird. Weitere Informationen finden Sie unter Aktivieren einer DNS-Auflösungsunterstützung für eine VPC-Peering-Verbindung.

Aktivieren einer DNS-Auflösungsunterstützung für eine VPC-Peering-Verbindung

Um eine VPC zu aktivieren, damit sie öffentliche IPv4 DNS-Hostnamen in private IPv4-Adressen auflöst, wenn dies von Instances in der Peer-VPC angefordert wird, müssen Sie die vorhandene Peering-Verbindung ändern.

Beide VPCs müssen für DNS-Hostnamen und DNS-Auflösung aktiviert sein.

Sie können die Unterstützung der DNS-Auflösung nicht aktivieren, wenn Sie eine neue Peering-Verbindung erstellen. Sie können die Unterstützung der DNS-Auflösung für eine vorhandene Peering-Verbindung aktivieren, die sich im Status `active` befindet.

Aktivieren einer DNS-Auflösung für eine Peering-Verbindung

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Peering connections (Peering-Verbindungen) aus.
3. Wählen Sie erst die VPC-Peering-Verbindung und dann Aktionen und DNS-Einstellungen bearbeiten aus.
4. Um sicherzustellen, dass Abfragen aus der Peer-VPC in private IP-Adressen in Ihrer lokalen VPC aufgelöst werden, wählen Sie die Option zur Aktivierung der DNS-Auflösung für Abfragen aus der Peer-VPC aus. Diese Option ist Requester DNS resolution (DNS-Auflösung des Anforderers) oder Accepter DNS resolution (DNS-Auflösung des Annehmers), je nachdem, ob die VPC die Anforderer- oder Annehmer-VPC ist.
5. Wenn sich die Peer-VPC im selben AWS-Konto befindet, können Sie die DNS-Auflösung für beide VPCs in der Peering-Verbindung aktivieren.
6. Wählen Sie Save Changes.
7. Befindet sich die Peer-VPC in einem anderen AWS oder einer anderen Region, muss der Eigentümer der Peer-VPC sich an der VPC-Konsole anmelden, die Schritte 2 bis 4 ausführen und dann die Option Speichern auswählen.

So aktivieren Sie eine DNS-Auflösung über die Befehlszeile oder eine API

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

Sie müssen die VPC-Peering-Optionen des Auftraggebers ändern, wenn Sie der Auftraggeber der VPC-Peering-Verbindung sind, und Sie müssen die VPC-Peering-Optionen des Annehmenden ändern, wenn Sie der Annehmende der VPC-Peering-Verbindung sind. Sie können den Befehl describe-vpc-peering-connections oder Get-EC2VpcPeeringConnections verwenden, um zu überprüfen, welche VPC der Akzeptierende und welche der Anfordernde der VPC-Peering-Verbindung ist. Für regionsübergreifende Peering-Verbindungen müssen Sie die Region für die VPC des Anforderers verwenden, um die VPC-Peering-Optionen des Anforderers zu ändern, und die Region für die VPC des Annehmenden, um die VPC-Peering-Optionen des Annehmenden zu ändern.

In diesem Beispiel sind Sie der Auftraggeber der VPC-Peering-Verbindung, daher müssen Sie die Optionen der Peering-Verbindung mithilfe von AWS CLI folgendermaßen ändern:

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

Sie löschen eine VPC-Peering-Verbindung

Beide VPC-Eigentümer in einer Peering-Verbindung können die VPC-Peering-Verbindung jederzeit löschen. Sie können auch eine VPC-Peering-Verbindung ablehnen, die Sie angefordert haben und die sich noch immer im Status `pending-acceptance` befindet.

Sie können die VPC-Peering-Verbindung nicht löschen, wenn die VPC-Peering-Verbindung den Status `rejected` hat. Die Verbindung wird von uns automatisch für Sie gelöscht.

Wenn Sie eine VPC in der Amazon VPC-Konsole löschen, die Teil einer aktiven VPC-Peering-Verbindung ist, wird auch die VPC-Peering-Verbindung gelöscht. Wenn Sie eine VPC-Peering-Verbindung zu einer VPC in einem anderen Konto angefordert haben und Sie Ihre VPC löschen, bevor die andere Seite die Anforderung akzeptiert hat, wird die VPC-Peering-Verbindung ebenfalls gelöscht. Sie können eine VPC, für die Sie eine Anforderung mit dem Status `pending-acceptance` aus einer VPC in einem anderen Konto vorliegen haben, nicht löschen. Sie müssen zunächst die Anforderung für die VPC-Peering-Verbindung ablehnen.

Wenn Sie eine Peering-Verbindung löschen, wird der Status auf `Deleting` und dann auf `Deleted` gesetzt. Nachdem Sie eine Verbindung gelöscht haben, kann diese nicht angenommen, abgewiesen oder bearbeitet werden. Weitere Informationen zur Dauer der Sichtbarkeit der Peering-Verbindung finden Sie unter Lebenszyklus einer VPC-Peering-Verbindung.

So löschen Sie eine VPC-Peering-Verbindung

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Peering connections (Peering-Verbindungen) aus.
3. Wählen Sie die VPC-Peering-Verbindung aus.
4. Wählen Sie Actions (Aktionen), Delete peering connection (Peering-Verbindung löschen) aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.

So löschen Sie eine VPC-Peering-Verbindung über die Befehlszeile oder eine API

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

Fehlerbehebung bei einer VPC-Peering-Verbindung

Wenn Sie Probleme haben, von einer Ressource in einer Peer-VPC aus eine Verbindung zu einer Ressource in einer VPC herzustellen, gehen Sie wie folgt vor:

- Stellen Sie für jede Ressource in jeder VPC sicher, dass die Routing-Tabelle für ihr Subnetz eine Route enthält, die den für die Peer-VPC bestimmten Datenverkehr an die VPC-Peering-Verbindung sendet. Weitere Informationen finden Sie unter Aktualisieren von Routing-Tabellen.
- Stellen Sie bei EC2-Instances sicher, dass die Sicherheitsgruppen für die EC2-Instances Datenverkehr von der Peer-VPC zulassen. Weitere Informationen finden Sie unter Auf Peer-Sicherheitsgruppen verweisen.
- Stellen Sie für jede Ressource in jeder VPC sicher, dass die Netzwerk-ACL für ihr Subnetz den Datenverkehr von der Peer-VPC zulässt.

Sie können Reachability Analyzer auch verwenden, um die Komponente mit einem Konfigurationsproblem zu identifizieren, z. B. einer Routing-Tabelle, einer Sicherheitsgruppe oder einer Netzwerk-ACL. Weitere Informationen finden Sie im Leitfaden Reachability Analyzer.

VPC-Peering-Konfigurationen

Die folgende Dokumentation beschreibt die unterstützten VPC-Peering-Konfigurationen.

Konfigurationen

- VPC-Peering-Konfigurationen mit Routen zu einer gesamten VPC
- VPC-Peering-Konfigurationen mit spezifischen Routen

VPC-Peering-Konfigurationen mit Routen zu einer gesamten VPC

Sie können VPC-Peering-Verbindungen konfigurieren, sodass Ihre Routing-Tabellen auf den gesamten CIDR-Block der Peer-VPC Zugriff haben. Weitere Informationen zu Szenarien, in denen Sie eine spezifische VPC-Peering-Verbindungskonfiguration benötigen, finden Sie unter VPC Peering-Szenarien. Weitere Informationen zum Erstellen von und zum Arbeiten mit VPC-Peering-Verbindungen finden Sie unter Arbeiten mit VPC-Peering-Verbindungen.

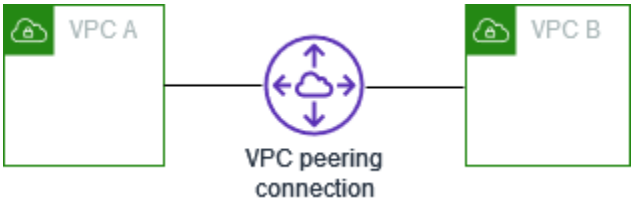
Weitere Informationen zur Aktualisierung Ihrer Routing-Tabellen finden Sie unter Aktualisieren Sie ihre Routing-Tabellen für eine VPC-Peering-Verbindung.

Konfigurationen

- Zwei durch Peering verbundene VPCs
- Eine VPC, die mit zwei VPCs durch Peering verbunden ist
- Drei durch Peering verbundene VPCs
- Mehrere durch Peering verbundene VPCs

Zwei durch Peering verbundene VPCs

In dieser Konfiguration besteht eine Peering-Verbindung zwischen VPC A und VPC B (`pcx-11112222`). Die VPCs befinden sich im selben AWS-Konto und haben keine sich überschneidenden CIDR-Blöcke.



Sie können diese Konfiguration verwenden, wenn Sie zwei VPCs haben, die Zugriff auf die Ressourcen der jeweils anderen benötigen. Sie richten beispielsweise VPC A für die Buchhaltungssätze ein und VPC B für die Finanzdaten, wobei jede VPC uneingeschränkten Zugriff auf die Ressourcen der anderen haben soll.

Einzelnes VPC-CIDR

Aktualisieren Sie die Routing-Tabelle für jede VPC mit einer Route, die den Datenverkehr für den CIDR-Block der Peer-VPC an die VPC-Peering-Verbindung sendet.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-11112222
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-11112222

Mehrere IPv4-VPC-CIDRs

Wenn VPC A und VPC B über mehrere zugeordnete IPv4-CIDR-Blöcke verfügen, können Sie die Routing-Tabelle für jede VPC mit Routen für einige oder alle IPv4-CIDR-Blöcke der Peer-VPC aktualisieren.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC-A-CIDR 1*	Local
	VPC-A-CIDR 2	Local
	VPC-B-CIDR 1	pcx-11112222
	VPC-B-CIDR 2	pcx-11112222
VPC B	*VPC-B-CIDR 1*	Local
	VPC-B-CIDR 2	Local

Routing-Tabelle	Zielbereich	Ziel
	VPC-A-CIDR 1	pcx-11112222
	VPC-A-CIDR 2	pcx-11112222

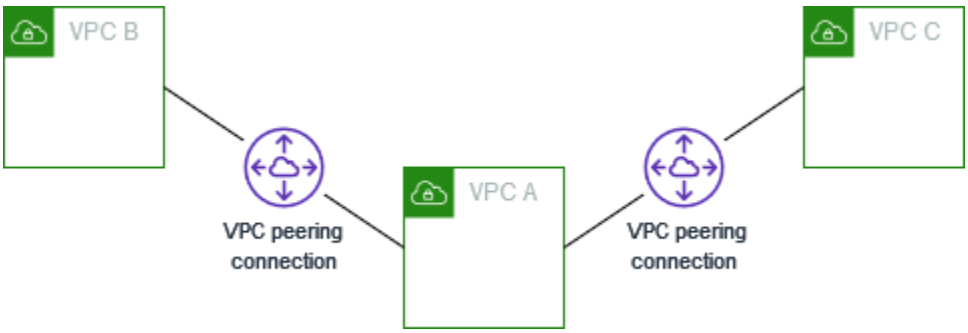
IPv4- und IPv6-VPC-CIDRs

Wenn VPC A und VPC B über mehrere zugeordnete IPv6-CIDR-Blöcke verfügen, können Sie die Routing-Tabelle für jede VPC mit Routen für einige oder alle IPv4- und IPv6-CIDR-Blöcke der Peer-VPC aktualisieren.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC-A-IPv4-CIDR*	Local
	VPC-A-IPv6-CIDR	Local
	VPC-B-IPv4-CIDR	pcx-11112222
	VPC-B-IPv6-CIDR	pcx-11112222
VPC B	*VPC-B-IPv4-CIDR*	Local
	VPC-B-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-11112222
	VPC-A-IPv6-CIDR	pcx-11112222

Eine VPC, die mit zwei VPCs durch Peering verbunden ist

Die Konfiguration enthält eine zentrale VPC (VPC A), eine Peering-Verbindung zwischen VPC A und VPC B (`pcx-12121212`) und eine Peering-Verbindung zwischen VPC A und VPC C (`pcx-23232323`). Alle drei VPCs befinden sich im selben AWS-Konto und haben keine sich überschneidenden CIDR-Blöcke.



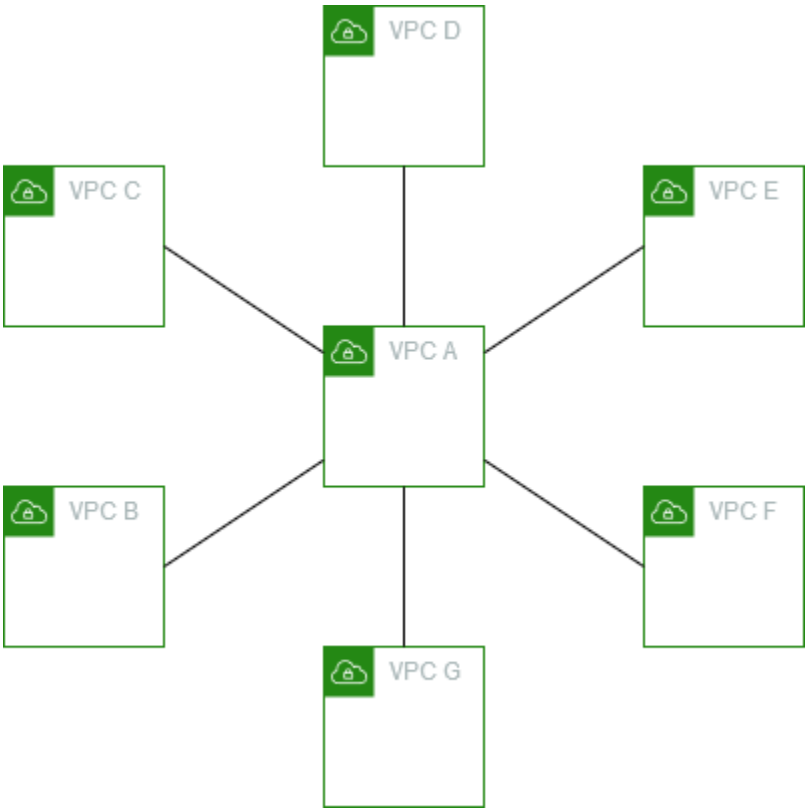
VPC B und VPC C können ihren Datenverkehr nicht direkt über VPC A aneinander senden, da VPC-Peering keine transitiven Peering-Beziehungen unterstützt. Sie können eine VPC-Peering-Verbindung zwischen VPC B und VPC C erstellen, wie in Drei durch Peering verbundene VPCs gezeigt. Weitere Informationen zu nicht unterstützten Peering-Szenarien finden Sie unter the section called “VPC Peering-Einschränkungen”.

Sie können diese Konfiguration verwenden, wenn Sie Ressourcen auf einer zentralen VPC haben, wie beispielsweise ein Repository von Services, auf die andere VPCs zugreifen müssen. Die anderen VPCs müssen nicht gegenseitig auf ihre Ressourcen zugreifen; sie brauchen nur auf die Ressourcen der zentralen VPC zuzugreifen.

Aktualisieren Sie die Routing-Tabelle für jede VPC wie folgt, um diese Konfiguration mit einem CIDR-Block pro VPC zu implementieren.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-12121212
	VPC C CIDR	pcx-23232323
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-12121212
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-23232323

Sie können diese Konfiguration auf zusätzliche VPCs erweitern. Beispielsweise ist VPC A durch Peering mit VPC B über VPC G verbunden, wobei sowohl IPv4- als auch IPv6-CIDRs verwendet werden, aber die anderen VPCs sind nicht untereinander verbunden. In diesem Diagramm stellen die Linien VPC-Peering-Verbindungen dar.



Aktualisieren Sie die Routing-Tabelle wie folgt.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC-A-IPv4-CIDR*	Local
	VPC-A-IPv6-CIDR	Local
	VPC-B-IPv4-CIDR	pcx-aaaabbbb
	VPC-B-IPv6-CIDR	pcx-aaaabbbb
	VPC-C-IPv4-CIDR	pcx-aaaacccc
	VPC-C-IPv6-CIDR	pcx-aaaacccc

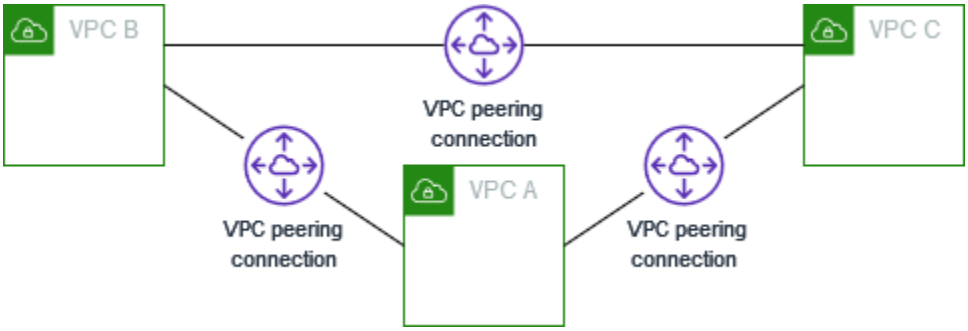
Routing-Tabelle	Zielbereich	Ziel
	VPC-D-IPv4-CIDR	pcx-aaaadddd
	VPC-D-IPv6-CIDR	pcx-aaaadddd
	VPC-E-IPv4-CIDR	pcx-aaaaeeee
	VPC-E-IPv6-CIDR	pcx-aaaaeeee
	VPC-F-IPv4-CIDR	pcx-aaaaffff
	VPC-F-IPv6-CIDR	pcx-aaaaffff
	VPC-G-IPv4-CIDR	pcx-aaaagggg
	VPC-G-IPv6-CIDR	pcx-aaaagggg
VPC B	*VPC-B-IPv4-CIDR*	Local
	VPC-B-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaabbbb
	VPC-A-IPv6-CIDR	pcx-aaaabbbb
VPC C	*VPC-C-IPv4-CIDR*	Local
	VPC-C-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaacccc
	VPC-A-IPv6-CIDR	pcx-aaaacccc
VPC D	*VPC-D-IPv4-CIDR*	Local
	VPC-D-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaadddd
	VPC-A-IPv6-CIDR	pcx-aaaadddd

Routing-Tabelle	Zielbereich	Ziel
VPC E	*VPC-E-IPv4-CIDR*	Local
	VPC-E-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaaeeee
	VPC-A-IPv6-CIDR	pcx-aaaaeeee
VPC F	*VPC-F-IPv4-CIDR*	Local
	VPC-F-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaaffff
	VPC-A-IPv6-CIDR	pcx-aaaaffff
VPC G	*VPC-G-IPv4-CIDR*	Local
	VPC-G-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaagggg
	VPC-A-IPv6-CIDR	pcx-aaaagggg

Drei durch Peering verbundene VPCs

In dieser Konfiguration befinden sich drei VPCs im selben AWS-Konto mit CIDR-Blöcken, die sich nicht überschneiden. Die VPCs werden in einem vollständigen Mesh wie folgt gepeert:

- VPC A ist über eine VPC-Peering-Verbindung mit VPC B verbunden `pcx-aaaabbbb`
- VPC A ist über eine VPC-Peering-Verbindung mit VPC C verbunden `pcx-aaaacccc`
- VPC B ist über eine VPC-Peering-Verbindung mit VPC C verbunden `pcx-bbbbcccc`



Sie können diese Konfiguration verwenden, wenn Sie VPCs haben, die Ressourcen ohne Einschränkungen miteinander teilen müssen. Zum Beispiel als Filesharing-System.

Aktualisieren Sie die Routing-Tabelle für jede VPC wie folgt, um diese Konfiguration zu implementieren.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-bbbbcccc
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc

Wenn VPC A und VPC B sowohl IPv4- als auch IPv6-CIDR-Blöcke haben, VPC C jedoch keinen IPv6-CIDR-Block hat, aktualisieren Sie die Routing-Tabellen wie folgt. Ressourcen in VPC A und VPC B können mit IPv6 über die VPC-Peering-Verbindung kommunizieren. VPC C kann jedoch weder mit VPC A noch mit VPC B über IPv6 kommunizieren.

Routing-Tabellen	Ziel	Ziel
VPC A	*VPC-A-IPv4-CIDR*	Local
	VPC-A-IPv6-CIDR	Local
	VPC-B-IPv4-CIDR	pcx-aaaabbbb
	VPC-B-IPv6-CIDR	pcx-aaaabbbb
	VPC-C-IPv4-CIDR	pcx-aaaacccc
VPC B	*VPC-B-IPv4-CIDR*	Local
	VPC-B-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaabbbb
	VPC-A-IPv6-CIDR	pcx-aaaabbbb
	VPC-C-IPv4-CIDR	pcx-bbbbcccc
VPC C	*VPC-C-IPv4-CIDR*	Local
	VPC-A-IPv4-CIDR	pcx-aaaacccc
	VPC-B-IPv4-CIDR	pcx-bbbbcccc

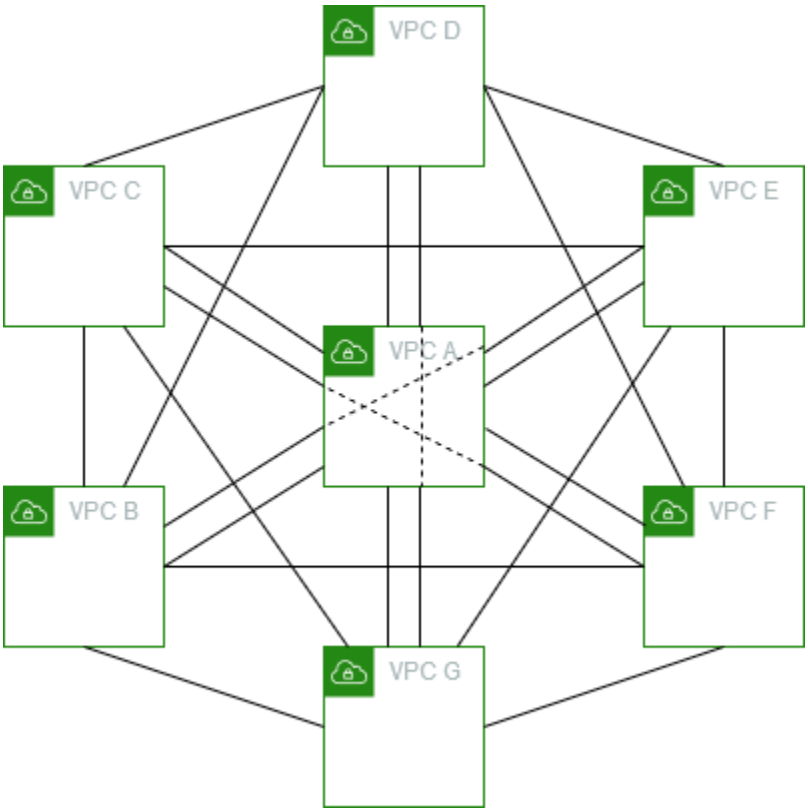
Mehrere durch Peering verbundene VPCs

In dieser Konfiguration haben Sie sieben VPCs in einer vollständigen Mesh-Konfiguration durch Peering verbunden. Die VPCs befinden sich im selben AWS-Konto und haben keine sich überschneidenden CIDR-Blöcke.

VPC	VPC	VPC-Peering-Verbindung
A	B	pcx-aaaabbbb
A	C	pcx-aaaacccc

VPC	VPC	VPC-Peering-Verbindung
A	D	pcx-aaaadddd
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

Sie können diese vollständige Mesh-Konfiguration verwenden, wenn Sie mehrere VPCs haben, die in der Lage sein müssen, ohne Einschränkungen auf die Ressourcen der anderen zuzugreifen. Zum Beispiel als Filesharing-Netzwerk. In diesem Diagramm stellen die Linien VPC-Peering-Verbindungen dar.



Aktualisieren Sie die Routing-Tabelle für jede VPC wie folgt, um diese Konfiguration zu implementieren.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
	VPC D CIDR	pcx-aaaadddd
	VPC-E-CIDR	pcx-aaaaeeee
	VPC-F-CIDR	pcx-aaaaffff

Routing-Tabelle	Zielbereich	Ziel
	VPC-G-CIDR	pcx-aaaagggg
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-bbbbdddd
	VPC-E-CIDR	pcx-bbbbeeee
	VPC-F-CIDR	pcx-bbbbffff
	VPC-G-CIDR	pcx-bbbbgggg
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-ccccdddd
	VPC-E-CIDR	pcx-cccceeee
	VPC-F-CIDR	pcx-ccccffff
	VPC-G-CIDR	pcx-ccccgggg
VPC D	*VPC D CIDR*	Local
	VPC A CIDR	pcx-aaaadddd
	VPC B CIDR	pcx-bbbbdddd
	VPC C CIDR	pcx-ccccdddd
	VPC-E-CIDR	pcx-ddddeeee

Routing-Tabelle	Zielbereich	Ziel
	VPC-F-CIDR	pcx-ddddffff
	VPC-G-CIDR	pcx-ddddgggg
VPC E	*VPC-E-CIDR*	Local
	VPC A CIDR	pcx-aaaaeeee
	VPC B CIDR	pcx-bbbbeeee
	VPC C CIDR	pcx-cccceeee
	VPC D CIDR	pcx-ddddeeee
	VPC-F-CIDR	pcx-eeeeffff
	VPC-G-CIDR	pcx-eeeegggg
VPC F	*VPC-F-CIDR*	Local
	VPC A CIDR	pcx-aaaaffff
	VPC B CIDR	pcx-bbbbffff
	VPC C CIDR	pcx-ccccffff
	VPC D CIDR	pcx-ddddffff
	VPC-E-CIDR	pcx-eeeeffff
	VPC-G-CIDR	pcx-ffffgggg
VPC G	*VPC-G-CIDR*	Local
	VPC A CIDR	pcx-aaaagggg
	VPC B CIDR	pcx-bbbbgggg
	VPC C CIDR	pcx-ccccgggg

Routing-Tabelle	Zielbereich	Ziel
	VPC D CIDR	pcx-ddddgggg
	VPC-E-CIDR	pcx-eeeegggg
	VPC-F-CIDR	pcx-ffffgggg

Wenn allen VPCs IPv6-CIDR-Blöcke zugeordnet sind, aktualisieren Sie die Routing-Tabellen wie folgt.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC-A-IPv4-CIDR*	Local
	VPC-A-IPv6-CIDR	Local
	VPC-B-IPv4-CIDR	pcx-aaaabbbb
	VPC-B-IPv6-CIDR	pcx-aaaabbbb
	VPC-C-IPv4-CIDR	pcx-aaaacccc
	VPC-C-IPv6-CIDR	pcx-aaaacccc
	VPC-D-IPv4-CIDR	pcx-aaaadddd
	VPC-D-IPv6-CIDR	pcx-aaaadddd
	VPC-E-IPv4-CIDR	pcx-aaaaeeee
	VPC-E-IPv6-CIDR	pcx-aaaaeeee
	VPC-F-IPv4-CIDR	pcx-aaaaffff
	VPC-F-IPv6-CIDR	pcx-aaaaffff
	VPC-G-IPv4-CIDR	pcx-aaaagggg
	VPC-G-IPv6-CIDR	pcx-aaaagggg

Routing-Tabelle	Zielbereich	Ziel
VPC B	*VPC-B-IPv4-CIDR*	Local
	VPC-B-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaabbbb
	VPC-A-IPv6-CIDR	pcx-aaaabbbb
	VPC-C-IPv4-CIDR	pcx-bbbbcccc
	VPC-C-IPv6-CIDR	pcx-bbbbcccc
	VPC-D-IPv4-CIDR	pcx-bbbbdddd
	VPC-D-IPv6-CIDR	pcx-bbbbdddd
	VPC-E-IPv4-CIDR	pcx-bbbbeeee
	VPC-E-IPv6-CIDR	pcx-bbbbeeee
	VPC-F-IPv4-CIDR	pcx-bbbbffff
	VPC-F-IPv6-CIDR	pcx-bbbbffff
	VPC-G-IPv4-CIDR	pcx-bbbbgggg
	VPC-G-IPv6-CIDR	pcx-bbbbgggg
VPC C	*VPC-C-IPv4-CIDR*	Local
	VPC-C-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaacccc
	VPC-A-IPv6-CIDR	pcx-aaaacccc
	VPC-B-IPv4-CIDR	pcx-bbbbcccc
	VPC-B-IPv6-CIDR	pcx-bbbbcccc

Routing-Tabelle	Zielbereich	Ziel
	VPC-D-IPv4-CIDR	pcx-ccccdddd
	VPC-D-IPv6-CIDR	pcx-ccccdddd
	VPC-E-IPv4-CIDR	pcx-cccceeee
	VPC-E-IPv6-CIDR	pcx-cccceeee
	VPC-F-IPv4-CIDR	pcx-ccccffff
	VPC-F-IPv6-CIDR	pcx-ccccffff
	VPC-G-IPv4-CIDR	pcx-ccccgggg
	VPC-G-IPv6-CIDR	pcx-ccccgggg
VPC D	*VPC-D-IPv4-CIDR*	Local
	VPC-D-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaadddd
	VPC-A-IPv6-CIDR	pcx-aaaadddd
	VPC-B-IPv4-CIDR	pcx-bbbbdddd
	VPC-B-IPv6-CIDR	pcx-bbbbdddd
	VPC-C-IPv4-CIDR	pcx-ccccdddd
	VPC-C-IPv6-CIDR	pcx-ccccdddd
	VPC-E-IPv4-CIDR	pcx-ddddeeee
	VPC-E-IPv6-CIDR	pcx-ddddeeee
	VPC-F-IPv4-CIDR	pcx-ddddffff
	VPC-F-IPv6-CIDR	pcx-ddddffff

Routing-Tabelle	Zielbereich	Ziel
	VPC-G-IPv4-CIDR	pcx-ddddgggg
	VPC-G-IPv6-CIDR	pcx-ddddgggg
VPC E	*VPC-E-IPv4-CIDR*	Local
	VPC-E-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaaeeee
	VPC-A-IPv6-CIDR	pcx-aaaaeeee
	VPC-B-IPv4-CIDR	pcx-bbbbeeee
	VPC-B-IPv6-CIDR	pcx-bbbbeeee
	VPC-C-IPv4-CIDR	pcx-cccceeee
	VPC-C-IPv6-CIDR	pcx-cccceeee
	VPC-D-IPv4-CIDR	pcx-ddddeeee
	VPC-D-IPv6-CIDR	pcx-ddddeeee
	VPC-F-IPv4-CIDR	pcx-eeeeffff
	VPC-F-IPv6-CIDR	pcx-eeeeffff
	VPC-G-IPv4-CIDR	pcx-eeeegggg
	VPC-G-IPv6-CIDR	pcx-eeeegggg
VPC F	*VPC-F-IPv4-CIDR*	Local
	VPC-F-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaaffff
	VPC-A-IPv6-CIDR	pcx-aaaaffff

Routing-Tabelle	Zielbereich	Ziel
	VPC-B-IPv4-CIDR	pcx-bbbbffff
	VPC-B-IPv6-CIDR	pcx-bbbbffff
	VPC-C-IPv4-CIDR	pcx-ccccffff
	VPC-C-IPv6-CIDR	pcx-ccccffff
	VPC-D-IPv4-CIDR	pcx-ddddffff
	VPC-D-IPv6-CIDR	pcx-ddddffff
	VPC-E-IPv4-CIDR	pcx-eeeeffff
	VPC-E-IPv6-CIDR	pcx-eeeeffff
	VPC-G-IPv4-CIDR	pcx-ffffgggg
	VPC-G-IPv6-CIDR	pcx-ffffgggg
VPC G	*VPC-G-IPv4-CIDR*	Local
	VPC-G-IPv6-CIDR	Local
	VPC-A-IPv4-CIDR	pcx-aaaagggg
	VPC-A-IPv6-CIDR	pcx-aaaagggg
	VPC-B-IPv4-CIDR	pcx-bbbbgggg
	VPC-B-IPv6-CIDR	pcx-bbbbgggg
	VPC-C-IPv4-CIDR	pcx-ccccgggg
	VPC-C-IPv6-CIDR	pcx-ccccgggg
	VPC-D-IPv4-CIDR	pcx-ddddgggg
	VPC-D-IPv6-CIDR	pcx-ddddgggg

Routing-Tabelle	Zielbereich	Ziel
	VPC-E-IPv4-CIDR	pcx-eeeegggg
	VPC-E-IPv6-CIDR	pcx-eeeegggg
	VPC-F-IPv4-CIDR	pcx-ffffgggg
	VPC-F-IPv6-CIDR	pcx-ffffgggg

VPC-Peering-Konfigurationen mit spezifischen Routen

Sie können Routing-Tabellen für eine VPC-Peering-Verbindung konfigurieren, um Zugriff auf einen Subnetz des CIDR-Blocks, einen bestimmten CIDR-Block (wenn die VPC mehrere CIDR-Blöcke besitzt) oder eine spezifische Ressource innerhalb der Peer-VPC einzuschränken. In diesen Beispielen wird eine zentrale VPC mit mindestens zwei VPCs verbunden, die überlappende CIDR-Blöcke nutzen.

Weitere Beispiele zu Szenarien, in denen Sie eine spezifische VPC-Peering-Verbindungskonfiguration benötigen, finden Sie unter VPC Peering-Szenarien. Weitere Informationen zum Erstellen von und zum Arbeiten mit VPC-Peering-Verbindungen finden Sie unter Arbeiten mit VPC-Peering-Verbindungen. Weitere Informationen zur Aktualisierung Ihrer Routing-Tabellen finden Sie unter Aktualisieren Sie ihre Routing-Tabellen für eine VPC-Peering-Verbindung.

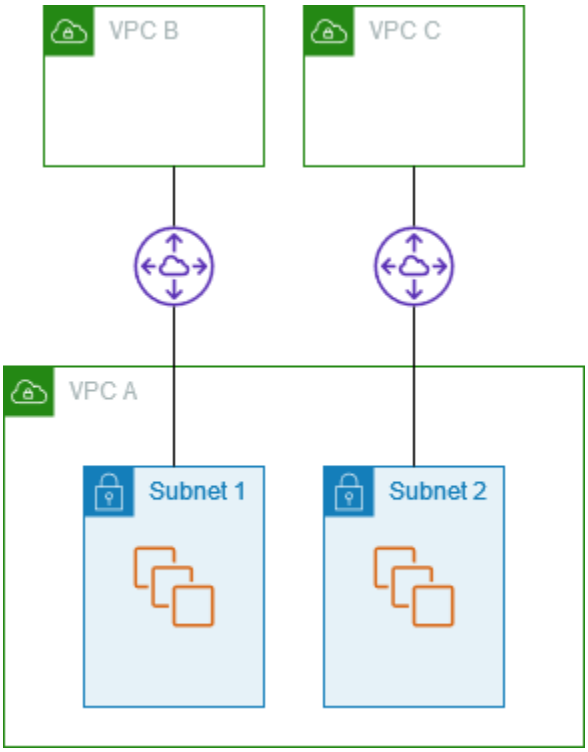
Konfigurationen

- Zwei VPCs, die auf bestimmte Subnetze in einer VPC zugreifen
- Zwei VPCs, die auf bestimmte Subnetze in einer VPC zugreifen
- Eine VPC, die auf bestimmte Subnetze in zwei VPCs zugreift
- Instances in einer VPC, die auf bestimmte Instances in zwei VPCs zugreifen
- Eine VPC, die auf zwei VPCs zugreift und dabei die längsten Präfixe verwendet
- Mehrere VPC-Konfigurationen

Zwei VPCs, die auf bestimmte Subnetze in einer VPC zugreifen

Die Konfiguration enthält eine zentrale VPC mit zwei Subnetzen (VPC A), eine Peering-Verbindung zwischen VPC A und VPC B (`pcx-aaaabbbb`) und eine Peering-Verbindung zwischen VPC A und

VPC C (pcx-aaaacccc). Jede VPC benötigt Zugriff auf die Ressourcen in nur einem der Subnetze in VPC A.



Die Routing-Tabelle für Subnetz 1 verweist auf die VPC-Peering-Verbindung pcx-aaaabbbb, um auf den gesamten CIDR-Block von VPC B zuzugreifen. Die Routing-Tabelle von VPC B verwendet pcx-aaaabbbb, um auf den CIDR-Block von Subnetz 1 in VPC A zuzugreifen. Die Routing-Tabelle für Subnetz 2 verwendet die VPC-Peering-Verbindung pcx-aaaacccc, um auf den gesamten CIDR-Block von VPC C zuzugreifen. Die Routing-Tabelle von VPC C verwendet pcx-aaaacccc, um auf den CIDR-Block nur von Subnetz 2 in VPC A zuzugreifen.

Routing-Tabelle	Zielbereich	Ziel
Subnetz 1 in (VPC A)	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb
Subnetz 2 in (VPC A)	*VPC A CIDR*	Local
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local

Routing-Tabelle	Zielbereich	Ziel
	Subnetz-1-CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local
	Subnetz-2-CIDR	pcx-aaaacccc

Sie können diese Konfiguration auf mehrere CIDR-Blöcke erweitern. Nehmen wir an, dass VPC A und VPC B sowohl IPv4- als auch IPv6-CIDR-Blöcke haben und dass Subnetz 1 einen zugehörigen IPv6-CIDR-Block hat. Sie können VPC B für die Kommunikation mit Subnetz 1 in VPC A über IPv6 über die VPC-Peering-Verbindung aktivieren. Hierzu fügen Sie der Routing-Tabelle für VPC A eine Route mit dem Zielbereich des IPv6-CIDR-Blocks von VPC B hinzu. Außerdem fügen Sie der Routing-Tabelle von VPC B eine Route mit dem Zielbereich der IPv6-CIDR von Subnetz 1 in VPC A hinzu.

Routing-Tabelle	Zielbereich	Ziel	Hinweise
Subnetz 1 in VPC A	*VPC-A-IPv4-CIDR*	Local	
	VPC-A-IPv6-CIDR	Local	Eine lokale Route, die automatisch für die IPv6-Kommunikation innerhalb der VPC hinzugefügt wird.
	VPC-B-IPv4-CIDR	pcx-aaaabbbb	
	VPC-B-IPv6-CIDR	pcx-aaaabbbb	Route zum IPv6 CIDR-Block von VPC B.
Subnetz 2 in VPC A	*VPC-A-IPv4-CIDR*	Local	
	VPC-A-IPv6-CIDR	Local	Eine lokale Route, die automatisch für die IPv6-Kommunikation

Routing-Tabelle	Zielbereich	Ziel	Hinweise
			innerhalb der VPC hinzugefügt wird.
	VPC-C-IPv4-CIDR	pcx-aaaacccc	
VPC B	*VPC-B-IPv4-CIDR*	Local	
	VPC-B-IPv6-CIDR	Local	Eine lokale Route, die automatisch für die IPv6-Kommunikation innerhalb der VPC hinzugefügt wird.
	Subnetz-1-IPv4-CIDR	pcx-aaaabbbb	
	Subnetz-2-IPv4-CIDR	pcx-aaaabbbb	Route zum IPv6 CIDR-Block von VPC A.
VPC C	*VPC-C-IPv4-CIDR*	Local	
	Subnetz-2-IPv4-CIDR	pcx-aaaacccc	

Zwei VPCs, die auf bestimmte Subnetze in einer VPC zugreifen

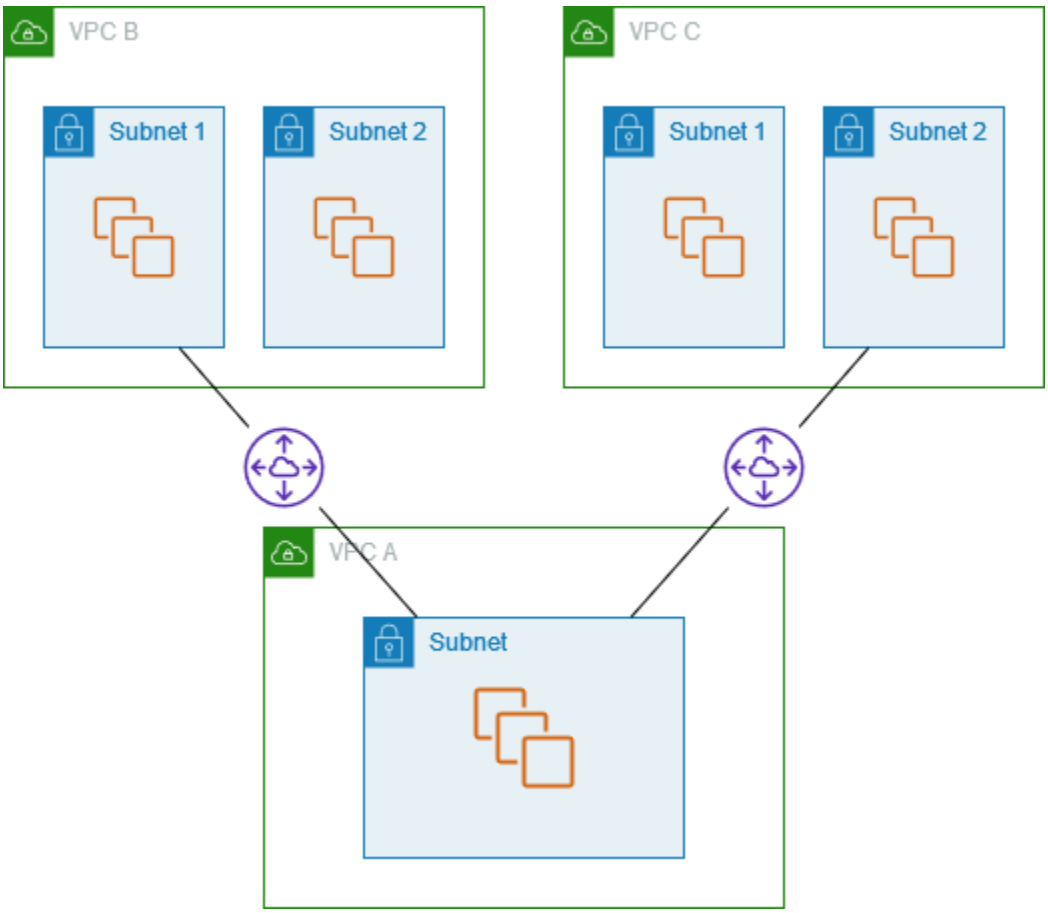
Die Konfiguration enthält eine zentrale VPC (VPC A), eine Peering-Verbindung zwischen VPC A und VPC B (`pcx-aaaabbbb`) und eine Peering-Verbindung zwischen VPC A und VPC C (`pcx-aaaacccc`). VPC A hat einen CIDR-Block für jede VPC-Peering-Verbindung.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC-A-CIDR 1*	Local
	VPC-A-CIDR 2	Local

Routing-Tabelle	Zielbereich	Ziel
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local
	VPC-A-CIDR 1	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local
	VPC-A-CIDR 2	pcx-aaaacccc

Eine VPC, die auf bestimmte Subnetze in zwei VPCs zugreift

Die Konfiguration enthält eine zentrale VPC (VPC A) mit einem Subnetz, eine Peering-Verbindung zwischen VPC A und VPC B (`pcx-aaaabbbb`) und eine Peering-Verbindung zwischen VPC A und VPC C (`pcx-aaaacccc`). VPC B und VPC C haben jeweils zwei Subnetze. Die Peering-Verbindung zwischen VPC A und VPC B verwendet nur eines der Subnetze in VPC B. Die Peering-Verbindung zwischen VPC A und VPC C verwendet nur eines der Subnetze in VPC C.



Verwenden Sie diese Konfiguration, wenn Sie eine zentrale VPC haben, die über einen einzigen Satz von Ressourcen verfügt, wie zum Beispiel Active-Directory-Services, auf die andere VPCs zugreifen müssen. Die zentrale VPC benötigt keinen Vollzugriff auf die verbundene VPC.

Die Routing-Tabelle für VPC A verwendet die Peering-Verbindungen, um nur auf bestimmte Subnetze in den Peering-VPCs zuzugreifen. Die Routing-Tabelle für Subnetz 1 verwendet die Peering-Verbindung mit VPC A, um auf das Subnetz in VPC A zuzugreifen. Die Routing-Tabelle für Subnetz 2 verwendet die Peering-Verbindung mit VPC A, um auf das Subnetz in VPC A zuzugreifen.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC A CIDR*	Local
	Subnetz-1-CIDR	pcx-aaaabbbb
	Subnetz-2-CIDR	pcx-aaaacccc
Subnetz 1 (VPC B)	*VPC B CIDR*	Local

Routing-Tabelle	Zielbereich	Ziel
	Subnetz in VPC-A-CIDR	pcx-aaaabbbb
Subnetz 2 (VPC C)	*VPC C CIDR*	Local
	Subnetz in VPC-A-CIDR	pcx-aaaacccc

Routing für Antwortdatenverkehr

Wenn Sie eine VPC über ein Peering mit mehreren VPCs verbinden, die sich überschneidende oder sich entsprechende CIDR-Blöcke haben, stellen Sie sicher, dass Ihre Routing-Tabellen so konfiguriert sind, dass kein Antwortdatenverkehr von Ihrer VPC an die falsche VPC gesendet wird. AWS unterstützt derzeit kein Unicast Reverse Path Forwarding in VPC-Peering-Verbindungen, das die Quell-IP von Paketen prüft und Antwortpakete zurück zur Quelle leitet.

VPC A ist beispielsweise mit VPC B und VPC C verbunden. VPC B und VPC C haben übereinstimmende CIDR-Blöcke und ihre Subnetze haben übereinstimmende CIDR-Blöcke. Die Routing-Tabelle für Subnetz 2 in VPC B verweist auf die VPC-Peering-Verbindung `pcx-aaaabbbb`, um auf das VPC-A-Subnetz zuzugreifen. Die Routing-Tabelle von VPC A ist so konfiguriert, dass Sie Datenverkehr an die VPC-CIDR-Peering-Verbindung `pcx-aaaaccccc` sendet.

Routing-Tabelle	Zielbereich	Ziel
Subnetz 2 (VPC B)	*VPC B CIDR*	Local
	Subnetz in VPC-A-CIDR	pcx-aaaabbbb
VPC A	*VPC A CIDR*	Local
	VPC C CIDR	pcx-aaaacccc

Angenommen, eine Instance in Subnetz 2 in VPC B sendet Datenverkehr an den Active-Directory-Server in VPC A über die VPC-Peering-Verbindung `pcx-aaaabbbb`. VPC A sendet den Antwortdatenverkehr an den Active-Directory-Server. Die VPC-A-Routing-Tabelle ist jedoch so konfiguriert, dass der gesamte Verkehr innerhalb des VPC-CIDR-Bereichs an die VPC-Peering-Verbindung `pcx-aaaacccc` gesendet wird. Wenn Subnetz 2 in VPC C eine Instance mit der gleichen

IP-Adresse hat wie die Instance in Subnetz 2 von VPC B, empfängt sie den Antwortverkehr von VPC A. Die Instance in Subnetz 2 in VPC B erhält keine Antwort auf ihre Anfrage an VPC A.

Um dies zu verhindern, können Sie der Routing-Tabelle von VPC A eine spezielle Route mit der CIDR von Subnetz 2 in VPC B als Bestimmungsort und einem Ziel von `pcx-aaaabbbb`. Die neue Route an ist spezifischer. Daher wird der Datenverkehr für das Subnetz-2-CIDR an die VPC-Peering-Verbindung `pcx-aaaabbbb` geleitet

Als Alternative hat die Routing-Tabelle für VPC A im folgenden Beispiel eine Route für jedes Subnetz für jede VPC-Peering-Verbindung. VPC A kann mit Subnetz B in VPC B und mit Subnetz A in VPC C kommunizieren. Dieses Szenario ist nützlich, wenn Sie eine weitere VPC-Peering-Verbindung mit einem anderen Subnetz hinzufügen müssen, das in denselben Adressbereich wie VPC B und VPC C fällt – Sie können einfach eine weitere Route für dieses spezielle Subnetz hinzufügen.

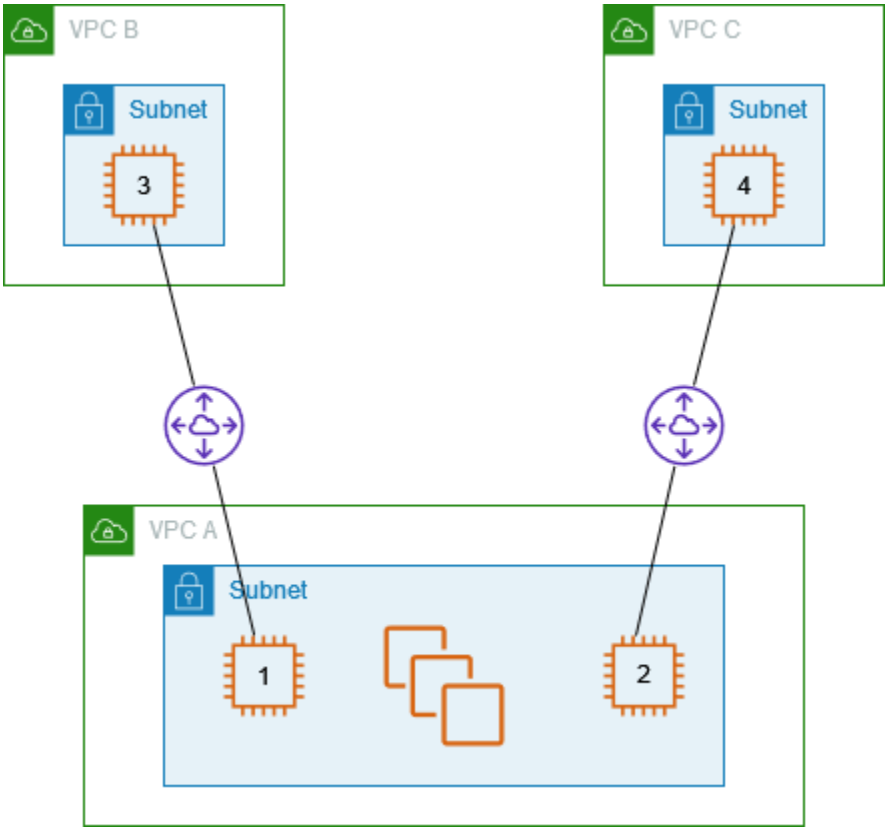
Bestimmungsort	Ziel
VPC A CIDR	Local
Subnetz-2-CIDR	pcx-aaaabbbb
Subnetz-1-CIDR	pcx-aaaacccc

Je nach Ihrem Nutzungsszenario können Sie alternativ eine Route für eine spezifische IP-Adresse in VPC B erstellen und so dafür sorgen, dass der Datenverkehr an den richtigen Server zurückgeroutet wird (die Routing-Tabelle nutzt den längsten Präfix als Priorität für die Routen):

Bestimmungsort	Ziel
VPC A CIDR	Local
Spezifische IP-Adresse in Subnetz 2	pcx-aaaabbbb
VPC B CIDR	pcx-aaaacccc

Instances in einer VPC, die auf bestimmte Instances in zwei VPCs zugreifen

Die Konfiguration enthält eine zentrale VPC (VPC A) mit einem Subnetz, eine Peering-Verbindung zwischen VPC A und VPC B (`pcx-aaaabbbb`) und eine Peering-Verbindung zwischen VPC A und VPC C (`pcx-aaaacccc`). VPC A hat ein Subnetz mit einer Instance für jede Peering-Verbindung. Sie können diese Konfiguration nutzen, um den Peering-Datenverkehr auf bestimmte Instances zu beschränken.



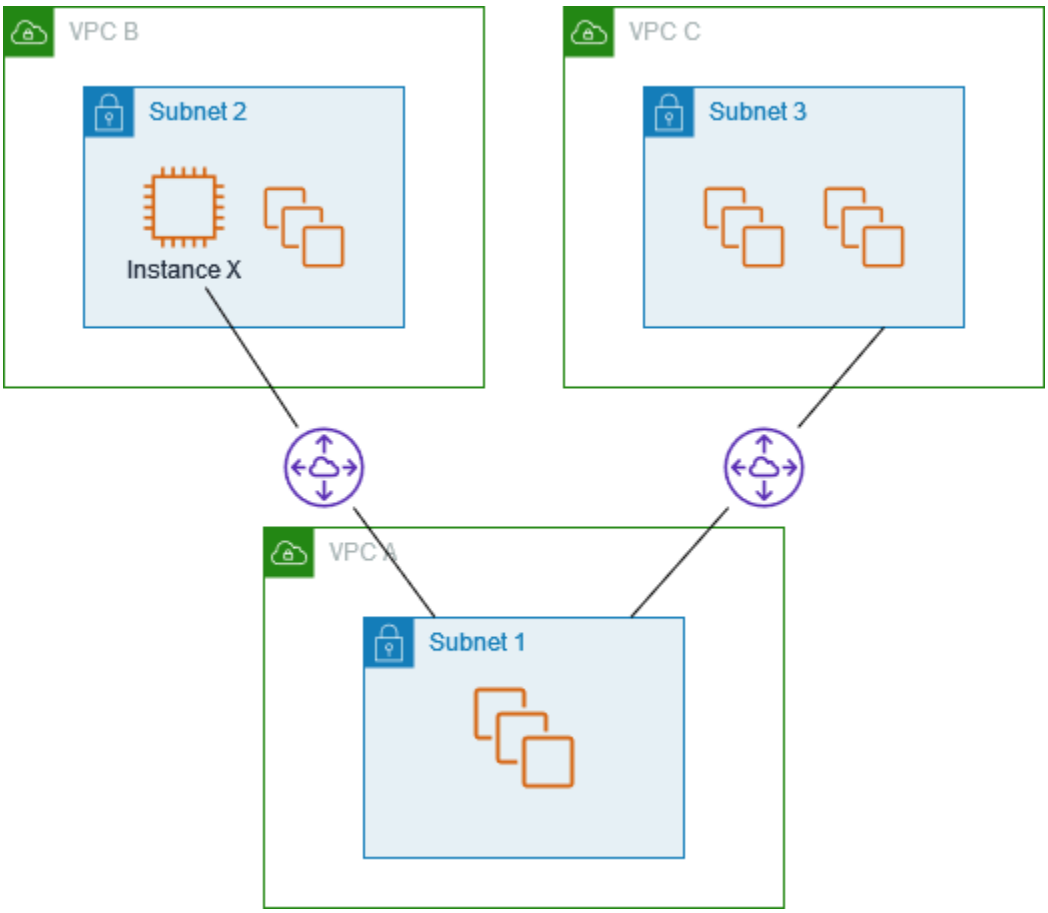
Jede VPC-Routing-Tabelle zeigt auf die relevante VPC-Peering-Verbindung, um so auf eine einzelne IP-Adresse (und somit auf eine bestimmte Instance) im Peer-VPC zugreifen zu können.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC A CIDR*	Local
	Instance-3-IP-Addresse	pcx-aaaabbbb
	Instance-4-IP-Addresse	pcx-aaaacccc

Routing-Tabelle	Zielbereich	Ziel
VPC B	*VPC B CIDR*	Local
	Instance-1-IP-Addresse	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local
	Instance-2-IP-Addresse	pcx-aaaacccc

Eine VPC, die auf zwei VPCs zugreift und dabei die längsten Präfixe verwendet

Die Konfiguration enthält eine zentrale VPC (VPC A) mit einem Subnetz, eine Peering-Verbindung zwischen VPC A und VPC B (`pcx-aaaabbbb`) und eine Peering-Verbindung zwischen VPC A und VPC C (`pcx-aaaacccc`). VPC B und VPC C haben übereinstimmende CIDR-Blöcke. Sie möchten die VPC-Peering-Verbindung `pcx-aaaabbbb` zur Weiterleitung von Datenverkehr zwischen VPC A und einer spezifischen Instance in VPC B verwenden. Der gesamte restliche Datenverkehr an den IP-Adressbereich wird über `pcx-aaaacccc` zwischen VPC A und VPC C geroutet.



VPC-Routing-Tabellen verwenden den längsten übereinstimmenden Präfix, um die eindeutigste Route über die gewünschte VPC-Peering-Verbindung zu ermitteln. Der gesamte restliche Datenverkehr wird über die nächste übereinstimmende Route geroutet (in diesem Fall über die VPC-Peering-Verbindung `pcx-aaaacccc`).

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC-A-CIDR-Block*	Local
	Instance-X-IP-Addresse	pcx-aaaabbbb
	VPC-C-CIDR-Block	pcx-aaaacccc
VPC B	*VPC-B-CIDR-Block*	Local
	VPC-A-CIDR-Block	pcx-aaaabbbb

Routing-Tabelle	Zielbereich	Ziel
VPC C	*VPC-C-CIDR-Block*	Local
	VPC-A-CIDR-Block	pcx-aaaacccc

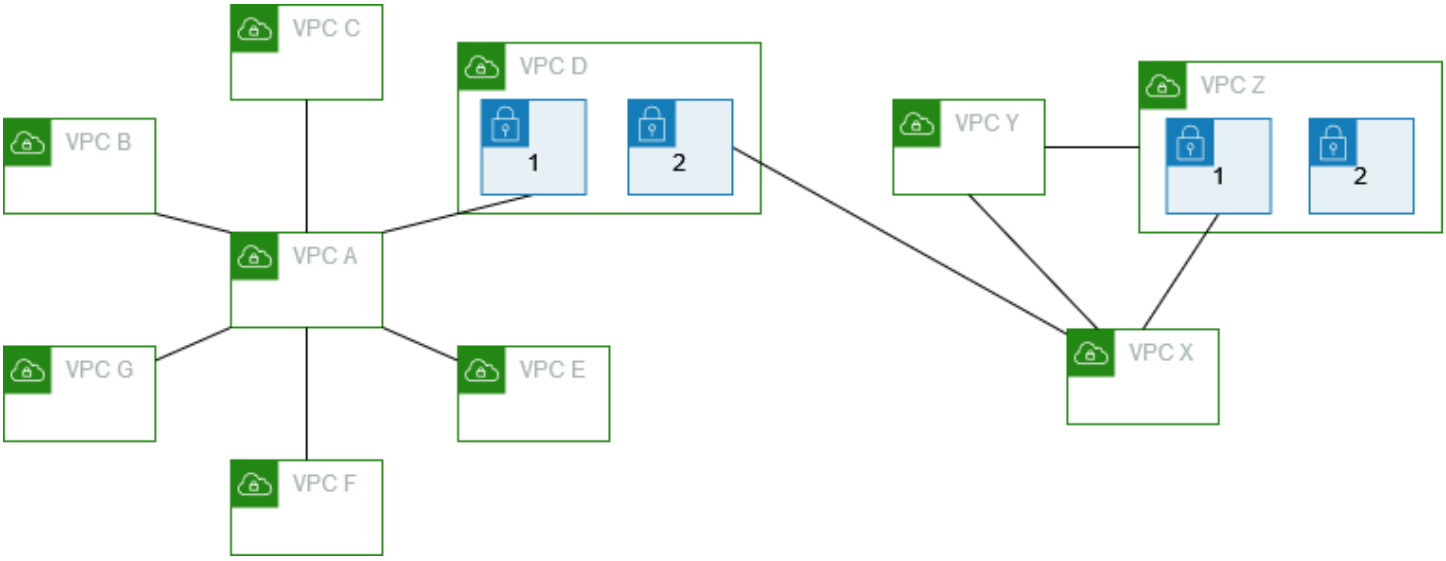
> **Important**
>
> Wenn eine andere Instance als Instance X in VPC B Verkehr an VPC A sendet, wird der Antwortverkehr möglicherweise an VPC C statt an VPC B weitergeleitet. Weitere Informationen finden Sie unter Routing für Antwortdatenverkehr.

Mehrere VPC-Konfigurationen

In diesem Beispiel ist eine zentrale VPC (VPC A) in einer Spoke-Konfiguration mit mehreren VPCs verbunden. Sie haben außerdem drei VPCs (VPCs X, Y und Z), die in einer vollständigen Mesh-Konfiguration verbunden sind.

VPC D hat außerdem eine VPC-Peering-Verbindung mit VPC X (`pcx-ddddxxxx`). VPC A und VPC X haben überlappende CIDR-Blöcke. Dies bedeutet, dass der Peering-Datenverkehr zwischen VPC A und VPC D auf ein bestimmtes Subnetz (Subnetz 1) in VPC D beschränkt ist. Dies soll sicherstellen, dass wenn VPC D eine Anfrage von VPC A oder VPC X empfängt, der Antwortdatenverkehr an die richtige VPC gesendet wird. unterstützt AWS kein Unicast Reverse Path Forwarding in VPC-Peering-Verbindungen, das die Quell-IP von Paketen überprüft und Antwortpakete zurück an die Quelle weiterleitet. Weitere Informationen finden Sie unter Routing für Antwortdatenverkehr.

VPC D und VPC Z haben ebenfalls überlappende CIDR-Blöcke. Der Peering-Verkehr zwischen VPC D und VPC X ist auf das Subnetz 2 in VPC D beschränkt, und der Peering-Verkehr zwischen VPC X und VPC Z ist auf das Subnetz 1 in VPC Z beschränkt. Damit soll sichergestellt werden, dass VPC X, wenn es Peering-Verkehr von VPC D oder VPC Z erhält, den Antwortverkehr an die richtige VPC zurücksendet.



Die Routing-Tabellen für VPCs B, C, E, F und G verweisen auf die entsprechenden Peering-Verbindungen, um auf den vollständigen CIDR-Block für VPC A zuzugreifen, und die Routing-Tabelle von VPC A verweist auf die entsprechenden Peering-Verbindungen für VPCs B, C, E, F und G, um auf deren vollständige CIDR-Blöcke zuzugreifen. Für die Peering-Verbindung `pcx-aaaadddd` leitet die Routing-Tabelle von VPC A den Verkehr nur an das Subnetz 1 in VPC D weiter, und die Routing-Tabelle von Subnetz 1 in VPC D verweist auf den vollständigen CIDR-Block von VPC A.

Die VPC-Y-Routing-Tabelle verweist auf die relevanten Peering-Verbindungen, um auf die vollen CIDR-Blöcke von VPC X und VPC Z zuzugreifen, und die VPC-Z-Routing-Tabelle verweist auf die relevante Peering-Verbindung, um auf den vollen CIDR-Block von VPC Y zuzugreifen. Die Subnetz-1-Routing-Tabelle in VPC Z verweist auf die relevante Peering-Verbindung, um auf den vollen CIDR-Block von VPC Y zuzugreifen. Die VPC X-Routing-Tabelle verweist auf die relevante Peering-Verbindung, um auf Subnetz 2 in VPC D und Subnetz 1 in VPC Z zuzugreifen.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
	Subnetz-1-CIDR in VPC D	pcx-aaaadddd

Routing-Tabelle	Zielbereich	Ziel
	VPC-E-CIDR	pcx-aaaaeeee
	VPC-F-CIDR	pcx-aaaaffff
	VPC-G-CIDR	pcx-aaaagggg
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-aaaacccc
Subnetz 1 in VPC D	*VPC D CIDR*	Local
	VPC A CIDR	pcx-aaaadddd
Subnetz 2 in VPC D	*VPC D CIDR*	Local
	VPC-X-CIDR	pcx-ddddxxxx
VPC E	*VPC-E-CIDR*	Local
	VPC A CIDR	pcx-aaaaeeee
VPC F	*VPC-F-CIDR*	Local
	VPC A CIDR	pcx-aaaaffff
VPC G	*VPC-G-CIDR*	Local
	VPC A CIDR	pcx-aaaagggg
VPC X	*VPC-X-CIDR*	Local
	Subnetz-2-CIDR in VPC D	pcx-ddddxxxx
	VPC-Y-CIDR	pcx-xxxxyyyy

Routing-Tabelle	Zielbereich	Ziel
	Subnetz-1-CIDR in VPC Z	pcx-xxxxzzzz
VPC Y	*VPC-Y-CIDR*	Local
	VPC-X-CIDR	pcx-xxxxyyyy
	VPC-Z-CIDR	pcx-yyyyzzzz
VPC Z	*VPC-Z-CIDR*	Local
	VPC-Y-CIDR	pcx-yyyyzzzz
	VPC-X-CIDR	pcx-xxxxzzzz

VPC Peering-Szenarien

Es gibt eine Reihe von Gründen, warum Sie eine VPC-Peering-Verbindung zwischen Ihren VPCs oder zwischen einer VPC, die Sie besitzen, und einer VPC in einem anderen AWS-Konto einrichten müssen. Die folgenden Szenarien helfen Ihnen dabei herauszufinden, welche Konfiguration für Ihr Netzwerk am besten geeignet ist.

Szenarien

- Peering von zwei oder mehr VPCs mit Vollzugriff auf Ressourcen
- Peering mit einer VPC, um Zugriff auf zentrale Ressourcen zu gewähren

Peering von zwei oder mehr VPCs mit Vollzugriff auf Ressourcen

In diesem Szenario haben Sie zwei oder mehr VPCs, die Sie per Peering miteinander verbinden möchten, um allen VPCs Vollzugriff auf sämtliche Ressourcen zu gewähren. Im Folgenden sind einige Beispiele aufgeführt:

- Ihr Unternehmen hat eine VPC für die Finanzabteilung und eine weitere VPC für die Buchhaltungsabteilung. Die Finanzabteilung benötigt Zugriff auf alle Ressourcen der Buchhaltungsabteilung und die Buchhaltungsabteilung benötigt Zugriff auf alle Ressourcen der Finanzabteilung.
- Ihr Unternehmen verfügt über mehrere IT-Abteilungen, die jeweils eine eigene VPC betreiben. Einige VPCs befinden sich im selben AWS-Konto, andere wiederum in einem anderen AWS-Konto. Sie möchten alle VPCs per Peering verbinden, damit die IT-Abteilungen Vollzugriff auf die Ressourcen der anderen Abteilungen haben.

Weitere Informationen zum Einrichten der VPC-Peering-Verbindungskonfiguration und Routing-Tabellen für dieses Szenario finden Sie in der folgenden Dokumentation:

- Zwei durch Peering verbundene VPCs
- Drei durch Peering verbundene VPCs
- Mehrere durch Peering verbundene VPCs

Weitere Informationen zum Erstellen von und Arbeiten mit VPC-Peering-Verbindungen in der Amazon VPC-Konsole finden Sie unter Arbeiten mit VPC-Peering-Verbindungen.

Peering mit einer VPC, um Zugriff auf zentrale Ressourcen zu gewähren

In diesem Szenario betreiben Sie eine zentrale VPC, die Ressourcen enthält, die Sie für andere VPCs freigeben möchten. Die zentrale VPC kann Voll- oder Teilzugriff auf die per Peering verbundenen VPCs haben und umgekehrt haben die per Peering verbundenen VPCs Voll- oder Teilzugriff auf die zentrale VPC. Im Folgenden sind einige Beispiele aufgeführt:

- Die IT-Abteilung Ihres Unternehmens betreibt eine VPC für die Dateifreigabe. Sie möchten andere VPCs per Peering mit der zentralen VPC verbinden, Sie möchten aber nicht, dass die anderen VPCs in der Lage sind, Daten auszutauschen.
- Ihr Unternehmen betreibt eine VPC, die Sie für Ihre Kunden freigeben möchten. Jeder Kunde kann eine VPC-Peering-Verbindung zu Ihrer VPC herstellen, jedoch können Kunden keinen Datenverkehr an andere mit Ihrer VPC per Peering verbundene VPCs senden und auch die Routen anderer Kunden nicht einsehen.
- Sie betreiben eine zentrale VPC, die für Active Directory-Service verwendet wird. Bestimmte Instances in Peer-VPCs senden Anfragen an die Active Directory-Server und benötigen dafür Vollzugriff auf die zentrale VPC. Die zentrale VPC benötigt keinen Vollzugriff auf die Peer-VPCs, sondern muss nur Antwortdatenverkehr an die jeweiligen Instances leiten.

Weitere Informationen zum Erstellen von und Arbeiten mit VPC-Peering-Verbindungen in der Amazon VPC-Konsole finden Sie unter Arbeiten mit VPC-Peering-Verbindungen.

Identity and Access Management für VPC Peering

Standardmäßig können -Benutzer keine VPC-Peering-Verbindungen erstellen oder ändern. Um den Zugriff auf VPC-Peering-Ressourcen zu gewähren, ordnen Sie eine IAM-Richtlinie einer IAM-Identität zu, z. B. einer Rolle.

Beispiele

- Beispiel: Erstellen einer VPC-Peering-Verbindung
- Beispiel: Akzeptieren einer VPC-Peering-Verbindung
- Beispiel: Löschen einer VPC-Peering-Verbindung
- Beispiel: Arbeiten innerhalb eines bestimmten Kontos
- Beispiel: VPC-Peering-Verbindungen mithilfe der Konsole verwalten

Eine Liste der Amazon VPC-Aktionen und der unterstützten Ressourcen und Bedingungsschlüssel für jede Aktion finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 in der Service-Autorisierungsreferenz.

Beispiel: Erstellen einer VPC-Peering-Verbindung

Die folgende Richtlinie gewährt Benutzern die Erlaubnis, Anfragen für die VPC-Peering-Verbindung unter Verwendung von VPCs zu erstellen, die mit dem Tag `Purpose=Peering` versehen sind. In der ersten Anweisung wird ein Bedingungsschlüssel (`ec2:ResourceTag`) auf die VPC-Ressource angewendet. Beachten Sie, dass die VPC-Ressource für die Aktion `CreateVpcPeeringConnection` immer die VPC des Anfragestellers ist.

Die zweite Anweisung erteilt Benutzern die Berechtigung, die Ressourcen für die VPC-Peering-Verbindung zu erstellen, und verwendet daher den Platzhalter * anstelle einer spezifischen Ressourcen-ID.

```
{
  "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/*"
    }
  ]
}
```

Die folgende Richtlinie gewährt Benutzern im angegebenen AWS-Konto die Berechtigung, VPC-Peering-Verbindungen mit einer beliebigen VPC in der angegebenen Region zu erstellen, jedoch nur, wenn die VPC, die die Peering-Verbindung akzeptiert, eine bestimmte VPC im angegebenen Konto ist.

```
{
  "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"
        }
      }
    }
  ]
}
```

Beispiel: Akzeptieren einer VPC-Peering-Verbindung

Mit der folgenden Richtlinie wird Benutzern die Berechtigung zum Akzeptieren von Anfragen für die VPC-Peering-Verbindung von einem spezifischen AWS-Konto gewährt. So wird verhindert, dass Benutzer VPC-Peering-Verbindungsanfragen von unbekannten Konten akzeptieren können. Die Anweisung verwendet den Bedingungsschlüssel `ec2:RequesterVpc`, um dies zu erzwingen.

```
{
  "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/*"
        }
      }
    }
  ]
}
```

Die folgende Richtlinie erlaubt es Benutzern, VPC-Peering-Anfragen zu akzeptieren, wenn ihre VPC über das Tag `Purpose=Peering` verfügt.

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

Beispiel: Löschen einer VPC-Peering-Verbindung

Die folgende Richtlinie gewährt Benutzern des angegebenen Kontos die Berechtigung, jede VPC-Peering-Verbindung zu löschen, mit Ausnahme derjenigen, die die angegebene VPC verwenden, die sich im selben Konto befindet. In der Richtlinie werden die beiden Bedingungsschlüssel `ec2:AccepterVpc` und `ec2:RequesterVpc` verwendet, da in der ursprünglichen VPC-Peering-Verbindungsanfrage die VPC sowohl die des Anfragestellers als auch die Peer-VPC sein könnte.

```
{
  "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"
        }
      }
    }
  ]
}
```

Beispiel: Arbeiten innerhalb eines bestimmten Kontos

Mit der folgenden Richtlinie wird Benutzern die Berechtigung zum Arbeiten mit VPC-Peering-Verbindungen in einem bestimmten Konto gewährt. Benutzer können VPC-Peering-Verbindungen anzeigen, erstellen, akzeptieren, ablehnen und löschen, die sich im gleichen AWS-Konto befinden.

Die erste Anweisung gewährt Benutzern das Anzeigen aller VPC-Peering-Verbindungen. Für das Element `Resource` ist in diesem Fall das Sternchen (*) als Platzhalter erforderlich, da für diese API-Aktion (`DescribeVpcPeeringConnections`) derzeit Berechtigungen auf Ressourcenebene nicht unterstützt werden.

Mit der zweiten Anweisung wird Benutzern die Berechtigung zum Erstellen von VPC-Peering-Verbindungen, sowie der Zugriff auf sämtliche VPCs im angegebenen Konto, um das zu tun, gewährt.

Die dritte Anweisung verwendet einen Platzhalter * als Teil des Elements `Action`, um die Genehmigung für alle VPC-Peering-Verbindungsaktionen zu erteilen. Durch die Bedingungsschlüssel wird sichergestellt, dass die Aktionen nur für VPC-Peering-Verbindungen in VPCs im Konto ausgeführt werden können. Beispielsweise kann ein Benutzer eine VPC-Peering-Verbindung nicht löschen, wenn sich entweder der akzeptierende oder der anfordernde VPC in einem anderen Konto befindet. Benutzer können keine VPC-Peering-Verbindung zwischen VPCs in unterschiedlichen Konten erstellen.

```
{
  "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/*"
        }
      }
    }
  ]
}
```

Beispiel: VPC-Peering-Verbindungen mithilfe der Konsole verwalten

Um VPC-Peering-Verbindungen in der Amazon VPC-Konsole anzuzeigen, müssen Benutzer über die Berechtigung zum Verwenden der Aktion `ec2:DescribeVpcPeeringConnections`

verfügen. Um das Dialogfeld Create VPC Peering Connection (VPC Peering-Verbindung erstellen) zu verwenden, benötigen Benutzer die Berechtigung zum Verwenden der Aktion `ec2:DescribeVpcs`. Das gibt ihnen die Berechtigung, eine VPC anzeigen und auswählen. Sie können auf alle `ec2:*PeeringConnection`-Aktionen mit Ausnahme von `ec2:DescribeVpcPeeringConnections` Berechtigungen auf Ressourcenebene anwenden.

Die folgende Richtlinie gewährt Benutzern die Berechtigung, VPC-Peering-Verbindungen anzuzeigen und das Dialogfeld Create VPC Peering Connection (VPC-Peering-Verbindung erstellen) zu verwenden, um eine VPC-Peering-Verbindung zu erstellen, die nur eine bestimmte Anforderungs-VPC verwendet. Wenn Benutzer versuchen, eine VPC-Peering-Verbindung in einer anderen anfordernden VPC zu erstellen, schlägt die Anfrage fehl.

```
{
  "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/*"
      ]
    }
  ]
}
```

Kontingente für VPC-Peering-Verbindungen

Die folgenden Tabellen führen die Kontingente, ehemals als Limits bezeichnet, für die VPC-Peering-Verbindungen pro Region für Ihr AWS auf. Sofern nicht anders angegeben, können Sie eine Erhöhung dieser Kontingente beantragen.

Name	Standard	Anpassbar
Aktive VPC-Peering-Verbindungen pro VPC	50	Ja (bis zu 125)
Ausstehende VPC-Peering-Verbindungsanforderungen	25	Ja
Ablaufzeit für eine nicht akzeptierte VPC-Peering-Verbindungsanforderung	1 Woche (168 Stunden)	Nein

Für weitere Informationen zu VPC-Peering-Verbindungen schauen Sie VPC Peering-Einschränkungen.

Hinweise zum Bezug zusätzlicher VPC-Kontingente finden Sie unter Amazon-VPC-Kontingente im Amazon-VPC-Benutzerhandbuch.

Dokumentverlauf für den Leitfaden für Amazon-VPC-Peering

Die folgende Tabelle beschreibt die Dokumentation für diese Version des Leitfadens für Amazon-VPC-Peering.

Änderung	Beschreibung	Datum
Tag beim Erstellen	Sie können Markierungen hinzufügen, wenn Sie eine VPC-Peering-Verbindung und eine Routing-Tabelle erstellen.	20. Juli 2020
Interregionales Peering	Die Auflösung des DNS-Hostnamens wird für regionsübergreifende VPC-Peering-Verbindungen in der Region Asien-Pazifik (Hongkong) unterstützt.	26. August 2019
Interregionales Peering	Sie können eine VPC Peering-Verbindung zwischen VPCs in unterschiedlichen AWS-Regionen erstellen.	29. November 2017
Support für DNS-Auflösung für VPC-Peering	Sie können für lokale VPCs die Auflösung von öffentlichen DNS-Hostnamen zu privaten IP-Adressen aktivieren, wenn Anfragen von Instances in der Peer-VPC eingehen.	28. Juli 2016
Veraltete Sicherheitsgruppenregeln	Sie können feststellen, ob in den Regeln einer Sicherheitsgruppe in einer Peer-VPC auf eine Sicherheitsgruppe verwiesen wird, und Sie	12. Mai 2016

	können veraltete Sicherheitsgruppenregeln identifizieren.	
Verwenden von ClassicLink über eine VPC-Peering-Verbindung	Sie können für VPC-Peering-Verbindungen aktivieren, sodass lokale verknüpfte EC2-Classic-Instances mit Instances in einer Peer-VPC kommunizieren können.	26. April 2016
VPC-Peering	Sie können eine VPC-Peering-Verbindung zwischen zwei VPCs erstellen, um es Instances in beiden VPCs zu ermöglichen, miteinander über private IP-Adressen zu kommunizieren.	24. März 2014

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.