aws

VPC Peering

Amazon Virtual Private Cloud

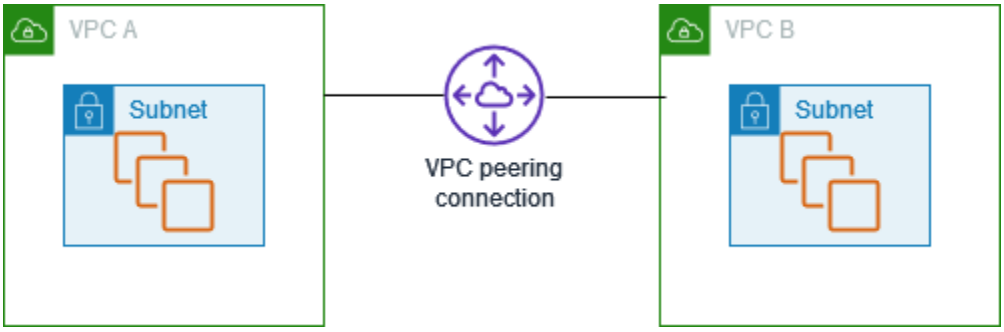
Amazon Virtual Private Cloud: VPC Peering

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 Cloud isoliert. AWS Sie können AWS Ressourcen wie EC2 Amazon-Instances in Ihrer VPC starten.

Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs , mit der Sie den Verkehr zwischen ihnen mithilfe von privaten IPv4 Adressen oder IPv6 Adressen weiterleiten können. Instances in jeder der VPCs können so miteinander kommunizieren, als befänden sie sich im selben Netzwerk. Sie können eine VPC-Peering-Verbindung zwischen Ihrem eigenen VPCs Konto oder mit einer VPC in einem anderen Konto herstellen. AWS VPCs Sie können sich in verschiedenen Regionen befinden (auch als interregionale 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 diese Konten miteinander verknüpfen, um ein Filesharing-Netzwerk zu erstellen. VPCs Sie können auch eine VPC-Peering-Verbindung verwenden, um anderen den Zugriff auf Ressourcen VPCs zu ermöglichen, die Sie in einer Ihrer haben. VPCs

Wenn Sie Peering-Beziehungen zwischen verschiedenen VPCs 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 bleibt im privaten IP-Adressbereich. 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 S-Angriffe reduziert werden. DDo Regionsübergreifendes VPC-Peering ist eine einfache und kostengünstige Möglichkeit, Ressourcen zwischen Regionen zu teilen oder Daten für eine 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, ist kostenlos, auch wenn sie zwischen verschiedenen Konten erfolgt. Für die Datenübertragung über VPC-Peering-Verbindungen, die Availability Zones und Regionen überschreiten, fallen Gebühren an. Weitere Informationen finden Sie unter EC2 Amazon-Preise EC2 .

So funktionieren VPC-Peering-Verbindungen

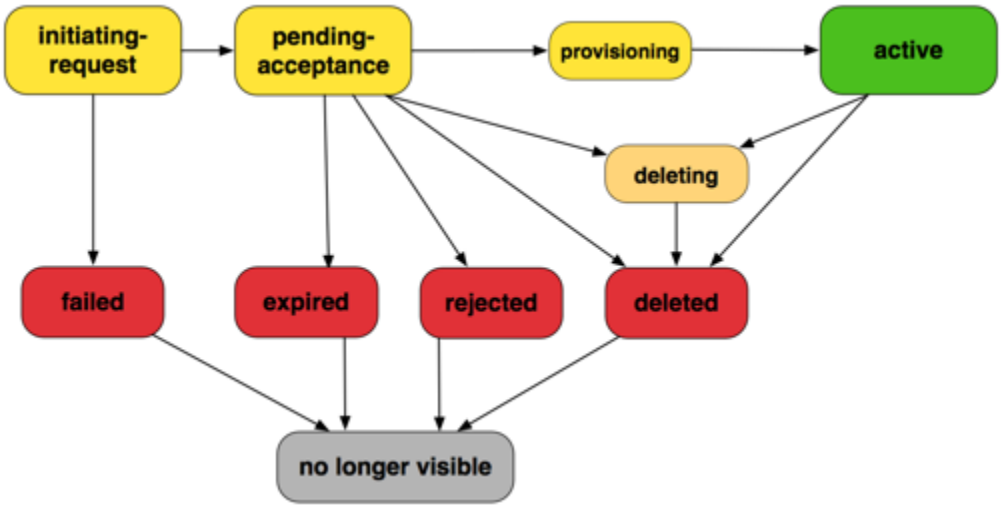
Die folgenden Schritte beschreiben den VPC-Peering-Prozess:

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 Besitzer der akzeptierenden VPC akzeptiert die VPC-Peering-Verbindungsanfrage zur Aktivierung der VPC-Peering-Verbindung.
3. Um den Verkehrsfluss zwischen den VPCs verwendeten privaten IP-Adressen zu ermöglichen, muss der Besitzer jeder VPC in der VPC-Peering-Verbindung manuell eine Route zu einer oder mehreren seiner VPC-Routentabellen 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 VPCs sich beide 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 Instance aufgelöst, wenn sich EC2 Instances auf beiden Seiten einer VPC-Peering-Verbindung gegenseitig mit einem öffentlichen DNS-Hostnamen adressieren. EC2
   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 über einen öffentlichen DNS-Hostnamen ansprechen, wird der Hostname nach der Aktivierung der DNS-Hostnamenauflösung in die private IP-Adresse der Instanz aufgelöst. EC2

Weitere Informationen finden Sie unter 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 der Verkehr kann zwischen den fließen VPCs (vorausgesetzt, dass Ihre Sicherheitsgruppen und Routing-Tabellen den Verkehrsfluss zulassen). In diesem Status können beide VPC-Eigentümer die VPC-Peering-Verbindung löschen, aber nicht ablehnen.

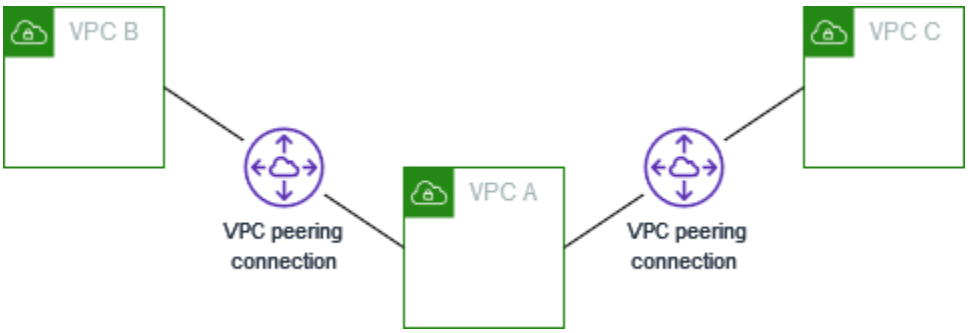
  > **Note**
  >
  > Falls ein Ereignis in einer Region, in der sich eine VPC befindet, den Datenverkehr verhindert, bleibt der Status der VPC-Peering-Verbindung `Active`.

- 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. Falls die VPC-Peering-Verbindung innerhalb desselben AWS -Kontos erstellt worden ist, bleibt die gelöschte Anforderung 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. Sie haben keine Peering-Beziehung mit VPCs der Ihre VPC nicht direkt verbunden ist.

Das folgende Diagramm ist ein Beispiel für eine VPC, die mit zwei verschiedenen VPCs verbunden ist. VPCs 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 für Transit-Gateway-Szenarien 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 zwei 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 in RFC 1918 angegebenen privaten 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 für die Kommunikation aktivieren. IPv6 Sie müssen jeder VPC einen IPv6 CIDR-Block zuordnen, die Instances für die IPv6 Kommunikation aktivieren und den VPCs für die Peer-VPC bestimmten IPv6 Datenverkehr an die VPC-Peering-Verbindung weiterleiten.
- 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 solchen mit übereinstimmenden oder überlappenden IPv4 oder CIDR-Blöcken herstellen. IPv6
- Wenn Sie über mehrere IPv4 CIDR-Blöcke verfügen, können Sie keine VPC-Peering-Verbindung erstellen, wenn sich einer der CIDR-Blöcke überschneidet, auch wenn Sie nur die nicht überlappenden CIDR-Blöcke oder nur CIDR-Blöcke verwenden möchten. IPv6

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 VPCs haben zusammen gebündelt.

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

- Bei Jumbo-Frames beträgt die maximale Übertragungseinheit (MTU) zwischen VPC-Peering-Verbindungen innerhalb derselben Region 9001 Byte. Die MTU für VPC-Peering-Verbindungen zwischen Regionen beträgt 8500 Byte. Weitere Informationen zu Jumbo Frames finden Sie unter Jumbo Frames (9001 MTU) im EC2 Amazon-Benutzerhandbuch.
- Sie müssen die DNS-Auflösungsunterstützung für die VPC-Peering-Verbindung aktivieren, um private DNS-Hostnamen der gepeerten VPC in private IP-Adressen aufzulösen, auch wenn der IPv4 CIDR für die VPC in die in RFC 1918 angegebenen privaten IPv4 Adressbereiche fällt.

VPCs Gemeinsam genutzte Netze 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.

VPC-Peering-Verbindungen

Mit VPC-Peering können Sie zwei VPCs in derselben oder unterschiedlichen AWS Regionen verbinden. So können Instances in einer VPC mit Instances in der anderen VPC kommunizieren, als ob sie alle Teil desselben Netzwerks wären.

VPC-Peering erstellt eine direkte Netzwerkroute zwischen den beiden VPCs mithilfe von privaten IPv4 Adressen oder IPv6 Adressen. Der Datenverkehr, der zwischen den verbundenen VPCs Personen gesendet wird, durchquert weder das Internet noch eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung. Dies macht das VPC-Peering zu einer sicheren Methode, um Ressourcen wie Datenbanken oder Webserver über VPC-Grenzen hinweg gemeinsam zu nutzen.

Um eine VPC-Peering-Verbindung herzustellen, erstellen Sie eine Peering-Verbindungsanfrage von einer VPC und der Besitzer der anderen VPC akzeptiert die Anfrage. Nachdem die Verbindung hergestellt wurde, können Sie Ihre Routentabellen aktualisieren, um den Verkehr zwischen den weiterzuleiten. VPCs Dadurch können Instances in einer VPC auf Ressourcen in der anderen VPC zugreifen.

VPC-Peering ist ein wichtiges Tool für den Aufbau von Multi-VPC-Architekturen und die gemeinsame Nutzung von Ressourcen über Unternehmensgrenzen in AWS hinweg. Es bietet eine einfache Möglichkeit, eine Verbindung mit niedriger Latenz herzustellen, VPCs ohne die Komplexität der Konfiguration eines VPN oder eines anderen Netzwerkdienstes.

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

Aufgaben

- Erstellen einer VPC-Peering-Verbindung
- Eine VPC-Peering-Verbindung akzeptieren oder ablehnen
- Aktualisieren Sie ihre Routing-Tabellen für eine VPC-Peering-Verbindung
- Aktualisieren Ihrer Sicherheitsgruppen, um auf Peer-Sicherheitsgruppen zu verweisen
- Aktivieren einer DNS-Auflösungsunterstützung für eine VPC-Peering-Verbindung
- 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. Zur Aktivierung der Anforderung muss der Eigentümer der annehmenden VPC die Anforderung akzeptieren. Die folgenden Peering-Verbindungen werden unterstützt:

- Zwischen VPCs demselben Konto und derselben Region
- Zwischen VPCs demselben Konto und verschiedenen Regionen
- Zwischen VPCs verschiedenen Konten und derselben Region
- Zwischen VPCs verschiedenen Konten und Regionen

Für eine regionsübergreifende VPC-Peering-Verbindung muss die Anfrage von der Region der anfordernden VPC aus gestellt werden, und die Anfrage muss von der Region der akzeptierenden VPC akzeptiert werden. Weitere Informationen finden Sie unter the section called “Akzeptieren oder ablehnen”.

Aufgaben

Voraussetzungen

- Lesen Sie die Einschränkungen für VPC-Peering-Verbindungen.
- Stellen Sie sicher, dass VPCs sie keine überlappenden CIDR-Blöcke IPv4 haben. Wenn sie sich überlappen, ändert sich der Status der VPC-Peering-Verbindung direkt in `failed`. Diese Einschränkung gilt auch dann, wenn sie eindeutige IPv6 CIDR-Blöcke VPCs haben.

Stellen Sie mithilfe der Konsole eine Peering-Verbindung her

Gehen Sie wie folgt vor, um eine VPC-Peering-Verbindung herzustellen.

So erstellen Sie eine Peering-Verbindung mithilfe der Konsole

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. (Optional) Geben Sie unter Name einen Namen für die VPC-Peering-Verbindung an. Dadurch wird ein Tag mit einem Schlüssel von erstellt Name und der Wert, den Sie angeben.
5. Wählen Sie für VPC-ID (Requester) eine VPC aus dem aktuellen Konto aus.
6. Gehen Sie unter Andere VPC für Peering auswählen wie folgt vor:
   a. Wählen Sie unter Konto die Option Anderes Konto aus, um Peering mit einer VPC in einem anderen Konto durchzuführen, und geben Sie die Konto-ID ein. Andernfalls behalten Sie Mein Konto.
   b. Um mit einer VPC in einer anderen Region eine Verbindung herzustellen, wählen Sie unter Region die Option Andere Region und dann die Region aus. Andernfalls behalten Sie Diese Region bei.
   c. Wählen Sie für VPC-ID (Accepter) eine VPC aus dem angegebenen Konto und der angegebenen Region aus.
7. (Optional) Sie fügen ein Tag hinzu, indem Sie Add new tag (Neuen Tag hinzufügen) auswählen und den Tag-Schlüssel und -Wert eingeben.
8. Wählen Sie Create peering connection (Peering-Verbindung erstellen).
9. Der Besitzer des akzeptierenden Kontos muss die Peering-Verbindung akzeptieren. Weitere Informationen finden Sie unter the section called “Akzeptieren oder ablehnen”.
10. Aktualisieren Sie die Routentabellen für beide VPCs , um die Kommunikation zwischen ihnen zu ermöglichen. Weitere Informationen finden Sie unter the section called “Aktualisieren von Routing-Tabellen”.

Erstellen Sie über die Befehlszeile eine Peering-Verbindung

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)

Eine VPC-Peering-Verbindung akzeptieren oder ablehnen

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 VPC-Peering-Verbindungsanfrage annehmen, die Sie an ein anderes AWS Konto gesendet haben. Um eine VPC-Peering-Verbindung zwischen VPCs demselben AWS Konto herzustellen, können Sie die Anfrage sowohl selbst erstellen als auch annehmen.

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 akzeptieren AWS-Konten , die Sie kennen und denen Sie vertrauen. Sie können alle unerwünschten Anfragen ablehnen. Weitere Informationen zum `Rejected`-Peering-Verbindungsstatus finden Sie unter Lebenszyklus einer VPC-Peering-Verbindung.

> **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 VPC-Peering-Verbindungsanfragen sicher ablehnen, ohne dass das Risiko besteht, dass der Anforderer Zugriff auf Informationen über Ihr AWS Konto oder Ihre VPC erhält. Weitere Informationen finden Sie unter Eine VPC-Peering-Verbindung akzeptieren oder ablehnen. Sie können eine solche Anforderung auch ignorieren und sie verfallen lassen; standardmäßig verfallen Anforderungen nach sieben Tagen.

So akzeptieren oder lehnen Sie eine Peering-Verbindung über die Konsole ab

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 die VPC-Peering-Verbindung aus und klicken Sie auf Aktionen und Anforderung ablehnen, um eine Peering-Verbindung abzulehnen. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Anforderung ablehnen aus.

5. Wählen Sie erst die ausstehende VPC-Peering-Verbindung (der Status lautet `pending-acceptance`) und dann Aktionen und Anforderung akzeptieren aus, um eine Peering-Verbindung zu akzeptieren. Weitere Informationen zum Lebenszyklusstatus von Peering-Verbindungen finden Sie unter Lebenszyklus einer VPC-Peering-Verbindung.

   Wenn keine VPC-Peering-Verbindung aussteht, stellen Sie sicher, dass Sie die Region der akzeptierenden VPC ausgewählt haben.
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.

Um eine Peering-Verbindung über die Befehlszeile zu akzeptieren

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

Um eine Peering-Verbindung über die Befehlszeile abzulehnen

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

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

Um privaten IPv4 Verkehr zwischen Peering-Instances zu ermöglichen VPCs, müssen Sie den Routing-Tabellen, die den Subnetzen für beide Instances zugeordnet sind, eine Route hinzufügen. 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 Routing-Tabellen, die die Kommunikation zwischen Instances in zwei Peering-Instanzen VPCs, VPC A und VPC B, ermöglichen. Jede Tabelle hat 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 VPCs der VPC-Peering-Verbindung IPv6 CIDR-Blöcke zugeordnet sind, Routen hinzufügen, die die Kommunikation mit der Peer-VPC ermöglichen. IPv6

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

Überlegungen

- Wenn Sie über ein Peering mit mehreren VPC verfügen VPCs , die überlappende oder übereinstimmende IPv4 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 keine Unicast-Reverse-Path-Weiterleitung in VPC-Peering-Verbindungen, die die Quell-IP von Paketen überprüft und Antwortpakete zurück an die Quelle weiterleitet. 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 eine IPv4 Route für eine VPC-Peering-Verbindung 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 Aktionen und dann Routen bearbeiten.
5. Wählen Sie Route hinzufügen aus.
6. Geben Sie unter Ziel den IPv4 Adressbereich ein, an den der Netzwerkverkehr in der VPC-Peering-Verbindung geleitet werden muss. Sie können den gesamten IPv4 CIDR-Block der Peer-VPC, einen bestimmten Bereich oder eine einzelne IPv4 Adresse angeben, z. B. die IP-Adresse der Instance, mit der kommuniziert werden 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 Änderungen speichern aus.

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 über Ressourcen in verschiedenen AWS Regionen verfügen, die IPv6 Adressen verwenden, können Sie eine regionsübergreifende Peering-Verbindung herstellen. Anschließend können Sie eine IPv6 Route für die Kommunikation zwischen den Ressourcen hinzufügen.

So fügen Sie eine IPv6 Route für eine VPC-Peering-Verbindung 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 Route hinzufügen aus.
6. Geben Sie unter Ziel den IPv6 Adressbereich für die Peer-VPC ein. Sie können den gesamten IPv6 CIDR-Block der Peer-VPC, einen bestimmten Bereich oder eine einzelne IPv6 Adresse angeben. 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 Änderungen speichern aus.

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

Um eine Route über die Befehlszeile hinzuzufügen oder zu ersetzen

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

Aktualisieren Ihrer Sicherheitsgruppen, um auf Peer-Sicherheitsgruppen zu verweisen

Sie können die Regeln für eingehende oder ausgehende Nachrichten für Ihre VPC-Sicherheitsgruppen aktualisieren, sodass sie auf Sicherheitsgruppen für Peered verweisen. VPCs Danach kann der Datenverkehr von und zu den Instances fließen, die der referenzierten Sicherheitsgruppe in der über Peering verbundenen VPC zugewiesen sind.

> **Note**
>
> Sicherheitsgruppen in einer Peer-VPC werden nicht in der Konsole angezeigt, um sie auswählen zu können.

Voraussetzungen

- Um auf eine Sicherheitsgruppe in einer Peer-VPC zu verweisen, muss die VPC-Peering-Verbindung den Status `active` haben.
- Die Peer-VPC kann eine VPC in Ihrem Konto oder eine VPC in einem anderen Konto sein. AWS Um auf eine Sicherheitsgruppe zu verweisen, die sich in einem anderen AWS Konto, aber

derselben Region befindet, geben Sie die Kontonummer mit der ID der Sicherheitsgruppe an. Beispiel, `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.
- 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. Wählen Sie die Sicherheitsgruppe aus und führen Sie einen der folgenden Schritte aus:
   - Um Regeln für eingehenden Datenverkehr zu ändern, wählen Sie Aktionen, Regeln für eingehenden Datenverkehr bearbeiten aus.
   - Um Regeln für ausgehenden Datenverkehr zu ändern, wählen Sie Aktionen, Regeln für ausgehenden Datenverkehr bearbeiten aus.
4. Um eine Regel hinzuzufügen, wählen Sie Regel hinzufügen und geben Sie bei Bedarf den Typ, das Protokoll und den Portbereich an. Für Quelle (Regel für eingehenden Datenverkehr) oder Ziel (Regel für ausgehenden Datenverkehr) aus und führen Sie einen der folgenden Schritte aus:
   - Geben Sie für eine Peer-VPC in demselben Konto und in derselben Region die ID der Sicherheitsgruppe ein.
   - Geben Sie für eine Peer-VPC in einem anderen Konto, aber in derselben Region, die Konto-ID und die Sicherheitsgruppen-ID ein, getrennt durch einen Schrägstrich (z. B.`123456789012/sg-1a2b3c4d`).
   - Geben Sie für eine Peer-VPC in einer anderen Region den CIDR-Block der Peer-VPC ein.
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 und revoke-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress und Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

Sie können beispielsweise den folgenden Befehl verwenden, um Ihre Sicherheitsgruppe `sg-aaaa1111` so zu aktualisieren, dass eingehender Datenverkehr über HTTP von `sg-bbbb2222` für eine Peer-VPC zulässig ist: Wenn sich die Peer-VPC in derselben Region, aber in einem anderen Konto befindet, fügen Sie hinzu `--group-owner`*`aws-account-id`*.

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

So aktualisieren Sie Regeln für ausgehenden Datenverkehr über die Befehlszeile

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

Nachdem Sie die Sicherheitsgruppenregeln aktualisiert haben, verwenden Sie den describe-security-groupsBefehl, um die Sicherheitsgruppe anzuzeigen, auf die in Ihren Sicherheitsgruppenregeln verwiesen wird.

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)

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.

Sicherheitsgruppenregeln anzeigen und löschen

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 die Regel nicht mehr als veraltet markiert, wenn Sie mit derselben eine neue VPC-Peering-Verbindung erstellen. VPCs

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 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 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).

Um Ihre veralteten Sicherheitsgruppenregeln mithilfe der Befehlszeile zu beschreiben

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

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"
        }
    ]
```

```
}
```

Nachdem Sie die veralteten Sicherheitsgruppenregeln identifiziert haben, können Sie sie mit den Befehlen revoke-security-group-ingressoder revoke-security-group-egresslöschen.

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

Die DNS-Einstellungen für eine VPC-Peering-Verbindung bestimmen, wie öffentliche DNS-Hostnamen für Anfragen aufgelöst werden, die die VPC-Peering-Verbindung durchqueren. Wenn eine EC2 Instance auf der einen Seite einer VPC-Peering-Verbindung unter Verwendung des öffentlichen IPv4 DNS-Hostnamens der EC2 Instance eine Anfrage an eine Instance auf der anderen Seite sendet, wird der DNS-Hostname wie folgt aufgelöst.

Die DNS-Auflösung ist deaktiviert (Standard)

Der öffentliche IPv4 DNS-Hostname wird in die öffentliche IPv4 Adresse der Instanz aufgelöst.

DNS-Auflösung aktiviert

Der öffentliche IPv4 DNS-Hostname wird in die private IPv4 Adresse der Instanz aufgelöst.

Voraussetzungen

- Beide VPCs müssen für DNS-Hostnamen und DNS-Auflösung aktiviert sein. Weitere Infomationen finden Sie unter DNS-Attribute für Ihre VPC im Amazon VPC-Benutzerhandbuch.
- Die Peering-Verbindung muss sich im `active` Status befinden. Sie können die DNS-Auflösung nicht aktivieren, wenn Sie eine Peering-Verbindung herstellen.
- Der Besitzer der Anforderer-VPC muss die VPC-Peering-Optionen des Anforderers ändern, und der Besitzer der akzeptierenden VPC muss die VPC-Peering-Optionen des Anforderers ändern. Wenn sie sich im selben Konto und in derselben Region VPCs befinden, können Sie die DNS-Auflösung für den Anforderer und den Akzeptierenden gleichzeitig aktivieren. VPCs

So aktivieren Sie die DNS-Auflösung für eine Peering-Verbindung mithilfe der Konsole

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 Aktionen, DNS-Einstellungen bearbeiten aus.
5. Um die DNS-Auflösung für Anfragen von der VPC des Anforderers zu aktivieren, wählen Sie DNS-Auflösung des Anforderers, Zulassen, dass die akzeptierende VPC den DNS der anfordernden VPC auflöst.
6. Um die DNS-Auflösung für Anfragen von der akzeptierenden VPC sicherzustellen, wählen Sie Accepter DNS resolution, Allow Requester VPC to resolve the DNS of Accepter VPC.
7. Wählen Sie Änderungen speichern aus.

Um die DNS-Auflösung über die Befehlszeile zu aktivieren

- modify-vpc-peering-connection-Optionen ()AWS CLI
- Edit-EC2VpcPeeringConnectionOption (AWS Tools for Windows PowerShell)

Um die Verbindungsoptionen für das VPC-Peering mithilfe der Befehlszeile zu beschreiben

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

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

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

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. Dadurch wird sichergestellt, dass der Netzwerkverkehr ordnungsgemäß zwischen den beiden fließen kann. VPCs Weitere Informationen finden Sie unter Aktualisieren von Routing-Tabellen.
- Stellen Sie für alle beteiligten EC2 Instances sicher, dass die Sicherheitsgruppen für diese Instances eingehenden und ausgehenden Datenverkehr von der Peer-VPC zulassen. Sicherheitsgruppenregeln steuern, welcher Datenverkehr auf Ihre Instances zugreifen darf. EC2 Weitere Informationen finden Sie unter Auf Peer-Sicherheitsgruppen verweisen.
- Vergewissern Sie sich, dass das Netzwerk ACLs für die Subnetze, die Ihre Ressourcen enthalten, den erforderlichen Datenverkehr von der Peer-VPC zulässt. Netzwerke ACLs sind eine zusätzliche Sicherheitsebene, die den Verkehr auf Subnetzebene filtert.

Wenn Sie immer noch Probleme haben, können Sie Reachability Analyzer verwenden. Reachability Analyzer kann dabei helfen, die spezifische Komponente zu identifizieren — sei es eine Routing-Tabelle, eine Sicherheitsgruppe oder eine Netzwerk-ACL —, die das Konnektivitätsproblem zwischen den beiden verursacht. VPCs Weitere Informationen finden Sie im Leitfaden Reachability Analyzer.

Eine gründliche Überprüfung Ihrer VPC-Netzwerkkonfigurationen ist der Schlüssel zur Fehlerbehebung und Lösung aller Probleme mit der VPC-Peering-Verbindung, auf die Sie unter Umständen stoßen.

Gängige Konfigurationen für die VPC-Peering-Verbindung

In diesem Abschnitt werden zwei gängige Arten von VPC-Peering-Konfigurationen beschrieben, die Sie implementieren können:

- VPC-Peering-Konfigurationen mit Routen zu einer gesamten VPC: In dieser Konfiguration erstellen Sie in der Routing-Tabelle jeder VPC eine Route, die den gesamten für die Peer-VPC bestimmten Datenverkehr an die VPC-Peering-Verbindung leitet. Dadurch kann jede Ressource in einer VPC mit jeder Ressource in der Peer-VPC kommunizieren, was die Verwaltung vereinfacht. Dies bedeutet jedoch auch, dass der gesamte Datenverkehr zwischen den VPCs beiden über die Peering-Verbindung fließt, was bei einem hohen Verkehrsaufkommen zu einem Engpass werden kann.
- VPC-Peering-Konfigurationen mit spezifischen Routen: Alternativ können Sie in der Routing-Tabelle jeder VPC differenziertere Routen erstellen, die Datenverkehr nur an bestimmte Subnetze oder Ressourcen in der Peer-VPC leiten. Dadurch können Sie den Datenverkehr, der über die Peering-Verbindung fließt, auf das Notwendige beschränken, was effizienter sein kann. Allerdings ist damit auch ein höherer Wartungsaufwand verbunden, da Sie die Routing-Tabellen jedes Mal aktualisieren müssen, wenn Sie neue Ressourcen in der Peer-VPC hinzufügen, die kommunizieren müssen.

Der beste Ansatz hängt von Faktoren wie der Größe und Komplexität Ihrer VPC-Architektur, dem erwarteten Datenverkehrsvolumen zwischen den VPCs und Ihren organisatorischen Anforderungen in Bezug auf Sicherheit und Ressourcenzugriff ab. Viele Unternehmen verwenden einen hybriden Ansatz mit breiten Routen für gängige Datenverkehrsmuster und spezifischen Routen für sensiblere oder bandbreitenintensivere Anwendungsfälle.

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

Netzwerkszenarien einer VPC-Peering-Verbindung. Weitere Informationen zum Erstellen von und zum Arbeiten mit VPC-Peering-Verbindungen finden Sie unter VPC-Peering-Verbindungen.

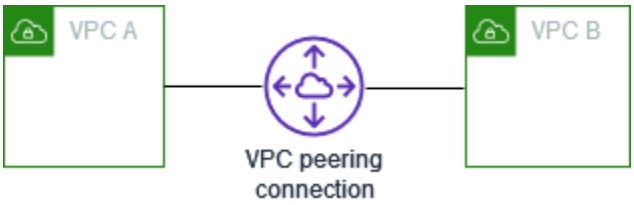
Weitere Informationen zur Aktualisierung Ihrer Routing-Tabellen finden Sie unter Aktualisieren Sie ihre Routing-Tabellen für eine VPC-Peering-Verbindung.

Konfigurationen

- Zwei VPCs schauten zusammen
- Eine VPC wurde mit zwei gepeert VPCs
- Drei VPCs haben zusammen gebündelt
- Mehrere haben zusammen gepeert VPCs

Zwei VPCs schauten zusammen

In dieser Konfiguration besteht eine Peering-Verbindung zwischen VPC A und VPC B (`pcx-11112222`). Sie VPCs sind identisch AWS-Konto und ihre CIDR-Blöcke überschneiden sich nicht.



Sie können diese Konfiguration verwenden, wenn Sie zwei haben VPCs , die Zugriff auf die Ressourcen des 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

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

Mehrere IPv4 VPC CIDRs

Wenn VPC A und VPC B mehrere zugeordnete IPv4 CIDR-Blöcke haben, können Sie die Routentabelle 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
	VPC A CIDR 1	pcx-11112222
	VPC A CIDR 2	pcx-11112222

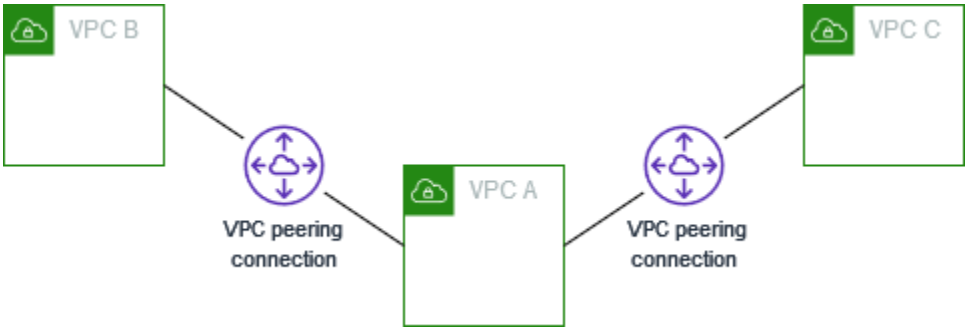
IPv4 und IPv6 VPC CIDRs

Wenn VPC A und VPC B zugeordnete IPv6 CIDR-Blöcke haben, können Sie die Routentabelle für jede VPC mit Routen sowohl für die als auch für die IPv6 CIDR-Blöcke der IPv4 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 wurde mit zwei gepeert VPCs

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 System AWS-Konto und ihre CIDR-Blöcke überschneiden sich nicht.



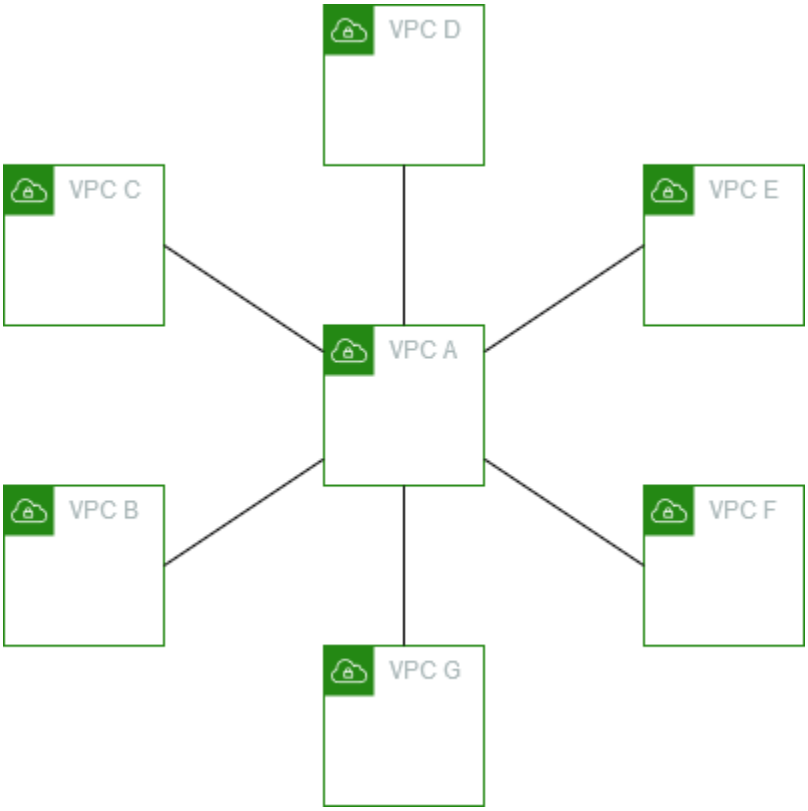
VPC B und VPC C können ihren Datenverkehr nicht direkt über VPC A aneinander senden, da VPC-Peering keine transitiven Peering-Beziehungen unterstützt. Sie können eine VPC-Peering-Verbindung zwischen VPC B und VPC C erstellen, wie in Drei VPCs haben zusammen gebündelt gezeigt. Weitere Informationen zu 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, z. B. ein Repository mit Diensten, auf die andere zugreifen VPCs müssen. Die anderen VPCs benötigen keinen Zugriff auf die Ressourcen der anderen; sie müssen nur auf Ressourcen in der zentralen VPC zugreifen.

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 weitere erweitern. VPCs Beispielsweise wird VPC A über VPC G mit VPC B gepeert, wobei IPv4 sowohl als auch verwendet wird IPv6 CIDRs, aber die anderen VPCs werden nicht miteinander gepeert. 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
	VPC D IPv4 CIDR	pcx-aaaadddd
	VPC D IPv6 CIDR	pcx-aaaadddd
	VPC E IPv4 CIDR	pcx-aaaaeeee

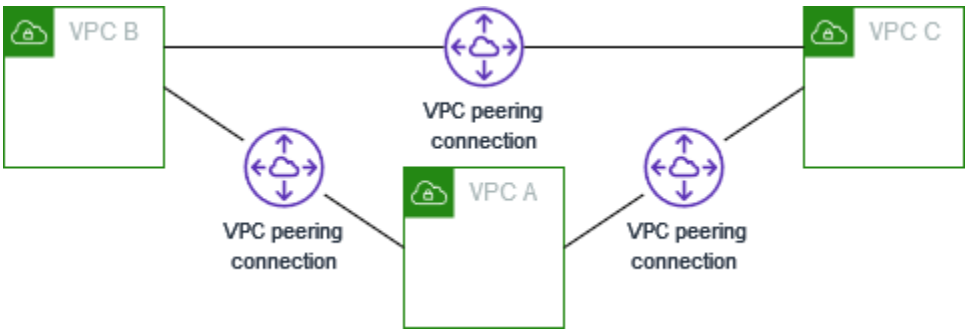
Routing-Tabelle	Zielbereich	Ziel
	VPC E IPv6 CIDR	pcx-aaaaeeee
	VPC F IPv4 CIDR	pcx-aaaaffff
	VPC F IPv6 CIDR	pcx-aaaaffff
	VPC G IPv4 CIDR	pcx-aaaagggg
	VPC G IPv6 CIDR	pcx-aaaagggg
VPC B	*VPC B IPv4 CIDR*	Local
	VPC B IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
VPC C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

Routing-Tabelle	Zielbereich	Ziel
	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 VPCs haben zusammen gebündelt

In dieser Konfiguration gibt es drei VPCs gleiche AWS-Konto CIDR-Blöcke, die sich nicht überlappen. Sie VPCs werden wie folgt in einem vollständigen Netz miteinander verbunden:

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

Routing-Tabellen	Bestimmungsort	Ziel
VPC A	*VPC A IPv4 CIDR*	Local
	VPC A IPv6 CIDR	Local
	VPC B IPv4 CIDR	pcx-aaaabbbb

Routing-Tabellen	Bestimmungsort	Ziel
	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

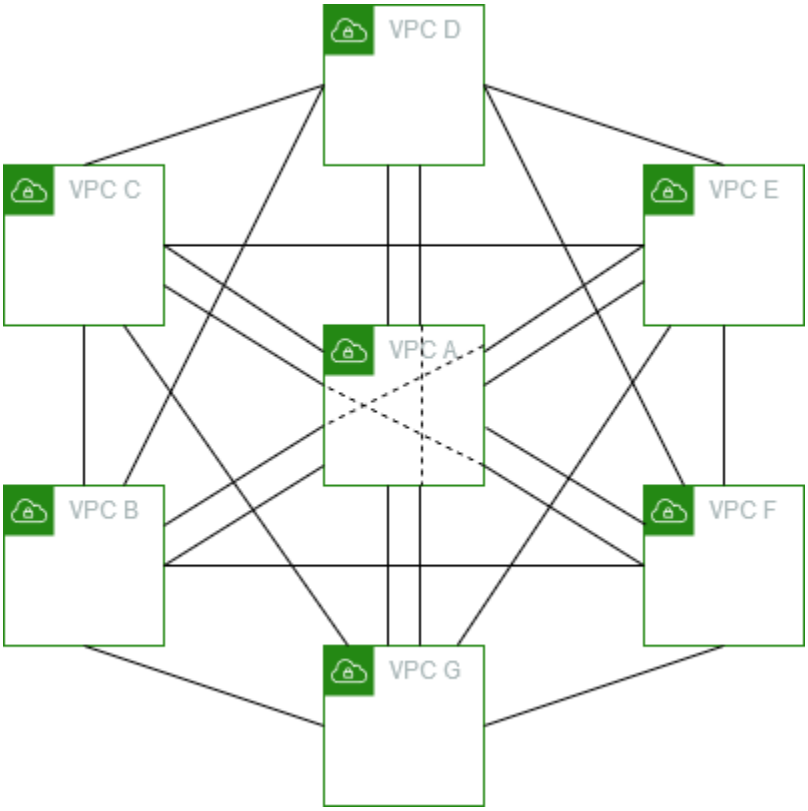
Mehrere haben zusammen gepeert VPCs

In dieser Konfiguration gibt es sieben VPCs Peering-Verbindungen in einer vollständigen Mesh-Konfiguration. Sie VPCs sind identisch AWS-Konto und ihre CIDR-Blöcke überschneiden sich nicht.

VPC	VPC	VPC-Peering-Verbindung
A	B	pcx-aaaabbbb
A	C	pcx-aaaacccc
A	D	pcx-aaaadddd
A	E	pcx-aaaaeeee
A	F	pcx-aaaaffff
A	G	pcx-aaaagggg

VPC	VPC	VPC-Peering-Verbindung
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 Konfiguration verwenden, wenn Sie mehrere haben VPCs , 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
	VPC G CIDR	pcx-aaaagggg
VPC B	*VPC B CIDR*	Local

Routing-Tabelle	Zielbereich	Ziel
	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
	VPC F CIDR	pcx-ddddffff
	VPC G CIDR	pcx-ddddgggg

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

Routing-Tabelle	Zielbereich	Ziel
	VPC F CIDR	pcx-ffffgggg

Wenn allen IPv6 CIDR-Blöcke zugeordnet VPCs sind, aktualisieren Sie die Routentabellen 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
VPC B	*VPC B IPv4 CIDR*	Local
	VPC B IPv6 CIDR	Local

Routing-Tabelle	Zielbereich	Ziel
	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
	VPC D IPv4 CIDR	pcx-ccccdddd
	VPC D IPv6 CIDR	pcx-ccccdddd

Routing-Tabelle	Zielbereich	Ziel
	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
	VPC G IPv4 CIDR	pcx-ddddgggg
	VPC G IPv6 CIDR	pcx-ddddgggg

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 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
	VPC B IPv4 CIDR	pcx-bbbbffff
	VPC B IPv6 CIDR	pcx-bbbbffff

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

Routing-Tabelle	Zielbereich	Ziel
	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 überlappenden CIDR-Blöcken VPCs per Peering verbunden.

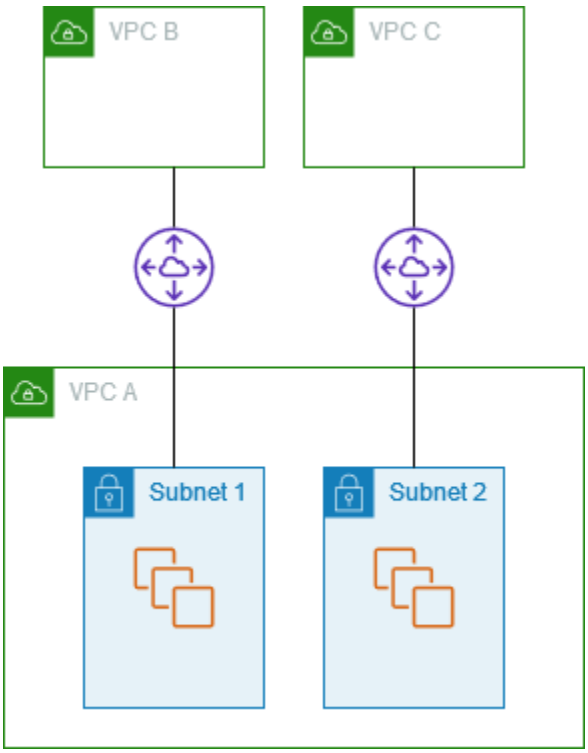
Weitere Beispiele zu Szenarien, in denen Sie eine spezifische VPC-Peering-Verbindungskonfiguration benötigen, finden Sie unter Netzwerkszenarien einer VPC-Peering-Verbindung. Weitere Informationen zum Erstellen von und zum Arbeiten mit VPC-Peering-Verbindungen finden Sie unter VPC-Peering-Verbindungen. 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 CIDR-Blöcke in einer VPC zugreifen
- Eine VPC, die auf bestimmte Subnetze in zwei zugreift VPCs
- Instances in einer VPC, die auf bestimmte Instances in zwei zugreifen VPCs
- Eine VPC, die VPCs mit den längsten Präfixübereinstimmungen auf zwei zugreift
- 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
	Subnet 1 CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local

Routing-Tabelle	Zielbereich	Ziel
	Subnet 2 CIDR	pcx-aaaacccc

Sie können diese Konfiguration auf mehrere CIDR-Blöcke erweitern. Nehmen wir an, dass VPC A und VPC B sowohl IPv4 CIDR-Blöcke als auch IPv6 CIDR-Blöcke haben und dass Subnetz 1 über einen zugehörigen CIDR-Block verfügt. IPv6 Sie können VPC B für die Kommunikation mit Subnetz 1 in VPC A über die IPv6 VPC-Peering-Verbindung aktivieren. Fügen Sie dazu der Routentabelle für VPC A eine Route mit einem Ziel des IPv6 CIDR-Blocks für VPC B und eine Route zur Routentabelle für VPC B mit einem Ziel des 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	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	Lokale Route, die automatisch für die IPv6 Kommunikation innerhalb der VPC hinzugefügt wird.
	VPC C IPv4 CIDR	pcx-aaaacccc	
VPC B	*VPC B IPv4 CIDR*	Local	

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

Zwei VPCs , die auf bestimmte CIDR-Blöcke in einer VPC zugreifen

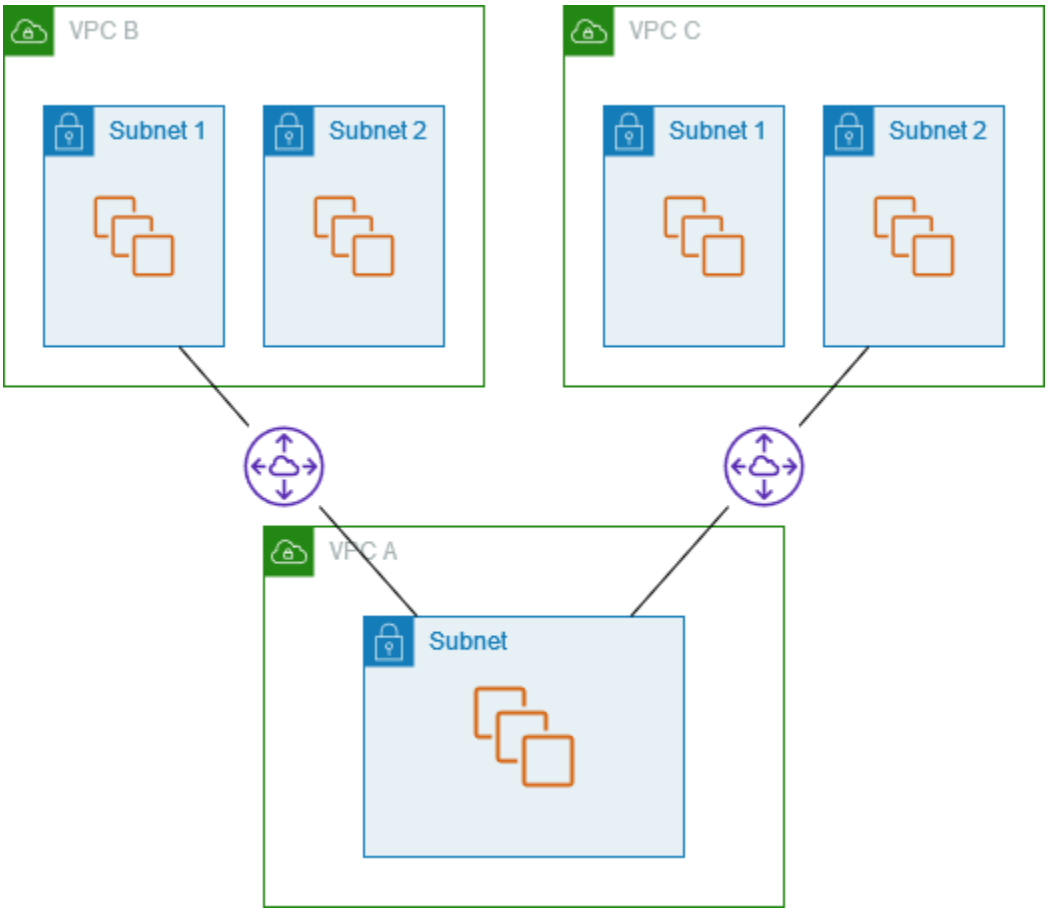
Die Konfiguration enthält eine zentrale VPC (VPC A), eine Peering-Verbindung zwischen VPC A und VPC B (`pcx-aaaabbbb`) und eine Peering-Verbindung zwischen VPC A und VPC C (`pcx-aaaacccc`). VPC A hat einen CIDR-Block für jede VPC-Peering-Verbindung.

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

Routing-Tabelle	Zielbereich	Ziel
	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 zugreift VPCs

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 über eine zentrale VPC verfügen, die über einen einzigen Satz von Ressourcen verfügt, z. B. Active Directory-Dienste, auf die andere zugreifen VPCs müssen. Die zentrale VPC benötigt keinen vollen Zugriff auf VPCs die, mit der sie gepeert wird.

Die Routentabelle für VPC A verwendet die Peering-Verbindungen, um nur auf bestimmte Subnetze im Peering zuzugreifen. VPCs 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
	Subnet 1 CIDR	pcx-aaaabbbb
	Subnet 2 CIDR	pcx-aaaacccc
Subnetz 1 (VPC B)	*VPC B CIDR*	Local
	Subnet in VPC A CIDR	pcx-aaaabbbb
Subnetz 2 (VPC C)	*VPC C CIDR*	Local
	Subnet in VPC A CIDR	pcx-aaaacccc

Routing für Antwortdatenverkehr

Wenn Sie über ein Peering mit mehreren VPC verfügen VPCs , die überlappende oder übereinstimmende 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 keine Unicast-Reverse-Path-Weiterleitung in VPC-Peering-Verbindungen, die die Quell-IP von Paketen überprüft und Antwortpakete zurück an die Quelle weiterleitet.

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
	Subnet 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 2 in VPC B und mit Subnetz 1 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.

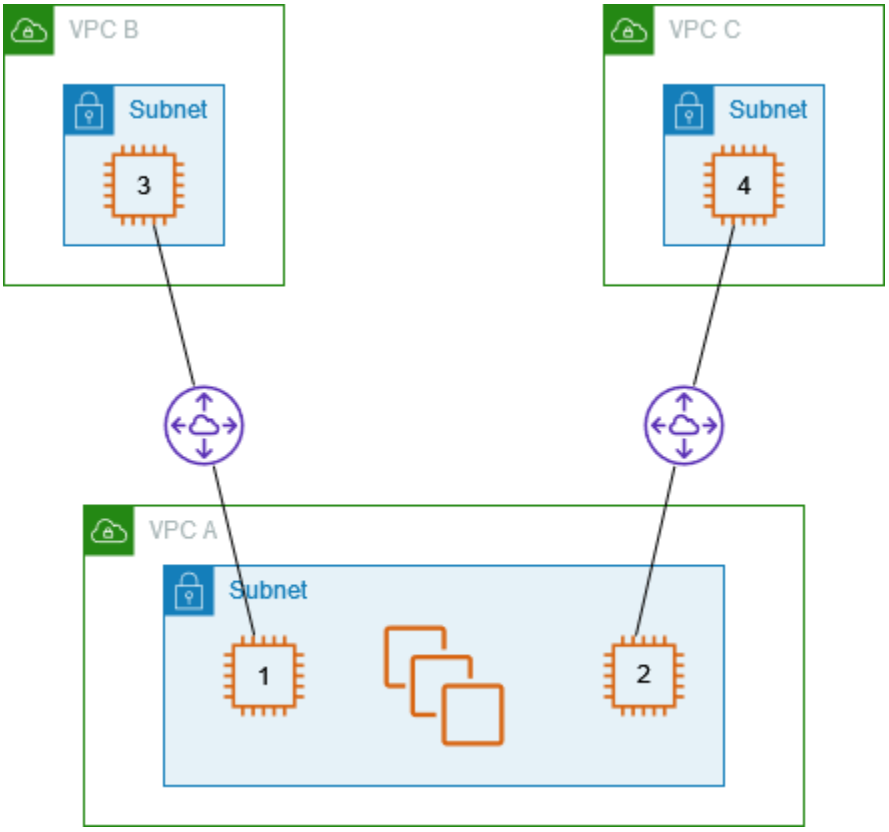
Bestimmungsort	Ziel
VPC A CIDR	Local
Subnet 2 CIDR	pcx-aaaabbbb
Subnet 1 CIDR	pcx-aaaacccc

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
Specific IP address in subnet 2	pcx-aaaabbbb
VPC B CIDR	pcx-aaaacccc

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

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.

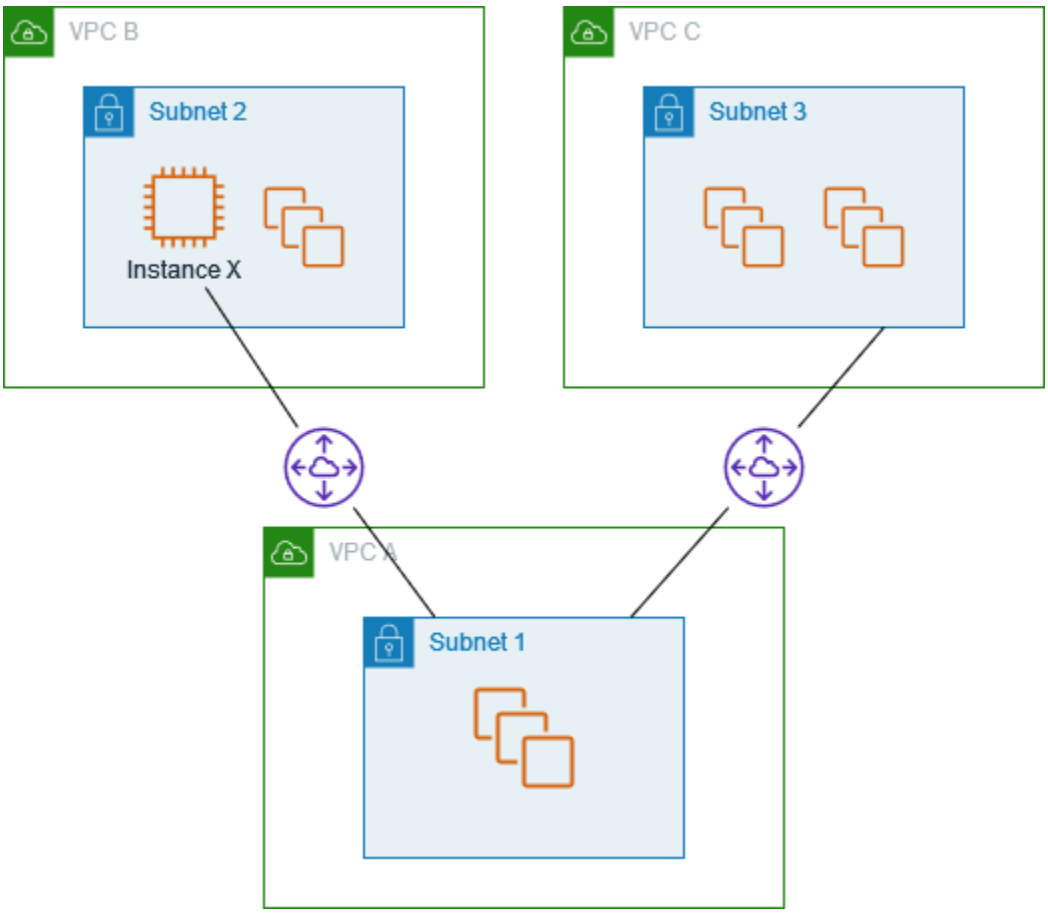


Jede VPC-Routing-Tabelle zeigt auf die relevante VPC-Peering-Verbindung, um so auf eine einzelne IP-Adresse (und somit auf eine bestimmte Instance) im Peer-VPC zugreifen zu können.

Routing-Tabelle	Zielbereich	Ziel
VPC A	*VPC A CIDR*	Local
	Instance 3 IP address	pcx-aaaabbbb
	Instance 4 IP address	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local
	Instance 1 IP address	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local
	Instance 2 IP address	pcx-aaaacccc

Eine VPC, die VPCs mit den längsten Präfixübereinstimmungen auf zwei 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 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 address	pcx-aaaabbbb
	VPC C CIDR block	pcx-aaaacccc
VPC B	*VPC B CIDR block*	Local
	VPC A CIDR block	pcx-aaaabbbb
VPC C	*VPC C CIDR block*	Local

Routing-Tabelle	Zielbereich	Ziel
	VPC A CIDR block	pcx-aaaacccc

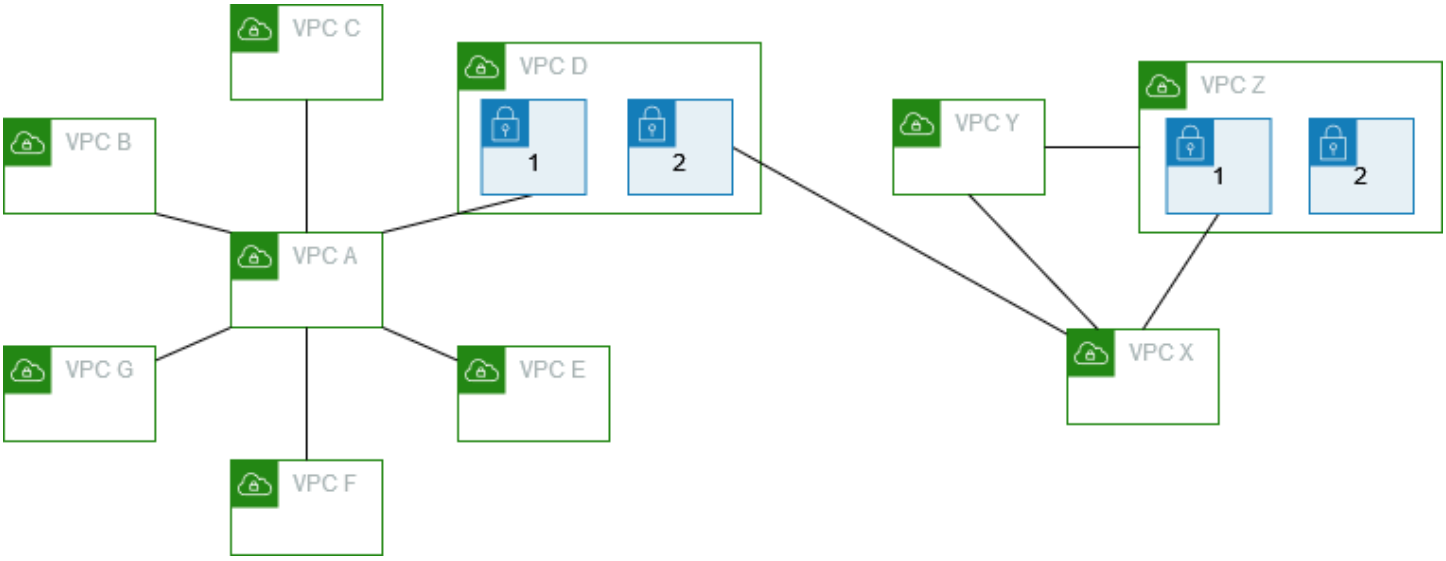
> **Important**
>
> Wenn eine andere Instance als Instance X in VPC B Verkehr an VPC A sendet, wird der Antwortverkehr möglicherweise an VPC C statt an VPC B weitergeleitet. Weitere Informationen finden Sie unter Routing für Antwortdatenverkehr.

Mehrere VPC-Konfigurationen

In dieser Konfiguration gibt es eine zentrale VPC (VPC A), die mit mehreren VPCs in einer Spoke-Konfiguration per Peering verbunden ist. In einer vollständigen Mesh-Konfiguration haben Sie außerdem drei VPCs (VPCs X, Y und Z) per Peering miteinander verbunden.

VPC D hat außerdem eine VPC-Peering-Verbindung mit VPC X (`pcx-ddddxxxx`). VPC A und VPC X haben überlappende CIDR-Blöcke. Das bedeutet, dass der Peering-Verkehr zwischen VPC A und VPC D auf ein bestimmtes Subnetz (Subnetz 1) in VPC D beschränkt ist. Dadurch soll sichergestellt werden, dass, wenn VPC D eine Anfrage von VPC A oder VPC X empfängt, der Antwortverkehr an die richtige VPC gesendet wird. AWS unterstützt keine Unicast-Reverse-Path-Weiterleitung in VPC-Peering-Verbindungen, die 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 Routentabellen 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 Routentabelle von VPC A verweist auf die entsprechenden Peering-Verbindungen für VPCs B, C, E, F und G, um auf ihre vollständigen 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
	Subnet 1 CIDR in VPC D	pcx-aaaadddd
	VPC E CIDR	pcx-aaaaeeee

Routing-Tabelle	Zielbereich	Ziel
	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-aaaaaffff
VPC G	*VPC G CIDR*	Local
	VPC A CIDR	pcx-aaaagggg
VPC X	*VPC X CIDR*	Local
	Subnet 2 CIDR in VPC D	pcx-ddddxxxx
	VPC Y CIDR	pcx-xxxxyyyy
	Subnet 1 CIDR in VPC Z	pcx-xxxxzzzz

Routing-Tabelle	Zielbereich	Ziel
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

Netzwerkszenarien einer VPC-Peering-Verbindung

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

Szenarien

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

Peering von zwei oder mehr Personen, um vollen Zugriff VPCs auf Ressourcen zu gewähren

In diesem Szenario haben Sie zwei oder mehr, VPCs die Sie miteinander verbinden möchten, um die vollständige gemeinsame Nutzung der Ressourcen zwischen allen VPCs zu ermöglichen. 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 innerhalb desselben AWS Kontos, andere in einem anderen AWS Konto. Sie möchten alle zusammenarbeiten VPCs , damit die IT-Abteilungen vollen Zugriff auf die Ressourcen der jeweils anderen haben.

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

- Zwei VPCs schauten zusammen
- Drei VPCs haben zusammen gebündelt
- Mehrere haben zusammen gepeert VPCs

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

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

In diesem Szenario verfügen Sie über eine zentrale VPC, die Ressourcen enthält, die Sie mit anderen VPCs teilen möchten. Ihre zentrale VPC benötigt möglicherweise vollständigen oder teilweisen Zugriff auf den Peer VPCs, und in ähnlicher Weise benötigt der Peer VPCs möglicherweise vollständigen oder teilweisen Zugriff auf die zentrale VPC. Im Folgenden sind einige Beispiele aufgeführt:

- Die IT-Abteilung Ihres Unternehmens betreibt eine VPC für die Dateifreigabe. Sie möchten eine Verbindung VPCs zu dieser zentralen VPC herstellen, möchten jedoch nicht, dass die andere VPCs Person Datenverkehr aneinander sendet.
- Ihr Unternehmen betreibt eine VPC, die Sie für Ihre Kunden freigeben möchten. Jeder Kunde kann eine VPC-Peering-Verbindung mit Ihrer VPC herstellen. Ihre Kunden können jedoch keinen Traffic an andere weiterleiten, VPCs die an Ihre VPC weitergeleitet werden, und sie kennen auch nicht die Routen der anderen Kunden.
- Sie betreiben eine zentrale VPC, die für Active Directory-Service verwendet wird. Bestimmte Instanzen in Peer VPCs senden Anfragen an die Active Directory-Server und benötigen vollen Zugriff auf die zentrale VPC. Die zentrale VPC benötigt keinen vollen Zugriff auf den Peer VPCs; sie muss lediglich den Antwortdatenverkehr an die spezifischen Instances weiterleiten.

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

Beispiel: Erstellen einer VPC-Peering-Verbindung

Die folgende Richtlinie gewährt Benutzern die Erlaubnis, VPC-Peering-Verbindungsanfragen unter Verwendung von mit VPCs markierten Verbindungen zu erstellen. `Purpose=Peering` 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.

JSON

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

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

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 es sich bei der VPC, die die Peering-Verbindung akzeptiert, um eine bestimmte VPC in einem bestimmten Konto handelt.

JSON

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

```
  ]
}
```

Beispiel: Akzeptieren einer VPC-Peering-Verbindung

Die folgende Richtlinie gewährt Benutzern die Erlaubnis, VPC-Peering-Verbindungsanfragen von einem bestimmten AWS Konto anzunehmen. So wird verhindert, dass Benutzer VPC-Peering-Verbindungsanfragen von unbekannten Konten akzeptieren können. Die Anweisung verwendet den Bedingungsschlüssel `ec2:RequesterVpc`, um dies zu erzwingen.

JSON

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

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

JSON

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

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

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.

JSON

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

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, sofern sie sich alle innerhalb desselben AWS Kontos 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.

Die zweite Anweisung gewährt Benutzern die Erlaubnis, VPC-Peering-Verbindungen herzustellen, und gewährt zu diesem VPCs Zweck Zugriff auf alle Verbindungen im angegebenen Konto.

Die dritte Anweisung verwendet einen Platzhalter * als Teil des Elements `Action`, um die Genehmigung für alle VPC-Peering-Verbindungsaktionen zu erteilen. Die Bedingungsschlüssel stellen sicher, dass die Aktionen nur auf VPC-Peering-Verbindungen ausgeführt werden können VPCs , die Teil des Kontos sind. 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.

JSON

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

```
      "Effect": "Allow",
      "Action": "ec2:*VpcPeeringConnection",
      "Resource": "arn:aws:ec2:*:account-id:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:*:account-id:vpc/*",
          "ec2:RequesterVpc": "arn:aws:ec2:*:account-id:vpc/*"
        }
      }
    }
  ]
}
```

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.

JSON

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

```
      ],
      "Resource": "*"
    },
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": [
        "arn:aws:ec2:*:*:vpc/vpc-id",
        "arn:aws:ec2:*:*:vpc-peering-connection/*"
      ]
    }
  ]
}
```

VPC-Peering-Verbindungskontingente für ein Konto

Mit VPC-Peering können Sie zwei verbinden. VPCs So können Ressourcen in einer VPC mit Ressourcen in der anderen VPC kommunizieren, als ob sie alle Teil desselben Netzwerks wären. VPC-Peering ist eine nützliche Funktion, um Ihre Verbindung herzustellen VPCs, unabhängig davon, ob sie sich in derselben AWS Region oder in verschiedenen Regionen befinden. In diesem Abschnitt werden die Kontingente beschrieben, die Sie bei der Arbeit mit VPC-Peering-Verbindungen beachten sollten.

In der folgenden Tabelle sind die Kontingente, früher als Limits bezeichnet, für VPC-Peering-Verbindungen für Ihr AWS Konto aufgeführt. Sofern nicht anders angegeben, können Sie eine Erhöhung dieser Kontingente beantragen.

Wenn Sie feststellen, dass Ihre aktuellen Anforderungen an die VPC-Peering-Verbindung die Standardkontingente überschreiten, empfehlen wir Ihnen, eine Anforderung zur Erhöhung des Service-Limits einzureichen. Wir werden Ihren Anwendungsfall überprüfen und gemeinsam mit Ihnen die Kontingente entsprechend anpassen, um sicherzustellen, dass Ihre VPC-Umgebung Ihren wachsenden Geschäftsanforderungen gerecht wird.

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. Weitere Informationen zu Kontingenten für Amazon VPC finden Sie unter Amazon-VPC-Kontigente im Benutzerhandbuch zu Amazon VPC.

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 verschiedenen VPCs AWS Regionen herstellen.	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.	
Verwendung ClassicLink über eine VPC-Peering-Verbindung	Sie können Ihre VPC-Peering-Verbindung so ändern, dass lokal verknüpfte EC2 -Classic-Instances mit Instances in einer Peer-VPC kommunizieren können oder umgekehrt.	26. April 2016
VPC-Peering	Sie können eine VPC-Peering-Verbindung zwischen zwei herstellen VPCs, sodass Instances in beiden VPC über private IP-Adressen miteinander kommunizieren können.	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.