Peering di VPC

Amazon Virtual Private Cloud

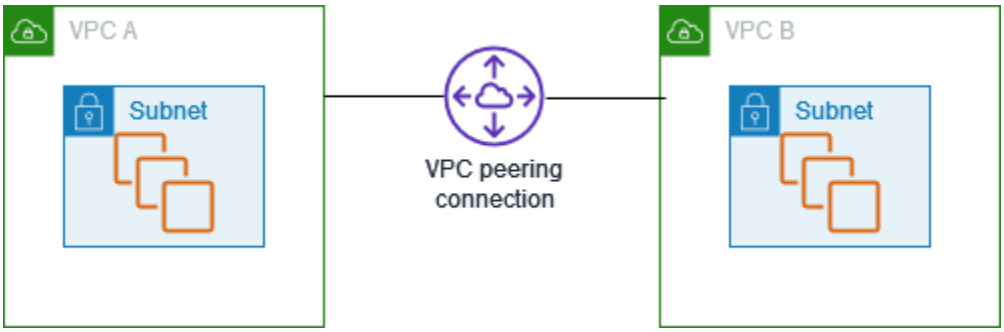
Amazon Virtual Private Cloud: Peering di VPC

Table of Contents

Che cos'è il peering VPC?

Un cloud privato virtuale (VPC) è una rete virtuale dedicata nel tuo account Account AWS. È logicamente isolato dalle altre reti virtuali nel AWS cloud. Puoi avviare AWS risorse, come le istanze Amazon EC2, nel tuo VPC.

Una connessione peering VPC è una connessione di rete tra due VPC che ti consente di instradare il traffico tra gli stessi utilizzando indirizzi IPv4 o IPv6 privati. Le istanze in uno qualsiasi dei VPC possono comunicare tra loro come se fossero nella stessa rete. È possibile creare una connessione peering VPC tra i VPC oppure con un VPC in un altro account AWS . I VPC possono essere in regioni differenti e in tal caso si parla di connessione peering VPC tra regioni.



AWS utilizza l'infrastruttura esistente di un VPC per creare una connessione peering VPC; non è né un gateway né una connessione VPN e non si basa su un hardware fisico separato. Non prevede alcun singolo punto di errore né colli di bottiglia.

Una connessione peering VPC facilita il trasferimento di dati. Ad esempio, se disponi di più di un AWS account, puoi peerizzare i VPC tra tali account per creare una rete di condivisione di file. Puoi anche utilizzare una connessione peering VPC per consentire ad altri VPC di accedere alle risorse disponibili in uno dei VPC.

Quando si stabiliscono relazioni di peering tra VPC in diverse AWS regioni, le risorse nei VPC (ad esempio, istanze EC2 e funzioni Lambda) in diverse AWS regioni possono comunicare tra loro utilizzando indirizzi IP privati, senza utilizzare un gateway, una connessione VPN o un'appliance di rete. Il traffico rimane nello spazio degli indirizzi IP privati. Tutto il traffico tra regioni viene crittografato senza alcun singolo punto di errore o colli di bottiglia della larghezza di banda. Il traffico rimane sempre sulla AWS spina dorsale globale e non attraversa mai la rete Internet pubblica, il che riduce le minacce, come gli exploit comuni e gli attacchi DDoS. Il peering VPC interregionale offre un modo semplice ed economico per condividere risorse tra regioni o replicare i dati per la ridondanza geografica.

Prezzi relativi a una connessione peering VPC

La creazione di una connessione peering VPC non comporta alcun addebito. Tutti i trasferimenti di dati tramite una connessione peering VPC che rimane all'interno di una zona di disponibilità (anche se tra account diversi) sono gratuiti. Si applicano costi per il trasferimento di dati tramite connessioni peering VPC tra più zone e regioni di disponibilità. Per ulteriori informazioni, consulta Prezzi di Amazon EC2.

Nozioni di base sul peering VPC

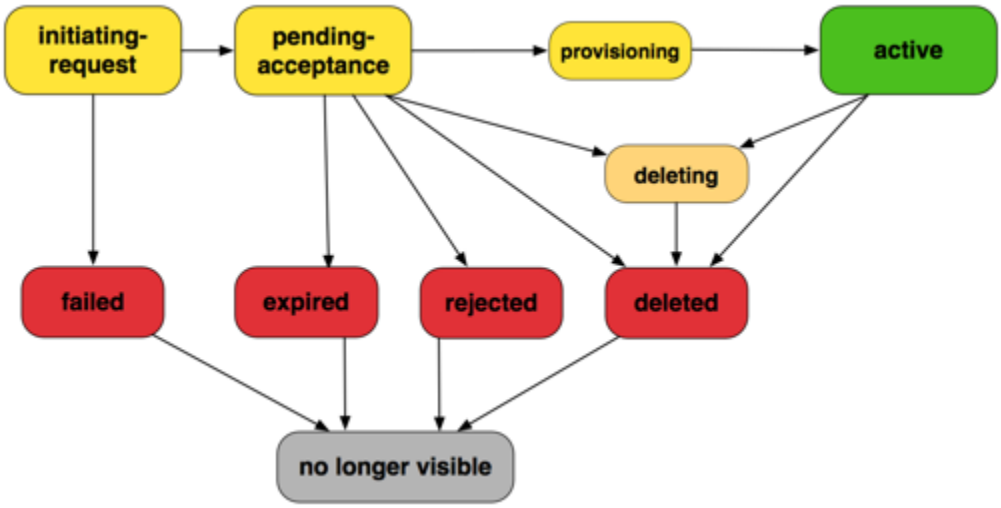
Di seguito viene descritta la procedura per stabilire una connessione peering VPC:

1. Il proprietario del VPC richiedente invia una richiesta al proprietario del VPC accettante per creare la connessione peering VPC. Il VPC accettante può essere di proprietà dell'utente o di AWS un altro account e non può avere un blocco CIDR che si sovrappone al blocco CIDR del VPC richiedente.
2. Il proprietario del VPC accettante accetta la richiesta di connessione peering VPC per attivare tale connessione.
3. Per abilitare il flusso di traffico tra i VPC utilizzando gli indirizzi IP privati, il proprietario di ogni VPC nella connessione peering VPC deve aggiungere manualmente una route a una o più delle relative tabelle di routing VPC che punta all'intervallo di indirizzi IP dell'altro VPC (il VPC in peering).
4. Se necessario, aggiorna le regole del gruppo di sicurezza associate alla tua istanza EC2 per garantire che il traffico da e verso il VPC peer non sia limitato. Se entrambi i VPC si trovano nella stessa regione, puoi fare riferimento a un gruppo di sicurezza del VPC peer come origine o destinazione per le regole in entrata o in uscita nel tuo gruppo di sicurezza.
5. Con le opzioni di connessione peering VPC predefinite, se le istanze EC2 su entrambi i lati di una connessione peering VPC si indirizzano a vicenda utilizzando un nome host DNS pubblico, il nome host si risolve nell'indirizzo IP pubblico dell'istanza EC2. Per modificare questo comportamento, abilita la risoluzione del nome host DNS per la tua connessione VPC. Dopo aver abilitato la risoluzione del nome host DNS, se le istanze EC2 su entrambi i lati della connessione peering VPC si indirizzano tra loro utilizzando un nome host DNS pubblico, il nome host si risolve nell'indirizzo IP privato dell'istanza EC2.

Per ulteriori informazioni, consulta Utilizzo di connessioni peering VPC.

Ciclo di vita delle connessioni peering VPC

Una connessione peering VPC è soggetta a varie fasi dal momento in cui è viene Effettuata la richiesta. È possibile che in ogni fase sia necessario eseguire alcune operazioni e che alla fine del relativo ciclo di vita, la connessione peering VPC rimanga visibile nell'API o nella riga di comando nonché nella console Amazon VPC per un determinato periodo di tempo.



- Initiating-request: una richiesta di connessione peering VPC è stata avviata. In questa fase, la connessione peering può non riuscire o passare allo stato `pending-acceptance`.
- Failed: la richiesta di connessione peering VPC non è riuscita. Quando è in questo stato, non può essere accettata, rifiutata o eliminata. La connessione peering VPC non riuscita rimane visibile al richiedente per 2 ore.
- Pending-acceptance: la richiesta di connessione peering VPC è in attesa di essere accettata dal proprietario del VPC accettante. Quando la richiesta è in questo stato, il proprietario del VPC richiedente può eliminarla e il proprietario del VPC accettante può accettarla o rifiutarla. Se non viene Eseguita alcuna operazione, la richiesta scade dopo 7 giorni.
- Expired: la richiesta di connessione peering VPC è scaduta e nessuna operazione può essere Eseguita dai due proprietari di VPC. La connessione peering VPC scaduta rimane visibile a entrambi i proprietari per 2 giorni.
- Rejected: il proprietario del VPC accettante ha rifiutato una richiesta di connessione peering VPC `pending-acceptance`. Durante tale stato, la richiesta non può essere accettata. La connessione peering VPC rifiutata rimane visibile al proprietario del VPC richiedente per 2 giorni e al proprietario del VPC accettante per 2 ore. Se la richiesta è stata creata all'interno dello stesso account, la richiesta rifiutata rimane visibile per 2 ore. AWS
- Provisioning: la richiesta di connessione peering VPC è stata accettata e a breve il suo stato sarà `active`.
- Active: la connessione peering VPC è attiva e il traffico può circolare tra i VPC (purché i gruppi di sicurezza e le tabelle di routing lo consentano). Durante questo stato, entrambi i proprietari di VPC possono eliminare la connessione peering VPC, ma non rifiutarla.

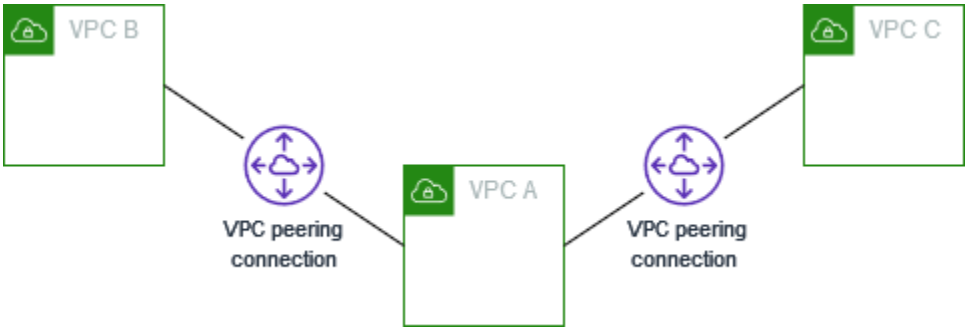
> **Note**
>
> Se un evento in una regione in cui risiede un VPC impedisce il flusso di traffico, lo stato della connessione peering VPC rimane invariato. `Active`

- Deleting (Eliminazione in corso): si applica a una connessione peering VPC tra regioni che sta per essere eliminata. Il proprietario di uno dei VPC ha inviato una richiesta di eliminazione di una connessione peering VPC `active` oppure il proprietario del VPC richiedente ha inviato una richiesta di eliminazione di una richiesta di connessione peering VPC `pending-acceptance`.
- Deleted: una connessione peering VPC `active` è stata eliminata da uno dei proprietari, oppure una richiesta di connessione peering VPC `pending-acceptance` è stata eliminata dal proprietario del VPC richiedente. Durante questo stato la connessione peering VPC non può essere accettata o rifiutata. La connessione peering VPC rimane visibile al proprietario che l'ha eliminata per 2 ore E all'altro proprietario per 2 giorni. Se la connessione peering VPC è stata creata all'interno dello stesso AWS account, la richiesta eliminata rimane visibile per 2 ore.

Molteplici connessioni peering VPC

Una connessione peering VPC è una relazione uno a uno tra due VPC. Puoi creare molteplici connessioni peering VPC per ogni tuo VPC, ma le relazioni peering transitive non sono supportate. Non disponi di alcuna relazione peering con i VPC ai quali il tuo VPC non è direttamente collegato in peering.

Il diagramma seguente è un esempio di VPC collegato in peering a due differenti VPC. Si hanno due connessioni peering VPC: VPC A è collegato in peering a VPC B e VPC C. VPC B e VPC C non sono collegati in peering e non puoi utilizzare VPC A come punto di transito per il peering tra VPC B e VPC C. Se vuoi abilitare il routing del traffico tra VPC B e VPC C, devi creare una connessione peering VPC univoca tra gli stessi.



Limitazioni relative al peering VPC

Considerare le seguenti limitazioni per le connessioni peering VPC. In alcuni casi, al posto della connessione peering VPC puoi utilizzare un collegamento del gateway di transito alla VPN. Per maggiori informazioni, consulta Esempi nei gateway Amazon VPC Transit.

Connessioni

- È presente una quota per il numero di connessioni peering VPC attive e in attesa per VPC. Per ulteriori informazioni, consulta Quote.
- Non puoi avere più di una connessione peering VPC tra due VPC nello stesso momento.
- I tag che crei per la connessione peering VPC sono applicati solo nell'account o nella regione in cui li crei.
- Non puoi connetterti o eseguire query sul server Amazon DNS in un VPC peer.
- Se il blocco CIDR IPv4 di un VPC in una connessione peering VPC non rientra negli intervalli di indirizzi IPv4 privati specificati da RFC 1918, i nomi host DNS privati per quel VPC non possono essere risolti in indirizzi IP privati. Per risolvere nomi host DNS privati in indirizzi IP privati, puoi abilitare il supporto per la risoluzione DNS per la connessione peering VPC. Per ulteriori informazioni, consulta Abilitazione della risoluzione DNS per una connessione peering VPC.
- È possibile abilitare le risorse su entrambi i lati di una connessione peering VPC affinché possano comunicare tramite IPv6. Devi associare un blocco CIDR IPv6 a ogni VPC, abilitare le istanze nei VPC per la comunicazione IPv6 e instradare il traffico IPv6 per il VPC in peering alla connessione peering VPC.
- La funzionalità RPF (Reverse Path Forwarding) unicast non è supportata nelle connessioni peering VPC. Per ulteriori informazioni, consulta Routing per traffico di risposta.

Blocchi CIDR sovrapposti

- Non puoi creare una connessione peering VPC tra VPC che hanno blocchi CIDR IPv4 o IPv6 corrispondenti o sovrapposti.
- Se hai più blocchi CIDR IPv4, non è possibile creare una connessione peering VPC se uno dei blocchi CIDR si sovrappone, anche se si intende utilizzare solo blocchi CIDR che non si sovrappongono o unicamente blocchi CIDR IPv6.

Peering transitivo

- Il peering di VPC non supporta relazioni di peering transitive. Ad esempio, se sono presenti connessioni peering VPC tra VPC A e VPC B e tra VPC A e VPC C, non è possibile instradare il traffico da VPC B a VPC C tramite VPC A. Per instradare il traffico tra VPC B e VPC C, è necessario creare una connessione peering VPC tra gli stessi. Per ulteriori informazioni, consulta Tre VPC collegati in peering tra loro.

Routing edge to edge via un gateway o una connessione privata

- Se il VPC A dispone di un gateway Internet, le risorse in VPC B non possono utilizzare il gateway Internet nel VPC A per accedere a Internet.
- Se VPC A ha un dispositivo NAT che fornisce l'accesso Internet alle sottoreti in VPC A, le risorse in VPC B non possono utilizzare il dispositivo NAT in VPC A per accedere a Internet.
- Se il VPC A dispone di una connessione VPN a una rete aziendale, le risorse in VPC B non possono utilizzare la connessione VPN per comunicare con la rete aziendale.
- Se il VPC A dispone di una AWS Direct Connect connessione a una rete aziendale, le risorse in VPC B non possono utilizzare la AWS Direct Connect connessione per comunicare con la rete aziendale.
- Se VPC A ha un endpoint gateway che fornisce connettività ad Amazon S3 a sottoreti private in VPC A, le risorse in VPC B non possono utilizzare l'endpoint gateway per accedere ad Amazon S3.

Connessioni peering VPC tra regioni

- L'unità massima di trasmissione (MTU) in una connessione peering VPC tra regioni è 1500 byte. I frame jumbo (MTU fino a 9001 byte) non sono supportati per le connessioni peering VPC tra regioni. Sono tuttavia supportati per le connessioni peering VPC nella stessa regione. Per ulteriori informazioni sui jumbo frame, consulta Jumbo frame (9001 MTU) nella Amazon EC2 User Guide.
- Per risolvere i nomi host DNS privati del VPC in peering in indirizzi IP privati, è necessario abilitare il supporto per la risoluzione DNS per la connessione VPC in peering, anche se il CIDR IPv4 per il VPC è incluso negli intervalli di indirizzi IPv4 privati specificato da RFC 1918.

VPC e sottoreti condivise

- Solo i proprietari di VPC possono utilizzare (descrivere, creare, accettare, rifiutare, modificare o eliminare) le connessioni peering. I partecipanti non possono lavorare con connessioni peering. Per

ulteriori informazioni, consulta Condivisione del VPC con altri account nella Guida per l'utente di Amazon VPC.

Utilizzo di connessioni peering VPC

Utilizza le seguenti procedure per creare e utilizzare connessioni peering VPC.

Processi

- Creazione di una connessione peering VPC
- Accettare una connessione peering VPC
- Rifiuto di una connessione peering VPC
- Visualizzazione delle connessioni peering VPC
- Aggiornamento delle tabelle di routing per una connessione peering VPC
- Aggiornamento dei gruppi di sicurezza per fare riferimento a gruppi di sicurezza peer di riferimento
- Modifica delle opzioni di connessione peering VPC
- Eliminazione di una connessione peering VPC
- Risoluzione dei problemi di una connessione peering VPC

Creazione di una connessione peering VPC

Per creare una connessione peering VPC, crea dapprima una richiesta di peering con un altro VPC. Puoi richiedere una connessione peering VPC a un altro VPC nel tuo account o a un VPC in un altro account AWS. Per una connessione peering VPC interregionale dove i VPC sono in Regioni differenti, la richiesta deve essere effettuata dalla Regione del VPC richiedente.

Per attivare la richiesta, il proprietario del VPC accettante deve accettare la richiesta. Per una connessione peering VPC interregionale, la richiesta deve essere accettata nella Regione del VPC accettante. Per ulteriori informazioni, consulta the section called “Accetta”. Per ulteriori informazioni sullo stato della connessione peering `Pending acceptance`, consulta Ciclo di vita delle connessioni peering VPC.

Processi

- Prerequisiti
- Creazione con VPC nello stesso account e nella stessa regione
- Creazione con VPC nello stesso account e in regioni differenti
- Creazione con VPC in account differenti e nella stessa regione

- Creazione con VPC in account e regioni differenti
- Creazione di una connessione peering VPC tramite la riga di comando

Prerequisiti

- Rivedi le limitazioni e le regole per connessioni peering VPC.
- Assicurati che i VPC non abbiano blocchi CIDR IPv4 che si sovrappongono. In caso contrario, lo stato della connessione peering VPC diventa immediatamente `failed`. Questa limitazione si applica anche se i VPC hanno blocchi CIDR IPv6 univoci.

Creazione con VPC nello stesso account e nella stessa regione

Creazione di una connessione peering VPC a VPC nello stesso account e nella stessa regione

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Peering connections (Connessioni peering).
3. Scegli Create peering connection (Crea connessione peering).
4. Configura le informazioni seguenti e scegli Crea connessione peering al termine dell'operazione:
   - Nome: puoi assegnare un nome alla connessione peering VPC.
   - ID VPC (richiedente): seleziona il VPC nell'account con cui creare la connessione peering VPC.
   - In Seleziona un altro VPC da collegare in peering, scegli Il mio account e seleziona un altro VPC.
   - (Facoltativo) Per aggiungere un tag, scegli Add new tag (Aggiungi nuovo tag) e immetti la chiave e il valore del tag.
5. Scegli Azioni, Accetta richiesta.
6. Quando viene chiesta la conferma, seleziona Accetta richiesta.
7. Scegli Modifica subito le tabelle di instradamento per aggiungere un instradamento alla tabella di instradamento del VPC in modo da poter inviare e ricevere traffico attraverso la connessione peering. Per ulteriori informazioni, consulta Aggiornamento delle tabelle di routing per una connessione peering VPC.

Creazione con VPC nello stesso account e in regioni differenti

Creazione di una connessione peering VPC a VPC nello stesso account e regioni differenti

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Peering connections (Connessioni peering).
3. Scegli Create peering connection (Crea connessione peering).
4. Configura le informazioni seguenti e scegli Crea connessione peering al termine dell'operazione:
   - Nome: puoi assegnare un nome alla connessione peering VPC. In questo modo viene creato un tag con una chiave di `Name` e il valore specificato.
   - ID VPC (richiedente): seleziona il VPC richiedente nell'account con cui richiedere la connessione peering VPC.
   - Account: scegli Il mio account.
   - Regione: scegli Altra regione e seleziona la regione in cui si trova il VPC accettante.
   - ID VPC: (accettante) seleziona il VPC accettante.
5. Nel selettore della Regione, selezionare la Regione del VPC accettante.
6. Nel pannello di navigazione, scegli Peering connections (Connessioni peering). Seleziona la connessione peering VPC creata e scegli Operazioni, Accetta richiesta.
7. Quando viene chiesta la conferma, seleziona Accetta richiesta.
8. Scegli Modifica subito le tabelle di instradamento per aggiungere un instradamento alla tabella di instradamento del VPC in modo da poter inviare e ricevere traffico attraverso la connessione peering. Per ulteriori informazioni, consulta Aggiornamento delle tabelle di routing per una connessione peering VPC.

Creazione con VPC in account differenti e nella stessa regione

Richiesta di una connessione peering VPC a VPC in account differenti e nella stessa regione

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Peering connections (Connessioni peering).
3. Scegli Create peering connection (Crea connessione peering).
4. Configura le informazioni come segue e scegli Crea connessione peering al termine dell'operazione:

- Nome: puoi assegnare un nome alla connessione peering VPC. In questo modo, si crea un tag con una chiave `Name` e un valore specificato. Questo tag non è visibile agli altri utenti; il proprietario del VPC in peering può creare i propri tag per la connessione peering VPC.
- ID VPC (richiedente): seleziona il VPC nell'account con cui creare la connessione peering VPC.
- Account: scegliere Another account (Un altro account).
- ID account: immetti l'ID dell'Account AWS proprietario del VPC accettante.
- ID VPC (accettante): immetti l'ID del VPC con cui creare la connessione peering VPC.

Creazione con VPC in account e regioni differenti

Richiesta di una connessione peering VPC a VPC in account e regioni differenti

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Peering connections (Connessioni peering).
3. Scegli Create peering connection (Crea connessione peering).
4. Configura le informazioni come segue e scegli Crea connessione peering al termine dell'operazione:

   - Nome: puoi assegnare un nome alla connessione peering VPC. In questo modo, si crea un tag con una chiave `Name` e un valore specificato. Questo tag non è visibile agli altri utenti; il proprietario del VPC in peering può creare i propri tag per la connessione peering VPC.
   - ID VPC (richiedente): seleziona il VPC nell'account con cui creare la connessione peering VPC.
   - Account: scegliere Another account (Un altro account).
   - ID account: immetti l'ID dell'Account AWS proprietario del VPC accettante.
   - Regione: scegli Altra Regione e seleziona la Regione in cui si trova il VPC accettante.
   - ID VPC (accettante): immetti l'ID del VPC con cui creare la connessione peering VPC.

Creazione di una connessione peering VPC tramite la riga di comando

È possibile creare una connessione peering VPC utilizzando i seguenti comandi:

- create-vpc-peering-connection (AWS CLI)

- New-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Accettare una connessione peering VPC

Una connessione peering VPC il cui stato è `pending-acceptance` deve Essere accettata dal proprietario del VPC accettante per essere attivata. Per ulteriori informazioni sullo stato della connessione peering `Deleted`, consulta Ciclo di vita delle connessioni peering VPC. Non puoi accettare una richiesta di connessione peering VPC che hai inviato a un altro account AWS. Se stai creando una connessione peering VPC nello stesso account AWS, devi creare e accettare personalmente la richiesta.

Se i VPC sono in Regioni differenti, la richiesta deve essere accettata nella Regione del VPC accettante.

> **Important**
>
> Non accettare connessioni peering VPC da account AWS sconosciuti. Un utente malintenzionato può averti inviato una richiesta di connessione peering VPC per ottenere un accesso di rete non autorizzato al tuo VPC. Questo tipo di azione è nota come "peer phishing". Puoi rifiutare senza problemi le richieste di connessione peering VPC non desiderate senza correre il rischio che il richiedente possa accedere alle informazioni sul tuo account AWS o VPC. Per ulteriori informazioni, consulta Rifiuto di una connessione peering VPC. Puoi anche ignorare la richiesta e lasciarla scadere. Per impostazione predefinita, la richiesta scade dopo 7 giorni.

Dopo aver accettato la connessione peering VPC, devi aggiungere una voce alle tabelle di instradamento per consentire il traffico tra i VPC collegati in peering. Per ulteriori informazioni, consulta Aggiornamento delle tabelle di routing per una connessione peering VPC.

Per accettare una connessione peering VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Utilizzare il selettore della regione per scegliere la regione del VPC accettante.
3. Nel pannello di navigazione, scegli Peering connections (Connessioni peering).

4. Seleziona la connessione peering VPC in attesa (lo stato è `pending-acceptance`) e scegli Operazioni, Accetta richiesta. Per ulteriori informazioni sugli stati del ciclo di vita di una connessione peering, consulta Ciclo di vita delle connessioni peering VPC.

   > **Tip**
   >
   > Se la connessione peering VPC in attesa non è visibile, controllare la Regione. Una richiesta di peering interregionale deve essere accettata nella Regione del VPC accettante.

5. Quando viene chiesta la conferma, seleziona Accetta richiesta.
6. Scegli Modifica subito le tabelle di instradamento per aggiungere un instradamento alla tabella di instradamento del VPC in modo da poter inviare e ricevere traffico attraverso la connessione peering. Per ulteriori informazioni, consulta Aggiornamento delle tabelle di routing per una connessione peering VPC.

Per accettare una connessione peering VPC tramite la riga di comando o un'API

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

Rifiuto di una connessione peering VPC

Puoi rifiutare qualsiasi richiesta di connessione peering VPC che hai ricevuto e il cui stato è `pending-acceptance`. Devi accettare connessioni peering VPC solo da Account AWS che conosci e che ritieni affidabili; puoi rifiutare qualsiasi altra richiesta non desiderata. Per ulteriori informazioni sullo stato della connessione peering `Rejected`, consulta Ciclo di vita delle connessioni peering VPC.

Per rifiutare una connessione peering VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Peering connections (Connessioni peering).
3. Seleziona la connessione peering VPC e scegli Operazioni, Rifiuta richiesta.
4. Quando viene chiesta la conferma, seleziona Rifiuta richiesta.

Per rifiutare una connessione peering VPC tramite la riga di comando o un'API

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

Visualizzazione delle connessioni peering VPC

Puoi visualizzare tutte le connessioni peering VPC nella console Amazon VPC. Per impostazione predefinita, la console visualizza tutte le connessioni peering VPC in stati differenti, incluse quelle Eliminate o rifiutate di recente. Per ulteriori informazioni sul ciclo di vita di una connessione peering VPC, consulta Ciclo di vita delle connessioni peering VPC.

Per visualizzare le connessioni peering VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Peering connections (Connessioni peering).
3. Tutte le connessioni peering VPC sono elencate. Utilizzare la barra di ricerca dei filtri per ridurre i risultati.

Per descrivere una connessione peering VPC tramite la riga di comando o un'API

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

Aggiornamento delle tabelle di routing per una connessione peering VPC

Per abilitare il traffico IPv4 privato tra istanze in VPC con peering, devi aggiungere una route alle tabelle di instradamento associate alle sottoreti per entrambe le istanze. La destinazione della route è il blocco CIDR (o una sua parte) del VPC peer e la destinazione è l'ID della connessione peering VPC. Per maggiori informazioni, consulta Configurazione delle tabelle di instradamento nella Guida per l'utente di Amazon VPC.

Di seguito è riportato un esempio delle tabelle di instradamento che consentono la comunicazione tra istanze in due VPC con peering, VPC A e VPC B. Ogni tabella ha una route locale e una route che invia il traffico per il VPC peer alla connessione peering VPC.

Tabella di routing	Destinazione	Target
VPC A	*VPC A CIDR*	Locale
	VPC B CIDR	pcx-*11112222*
VPC B	*VPC B CIDR*	Locale
	VPC A CIDR	pcx-*11112222*

Analogamente, se i VPC nella connessione peering VPC hanno blocchi CIDR IPv6 associati, potrai aggiungere route che consentono la comunicazione con il VPC peer via IPv6.

Per ulteriori informazioni sulle configurazioni di tabelle di routing supportate per le connessioni peering VPC, consulta Configurazioni di peering di VPC.

Considerazioni

- Se si dispone di un VPC collegato in peering a molti VPC che hanno blocchi CIDR IPv4 sovrapposti o corrispondenti, assicurarsi che le tabelle di routing siano configurate in modo da non inviare traffico di risposta dal proprio VPC al VPC sbagliato. Al momento AWS non supporta la funzionalità RPF (reverse path forwarding) unicast tra connessioni in peering VPC che controlla l'IP di origine di pacchetti e re-instrada i pacchetti di risposta all'origine. Per ulteriori informazioni, consulta Routing per traffico di risposta.
- Il tuo account ha una quota per il numero di voci che puoi aggiungere per tabella di instradamento. Se il numero di connessioni peering VPC nel tuo VPC supera la quota di voci per una singola tabella di instradamento, prendi in considerazione l'utilizzo di più sottoreti, ognuna associata a una tabella di instradamento personalizzata.
- Puoi aggiungere una route per una connessione peering VPC il cui stato è `pending-acceptance`. Tuttavia, la route avrà lo stato `blackhole` e non avrà effetto fino a che lo stato della connessione peering VPC non diventerà `active`.

Per aggiungere una route IPv4 per una connessione peering VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Route tables (Tabelle di routing).
3. Seleziona la casella di controllo accanto alla tabella di instradamento associata alla sottorete in cui si trova la tua istanza.

   Se non associ in maniera esplicita una tabella di instradamento a tale sottorete, alla sottorete sarà implicitamente associata la tabella di instradamento principale per il VPC.
4. Selezionare Actions (Operazioni), Edit routes (Modifica route).
5. Selezionare Add route (Aggiungi route).
6. In Destination (Destinazione), immettere l'intervallo di indirizzi IPv4 verso il quale il traffico di rete nella connessione peering VPC deve Essere diretto. È possibile specificare l'intero blocco CIDR IPv4 del VPC in peering, uno specifico intervallo o un singolo indirizzo IPv4, come l'indirizzo IP dell'istanza con la quale comunicare. Ad esempio, se il blocco CIDR del VPC in peering è `10.0.0.0/16`, è possibile specificare una parte `10.0.0.0/24` o uno specifico indirizzo IP `10.0.0.7/32`.
7. Per Destinazione seleziona la connessione peering VPC.
8. Seleziona Salva modifiche.

Il proprietario del VPC peer deve inoltre completare questi passaggi per aggiungere un routing per indirizzare il traffico al VPC tramite la connessione peering VPC.

Se disponi di risorse in Regioni AWS diverse che utilizzano indirizzi IPv6, puoi creare una connessione peering tra Regioni. Puoi quindi aggiungere un routing IPv6 per la comunicazione tra le risorse.

Per aggiungere una route IPv6 per una connessione peering VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Route tables (Tabelle di routing).
3. Seleziona la casella di controllo accanto alla tabella di instradamento associata alla sottorete in cui si trova la tua istanza.

> **Note**
>
> Se non si dispone di una tabella di instradamento associata a tale sottorete, selezionare la tabella di instradamento principale per il VPC, in quanto, per impostazione predefinita, la sottorete utilizza la tabella di instradamento.

4. Selezionare Actions (Operazioni), Edit routes (Modifica route).
5. Selezionare Add route (Aggiungi route).
6. In Destination (Destinazione), immettere l'intervallo di indirizzi IPv6 per il VPC in peering. È possibile specificare l'intero blocco CIDR IPv6 del VPC in peering, uno specifico intervallo o un singolo indirizzo IPv6. Ad esempio, se il blocco CIDR del VPC in peering è `2001:db8:1234:1a00::/56`, è possibile specificare una parte `2001:db8:1234:1a00::/64` o uno specifico indirizzo IP `2001:db8:1234:1a00::123/128`.
7. Per Destinazione seleziona la connessione peering VPC.
8. Seleziona Salva modifiche.

Per maggiori informazioni, consulta le tabelle dei percorsi nella Guida dell'utente di Amazon VPC.

Per aggiungere o sostituire una route tramite la riga di comando o un'API

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

Aggiornamento dei gruppi di sicurezza per fare riferimento a gruppi di sicurezza peer di riferimento

Puoi aggiornare le regole in entrata o in uscita per i gruppi di sicurezza VPC per fare riferimento a gruppi di sicurezza nel VPC collegato in peering. In questo modo, si consente il traffico verso e da istanze associate al gruppo di sicurezza a cui si fa riferimento nel VPC collegato in peering.

Requisiti

- Il VPC in peering può essere un VPC nel tuo account o un VPC in un altro account AWS. Per fare riferimento a un gruppo di sicurezza in un altro account AWS, includi il numero di account nel campo Origine o Destinazione, ad esempio`123456789012/sg-1a2b3c4d`.
- Non puoi fare riferimento al gruppo di sicurezza di un VPC in peering che si trova in una Regione differente. Puoi invece utilizzare il blocco CIDR del VPC in peering.
- Per fare riferimento a un gruppo di sicurezza in un VPC in peering, lo stato della connessione peering VPC deve Essere `active`.
- Se le route vengono configurate per inoltrare il traffico tra due istanze in sottoreti diverse attraverso un'appliance middlebox, è necessario assicurarsi che i gruppi di sicurezza per entrambe le istanze consentano il flusso del traffico tra le istanze. Il gruppo di sicurezza per ogni istanza deve fare riferimento all'indirizzo IP privato dell'altra istanza o all'intervallo CIDR della sottorete che contiene l'altra istanza come origine. Se si fa riferimento al gruppo di sicurezza dell'altra istanza come origine, allora il flusso del traffico tra le istanze non sarà consentito.

Per aggiornare le regole di gruppo di sicurezza tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegli Gruppi di sicurezza nel riquadro di navigazione.
3. Seleziona il gruppo di sicurezza e scegli Operazioni, Modifica regole in entrata per modificare le regole in entrata o scegli OperazioniModifica regole in uscita per modificare le regole in uscita.
4. Per aggiungere una regola, scegli Aggiungi regola e specifica il tipo, il protocollo e l'intervallo di porte. In Origine (regola di entrata) o Destinazione (regola di uscita), immetti l'ID del gruppo di sicurezza nel VPC in peering se è nella stessa regione oppure il blocco CIDR del VPC in peering se si trova in un'altra regione.

   > **Note**
   >
   > I gruppi di sicurezza in un VPC in peering non sono visualizzati automaticamente.

5. Per modificare una regola esistente, cambia i relativi valori (ad esempio, l'origine o la descrizione).
6. Per eliminare una regola, seleziona il pulsante Elimina accanto alla regola corrispondente.
7. Scegliere Save rules (Salva regole).

Per aggiornare le regole in entrata tramite la riga di comando

- 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)

Per aggiornare le regole in uscita tramite la riga di comando

- 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)

Ad esempio, per aggiornare il gruppo di sicurezza `sg-aaaa1111` allo scopo di consentire l'accesso in entrata via HTTP da `sg-bbbb2222` (situato in un VPC in peering), è possibile utilizzare il seguente comando AWS CLI:

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

Dopo aver aggiornato le regole di gruppo di sicurezza, utilizza il comando describe-security-groups per visualizzare il gruppo di sicurezza a cui si fa riferimento nelle regole di gruppo di sicurezza.

Identificazione dei gruppi di sicurezza a cui si fa riferimento

Per determinare se si fa riferimento al tuo gruppo di sicurezza nelle regole di un gruppo di sicurezza in un VPC in peering, utilizza uno dei seguenti comandi per uno o più gruppi di sicurezza nel tuo account.

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

Nell'esempio seguente, la risposta indica che un gruppo di sicurezza nel VPC `sg-bbbb2222` fa riferimento al gruppo di sicurezza `vpc-aaaaaaaa`:

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

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

Se la connessione peering VPC viene Eliminata o se il proprietario del VPC in peering elimina il gruppo di sicurezza a cui si fa riferimento, la regola di gruppo di sicurezza diventa obsoleta.

Utilizzo di regole del gruppo di sicurezza obsolete

Una regola di gruppo di sicurezza obsoleta è una regola che fa riferimento a un gruppo di sicurezza eliminato nello stesso VPC o in un VPC simile, o che fa riferimento a un gruppo di sicurezza in un VPC simile per il quale la connessione peering VPC è stata eliminata. Quando una regola di gruppo di sicurezza diventa obsoleta, non viene automaticamente rimossa dal gruppo di sicurezza, ma deve essere eliminata manualmente. Se una regola di gruppo di sicurezza è obsoleta perché la connessione peering VPC è stata eliminata, la regola non sarà più considerata obsoleta se crei una nuova connessione peering VPC con gli stessi VPC.

Puoi visualizzare ed eliminare le regole di gruppo di sicurezza obsolete per un VPC tramite la console Amazon VPC.

Per visualizzare Ed eliminare regole di gruppo di sicurezza obsolete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, fai clic su Security groups (Gruppi di sicurezza).
3. Seleziona Actions (Operazioni), Manage stale rules (Gestisci regole obsolete).
4. Per VPC, seleziona il VPC con le regole obsolete.
5. Seleziona Edit (Modifica).
6. Scegliere il pulsante Delete (Elimina) a destra della regola da eliminare. Scegliere Preview changes (Anteprima modifiche), Save rules (Salva regole).

Per descrivere regole di gruppo di sicurezza obsolete tramite la riga di comando o un'API

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

Nell'esempio seguente, VPC A (`vpc-aaaaaaaa`) e VPC B erano collegati in peering e la connessione peering VPC è stata eliminata. Il gruppo di sicurezza `sg-aaaa1111` in VPC A fa riferimento a `sg-bbbb2222` in VPC B. Quando esegui il comando `describe-stale-security-groups` per il tuo VPC, la risposta indica che il gruppo di sicurezza `sg-aaaa1111` ha una regola SSH obsoleta che fa riferimento a `sg-bbbb2222`.

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

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

```
    ]
}
```

Dopo aver identificato le regole di gruppo di sicurezza obsolete, puoi eliminarle utilizzando i comandi revoke-security-group-ingress or revoke-security-group-egress.

Modifica delle opzioni di connessione peering VPC

Puoi modificare una connessione peering VPC per eseguire queste operazioni:

- Consentire a un VPC di risolvere nomi host DNS IPv4 pubblici in indirizzi IPv4 privati quando viene interrogato da istanze nel VPC in peering. Per ulteriori informazioni, consulta Abilitazione della risoluzione DNS per una connessione peering VPC.

Abilitazione della risoluzione DNS per una connessione peering VPC

Per consentire a un VPC di risolvere nomi host DNS IPv4 pubblici in indirizzi IPv4 privati quando viene interrogato da istanze nel VPC in peering, devi modificare la connessione peering esistente.

Entrambi i VPC devono essere abilitati per i nomi host DNS e la risoluzione DNS.

Non è possibile abilitare il supporto per la risoluzione DNS quando si crea una nuova connessione peering. È possibile abilitare il supporto della risoluzione DNS per una connessione peering esistente nello stato `active`.

Come abilitare la risoluzione DNS per una connessione peering

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Peering connections (Connessioni peering).
3. Seleziona la connessione peering VPC e scegli Operazioni, Modifica impostazioni DNS.
4. Per assicurarsi che le query dal VPC in peering siano risolte in indirizzi IP privati nel VPC locale, scegliere l'opzione per abilitare la risoluzione DNS per le query dal VPC in peering. Questa opzione è Requester DNS resolution (Risoluzione DNS richiedente) o Accepter DNS resolution (Risoluzione DNS accettante), a seconda che il VPC sia il VPC richiedente o accettante.
5. Se il VPC peer si trova nello stesso Account AWS, puoi abilitare la risoluzione DNS per entrambi i VPC nella connessione in peering.
6. Seleziona Salva modifiche.

7. Se il VPC in peering si trova in un AWS diverso o in una regione differente, il proprietario del VPC deve accedere alla console VPC, eseguire i passaggi da 2 a 4 e scegliere Salva.

Per abilitare la risoluzione DNS tramite la riga di comando o un'API

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

Devo modificare le opzioni di peering del VPC richiedente se sei il richiedente della connessione peering VPC e devi modificare quelle del VPC accettante se sei l'accettante della connessione peering VPC. Puoi utilizzare i comandi describe-vpc-peering-connections o Get-EC2VpcPeeringConnections per verificare quale VPC è l'accettante E quale il richiedente di una connessione peering VPC. Per le connessioni peering interregionali, è necessario utilizzare la Regione per il VPC del richiedente per modificare le opzioni di peering del VPC richiedente e la Regione per il VPC dell'accettante per modificare le opzioni di peering VPC accettante.

In questo esempio, sei il richiedente della connessione peering VPC, quindi modifica le opzioni di connessione peering tramite l'AWS CLI come segue:

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

Eliminazione di una connessione peering VPC

Ogni proprietario di un VPC in una connessione peering può eliminare la connessione peering VPC in qualsiasi momento. Puoi anche Eliminare una connessione peering VPC che hai richiesto e il cui stato è ancora `pending-acceptance`.

Non è possibile eliminare la connessione peering VPC quando la connessione peering VPC è nello stato `rejected`. Cancelliamo automaticamente la connessione per te.

L'eliminazione nella console Amazon VPC di un VPC che è parte di una connessione peering VPC attiva comporta anche l'eliminazione della connessione peering VPC. Se hai richiesto una connessione peering VPC con un VPC in un altro account ed elimini il tuo VPC prima che l'altra parte accetti la richiesta, anche la connessione peering VPC viene Eliminata. Non puoi eliminare un

VPC per il quale Esiste una richiesta `pending-acceptance` da un VPC in un altro account. Devi dapprima rifiutare la richiesta di connessione peering VPC.

Quando elimini una connessione peering, lo stato viene impostato su `Deleting`, poi su `Deleted`. Una connessione eliminata non può essere accettata, rifiutata o modificata. Per ulteriori informazioni sulla durata della visibilità della connessione di peering, consulta Ciclo di vita delle connessioni peering VPC.

Per eliminare una connessione peering VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Peering connections (Connessioni peering).
3. Seleziona la connessione peering VPC.
4. Scegli Actions (Operazioni), Delete peering connection (Elimina connessione peering).
5. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Per eliminare una connessione peering VPC tramite la riga di comando o un'API

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

Risoluzione dei problemi di una connessione peering VPC

In caso di problemi di connessione a una risorsa in un VPC da una risorsa in un VPC peer, completa le seguenti operazioni:

- Per ogni risorsa in ogni VPC, verifica che la tabella di instradamento per la relativa sottorete contenga una route che invii il traffico destinato al VPC peer alla connessione peering VPC. Per ulteriori informazioni, consulta Aggiorna le tabelle di routing.
- Per le istanze EC2, verifica che i gruppi di sicurezza per le istanze EC2 consentano il traffico dal VPC peer. Per ulteriori informazioni, consulta Gruppi di sicurezza peer di riferimento.
- Per ogni risorsa in ciascun VPC, verifica che l'ACL di rete per la relativa sottorete consenta il traffico dal VPC peer.

Puoi utilizzare Reachability Analyzer anche per identificare il componente che ha un problema di configurazione, ad esempio una tabella di instradamento, un gruppo di sicurezza o un'ACL di rete. Per ulteriori informazioni, consulta la Guida di Reachability Analyzer.

Configurazioni di peering di VPC

Nella seguente documentazione sono descritti i diversi tipi di configurazioni di peering VPC.

Configurazioni

- Configurazioni peering VPC con instradamenti verso un intero VPC
- Configurazioni peering VPC con instradamenti specifici

Configurazioni peering VPC con instradamenti verso un intero VPC

Puoi configurare le connessioni peering VPC di modo che le tabella di routing abbiano accesso all'intero blocco CIDR del VPC in peering. Per ulteriori informazioni sugli scenari in cui potresti necessitare di una specifica configurazione di connessione peering VPC, consulta Scenari di peering VPC. Per ulteriori informazioni sulla creazione e sull'utilizzo di connessioni peering VPC, consulta Utilizzo di connessioni peering VPC.

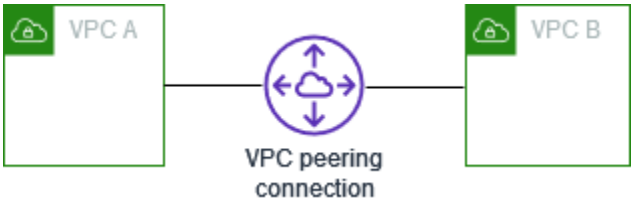
Per ulteriori informazioni sull'aggiornamento delle tabelle di routing, consulta Aggiornamento delle tabelle di routing per una connessione peering VPC.

Configurazioni

- Due VPC collegati in peering tra loro
- Un VPC collegato in peering a due VPC
- Tre VPC collegati in peering tra loro
- Molteplici VPC collegati in peering tra loro

Due VPC collegati in peering tra loro

In questa configurazione, esiste una connessione peering tra VPC A e VPC B (`pcx-11112222`). I VPC sono nello stesso Account AWS e i loro blocchi CIDR non si sovrappongono.



Puoi utilizzare questa configurazione quando disponi di due VPC e ognuno richiede l'accesso alle risorse dell'altro. Ad esempio, se configuri VPC A per i tuoi record di contabilità e VPC B per quelli finanziari, ogni VPC deve poter accedere alle risorse dell'altro senza alcuna limitazione.

CIDR VPC singolo

Aggiorna la tabella di instradamento per ogni VPC con un instradamento che invii il traffico per il blocco CIDR del VPC peer alla connessione peering VPC.

Tabella di routing	Destinazione	Target
VPC A	*VPC A CIDR*	Locale
	VPC B CIDR	pcx-11112222
VPC B	*VPC B CIDR*	Locale
	VPC A CIDR	pcx-11112222

Più CIDR VPC IPv4

Se VPC A e VPC B hanno più blocchi CIDR IPv4 associati, è possibile aggiornare la tabella di instradamento per ogni VPC con gli instradamenti per alcuni o tutti i blocchi CIDR IPv4 del VPC peer.

Tabella di routing	Destinazione	Target
VPC A	*CIDR 1 VPC A*	Locale
	CIDR 2 VPC A	Locale
	CIDR 1 VPC B	pcx-11112222
	CIDR 2 VPC B	pcx-11112222
VPC B	*CIDR 1 VPC B*	Locale
	CIDR 2 VPC B	Locale
	CIDR 1 VPC A	pcx-11112222

Tabella di routing	Destinazione	Target
	CIDR 2 VPC A	pcx-11112222

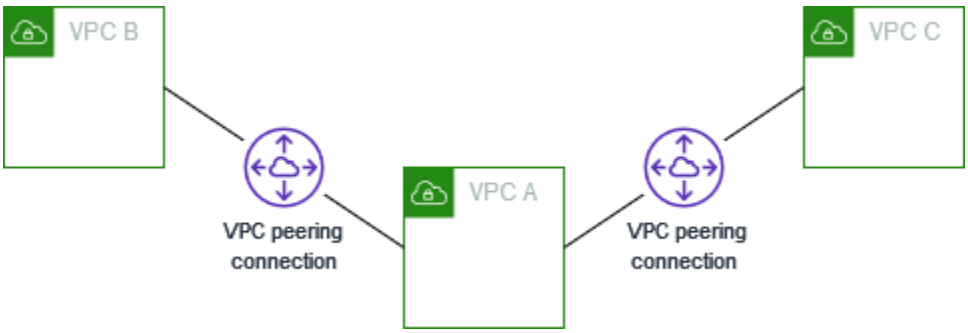
CIDR VPC IPv4 e IPv6

Se VPC A e VPC B hanno più blocchi CIDR IPv6 associati, puoi aggiornare la tabella di instradamento per ogni VPC con gli instradamenti per i blocchi CIDR IPv4 e IPv6 del VPC peer.

Tabella di routing	Destinazione	Target
VPC A	*CIDR IPv4 del VPC A*	Locale
	CIDR IPv6 del VPC A	Locale
	CIDR IPv4 del VPC B	pcx-11112222
	CIDR IPv6 del VPC B	pcx-11112222
VPC B	*CIDR IPv4 del VPC B*	Locale
	CIDR IPv6 del VPC B	Locale
	CIDR IPv4 del VPC A	pcx-11112222
	CIDR IPv6 del VPC A	pcx-11112222

Un VPC collegato in peering a due VPC

In questa configurazione, esistono un VPC centrale (VPC A), una connessione peering tra VPC A e VPC B (`pcx-12121212`) e una connessione peering tra VPC A e VPC C (`pcx-23232323`). Tutti e tre i VPC sono nello stesso Account AWS e i loro blocchi CIDR non si sovrappongono.



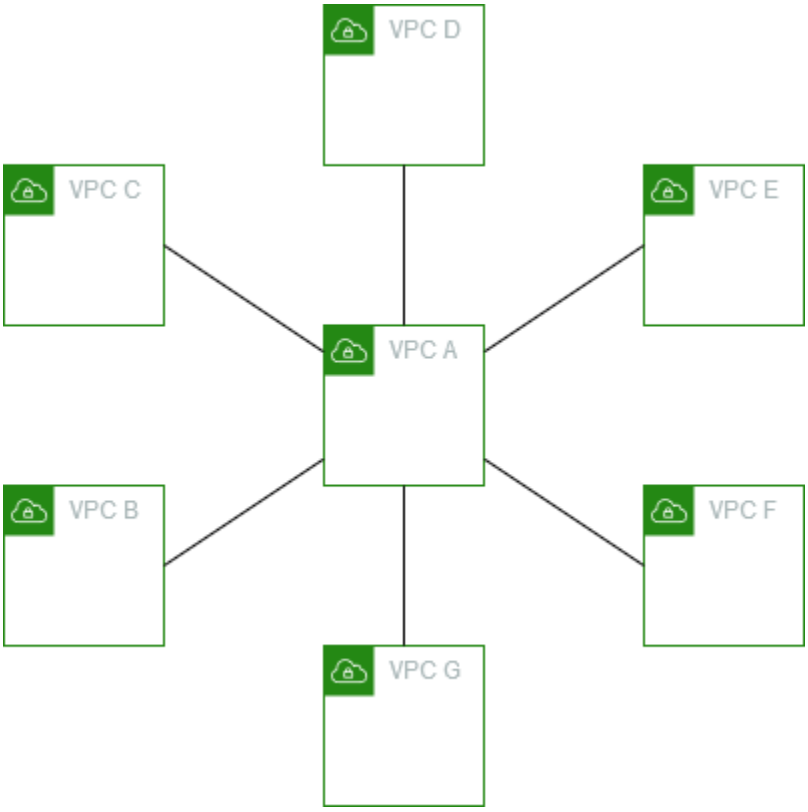
Il VPC B e il VPC C non possono inviare traffico direttamente l'uno all'altro tramite VPC A perché il peering VPC non supporta relazioni di peering transitive. È possibile creare una connessione peering VPC tra VPC B e VPC C, come mostrato in Tre VPC collegati in peering tra loro. Per ulteriori informazioni sugli scenari di peering non supportati, consulta the section called “Limitazioni relative al peering VPC”.

Utilizza questa configurazione quando disponi di risorse su un VPC centrale, come un repository di servizi, a cui devono accedere altri VPC. Gli altri VPC non hanno bisogno di accedere alle risorse degli altri, ma solo a quelle del VPC centrale.

Aggiorna la tabella di instradamento per ogni VPC come segue per implementare questa configurazione utilizzando un blocco CIDR per VPC.

Tabella di routing	Destinazione	Target
VPC A	*VPC A CIDR*	Locale
	VPC B CIDR	pcx-12121212
	VPC C CIDR	pcx-23232323
VPC B	*VPC B CIDR*	Locale
	VPC A CIDR	pcx-12121212
VPC C	*VPC C CIDR*	Locale
	VPC A CIDR	pcx-23232323

È possibile estendere questa configurazione ad altri VPC. Ad esempio, VPC A è collegato in peering a VPC B tramite VPC G mediante CIDR IPv4 e IPv6, ma gli altri VPC non sono collegati in peering tra loro. In questo diagramma, le linee rappresentano le connessioni peering VPC.



Aggiorna la tabella di instradamento come segue.

Tabella di routing	Destinazione	Target
VPC A	*CIDR IPv4 del VPC A*	Locale
	CIDR IPv6 del VPC A	Locale
	CIDR IPv4 del VPC B	pcx-aaaabbbb
	CIDR IPv6 del VPC B	pcx-aaaabbbb
	CIDR IPv4 del VPC C	pcx-aaaacccc
	CIDR IPv6 del VPC C	pcx-aaaacccc
	CIDR IPv4 del VPC D	pcx-aaaadddd

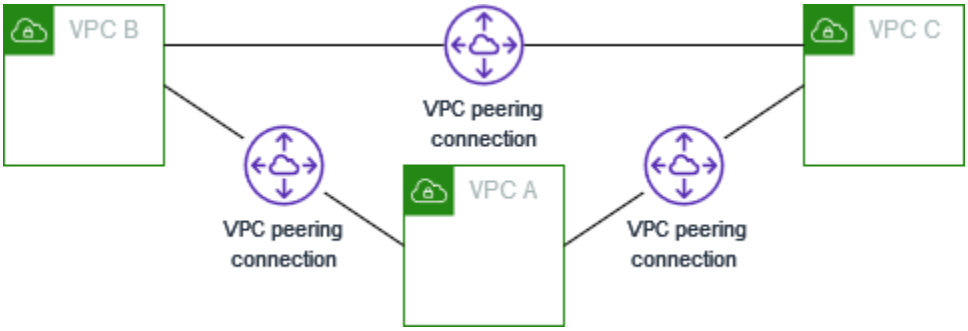
Tabella di routing	Destinazione	Target
	CIDR IPv6 del VPC D	pcx-aaaadddd
	CIDR IPv4 del VPC E	pcx-aaaaeeee
	CIDR IPv6 del VPC E	pcx-aaaaeeee
	CIDR IPv4 del VPC F	pcx-aaaaffff
	CIDR IPv6 del VPC F	pcx-aaaaffff
	CIDR IPv4 del VPC G	pcx-aaaagggg
	CIDR IPv6 del VPC G	pcx-aaaagggg
VPC B	*CIDR IPv4 del VPC B*	Locale
	CIDR IPv6 del VPC B	Locale
	CIDR IPv4 del VPC A	pcx-aaaabbbb
	CIDR IPv6 del VPC A	pcx-aaaabbbb
VPC C	*CIDR IPv4 del VPC C*	Locale
	CIDR IPv6 del VPC C	Locale
	CIDR IPv4 del VPC A	pcx-aaaacccc
	CIDR IPv6 del VPC A	pcx-aaaacccc
VPC D	*CIDR IPv4 del VPC D*	Locale
	CIDR IPv6 del VPC D	Locale
	CIDR IPv4 del VPC A	pcx-aaaadddd
	CIDR IPv6 del VPC A	pcx-aaaadddd
VPC E	*CIDR IPv4 del VPC E*	Locale

Tabella di routing	Destinazione	Target
	CIDR IPv6 del VPC E	Locale
	CIDR IPv4 del VPC A	pcx-aaaaeeee
	CIDR IPv6 del VPC A	pcx-aaaaeeee
VPC F	*CIDR IPv4 del VPC F*	Locale
	CIDR IPv6 del VPC F	Locale
	CIDR IPv4 del VPC A	pcx-aaaaffff
	CIDR IPv6 del VPC A	pcx-aaaaffff
VPC G	*CIDR IPv4 del VPC G*	Locale
	CIDR IPv6 del VPC G	Locale
	CIDR IPv4 del VPC A	pcx-aaaagggg
	CIDR IPv6 del VPC A	pcx-aaaagggg

Tre VPC collegati in peering tra loro

In questa configurazione, ci sono tre VPC nello stesso Account AWS con blocchi CIDR che non si sovrappongono. I VPC vengono connessi in peering in una configurazione mesh completa come segue:

- VPC A è collegato in peering a VPC B via la connessione peering VPC `pcx-aaaabbbb`
- VPC A è collegato in peering a VPC C via la connessione peering VPC `pcx-aaaacccc`
- VPC B è collegato in peering a VPC C via la connessione peering VPC `pcx-bbbbcccc`



Puoi utilizzare questa configurazione quando disponi di VPC che devono condividere risorse tra loro senza restrizioni. Ad esempio, come sistema di condivisione di file.

Aggiorna la tabella di instradamento per ogni VPC come segue per implementare questa configurazione.

Tabella di routing	Destinazione	Target
VPC A	*VPC A CIDR*	Locale
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Locale
	VPC A CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-bbbbcccc
VPC C	*VPC C CIDR*	Locale
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc

Se VPC A e VPC B hanno blocchi CIDR IPv4 e IPv6, ma VPC C non ha un blocco CIDR IPv6, aggiorna le tabelle di instradamento come segue. Le risorse in VPC A e VPC B possono comunicare utilizzando IPv6 tramite la connessione peering VPC. Tuttavia, VPC C non può comunicare con VPC A o VPC B tramite IPv6.

Tabelle di instradamento	Destinazione	Target
VPC A	*CIDR IPv4 del VPC A*	Locale
	CIDR IPv6 del VPC A	Locale
	CIDR IPv4 del VPC B	pcx-aaaabbbb
	CIDR IPv6 del VPC B	pcx-aaaabbbb
	CIDR IPv4 del VPC C	pcx-aaaacccc
VPC B	*CIDR IPv4 del VPC B*	Locale
	CIDR IPv6 del VPC B	Locale
	CIDR IPv4 del VPC A	pcx-aaaabbbb
	CIDR IPv6 del VPC A	pcx-aaaabbbb
	CIDR IPv4 del VPC C	pcx-bbbbcccc
VPC C	*CIDR IPv4 del VPC C*	Locale
	CIDR IPv4 del VPC A	pcx-aaaacccc
	CIDR IPv4 del VPC B	pcx-bbbbcccc

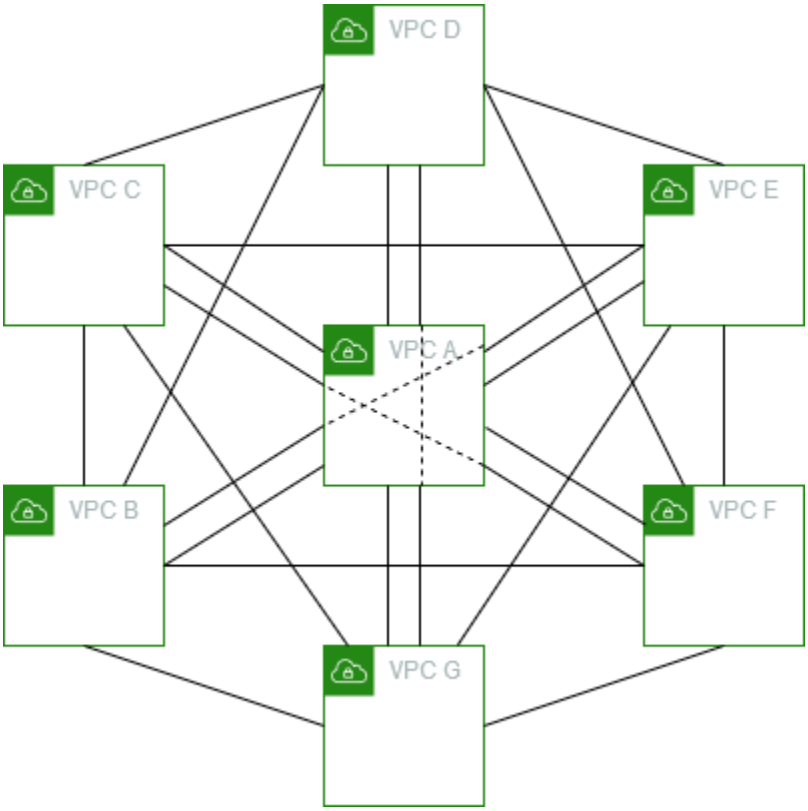
Molteplici VPC collegati in peering tra loro

In questa configurazione, ci sono sette VPC in peering in una configurazione mesh completa. I VPC sono nello stesso Account AWS e i loro blocchi CIDR non si sovrappongono.

VPC	VPC	Connessione di peering di VPC
A	B	pcx-aaaabbbb
A	C	pcx-aaaacccc
A	D	pcx-aaaadddd

VPC	VPC	Connessione di peering di VPC
A	E	pcx-aaaaeeee
A	F	pcx-aaaaffff
A	G	pcx-aaaagggg
B	C	pcx-bbbbcccc
B	D	pcx-bbbbdddd
B	E	pcx-bbbbeeee
B	F	pcx-bbbbffff
B	G	pcx-bbbbgggg
C	D	pcx-ccccdddd
C	E	pcx-cccceeee
C	F	pcx-ccccffff
C	G	pcx-ccccgggg
D	E	pcx-ddddeeee
D	F	pcx-ddddffff
D	G	pcx-ddddgggg
E	F	pcx-eeeeffff
E	G	pcx-eeeegggg
F	G	pcx-ffffgggg

Puoi utilizzare questa configurazione quando disponi di più VPC e ognuno deve essere in grado di accedere alle risorse degli altri senza restrizioni. Ad esempio, come rete di condivisione file. In questo diagramma, le linee rappresentano le connessioni peering VPC.



Aggiorna la tabella di instradamento per ogni VPC come segue per implementare questa configurazione.

Tabella di routing	Destinazione	Target
VPC A	*VPC A CIDR*	Locale
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
	CIDR VPC D	pcx-aaaadddd
	CIDR VPC E	pcx-aaaaeeee
	CIDR VPC F	pcx-aaaaffff
	CIDR VPC G	pcx-aaaagggg
VPC B	*VPC B CIDR*	Locale

Tabella di routing	Destinazione	Target
	VPC A CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-bbbbcccc
	CIDR VPC D	pcx-bbbbdddd
	CIDR VPC E	pcx-bbbbeeee
	CIDR VPC F	pcx-bbbbffff
	CIDR VPC G	pcx-bbbbgggg
VPC C	*VPC C CIDR*	Locale
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc
	CIDR VPC D	pcx-ccccdddd
	CIDR VPC E	pcx-ccceeeee
	CIDR VPC F	pcx-ccccffff
	CIDR VPC G	pcx-ccccgggg
VPC D	*CIDR VPC D*	Locale
	VPC A CIDR	pcx-aaaadddd
	VPC B CIDR	pcx-bbbbdddd
	VPC C CIDR	pcx-ccccdddd
	CIDR VPC E	pcx-ddddeeee
	CIDR VPC F	pcx-ddddffff
	CIDR VPC G	pcx-ddddgggg

Tabella di routing	Destinazione	Target
VPC E	*CIDR VPC E*	Locale
	VPC A CIDR	pcx-aaaaeeee
	VPC B CIDR	pcx-bbbbeeee
	VPC C CIDR	pcx-cccceeee
	CIDR VPC D	pcx-ddddeeee
	CIDR VPC F	pcx-eeeeffff
	CIDR VPC G	pcx-eeeegggg
VPC F	*CIDR VPC F*	Locale
	VPC A CIDR	pcx-aaaaffff
	VPC B CIDR	pcx-bbbbffff
	VPC C CIDR	pcx-ccccffff
	CIDR VPC D	pcx-ddddffff
	CIDR VPC E	pcx-eeeeffff
	CIDR VPC G	pcx-ffffgggg
VPC G	*CIDR VPC G*	Locale
	VPC A CIDR	pcx-aaaagggg
	VPC B CIDR	pcx-bbbbgggg
	VPC C CIDR	pcx-ccccgggg
	CIDR VPC D	pcx-ddddgggg
	CIDR VPC E	pcx-eeeegggg

Tabella di routing	Destinazione	Target
	CIDR VPC F	pcx-ffffgggg

Se tutti i VPC hanno blocchi CIDR IPv6 associati, aggiorna le tabelle di instradamento come segue.

Tabella di routing	Destinazione	Target
VPC A	*CIDR IPv4 del VPC A*	Locale
	CIDR IPv6 del VPC A	Locale
	CIDR IPv4 del VPC B	pcx-aaaabbbb
	CIDR IPv6 del VPC B	pcx-aaaabbbb
	CIDR IPv4 del VPC C	pcx-aaaacccc
	CIDR IPv6 del VPC C	pcx-aaaacccc
	CIDR IPv4 del VPC D	pcx-aaaadddd
	CIDR IPv6 del VPC D	pcx-aaaadddd
	CIDR IPv4 del VPC E	pcx-aaaaeeee
	CIDR IPv6 del VPC E	pcx-aaaaeeee
	CIDR IPv4 del VPC F	pcx-aaaaffff
	CIDR IPv6 del VPC F	pcx-aaaaffff
	CIDR IPv4 del VPC G	pcx-aaaagggg
	CIDR IPv6 del VPC G	pcx-aaaagggg
VPC B	*CIDR IPv4 del VPC B*	Locale
	CIDR IPv6 del VPC B	Locale

Tabella di routing	Destinazione	Target
	CIDR IPv4 del VPC A	pcx-aaaabbbb
	CIDR IPv6 del VPC A	pcx-aaaabbbb
	CIDR IPv4 del VPC C	pcx-bbbbcccc
	CIDR IPv6 del VPC C	pcx-bbbbcccc
	CIDR IPv4 del VPC D	pcx-bbbbdddd
	CIDR IPv6 del VPC D	pcx-bbbbdddd
	CIDR IPv4 del VPC E	pcx-bbbbeeee
	CIDR IPv6 del VPC E	pcx-bbbbeeee
	CIDR IPv4 del VPC F	pcx-bbbbffff
	CIDR IPv6 del VPC F	pcx-bbbbffff
	CIDR IPv4 del VPC G	pcx-bbbbgggg
	CIDR IPv6 del VPC G	pcx-bbbbgggg
VPC C	*CIDR IPv4 del VPC C*	Locale
	CIDR IPv6 del VPC C	Locale
	CIDR IPv4 del VPC A	pcx-aaaacccc
	CIDR IPv6 del VPC A	pcx-aaaacccc
	CIDR IPv4 del VPC B	pcx-bbbbcccc
	CIDR IPv6 del VPC B	pcx-bbbbcccc
	CIDR IPv4 del VPC D	pcx-ccccdddd
	CIDR IPv6 del VPC D	pcx-ccccdddd

Tabella di routing	Destinazione	Target
	CIDR IPv4 del VPC E	pcx-ccccceeee
	CIDR IPv6 del VPC E	pcx-ccccceeee
	CIDR IPv4 del VPC F	pcx-ccccffff
	CIDR IPv6 del VPC F	pcx-ccccffff
	CIDR IPv4 del VPC G	pcx-ccccgggg
	CIDR IPv6 del VPC G	pcx-ccccgggg
VPC D	*CIDR IPv4 del VPC D*	Locale
	CIDR IPv6 del VPC D	Locale
	CIDR IPv4 del VPC A	pcx-aaaadddd
	CIDR IPv6 del VPC A	pcx-aaaadddd
	CIDR IPv4 del VPC B	pcx-bbbbdddd
	CIDR IPv6 del VPC B	pcx-bbbbdddd
	CIDR IPv4 del VPC C	pcx-ccccdddd
	CIDR IPv6 del VPC C	pcx-ccccdddd
	CIDR IPv4 del VPC E	pcx-ddddeeee
	CIDR IPv6 del VPC E	pcx-ddddeeee
	CIDR IPv4 del VPC F	pcx-ddddffff
	CIDR IPv6 del VPC F	pcx-ddddffff
	CIDR IPv4 del VPC G	pcx-ddddgggg
	CIDR IPv6 del VPC G	pcx-ddddgggg

Tabella di routing	Destinazione	Target
VPC E	*CIDR IPv4 del VPC E*	Locale
	CIDR IPv6 del VPC E	Locale
	CIDR IPv4 del VPC A	pcx-aaaaeeee
	CIDR IPv6 del VPC A	pcx-aaaaeeee
	CIDR IPv4 del VPC B	pcx-bbbbeeee
	CIDR IPv6 del VPC B	pcx-bbbbeeee
	CIDR IPv4 del VPC C	pcx-cccceeee
	CIDR IPv6 del VPC C	pcx-cccceeee
	CIDR IPv4 del VPC D	pcx-ddddeeee
	CIDR IPv6 del VPC D	pcx-ddddeeee
	CIDR IPv4 del VPC F	pcx-eeeeffff
	CIDR IPv6 del VPC F	pcx-eeeeffff
	CIDR IPv4 del VPC G	pcx-eeeegggg
	CIDR IPv6 del VPC G	pcx-eeeegggg
VPC F	*CIDR IPv4 del VPC F*	Locale
	CIDR IPv6 del VPC F	Locale
	CIDR IPv4 del VPC A	pcx-aaaaffff
	CIDR IPv6 del VPC A	pcx-aaaaffff
	CIDR IPv4 del VPC B	pcx-bbbbffff
	CIDR IPv6 del VPC B	pcx-bbbbffff

Tabella di routing	Destinazione	Target
	CIDR IPv4 del VPC C	pcx-ccccffff
	CIDR IPv6 del VPC C	pcx-ccccffff
	CIDR IPv4 del VPC D	pcx-ddddffff
	CIDR IPv6 del VPC D	pcx-ddddffff
	CIDR IPv4 del VPC E	pcx-eeeeffff
	CIDR IPv6 del VPC E	pcx-eeeeffff
	CIDR IPv4 del VPC G	pcx-ffffgggg
	CIDR IPv6 del VPC G	pcx-ffffgggg
VPC G	*CIDR IPv4 del VPC G*	Locale
	CIDR IPv6 del VPC G	Locale
	CIDR IPv4 del VPC A	pcx-aaaagggg
	CIDR IPv6 del VPC A	pcx-aaaagggg
	CIDR IPv4 del VPC B	pcx-bbbbgggg
	CIDR IPv6 del VPC B	pcx-bbbbgggg
	CIDR IPv4 del VPC C	pcx-ccccgggg
	CIDR IPv6 del VPC C	pcx-ccccgggg
	CIDR IPv4 del VPC D	pcx-ddddgggg
	CIDR IPv6 del VPC D	pcx-ddddgggg
	CIDR IPv4 del VPC E	pcx-eeeegggg
	CIDR IPv6 del VPC E	pcx-eeeegggg

Tabella di routing	Destinazione	Target
	CIDR IPv4 del VPC F	pcx-ffffgggg
	CIDR IPv6 del VPC F	pcx-ffffgggg

Configurazioni peering VPC con instradamenti specifici

Puoi configurare le tabelle di instradamento per una connessione peering VPC per limitare l'accesso a un blocco CIDR della sottorete, un blocco CIDR specifico (se il VPC dispone di più blocchi CIDR) o una risorsa specifica all'interno del VPC in peering. In questi esempi, un VPC centrale viene connesso in peering ad almeno due VPC con blocchi CIDR che si sovrappongono.

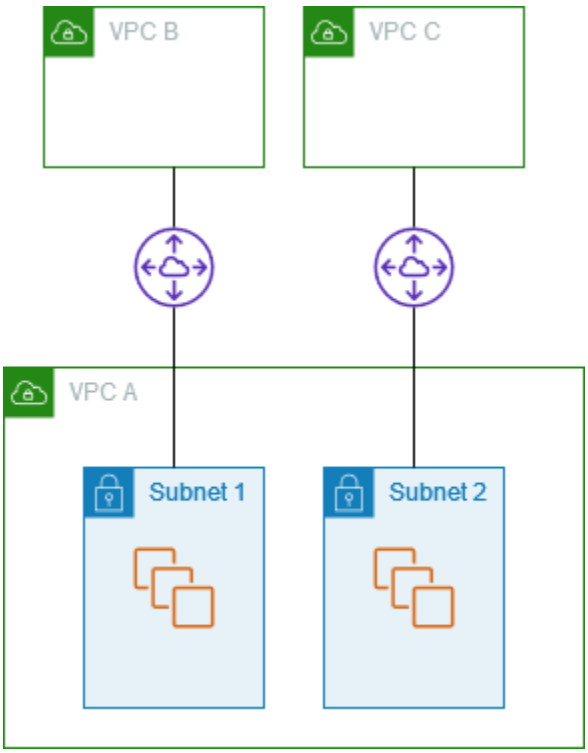
Per esempi di scenari in cui è richiesta una configurazione della connessione peering VPC specifica, consulta Scenari di peering VPC. Per ulteriori informazioni sull'utilizzo delle connessioni peering VPC, consulta la pagina Utilizzo di connessioni peering VPC. Per ulteriori informazioni sull'aggiornamento delle tabelle di routing, consulta Aggiornamento delle tabelle di routing per una connessione peering VPC.

Configurazioni

- Due VPC che accedono a sottoreti specifiche in un VPC
- Due VPC che accedono a blocchi CIDR specifici in un VPC
- Un VPC che accede a sottoreti specifiche in due VPC
- Istanze in un VPC che accedono a istanze specifiche in due VPC
- Un VPC che accede a due VPC utilizzando corrispondenze con il prefisso più lungo
- Configurazioni VPC multiple

Due VPC che accedono a sottoreti specifiche in un VPC

In questa configurazione, si hanno un VPC centrale con due sottoreti (VPC A), una connessione peering tra VPC A e VPC B (`pcx-aaaabbbb`) e una connessione peering tra VPC A e VPC C (`pcx-aaaacccc`). Ogni VPC richiede l'accesso alle risorse in una sola delle sottoreti di VPC A.



La tabella di instradamento per la sottorete 1 utilizza a una connessione peering VPC `pcx-aaaabbbb` per accedere all'intero blocco CIDR di VPC B. La tabella di instradamento di VPC B utilizza `pcx-aaaabbbb` per accedere al blocco CIDR della sola sottorete 1 in VPC A. La tabella di instradamento per la sottorete 2 utilizza la connessione peering VPC `pcx-aaaacccc` per accedere all'intero blocco CIDR di VPC C. La tabella di instradamento di VPC C utilizza `pcx-aaaacccc` per accedere al blocco CIDR della sola sottorete 2 in VPC A.

Tabella di routing	Destinazione	Target
Sottorete 1 (VPC A)	*VPC A CIDR*	Locale
	VPC B CIDR	pcx-aaaabbbb
Sottorete 2 (VPC A)	*VPC A CIDR*	Locale
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Locale
	CIDR sottorete 1	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Locale

Tabella di routing	Destinazione	Target
	CIDR sottorete 2	pcx-aaaacccc

È possibile estendere questa configurazione a più blocchi CIDR. Supponiamo che VPC A e VPC B abbiano sia blocchi CIDR IPv4 che IPv6 e che la sottorete 1 abbia un blocco CIDR IPv6. Puoi abilitare la comunicazione tra VPC B e la sottorete 1 in VPC A su IPv6 utilizzando la connessione peering VPC. Per farlo, aggiungi un instradamento alla tabella di instradamento per VPC A con una destinazione del blocco CIDR IPv6 per VPC B e un instradamento alla tabella di instradamento per VPC B con una destinazione del CIDR IPv6 della sottorete 1 in VPC A.

Tabella di routing	Destinazione	Target	Note
Sottorete 1 in VPC A	*CIDR IPv4 del VPC A*	Locale	
	CIDR IPv6 del VPC A	Locale	Route locale che viene aggiunta automaticamente per la comunicazione IPv6 all'interno del VPC.
	CIDR IPv4 del VPC B	pcx-aaaabbbb	
	CIDR IPv6 del VPC B	pcx-aaaabbbb	Route al blocco CIDR IPv6 di VPC B.
Sottorete 2 in VPC A	*CIDR IPv4 del VPC A*	Locale	
	CIDR IPv6 del VPC A	Locale	Route locale che viene aggiunta automaticamente per la comunicazione

Tabella di routing	Destinazione	Target	Note
			IPv6 all'interno del VPC.
	CIDR IPv4 del VPC C	pcx-aaaacccc	
VPC B	*CIDR IPv4 del VPC B*	Locale	
	CIDR IPv6 del VPC B	Locale	Route locale che viene aggiunta automaticamente per la comunicazione IPv6 all'interno del VPC.
	CIDR IPv4 della sottorete 1	pcx-aaaabbbb	
	CIDR IPv4 della sottorete 2	pcx-aaaabbbb	Route al blocco CIDR IPv6 di VPC A.
VPC C	*CIDR IPv4 del VPC C*	Locale	
	CIDR IPv4 della sottorete 2	pcx-aaaacccc	

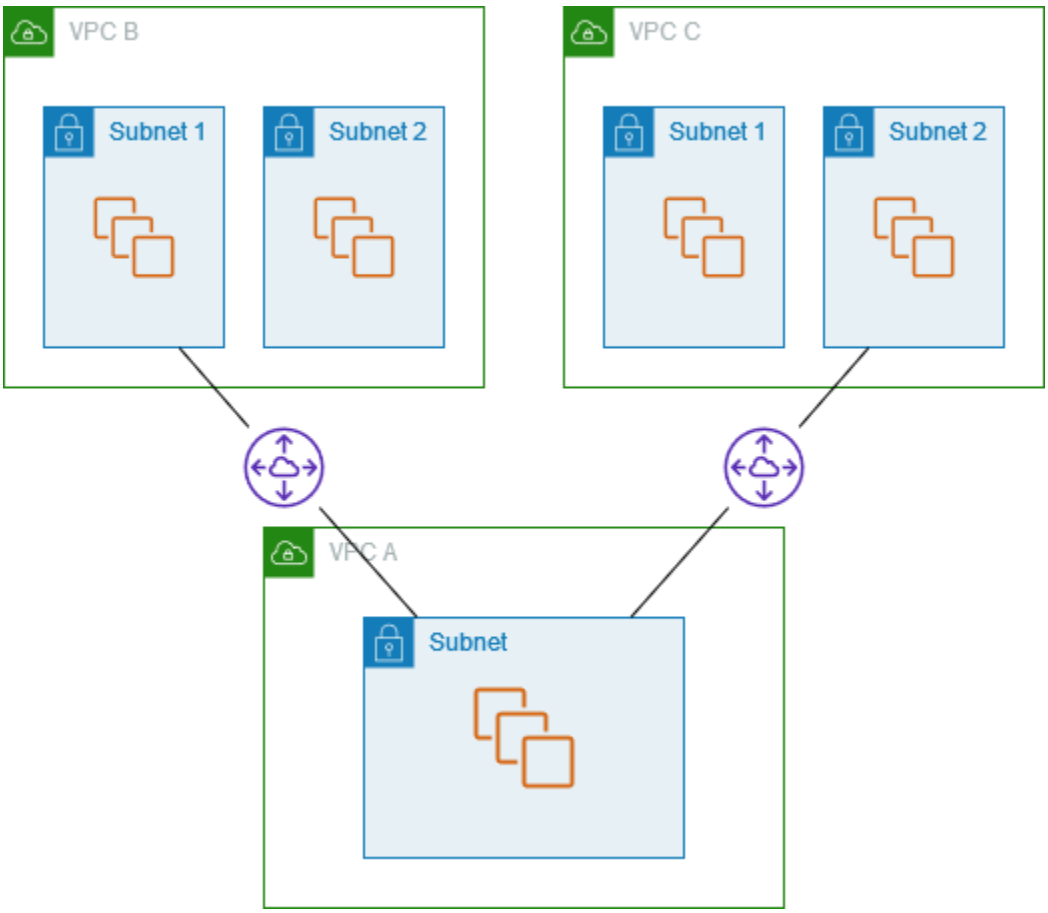
Due VPC che accedono a blocchi CIDR specifici in un VPC

In questa configurazione, esistono un VPC centrale (VPC A), una connessione peering tra VPC A e VPC B (`pcx-aaaabbbb`) e una connessione peering tra VPC A e VPC C (`pcx-aaaacccc`). VPC A dispone di un blocco CIDR per ogni connessione peering.

Tabella di routing	Destinazione	Target
VPC A	*CIDR 1 VPC A*	Locale
	CIDR 2 VPC A	Locale
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Locale
	CIDR 1 VPC A	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Locale
	CIDR 2 VPC A	pcx-aaaacccc

Un VPC che accede a sottoreti specifiche in due VPC

In questa configurazione, si hanno un VPC centrale con una sottorete (VPC A), una connessione peering tra VPC A e VPC B (`pcx-aaaabbbb`) e una connessione peering tra VPC A e VPC C (`pcx-aaaacccc`). VPC B e VPC C dispongono ciascuno di due sottoreti. La connessione peering tra VPC A e VPC B utilizza solo una delle sottoreti in VPC B. La connessione peering tra VPC A e VPC C utilizza solo una delle sottoreti in VPC C.



Utilizza questa configurazione quando disponi di un VPC centrale con un singolo set di risorse, ad esempio servizi Active Directory, a cui devono accedere altri VPC. Il VPC centrale non richiede l'accesso completo ai VPC cui è collegato in peering.

La tabella di instradamento per VPC A utilizza le connessioni peering per accedere solo a sottoreti specifiche nei VPC connessi in peering. La tabella di instradamento per la sottorete 1 utilizza la connessione peering con VPC A per accedere alla sottorete in VPC A. La tabella di instradamento per la sottorete 2 utilizza la connessione peering con VPC A per accedere alla sottorete in VPC A.

Tabella di routing	Destinazione	Target
VPC A	*VPC A CIDR*	Locale
	CIDR sottorete 1	pcx-aaaabbbb
	CIDR sottorete 2	pcx-aaaacccc
Sottorete 1 (VPC B)	*VPC B CIDR*	Locale

Tabella di routing	Destinazione	Target
	Sottorete nel CIDR del VPC A	pcx-aaaabbbb
Sottorete 2 (VPC C)	*VPC C CIDR*	Locale
	Sottorete nel CIDR del VPC A	pcx-aaaacccc

Routing per traffico di risposta

Se disponi di un VPC connessi in peering a molti VPC che hanno blocchi CIDR sovrapposti o corrispondenti, assicurati che le tabelle di instradamento siano configurate in modo da non inviare traffico di risposta dal VPC al VPC sbagliato. AWS non supporta la funzionalità reverse path forwarding unicast (trasmissione uno a uno) nelle connessioni peering VPC che controlla l'IP di origine di pacchetti e reinstrada i pacchetti di risposta all'origine.

Ad esempio, VPC A è collegato in peering a VPC B e VPC C. VPC B e VPC C dispongono di blocchi CIDR corrispondenti e le relative sottoreti dispongono di blocchi CIDR corrispondenti. La tabella di instradamento per la sottorete 2 in VPC B fa riferimento alla connessione peering VPC `pcx-aaaabbbb` per accedere alla sottorete di VPC A. La tabella di instradamento di VPC A è configurata per inviare il traffico destinato al CIDR del VPC alla connessione peering `pcx-aaaaccccc`.

Tabella di routing	Destinazione	Target
Sottorete 2 (VPC B)	*VPC B CIDR*	Locale
	Sottorete nel CIDR del VPC A	pcx-aaaabbbb
VPC A	*VPC A CIDR*	Locale
	VPC C CIDR	pcx-aaaacccc

Supponiamo che un'istanza nella sottorete 2 nel VPC B invii il traffico al server Active Directory nel VPC A utilizzando la connessione peering VPC `pcx-aaaabbbb`. VPC A invia il traffico di risposta al

server Active Directory. Tuttavia, la tabella di instradamento di VPC A è configurata per inviare tutto il traffico all'interno dell'intervallo CIDR di VPC alla connessione peering VPC `pcx-aaaacccc`. Se la sottorete 2 nel VPC C dispone di un'istanza con lo stesso indirizzo IP dell'istanza nella sottorete 2 di VPC B, riceve il traffico di risposta da VPC A. L'istanza nella sottorete 2 in VPC B non riceve una risposta alla sua richiesta a VPC A.

Per impedire ciò, puoi aggiungere un instradamento specifico alla tabella di instradamento di VPC A con il CIDR della sottorete 2 in VPC B come destinazione e target di `pcx-aaaabbbb`. Il nuovo instradamento è più specifico, pertanto il traffico destinato al CIDR della sottorete 2 viene instradato alla connessione peering VPC `pcx-aaaabbbb`

In alternativa, nel seguente esempio, la tabella di instradamento di VPC A dispone di un instradamento per ogni sottorete per ogni connessione peering VPC. VPC A può comunicare con la sottorete B in VPC B e con la sottorete A in VPC C. Questo scenario è utile se occorre aggiungere un'altra connessione peering VPC con un'altra sottorete che si trova all'interno dello stesso intervallo di indirizzi IP di VPC B e VPC C: puoi semplicemente aggiungere un altro instradamento per la sottorete specifica.

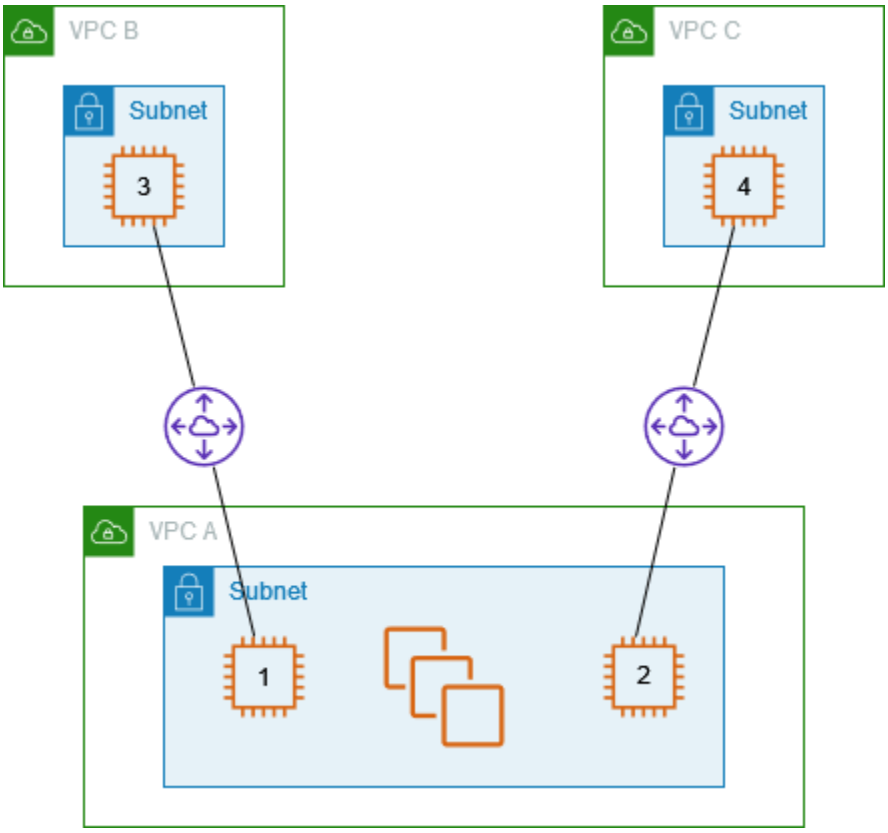
Destinazione	Target
VPC A CIDR	Locale
CIDR sottorete 2	pcx-aaaabbbb
CIDR sottorete 1	pcx-aaaacccc

In alternativa, a seconda del caso d'uso, puoi creare una route a un indirizzo IP specifico in VPC B per assicurarti che il traffico sia re-instradato al server corretto (la tabella di instradamento utilizza la corrispondenza prefisso più lungo per definire le priorità delle route):

Destinazione	Target
VPC A CIDR	Locale
Indirizzo IP specifico nella sottorete 2	pcx-aaaabbbb
VPC B CIDR	pcx-aaaacccc

Istanze in un VPC che accedono a istanze specifiche in due VPC

In questa configurazione, si hanno un VPC centrale con una sottorete (VPC A), una connessione peering tra VPC A e VPC B (`pcx-aaaabbbb`) e una connessione peering tra VPC A e VPC C (`pcx-aaaacccc`). VPC A ha una sottorete con un'istanza per ogni connessione peering. Puoi utilizzare questa configurazione per limitare il traffico di peering verso istanze specifiche.



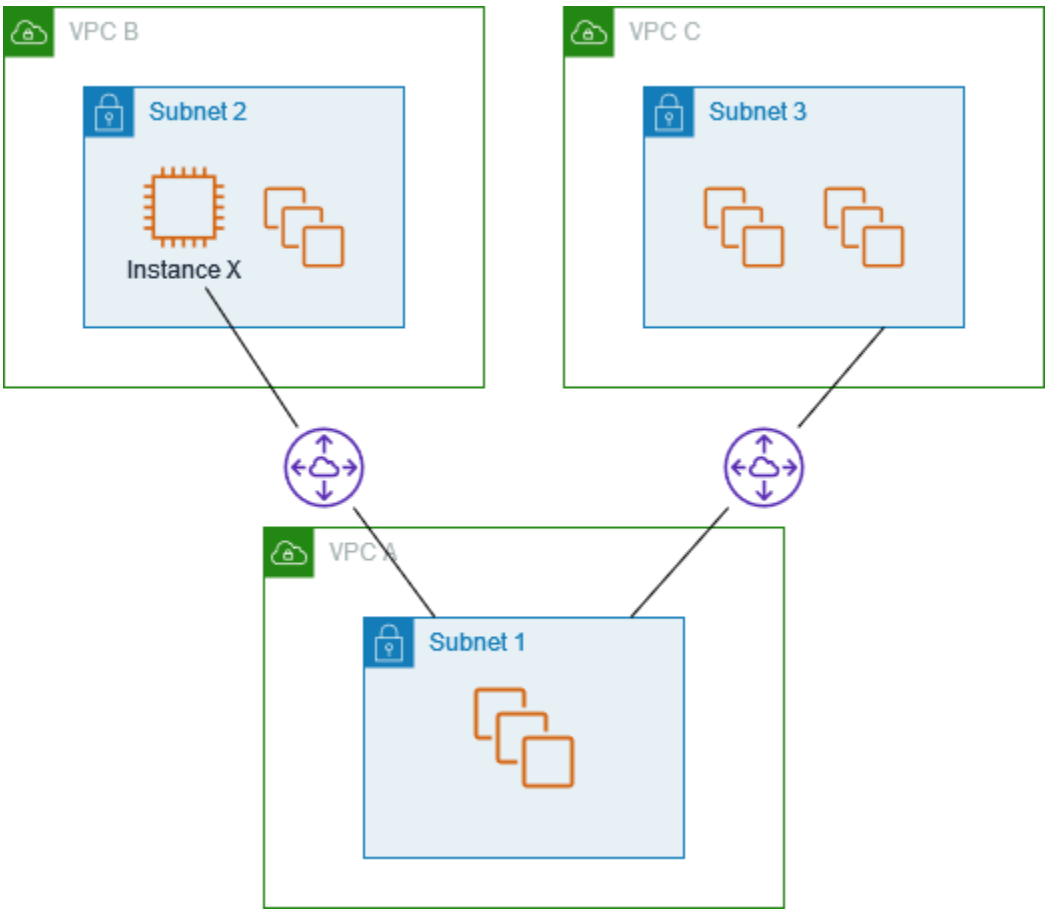
Ogni tabella di instradamento VPC punta alla connessione peering VPC pertinente per accedere a un singolo indirizzo IP (e pertanto un'istanza specifica) nel VPC in peering.

Tabella di routing	Destinazione	Target
VPC A	*VPC A CIDR*	Locale
	Indirizzo IP dell'istanza 3	pcx-aaaabbbb
	Indirizzo IP dell'istanza 4	pcx-aaaacccc

Tabella di routing	Destinazione	Target
VPC B	*VPC B CIDR*	Locale
	Indirizzo IP dell'istanza 1	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Locale
	Indirizzo IP dell'istanza 2	pcx-aaaacccc

Un VPC che accede a due VPC utilizzando corrispondenze con il prefisso più lungo

In questa configurazione, si hanno un VPC centrale con una sottorete (VPC A), una connessione peering tra VPC A e VPC B (`pcx-aaaabbbb`) e una connessione peering tra VPC A e VPC C (`pcx-aaaacccc`). VPC B e VPC C dispongono di blocchi CIDR corrispondenti. La connessione peering VPC `pcx-aaaabbbb` può essere utilizzata per instradare il traffico tra VPC A e un'istanza specifica in VPC B. Tutto il traffico rimanente destinato per l'intervallo di indirizzi del CIDR condiviso tra VPC B e VPC C viene istradato a VPC C tramite `pcx-aaaacccc`.



Le tabelle di routing VPC utilizzano la corrispondenza prefisso più lungo per selezionare la route più specifica sulla connessione peering VPC attesa. Tutto il traffico restante viene instradato tramite la successiva route corrispondente, in questo caso, sulla connessione peering VPC `pcx-aaaacccc`.

Tabella di routing	Destinazione	Target
VPC A	*Blocco CIDR del VPC A*	Locale
	Indirizzo IP dell'istanza X	pcx-aaaabbbb
	Blocco CIDR del VPC C	pcx-aaaacccc
VPC B	*Blocco CIDR del VPC B*	Locale
	Blocco CIDR del VPC A	pcx-aaaabbbb
VPC C	*Blocco CIDR del VPC C*	Locale

Tabella di routing	Destinazione	Target
	Blocco CIDR del VPC A	pcx-aaaacccc

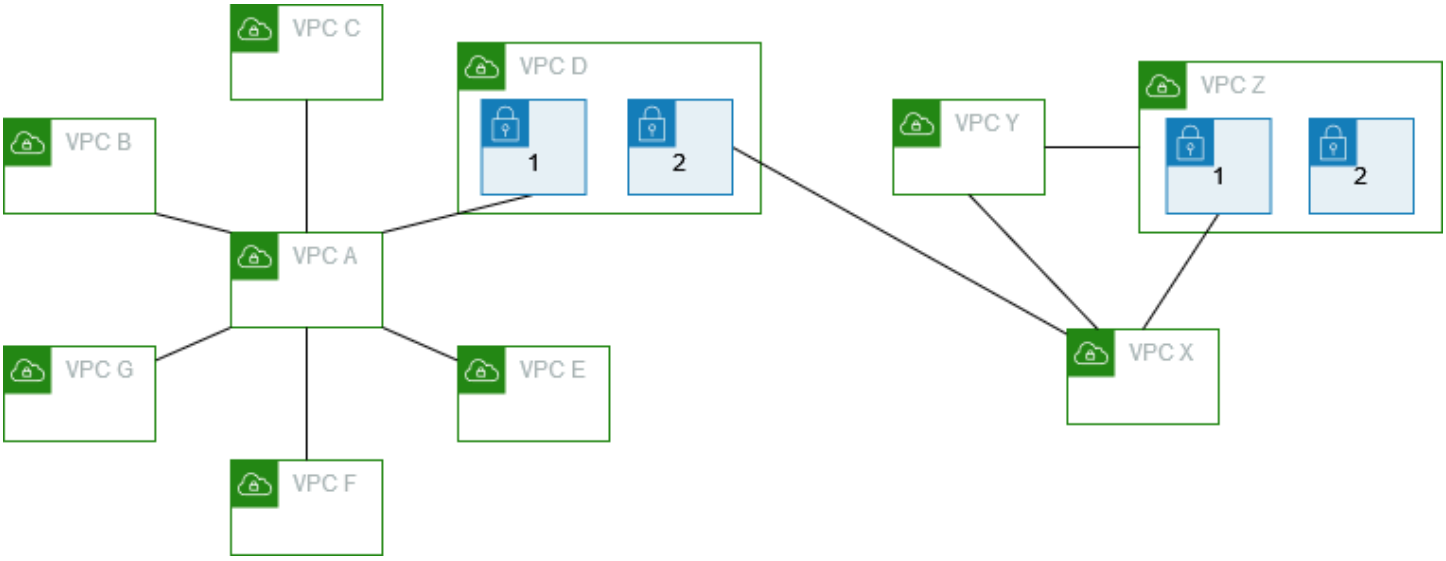
> **Important**
>
> Se un'istanza diversa dall'istanza X in VPC B invia il traffico a VPC A, il traffico di risposta può essere instradato a VPC C anziché a VPC B. Per ulteriori informazioni, consulta la pagina Routing per traffico di risposta.

Configurazioni VPC multiple

In questa configurazione, un VPC centrale (VPC A) è connesso in peering con più VPC in una configurazione spoke. Sono presenti anche tre VPC (VPC X, Y e Z) collegati in peering tra loro in una configurazione mesh completa.

VPC D dispone anche di una connessione peering VPC con VPC X (`pcx-ddddxxxx`). VPC A e VPC X dispongono di blocchi CIDR che si sovrappongono. Ciò significa che il traffico di peering tra VPC A e VPC D è limitato a una sottorete specifica (sottorete 1) in VPC D. Ciò serve a garantire che se VPC D riceve una richiesta dal VPC A o dal VPC X, invii il traffico di risposta al VPC corretto. AWSnon supporta l'inoltro unicast del percorso inverso nelle connessioni peering VPC che controllano l'IP di origine dei pacchetti e indirizzano i pacchetti di risposta all'origine. Per ulteriori informazioni, consulta Routing per traffico di risposta.

Analogamente, VPC D e VPC Z dispongono di blocchi CIDR che si sovrappongono. Il traffico di peering tra VPC D e VPC X è limitato alla sottorete 2 in VPC D e il traffico di peering tra VPC X e VPC Z è limitato alla sottorete 1 in VPC Z. Ciò garantisce che se VPC X riceve traffico di peering da VPC D o VPC Z, restituisce il traffico di risposta al VPC corretto.



Le tabelle di instradamento per i VPC B, C, E, F e G puntano alle connessioni peering pertinenti per accedere al blocco CIDR completo per VPC A e la tabella di instradamento di VPC A fa riferimento alle connessioni peering pertinenti per i VPC B, D, E, F e G per accedere ai rispettivi blocchi CIDR completi. Per la connessione peering `pcx-aaaadddd`, la tabella di instradamento di VPC A instrada il traffico solo alla sottorete 1 in VPC D e la tabella di instradamento della sottorete 1 in VPC D fa riferimento al blocco CIDR completo di VPC A.

La tabella di instradamento di VPC Y fa riferimento alle connessioni peering pertinenti per accedere ai blocchi CIDR completi di VPC X e VPC Z e la tabella di instradamento di VPC Z fa riferimento alla connessione peering pertinente per accedere al blocco CIDR completo di VPC Y. La tabella di instradamento della sottorete 1 in VPC Z fa riferimento alla connessione peering pertinente per accedere al blocco CIDR completo di VPC Y. La tabella di instradamento di VPC X fa riferimento alla connessione peering pertinente per accedere alla sottorete 2 in VPC D e alla sottorete 1 in VPC Z.

Tabella di routing	Destinazione	Target
VPC A	*VPC A CIDR*	Locale
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
	CIDR della sottorete 1 nel VPC D	pcx-aaaadddd

Tabella di routing	Destinazione	Target
	CIDR VPC E	pcx-aaaaeeee
	CIDR VPC F	pcx-aaaaffff
	CIDR VPC G	pcx-aaaagggg
VPC B	*VPC B CIDR*	Locale
	VPC A CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Locale
	VPC A CIDR	pcx-aaaacccc
Sottorete 1 in VPC D	*CIDR VPC D*	Locale
	VPC A CIDR	pcx-aaaadddd
Sottorete 2 in VPC D	*CIDR VPC D*	Locale
	CIDR VPC X	pcx-ddddxxxx
VPC E	*CIDR VPC E*	Locale
	VPC A CIDR	pcx-aaaaeeee
VPC F	*CIDR VPC F*	Locale
	VPC A CIDR	pcx-aaaaffff
VPC G	*CIDR VPC G*	Locale
	VPC A CIDR	pcx-aaaagggg
VPC X	*CIDR VPC X*	Locale
	CIDR della sottorete 2 nel VPC D	pcx-ddddxxxx
	CIDR VPC Y	pcx-xxxxyyyy

Tabella di routing	Destinazione	Target
	CIDR della sottorete 1 nel VPC Z	pcx-xxxxzzzz
VPC Y	*CIDR VPC Z*	Locale
	CIDR VPC X	pcx-xxxxyyyy
	CIDR VPC Z	pcx-yyyyzzzz
VPC Z	*CIDR VPC Z*	Locale
	CIDR VPC Z	pcx-yyyyzzzz
	CIDR VPC X	pcx-xxxxzzzz

Scenari di peering VPC

Esistono diversi motivi per cui potrebbe essere necessario configurare una connessione peering VPC tra i VPC o tra un VPC di tua proprietà e un VPC in un account AWS differente. I seguenti scenari consentono di determinare quale configurazione è più idonea ai requisiti di rete.

Scenari

- Collegamento in peering di due o più VPC per fornire accesso completo alle risorse
- Collegamento in peering a un VPC per accedere a risorse centralizzate

Collegamento in peering di due o più VPC per fornire accesso completo alle risorse

In questo scenario, si dispone di due o più VPC che si desidera collegare in peering per abilitare la condivisione completa di risorse tra tutti i VPC. Di seguito vengono mostrati alcuni esempi:

- L'azienda dispone di un VPC per il reparto finanziario e di un altro VPC per il reparto di contabilità. Il reparto finanziario richiede l'accesso a tutte le risorse disponibili nel reparto di contabilità e il reparto di contabilità richiede l'accesso a tutte le risorse nel reparto finanziario.
- L'azienda dispone di più reparti IT, ciascuno con il proprio VPC. Alcuni VPC si trovano all'interno dello stesso account AWS mentre altri si trovano in un account AWS differente. Si desidera collegare in peering tutti i VPC insieme per consentire ai reparti IT l'accesso completo alle risorse di ciascun altro.

Per ulteriori informazioni su come configurare la configurazione della connessione peering VPC e le tabelle di routing per questo scenario, consulta la documentazione seguente:

- Due VPC collegati in peering tra loro
- Tre VPC collegati in peering tra loro
- Molteplici VPC collegati in peering tra loro

Per ulteriori informazioni sulla creazione e sull'utilizzo di connessioni peering VPC nella console Amazon VPC, consulta Utilizzo di connessioni peering VPC.

Collegamento in peering a un VPC per accedere a risorse centralizzate

In questo scenario, si dispone di un VPC centrale che contiene risorse che si desidera condividere con altri VPC. Il VPC centrale può richiedere l'accesso completo o parziale ai VPC in peering e, analogamente, i VPC in peering possono richiedere l'accesso completo o parziale al VPC centrale. Di seguito vengono mostrati alcuni esempi:

- Il reparto IT dell'azienda dispone di un VPC per la condivisione file. Si desidera collegare in peering altri VPC al VPC centrale, senza però scambio di traffico tra gli altri VPC.
- L'azienda dispone di un VPC che desideri condividere con altri clienti. Ogni cliente può creare una connessione peering VPC con il VPC, tuttavia, i clienti non possono instradare il traffico verso altri VPC collegati in peering ai tuoi, né sono a conoscenza delle route degli altri clienti.
- Disponi di un VPC centrale che viene utilizzato per servizi Active Directory. Istanze specifiche in VPC in peering inviano richieste ai server Active Directory e richiedono l'accesso completo al VPC centrale. Il VPC centrale non richiede l'accesso completo ai VPC in peering; deve solo instradare il traffico di risposta alle istanze specifiche.

Per ulteriori informazioni sulla creazione e sull'utilizzo di connessioni peering VPC nella console Amazon VPC, consulta Utilizzo di connessioni peering VPC.

Identity and Access Management per il peering VPC

Per impostazione predefinita, gli utenti non possono creare o modificare connessioni peering VPC. Per concedere l'accesso alle risorse di peering del VPC, collega una policy IAM a un'identità IAM, come un ruolo.

Esempi

- Esempio: Creazione di una connessione peering VPC
- Esempio: Accettazione di una connessione peering VPC
- Esempio: Eliminazione di una connessione peering VPC
- Esempio: operazioni all'interno di un account specifico
- Esempio: gestione delle connessioni peering VPC tramite la console

Per un elenco delle operazioni di Amazon VPC e delle chiavi per le risorse e le condizioni supportate per ciascuna operazione, consulta Azioni, risorse e chiavi di condizione per Amazon EC2 in Service Authorization Reference.

Esempio: Creazione di una connessione peering VPC

La policy seguente concede agli utenti l'autorizzazione per creare richieste di connessione peering VPC utilizzando i VPC che sono contrassegnati con `Purpose=Peering`. La prima istruzione applica una chiave di condizione (`ec2:ResourceTag`) alla risorsa VPC. Nota che la risorsa VPC per l'operazione `CreateVpcPeeringConnection` è sempre il VPC richiedente.

La seconda istruzione concede agli utenti l'autorizzazione per creare le risorse della connessione peering VPC e pertanto utilizza il carattere jolly * al posto di un ID risorsa specifico.

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

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

La seguente policy concede agli utenti nell'account AWS specificato l'autorizzazione per creare connessioni peering VPC utilizzando qualsiasi VPC nella regione specificata, ma solo se il VPC che accetterà la connessione peering è un VPC specifico in un account specifico.

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

Esempio: Accettazione di una connessione peering VPC

La policy seguente concede agli utenti l'autorizzazione per accettare richieste di connessione peering VPC solo da un account AWS specifico. Questo impedisce agli utenti di accettare richieste

di connessione peering VPC da account sconosciuti. L'istruzione utilizza la chiave di condizione `ec2:RequesterVpc` per imporre ciò.

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

La seguente policy concede agli utenti l'autorizzazione per accettare richieste di peering VPC se il VPC contiene il tag `Purpose=Peering`.

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

Esempio: Eliminazione di una connessione peering VPC

La seguente policy concede agli utenti nell'account specificato l'autorizzazione per eliminare qualsiasi connessione peering VPC, tranne quelle che utilizzano il VPC specificato, che si trova nello stesso account. La policy specifica entrambe le chiavi di condizioni `ec2:AccepterVpc` ed `ec2:RequesterVpc`, poiché il VPC potrebbe essere stato il VPC richiedente o il VPC in peering nella richiesta di connessione peering VPC originale.

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

Esempio: operazioni all'interno di un account specifico

La seguente policy concede agli utenti l'autorizzazione per utilizzare le connessioni peering VPC all'interno di un account specifico. Gli utenti possono visualizzare, creare, accettare, rifiutare Ed eliminare connessioni peering VPC, purché si trovino tutte all'interno dello stesso account AWS.

La prima istruzione concede agli utenti l'autorizzazione per visualizzare tutte le connessioni peering VPC. L'elemento `Resource` richiede in questo caso un carattere jolly *, poiché questa operazione API (`DescribeVpcPeeringConnections`) attualmente non supporta autorizzazioni a livello di risorsa.

La seconda istruzione concede agli utenti l'autorizzazione per creare connessioni peering VPC e consente l'accesso a tutti i VPC nell'account specificato per consentire questa operazione.

La terza istruzione utilizza un carattere jolly * come parte dell'elemento `Action` per consentire tutte le operazioni della connessione peering VPC. Le chiavi di condizione garantiscono che le azioni possono essere Eseguite solo su connessioni peering VPC con VPC che sono parte dell'account. Ad esempio, un utente non può eliminare una connessione peering VPC se il VPC accettante o richiedente si trova in un account differente. Un utente non può creare una connessione peering VPC con un VPC in un account differente.

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

Esempio: gestione delle connessioni peering VPC tramite la console

Per visualizzare connessioni peering VPC nella console Amazon VPC, gli utenti devono disporre dell'autorizzazione per utilizzare l'operazione `ec2:DescribeVpcPeeringConnections`. Per utilizzare la finestra di dialogo Create Peering Connection (Crea connessione peering), gli utenti

devono disporre dell'autorizzazione per utilizzare l'operazione `ec2:DescribeVpcs`. Ciò consente loro di visualizzare e selezionare un VPC. Puoi applicare autorizzazioni a livello di risorsa a tutte le operazioni `ec2:*PeeringConnection`, tranne `ec2:DescribeVpcPeeringConnections`.

La seguente policy concede agli utenti l'autorizzazione per visualizzare connessioni peering VPC e utilizzare la finestra di dialogo Create VPC Peering Connection (Crea connessione peering VPC) per creare una connessione peering VPC utilizzando solo un VPC richiedente specifico. Se gli utenti tentano di creare una connessione peering VPC con un VPC richiedente diverso, la richiesta non va a buon fine.

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

Quote delle connessioni peering VPC

Nelle tabelle che seguono sono elencate le quote, dette anche limiti, relativi alle connessioni peering VPC per l'account AWS. Se non è diversamente indicato, è possibile chiedere un aumento di queste quote.

Nome	Default	Adattabile
Connessioni VPC in peering per VPC	50	Sì (fino a 125)
Richieste di connessione VPC in peering in sospeso	25	Sì
Periodo di validità per una richiesta di connessione VPC in peering non accettata	1 settimana (168 ore)	No

Per ulteriori informazioni sulle regole per l'uso delle connessioni peering VPC, consulta Limitazioni relative al peering VPC.

Per quote aggiuntive per Amazon VPC, consulta Quote di Amazon VPC nella Guida per l'utente di Amazon VPC.

Cronologia dei documenti per la Guida di Amazon VPC Peering

La seguente tabella riporta i vari rilasci della Guida al peering di Amazon VPC.

Modifica	Descrizione	Data
Tag alla creazione	È possibile aggiungere tag quando si crea una connessione peering VPC e una tabella di routing.	20 luglio 2020
Peering tra regioni	La risoluzione dei nomi host DNS è supportata per le connessioni peering VPC tra regioni nella regione Asia Pacifico (Hong Kong).	26 agosto 2019
Peering tra regioni	Puoi creare una connessione peering VPC tra VPC che si trovano in regioni AWS differenti.	29 novembre 2017
Supporto per la risoluzione DNS per il peering di VPC	Puoi abilitare un VPC locale per risolvere nomi host DNS in indirizzi IP privati quando viene interrogato da istanze nel VPC in peering.	28 luglio 2016
Regole obsolete del gruppo di sicurezza	Puoi determinare se al tuo gruppo di sicurezza si fa riferimento nelle regole di un gruppo di sicurezza in un VPC peer e identificare le regole del gruppo di sicurezza obsolete.	12 maggio 2016

Utilizzo di ClassicLink su una connessione peering VPC	Puoi modificare la connessione peering VPC per consentire alle istanze EC2-Classic collegate locali di comunicare con istanze in un VPC in peering o viceversa.	26 Aprile 2016
Peering VPC	Puoi creare una connessione peering VPC tra due VPC che consente alle istanze in entrambi i VPC di comunicare tra loro tramite indirizzi IP privati	24 marzo 2014

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.