



Peering di VPC

Amazon Virtual Private Cloud



Amazon Virtual Private Cloud: Peering di VPC

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

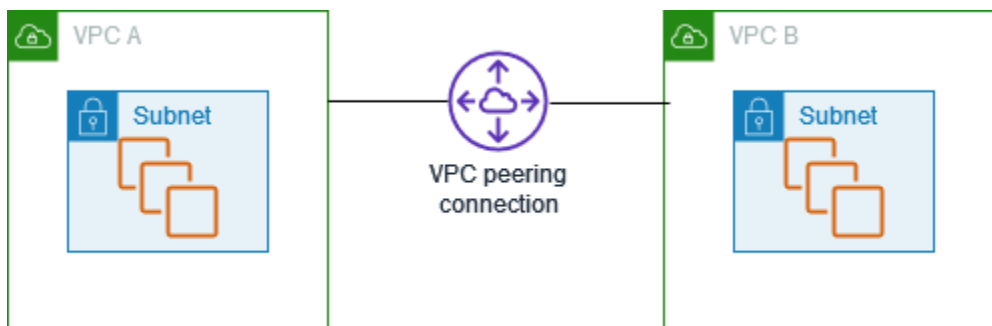
Che cos'è il peering VPC?	1
Prezzi relativi a una connessione peering VPC	2
Come funzionano le connessioni peering	3
Ciclo di vita delle connessioni peering VPC	3
Molteplici connessioni peering VPC	5
Limitazioni relative al peering VPC	6
Connessioni peering	9
Crea	10
Prerequisiti	10
Crea una connessione peering tramite la console	10
Creare una connessione peering tramite la riga di comando	11
Accetta o rifiuta	11
Aggiorna le tabelle di routing	13
Gruppi di sicurezza peer di riferimento	16
Identificazione dei gruppi di sicurezza a cui si fa riferimento	18
Visualizzazione ed eliminazione di regole del gruppo di sicurezza	19
Abilitazione della risoluzione DNS per una connessione peering VPC	20
Elimina	22
Risoluzione dei problemi	23
Configurazioni di peering VPC comuni	24
Instradamento verso un blocco CIDR VPC	24
Due VPC collegati in peering tra loro	25
Un VPC collegato in peering a due VPC	27
Tre VPC collegati in peering tra loro	31
Molteplici VPC collegati in peering tra loro	33
Instradamento verso indirizzi specifici	42
Due VPCs che accedono a sottoreti specifiche in un VPC	43
Due VPCs che accedono a blocchi CIDR specifici in un VPC	46
Un VPC che accede a sottoreti specifiche in due VPCs	46
Istanze in un VPC che accedono a istanze specifiche in due VPCs	50
Un VPC che accede a due VPCs utilizzando le corrispondenze di prefisso più lunghe	51
Configurazioni VPC multiple	52
Scenari di peering VPC	56
Peering di due o più risorse per fornire l'accesso completo VPCs alle risorse	56

Collegamento in peering a un VPC per accedere a risorse centralizzate	57
Gestione dell'identità e degli accessi	58
Creazione di una connessione peering VPC	58
Accettare una connessione peering VPC	60
Eliminazione di una connessione peering VPC	61
Utilizzo all'interno di un account specifico	62
Gestione delle connessioni peering VPC nella console	63
Quote	65
Cronologia dei documenti	66
.....	lxviii

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 cloud. AWS Puoi avviare AWS risorse, come le EC2 istanze Amazon, nel tuo VPC.

Una connessione peering VPC è una connessione di rete tra due VPCs che consente di instradare il traffico tra di loro utilizzando indirizzi o IPv4 indirizzi privati. IPv6 Le istanze in uno qualsiasi dei VPC possono comunicare tra loro come se fossero nella stessa rete. Puoi creare una connessione peering VPC tra la tua VPCs o con un VPC in un altro account. AWS VPCs Possono trovarsi in regioni diverse (nota anche come connessione peering VPC interregionale).



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 si dispone di più di un AWS account, è possibile eseguire il peering VPCs tra tali account per creare una rete di condivisione di file. Puoi anche utilizzare una connessione peering VPC per consentire ad altri di accedere VPCs alle risorse che hai in uno dei tuoi VPCs

Quando si stabiliscono relazioni di peering tra VPCs AWS regioni diverse, le risorse nelle diverse AWS regioni VPCs (ad esempio, EC2 istanze e funzioni Lambda) 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 dell'indirizzo IP privato. Tutto il traffico interregionale viene crittografato prima di lasciare le AWS strutture senza alcun punto di errore o collo 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 S. DDo Il peering VPC tra Regioni fornisce un modo semplice ed economico di condividere le risorse tra le Regioni o di 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 in una zona di disponibilità sono gratuiti, anche se tra diversi account. Si applicano costi per il trasferimento di dati tramite connessioni peering VPC tra più zone di disponibilità e regioni. Per ulteriori informazioni, consulta [Amazon EC2 Pricing Amazon EC2 Pricing](#) .

Come funzionano le connessioni peering VPC

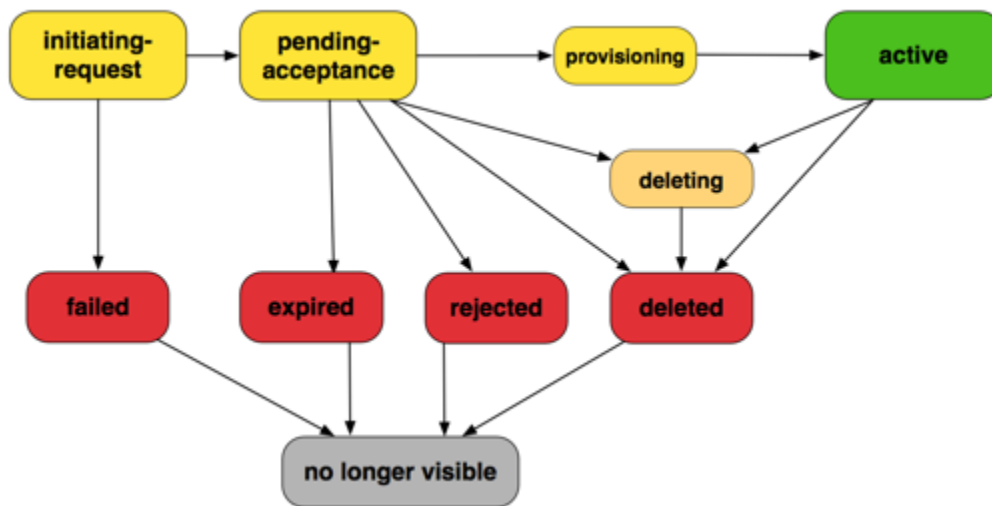
I passaggi seguenti descrivono il processo di peering VPC:

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 tua o di un altro account AWS 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 assicurarti che il traffico da e verso il VPC in peering non sia limitato. Se entrambi i VPC sono nella stessa Regione, puoi fare riferimento a un gruppo di sicurezza del VPC in peering come origine o destinazione delle regole in ingresso o in uscita nel gruppo di sicurezza.
5. Con le opzioni di connessione peering VPC predefinite, se le istanze EC2 su entrambi i lati di un indirizzo di connessione peering VPC comunicano tra loro utilizzando un nome host DNS pubblico, il nome host si risolve nell'indirizzo IP pubblico dell'istanza. Per modificare questo comportamento, abilita la risoluzione del nome host DNS per la tua connessione VPC. Dopo l'abilitazione della risoluzione del nome host DNS, se le istanze EC2 su entrambi i lati della connessione peering VPC comunicano tra loro utilizzando un nome host DNS pubblico, il nome host si risolve nell'indirizzo IP privato dell'istanza EC2.

Per ulteriori informazioni, consulta [Connessioni in peering di VPC](#).

Ciclo di vita delle connessioni peering VPC

Una connessione peering VPC è soggetta a varie fasi dal momento in cui 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 nello stesso account AWS, la richiesta rifiutata rimarrà visibile per 2 ore.
- **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

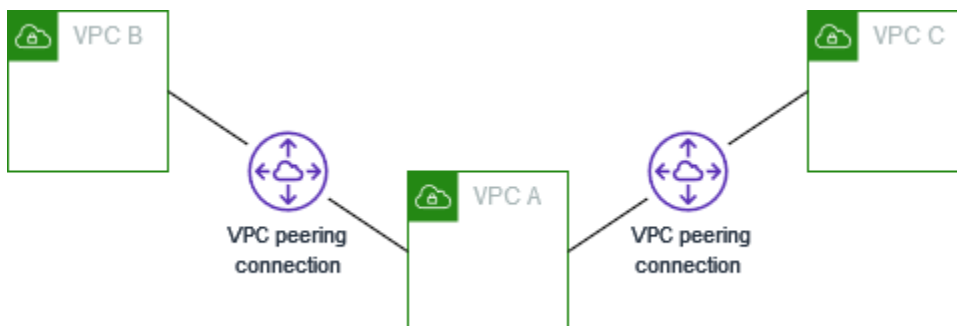
Se un evento in una Regione in cui si trova un VPC impedisce il flusso di traffico, lo stato della connessione peering VPC rimane Active.

- **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 nello stesso account AWS, la richiesta eliminata rimarrà 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 ulteriori informazioni, consulta [Example transit gateway scenarios](#) in Gateway di transito di Amazon VPC.

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 connessione Direct Connect a una rete aziendale, le risorse in VPC B non possono utilizzare la connessione Direct Connect 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

- Per i jumbo frame, l'unità di trasmissione massima (MTU) tra le connessioni peering VPC all'interno della stessa regione è di 9.001 byte. L'MTU per le connessioni peering VPC interregionali è di 8.500 byte. Per ulteriori informazioni sui jumbo frame, consulta [Jumbo frame \(9001 MTU\)](#) nella Guida per l'utente di Amazon EC2.
- 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.

Connessioni in peering di VPC

Il peering VPC consente di connettere due VPC nella stessa Regione AWS o in Regioni diverse. Ciò consente alle istanze di un VPC di comunicare con le istanze dell'altro VPC come se si trovassero nella stessa rete.

Un peering VPC crea un instradamento di rete diretto tra i due VPC utilizzando indirizzi IPv4 o IPv6 privati. Il traffico inviato tra i VPC connessi non attraversa Internet, una connessione VPN o una connessione AWS Direct Connect. Ciò rende il peering VPC un modo sicuro per condividere risorse, come database o server Web, oltre i confini del VPC.

Per stabilire una connessione peering VPC, devi creare una richiesta di connessione peering da un VPC e il proprietario dell'altro VPC deve accettare la richiesta. Una volta stabilita la connessione, puoi aggiornare le tabelle di routing per indirizzare il traffico tra i VPC. Ciò consente alle istanze di un VPC di accedere alle risorse dell'altro VPC.

Il peering VPC è uno strumento importante per la creazione di architetture multi-VPC e la condivisione di risorse oltre i confini organizzativi in AWS. Fornisce un modo semplice e a bassa latenza per connettere i VPC senza la complessità della configurazione di un VPN o di altri servizi di rete.

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

Attività

- [Creazione di una connessione peering VPC](#)
- [Accetta o rifiuta una connessione 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](#)
- [Abilitazione della risoluzione DNS per una 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. Per attivare la richiesta, il proprietario del VPC accettante deve accettare la richiesta. Sono supportate le seguenti connessioni peering:

- Tra VPC nello stesso account e nella stessa regione
- Tra VPC nello stesso account e in regioni differenti
- Tra VPC in account differenti e nella stessa regione
- Tra VPC in account e regioni differenti

Per una connessione peering VPC interregionale, la richiesta deve essere effettuata dalla regione del VPC richiedente e deve essere accettata dalla regione del VPC accettante. Per ulteriori informazioni, consulta [the section called “Accetta o rifiuta”](#).

Attività

- [Prerequisiti](#)
- [Crea una connessione peering tramite la console](#)
- [Creare una connessione peering tramite la riga di comando](#)

Prerequisiti

- Controlla le [limitazioni](#) per le 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.

Crea una connessione peering tramite la console

Utilizza la seguente procedura per creare una connessione peering VPC.

Creare una connessione peering tramite la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione, seleziona Connessioni peering.

3. Scegli **Create peering connection** (Crea connessione peering).
4. (Facoltativo) In **Nome**, indica un nome per la connessione peering VPC. In questo modo viene creato un tag con una chiave di **Name** e il valore specificato.
5. In **ID VPC (Richiedente)**, seleziona un VPC dall'account corrente.
6. In **Seleziona un altro VPC con cui effettuare il peering**, procedi come segue:
 - a. In **Account**, per effettuare il peering con un VPC in un altro account seleziona **Altro account** e inserisci l'ID dell'account. Altrimenti, mantieni l'Account personale.
 - b. In **Regione**, per effettuare il peering con un VPC in un'altra regione seleziona **Altra regione** e scegli la regione. Altrimenti, mantieni la Regione corrente.
 - c. In **ID VPC (Accettante)**, seleziona un VPC dall'account e dalla regione indicati.
7. (Facoltativo) Per aggiungere un tag, scegli **Add new tag** (Aggiungi nuovo tag) e inserisci la chiave e il valore del tag.
8. Scegli **Create peering connection** (Crea connessione peering).
9. Il proprietario dell'account accettante deve accettare la connessione peering. Per ulteriori informazioni, consulta [the section called "Accetta o rifiuta"](#).
10. Aggiorna le tabelle di routing per entrambi i VPC per consentire la comunicazione tra di loro. Per ulteriori informazioni, consulta [the section called "Aggiorna le tabelle di routing"](#).

Creare una connessione peering 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)

Accetta o rifiuta 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. Per creare una connessione peering VPC tra diversi VPC nello stesso account AWS, potrai creare e accettare personalmente la richiesta.

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](#).

 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 [Accetta o rifiuta una connessione peering VPC](#). Puoi anche ignorare la richiesta e lasciarla scadere. Per impostazione predefinita, la richiesta scade dopo 7 giorni.

Accettare o rifiutare una connessione peering tramite la console

1. Apri la 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 riquadro di navigazione, seleziona Connessioni peering.
4. Per rifiutare una connessione peering, seleziona la connessione peering VPC e scegli Operazioni, Rifiuta richiesta. Quando viene chiesta la conferma, seleziona Rifiuta richiesta.
5. Per accettare una connessione peering, 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](#).

Se non è presente una connessione peering VPC in sospeso, verifica di aver selezionato la regione del VPC accettante.

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](#).

Accettare una connessione peering tramite la riga di comando

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

Rifiutare una connessione peering tramite la riga di comando

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

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	<i>VPC A CIDR</i>	Locale
	<i>VPC B CIDR</i>	pcx- <i>11112222</i>
VPC B	<i>VPC B CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx- <i>11112222</i>

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 connessioni peering VPC comuni](#).

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 riquadro di navigazione, seleziona 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. Scegli Save changes (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 riquadro di navigazione, seleziona 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. Scegli Save changes (Salva modifiche).

Per ulteriori informazioni, consulta le [tabelle di routing](#) nella Guida per l'utente di Amazon VPC.

Aggiungere o sostituire una route tramite la riga di comando

- [create-route](#) e [replace-route](#)(AWS CLI)
- [New-EC2Route](#) e [Set-EC2Route](#)(AWS Tools for Windows PowerShell)

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.

Note

I gruppi di sicurezza in un VPC in peering non sono visualizzati nella console e possono essere selezionati dall'utente.

Requisiti

- Per fare riferimento a un gruppo di sicurezza in un VPC in peering, lo stato della connessione peering VPC deve Essere *active*.
- 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 che si trova in un altro account AWS ma nella stessa Regione, includi il numero di account con l'ID del gruppo di sicurezza. 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.
- 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. Nel pannello di navigazione, seleziona Gruppi di sicurezza.
3. Seleziona il gruppo di sicurezza ed esegui una delle seguenti operazioni:
 - Per modificare le regole in entrata, scegli Operazioni, Modifica regole in entrata.
 - Per modificare le regole in uscita, scegli Operazioni, Modifica regole in uscita.
4. Per aggiungere una regola, scegli Aggiungi regola e specifica il tipo, il protocollo e l'intervallo di porte. Per Origine (regole in entrata) o Destinazione (regole in uscita), effettua una delle seguenti operazioni:
 - Per un VPC in peering nello stesso account e nella stessa Regione, inserisci l'ID del gruppo di sicurezza.
 - Per un VPC in peering in un account diverso ma nella stessa Regione, inserisci l'ID dell'account e l'ID del gruppo di sicurezza, separati da una barra (ad esempio, 123456789012/sg-1a2b3c4d).
 - Per un VPC in peering in un'altra regione, inserisci il blocco CIDR del VPC in peering.
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 Salva regole.

Per aggiornare le regole in entrata tramite la riga di comando

- [authorize-security-group-ingress](#) e [revoke-security-group-ingress](#) (AWS CLI)
- [Grant-EC2SecurityGroupIngress](#) e [Revoke-EC2SecurityGroupIngress](#) (AWS Tools for Windows PowerShell)

Ad esempio, per aggiornare il gruppo di sicurezza sg-aaaa1111 allo scopo di consentire l'accesso in entrata su HTTP da sg-bbbb2222 per un VPC in peering, utilizza il seguente comando. Se il VPC in peering si trova nella stessa Regione ma ha un account diverso, aggiungi `--group-owner aws-account-id`.

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

Per aggiornare le regole in uscita tramite la riga di comando

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

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)

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.

Visualizzazione ed eliminazione di regole del gruppo di sicurezza

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).

Descrivere regole di un gruppo di sicurezza obsolete tramite la riga di comando

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

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](#).

Abilitazione della risoluzione DNS per una connessione peering VPC

Le impostazioni DNS per una connessione peering VPC determinano in che modo vengono risolti i nomi host DNS pubblici per le richieste che attraversano la connessione peering VPC. Se un'istanza EC2 da un lato di una connessione peering VPC invia una richiesta a un'istanza EC2 dall'altro lato utilizzando il nome host DNS IPv4 pubblico dell'istanza, il nome host DNS viene risolto come indicato di seguito.

Risoluzione DNS disabilitata (impostazione predefinita)

Il nome host DNS IPv4 pubblico si risolve nell'indirizzo IPv4 pubblico dell'istanza.

Risoluzione DNS abilitata

Il nome host DNS IPv4 pubblico si risolve nell'indirizzo IPv4 privato dell'istanza.

Requisiti

- Entrambi i VPC devono essere abilitati per i nomi host DNS e la risoluzione DNS. Per ulteriori informazioni, consulta [Attributi DNS per il VPC](#) nella Guida per l'utente di Amazon VPC.
- La connessione peering deve essere nello stato `active`. Non è possibile abilitare la risoluzione DNS quando si crea una connessione peering.
- Il proprietario del VPC richiedente deve modificarne le opzioni di peering, mentre il proprietario del VPC accettante deve, a sua volta, modificarne le opzioni di peering. Se i VPC sono nello stesso account, potrai abilitare contemporaneamente la risoluzione DNS per il VPC richiedente e per il VPC accettante. Questo metodo funziona sia con le connessioni peering VPC nella stessa regione che per quelle interregionali.

Abilitare la risoluzione DNS per una connessione peering tramite la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione, seleziona Connessioni peering.
3. Seleziona la connessione peering VPC.
4. Seleziona Operazioni, Modifica impostazioni DNS.
5. Per abilitare la risoluzione DNS per le richieste ricevute dal VPC richiedente, seleziona Risoluzione DNS richiedente, Consenti al VPC accettante di risolvere il DNS del VPC richiedente.
6. Per garantire la risoluzione DNS per le richieste ricevute dal VPC accettante, seleziona Risoluzione DNS accettante, Consenti al VPC richiedente di risolvere il DNS del VPC accettante.
7. Scegli Save changes (Salva modifiche).

Abilitare la risoluzione DNS tramite la riga di comando

- [modify-vpc-peering-connection-options](#) (AWS CLI)

- [Edit-EC2VpcPeeringConnectionOption](#) (AWS Tools for Windows PowerShell)

Descrivere le opzioni di una connessione peering VPC tramite la riga di comando

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

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 riquadro di navigazione, seleziona 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.

Eliminare una connessione peering VPC tramite la riga di comando

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

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. Ciò garantisce che il traffico di rete possa fluire correttamente tra i due VPC. Per ulteriori informazioni, consulta [Aggiorna le tabelle di routing](#).
- Per le istanze EC2 coinvolte, verifica che i gruppi di sicurezza per queste istanze consentano il traffico in entrata e in uscita dal VPC in peering. Le regole dei gruppi di sicurezza controllano il traffico autorizzato ad accedere alle istanze EC2. Per ulteriori informazioni, consulta [Gruppi di sicurezza peer di riferimento](#).
- Verifica che gli ACL di rete per le sottoreti contenenti le tue risorse consentano il traffico necessario dal VPC in peering. Gli ACL di rete sono un ulteriore livello di sicurezza che filtra il traffico a livello di sottorete.

Se i problemi persistono, puoi utilizzare Reachability Analyzer. Reachability Analyzer può aiutare a identificare il componente specifico, che si tratti di una tabella di routing, un gruppo di sicurezza o un ACL di rete, che sta causando il problema di connettività tra i due VPC. Per ulteriori informazioni, consulta la [Guida di Reachability Analyzer](#).

Una verifica approfondita delle configurazioni di rete VPC è fondamentale per la risoluzione dei problemi di connessione peering VPC che potresti riscontrare.

Configurazioni di connessioni peering VPC comuni

Questa sezione descrive due tipi comuni di configurazioni di peering VPC che è possibile implementare:

- Configurazioni di peering VPC con percorsi verso un intero VPC: in questa configurazione, crei un percorso nella tabella di routing di ciascun VPC per inviare tutto il traffico destinato al VPC in peering alla connessione peering VPC. Ciò consente a una risorsa in un VPC di comunicare con una risorsa nel VPC in peering, semplificando la gestione. Tuttavia, ciò significa anche che tutto il traffico intercorrente VPCs fluirà attraverso la connessione peering, il che potrebbe diventare un collo di bottiglia se il volume di traffico è elevato.
- Configurazioni di peering VPC con percorsi specifici: in alternativa, puoi creare percorsi più granulari nella tabella di routing di ogni VPC per inviare il traffico solo a sottoreti o risorse specifiche nel VPC in peering. Ciò consente di limitare il traffico che fluisce attraverso la connessione peering solo a ciò che è necessario, il che può essere più efficiente. Tuttavia, richiede anche una maggiore manutenzione, poiché dovrai aggiornare le tabelle di routing ogni volta che aggiungi nuove risorse nel VPC in peering che deve comunicare.

L'approccio migliore dipende da fattori come le dimensioni e la complessità dell'architettura VPC, il volume di traffico previsto tra le due e le VPCs esigenze organizzative in materia di sicurezza e accesso alle risorse. Molte aziende utilizzano un approccio ibrido, con percorsi ampi per modelli di traffico comuni e percorsi specifici per casi d'uso più sensibili o che richiedono un uso intensivo della larghezza di banda.

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 tabelle 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 rete di connessione peering VPC](#). Per ulteriori informazioni sulla creazione e sull'utilizzo di connessioni peering VPC, consulta [Connessioni in peering di VPC](#).

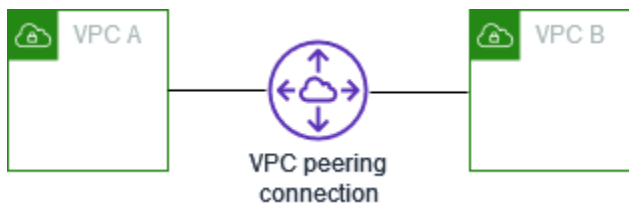
Per ulteriori informazioni sull'aggiornamento delle tabelle di routing, consulta [Aggiornamento delle tabelle di routing per una connessione peering VPC](#).

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	<i>VPC A CIDR</i>	Locale
	<i>VPC B CIDR</i>	pcx-11112222
VPC B	<i>VPC B CIDR</i>	Locale
	<i>VPC A CIDR</i>	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	<i>CIDR 1 VPC A</i>	Locale
	<i>CIDR 2 VPC A</i>	Locale
	<i>CIDR 1 VPC B</i>	pcx-11112222
	<i>CIDR 2 VPC B</i>	pcx-11112222
VPC B	<i>CIDR 1 VPC B</i>	Locale
	<i>CIDR 2 VPC B</i>	Locale
	<i>CIDR 1 VPC A</i>	pcx-11112222
	<i>CIDR 2 VPC A</i>	pcx-11112222

CIDR VPC IPv4 e IPv6

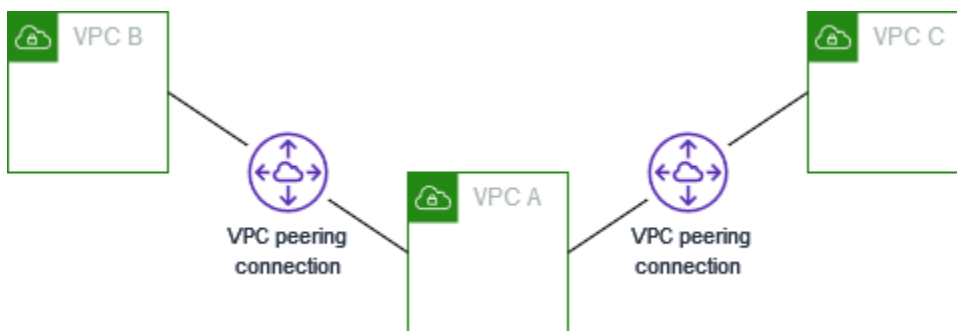
Se VPC A e VPC B hanno più blocchi CIDR IPv6 associati, puoi aggiornare la tabella di instradamento per ogni VPC con gli instradamenti per i blocchi CIDR IPv4 e IPv6 del VPC peer.

Tabella di routing	Destinazione	Target
VPC A	<i>CIDR IPv4 de1 VPC A</i>	Locale
	<i>CIDR IPv6 de1 VPC A</i>	Locale
	<i>CIDR IPv4 de1 VPC B</i>	pcx-11112222
	<i>CIDR IPv6 de1 VPC B</i>	pcx-11112222
VPC B	<i>CIDR IPv4 de1 VPC B</i>	Locale

Tabella di routing	Destinazione	Target
	<i>CIDR IPv6 deI VPC B</i>	Locale
	<i>CIDR IPv4 deI VPC A</i>	pcx-11112222
	<i>CIDR IPv6 deI VPC A</i>	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”](#).

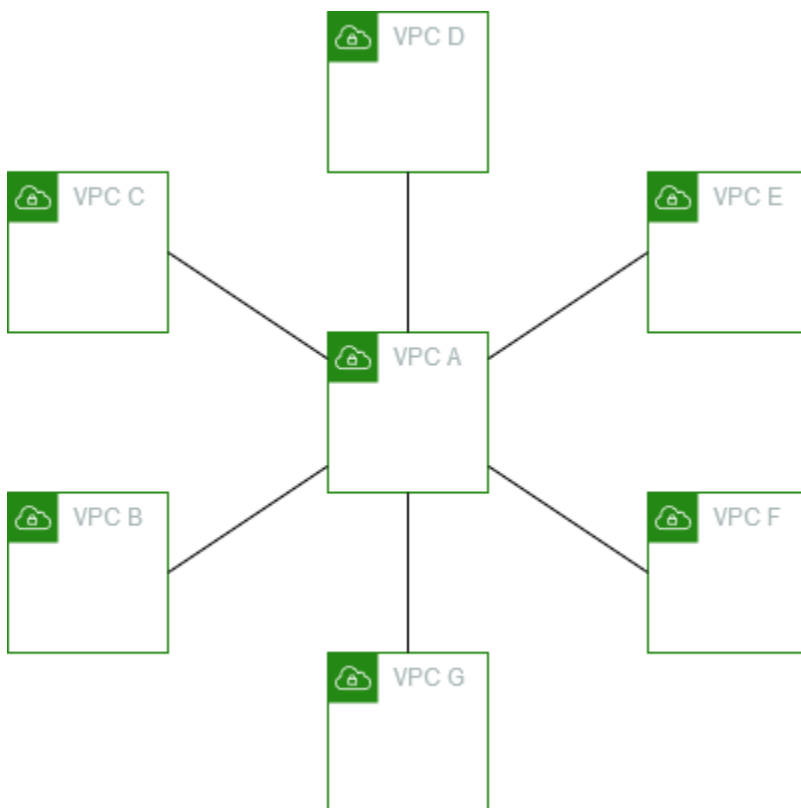
Utilizza questa configurazione quando disponi di risorse su un VPC centrale, come un repository di servizi, a cui devono accedere altri VPC. Gli altri VPC non hanno bisogno di accedere alle risorse degli altri, ma solo a quelle del VPC centrale.

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	<i>VPC A CIDR</i>	Locale

Tabella di routing	Destinazione	Target
	<i>VPC B CIDR</i>	pcx-12121212
	<i>VPC C CIDR</i>	pcx-23232323
VPC B	<i>VPC B CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx-12121212
VPC C	<i>VPC C CIDR</i>	Locale
	<i>VPC A CIDR</i>	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.

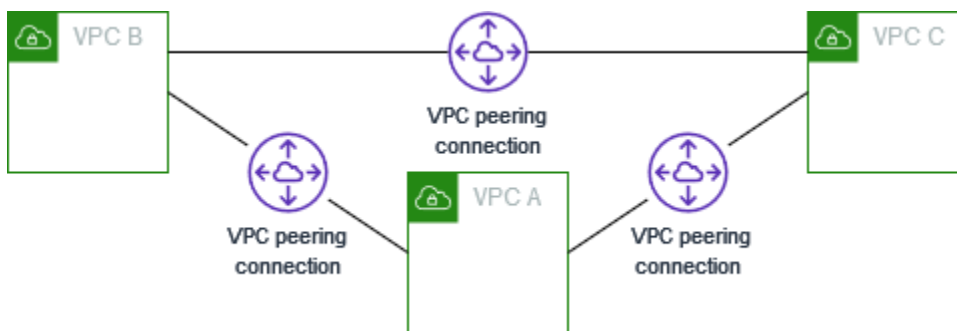
Tabella di routing	Destinazione	Target
VPC A	<i>CIDR IPv4 del VPC A</i>	Locale
	<i>CIDR IPv6 del VPC A</i>	Locale
	<i>CIDR IPv4 del VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv6 del VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv4 del VPC C</i>	pcx-aaaacccc
	<i>CIDR IPv6 del VPC C</i>	pcx-aaaacccc
	<i>CIDR IPv4 del VPC D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

Tabella di routing	Destinazione	Target
VPC D	<i>CIDR IPv4 deI VPC A</i>	pcx-aaaacccc
	<i>CIDR IPv6 deI VPC A</i>	pcx-aaaacccc
	<i>CIDR IPv4 deI VPC D</i>	Locale
	<i>CIDR IPv6 deI VPC D</i>	Locale
VPC E	<i>CIDR IPv4 deI VPC A</i>	pcx-aaaadddd
	<i>CIDR IPv6 deI VPC A</i>	pcx-aaaadddd
	<i>CIDR IPv4 deI VPC E</i>	Locale
	<i>CIDR IPv6 deI VPC E</i>	Locale
VPC F	<i>CIDR IPv4 deI VPC A</i>	pcx-aaaaeeee
	<i>CIDR IPv6 deI VPC A</i>	pcx-aaaaeeee
	<i>CIDR IPv4 deI VPC F</i>	Locale
	<i>CIDR IPv6 deI VPC F</i>	Locale
VPC G	<i>CIDR IPv4 deI VPC A</i>	pcx-aaaaffff
	<i>CIDR IPv6 deI VPC A</i>	pcx-aaaaffff
	<i>CIDR IPv4 deI VPC G</i>	Locale
	<i>CIDR IPv6 deI VPC G</i>	Locale
	<i>CIDR IPv4 deI VPC A</i>	pcx-aaaagggg
	<i>CIDR IPv6 deI VPC A</i>	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	<i>VPC A CIDR</i>	Locale
	<i>VPC B CIDR</i>	pcx-aaaabbbb
	<i>VPC C CIDR</i>	pcx-aaaacccc
VPC B	<i>VPC B CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaabbbb
	<i>VPC C CIDR</i>	pcx-bbbbcccc

Tabella di routing	Destinazione	Target
VPC C	<i>VPC C CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaacccc
	<i>VPC B CIDR</i>	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	<i>CIDR IPv4 del VPC A</i>	Locale
	<i>CIDR IPv6 del VPC A</i>	Locale
	<i>CIDR IPv4 del VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv6 del VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv4 del VPC C</i>	pcx-aaaacccc
VPC B	<i>CIDR IPv4 del VPC B</i>	Locale
	<i>CIDR IPv6 del VPC B</i>	Locale
	<i>CIDR IPv4 del VPC A</i>	pcx-aaaabbbb
	<i>CIDR IPv6 del VPC A</i>	pcx-aaaabbbb
	<i>CIDR IPv4 del VPC C</i>	pcx-bbbbcccc
VPC C	<i>CIDR IPv4 del VPC C</i>	Locale
	<i>CIDR IPv4 del VPC A</i>	pcx-aaaacccc
	<i>CIDR IPv4 del VPC B</i>	pcx-bbbbcccc

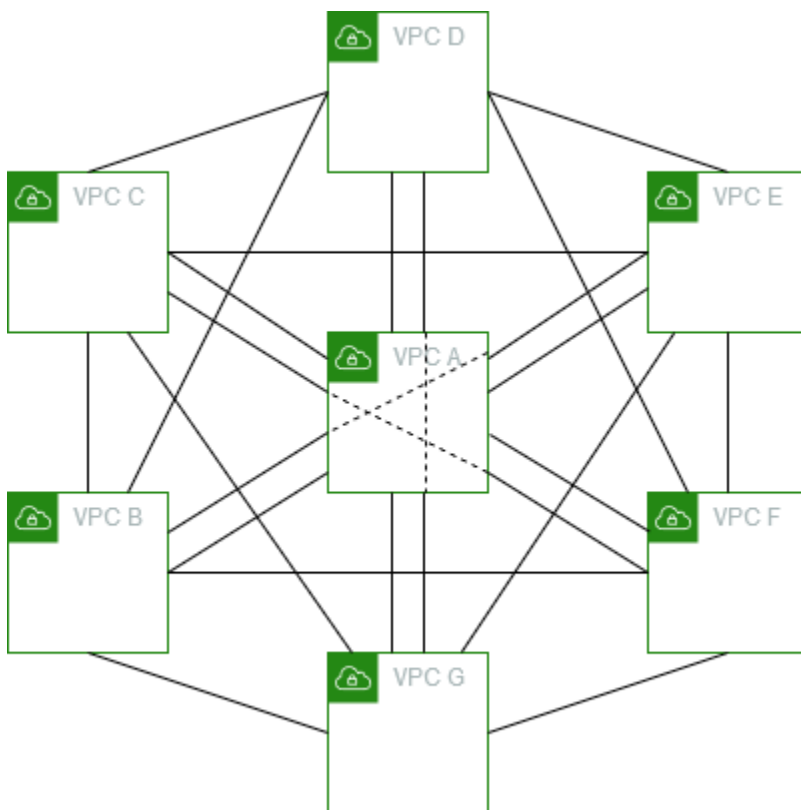
Molteplici VPC collegati in peering tra loro

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
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

VPC	VPC	Connessione di peering di VPC
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	<i>VPC A CIDR</i>	Locale
	<i>VPC B CIDR</i>	pcx-aaaabbbb

Tabella di routing	Destinazione	Target
	<i>VPC C CIDR</i>	pcx-aaaacccc
	<i>CIDR VPC D</i>	pcx-aaaadddd
	<i>CIDR VPC E</i>	pcx-aaaaeeee
	<i>CIDR VPC F</i>	pcx-aaaaffff
	<i>CIDR VPC G</i>	pcx-aaaagggg
VPC B	<i>VPC B CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaabbbb
	<i>VPC C CIDR</i>	pcx-bbbbcccc
	<i>CIDR VPC D</i>	pcx-bbbbdddd
	<i>CIDR VPC E</i>	pcx-bbbbeeee
	<i>CIDR VPC F</i>	pcx-bbbbffff
	<i>CIDR VPC G</i>	pcx-bbbbgggg
VPC C	<i>VPC C CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaacccc
	<i>VPC B CIDR</i>	pcx-bbbbcccc
	<i>CIDR VPC D</i>	pcx-ccccdddd
	<i>CIDR VPC E</i>	pcx-cccceeee
	<i>CIDR VPC F</i>	pcx-ccccffff
	<i>CIDR VPC G</i>	pcx-ccccgggg
VPC D	<i>CIDR VPC D</i>	Locale

Tabella di routing	Destinazione	Target
	<i>VPC A CIDR</i>	pcx-aaaadddd
	<i>VPC B CIDR</i>	pcx-bbbbddd
	<i>VPC C CIDR</i>	pcx-ccccddd
	<i>CIDR VPC E</i>	pcx-ddddeeee
	<i>CIDR VPC F</i>	pcx-ddddffff
	<i>CIDR VPC G</i>	pcx-ddddgggg
VPC E	<i>CIDR VPC E</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaaeeee
	<i>VPC B CIDR</i>	pcx-bbbbeeee
	<i>VPC C CIDR</i>	pcx-cccceeee
	<i>CIDR VPC D</i>	pcx-ddddeeee
	<i>CIDR VPC F</i>	pcx-eeeeffff
VPC F	<i>CIDR VPC G</i>	pcx-eeeegggg
	<i>CIDR VPC F</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaaffff
	<i>VPC B CIDR</i>	pcx-bbbbffff
	<i>VPC C CIDR</i>	pcx-ccccffff
	<i>CIDR VPC D</i>	pcx-ddddffff
	<i>CIDR VPC E</i>	pcx-eeeeffff
<i>CIDR VPC G</i>	pcx-ffffgggg	

Tabella di routing	Destinazione	Target
VPC G	<i>CIDR VPC G</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaagggg
	<i>VPC B CIDR</i>	pcx-bbbbgggg
	<i>VPC C CIDR</i>	pcx-ccccgggg
	<i>CIDR VPC D</i>	pcx-ddddgggg
	<i>CIDR VPC E</i>	pcx-eeeegggg
	<i>CIDR VPC F</i>	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	<i>CIDR IPv4 del VPC A</i>	Locale
	<i>CIDR IPv6 del VPC A</i>	Locale
	<i>CIDR IPv4 del VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv6 del VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv4 del VPC C</i>	pcx-aaaacccc
	<i>CIDR IPv6 del VPC C</i>	pcx-aaaacccc
	<i>CIDR IPv4 del VPC D</i>	pcx-aaaadddd
	<i>CIDR IPv6 del VPC D</i>	pcx-aaaadddd
	<i>CIDR IPv4 del VPC E</i>	pcx-aaaaeeee
	<i>CIDR IPv6 del VPC E</i>	pcx-aaaaeeee

Tabella di routing	Destinazione	Target
	<i>CIDR IPv4 deI VPC F</i>	pcx-aaaaffff
	<i>CIDR IPv6 deI VPC F</i>	pcx-aaaaffff
	<i>CIDR IPv4 deI VPC G</i>	pcx-aaaagggg
	<i>CIDR IPv6 deI VPC G</i>	pcx-aaaagggg
VPC B	<i>CIDR IPv4 deI VPC B</i>	Locale
	<i>CIDR IPv6 deI VPC B</i>	Locale
	<i>CIDR IPv4 deI VPC A</i>	pcx-aaaabbbb
	<i>CIDR IPv6 deI VPC A</i>	pcx-aaaabbbb
	<i>CIDR IPv4 deI VPC C</i>	pcx-bbbbcccc
	<i>CIDR IPv6 deI VPC C</i>	pcx-bbbbcccc
	<i>CIDR IPv4 deI VPC D</i>	pcx-bbbbdddd
	<i>CIDR IPv6 deI VPC D</i>	pcx-bbbbdddd
	<i>CIDR IPv4 deI VPC E</i>	pcx-bbbbeeee
	<i>CIDR IPv6 deI VPC E</i>	pcx-bbbbeeee
	<i>CIDR IPv4 deI VPC F</i>	pcx-bbbbffff
	<i>CIDR IPv6 deI VPC F</i>	pcx-bbbbffff
	<i>CIDR IPv4 deI VPC G</i>	pcx-bbbbgggg
	<i>CIDR IPv6 deI VPC G</i>	pcx-bbbbgggg
VPC C	<i>CIDR IPv4 deI VPC C</i>	Locale
	<i>CIDR IPv6 deI VPC C</i>	Locale

Tabella di routing	Destinazione	Target
	<i>CIDR IPv4 deI VPC A</i>	pcx-aaaacccc
	<i>CIDR IPv6 deI VPC A</i>	pcx-aaaacccc
	<i>CIDR IPv4 deI VPC B</i>	pcx-bbbbcccc
	<i>CIDR IPv6 deI VPC B</i>	pcx-bbbbcccc
	<i>CIDR IPv4 deI VPC D</i>	pcx-ccccdddd
	<i>CIDR IPv6 deI VPC D</i>	pcx-ccccdddd
	<i>CIDR IPv4 deI VPC E</i>	pcx-cccceeee
	<i>CIDR IPv6 deI VPC E</i>	pcx-cccceeee
	<i>CIDR IPv4 deI VPC F</i>	pcx-ccccffff
	<i>CIDR IPv6 deI VPC F</i>	pcx-ccccffff
	<i>CIDR IPv4 deI VPC G</i>	pcx-ccccgggg
	<i>CIDR IPv6 deI VPC G</i>	pcx-ccccgggg
VPC D	<i>CIDR IPv4 deI VPC D</i>	Locale
	<i>CIDR IPv6 deI VPC D</i>	Locale
	<i>CIDR IPv4 deI VPC A</i>	pcx-aaaadddd
	<i>CIDR IPv6 deI VPC A</i>	pcx-aaaadddd
	<i>CIDR IPv4 deI VPC B</i>	pcx-bbbbdddd
	<i>CIDR IPv6 deI VPC B</i>	pcx-bbbbdddd
	<i>CIDR IPv4 deI VPC C</i>	pcx-ccccdddd
	<i>CIDR IPv6 deI VPC C</i>	pcx-ccccdddd

Tabella di routing	Destinazione	Target
	<i>CIDR IPv4 deI VPC E</i>	pcx-ddddeeee
	<i>CIDR IPv6 deI VPC E</i>	pcx-ddddeeee
	<i>CIDR IPv4 deI VPC F</i>	pcx-ddddffff
	<i>CIDR IPv6 deI VPC F</i>	pcx-ddddffff
	<i>CIDR IPv4 deI VPC G</i>	pcx-ddddgggg
	<i>CIDR IPv6 deI VPC G</i>	pcx-ddddgggg
VPC E	<i>CIDR IPv4 deI VPC E</i>	Locale
	<i>CIDR IPv6 deI VPC E</i>	Locale
	<i>CIDR IPv4 deI VPC A</i>	pcx-aaaaeeee
	<i>CIDR IPv6 deI VPC A</i>	pcx-aaaaeeee
	<i>CIDR IPv4 deI VPC B</i>	pcx-bbbbeeee
	<i>CIDR IPv6 deI VPC B</i>	pcx-bbbbeeee
	<i>CIDR IPv4 deI VPC C</i>	pcx-cccceeee
	<i>CIDR IPv6 deI VPC C</i>	pcx-cccceeee
	<i>CIDR IPv4 deI VPC D</i>	pcx-ddddeeee
	<i>CIDR IPv6 deI VPC D</i>	pcx-ddddeeee
	<i>CIDR IPv4 deI VPC F</i>	pcx-eeeeffff
	<i>CIDR IPv6 deI VPC F</i>	pcx-eeeeffff
	<i>CIDR IPv4 deI VPC G</i>	pcx-eeeegggg
	<i>CIDR IPv6 deI VPC G</i>	pcx-eeeegggg

Tabella di routing	Destinazione	Target
VPC F	<i>CIDR IPv4 deI VPC F</i>	Locale
	<i>CIDR IPv6 deI VPC F</i>	Locale
	<i>CIDR IPv4 deI VPC A</i>	pcx-aaaaffff
	<i>CIDR IPv6 deI VPC A</i>	pcx-aaaaffff
	<i>CIDR IPv4 deI VPC B</i>	pcx-bbbbffff
	<i>CIDR IPv6 deI VPC B</i>	pcx-bbbbffff
	<i>CIDR IPv4 deI VPC C</i>	pcx-ccccffff
	<i>CIDR IPv6 deI VPC C</i>	pcx-ccccffff
	<i>CIDR IPv4 deI VPC D</i>	pcx-ddddffff
	<i>CIDR IPv6 deI VPC D</i>	pcx-ddddffff
	<i>CIDR IPv4 deI VPC E</i>	pcx-eeeeffff
	<i>CIDR IPv6 deI VPC E</i>	pcx-eeeeffff
	<i>CIDR IPv4 deI VPC G</i>	pcx-ffffgggg
	<i>CIDR IPv6 deI VPC G</i>	pcx-ffffgggg
VPC G	<i>CIDR IPv4 deI VPC G</i>	Locale
	<i>CIDR IPv6 deI VPC G</i>	Locale
	<i>CIDR IPv4 deI VPC A</i>	pcx-aaaagggg
	<i>CIDR IPv6 deI VPC A</i>	pcx-aaaagggg
	<i>CIDR IPv4 deI VPC B</i>	pcx-bbbbgggg
	<i>CIDR IPv6 deI VPC B</i>	pcx-bbbbgggg

Tabella di routing	Destinazione	Target
	<i>CIDR IPv4 deI VPC C</i>	pcx-ccccgggg
	<i>CIDR IPv6 deI VPC C</i>	pcx-ccccgggg
	<i>CIDR IPv4 deI VPC D</i>	pcx-ddddgggg
	<i>CIDR IPv6 deI VPC D</i>	pcx-ddddgggg
	<i>CIDR IPv4 deI VPC E</i>	pcx-eeeegggg
	<i>CIDR IPv6 deI VPC E</i>	pcx-eeeegggg
	<i>CIDR IPv4 deI VPC F</i>	pcx-ffffgggg
	<i>CIDR IPv6 deI VPC F</i>	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 collegato ad almeno due VPCs blocchi CIDR sovrapposti.

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

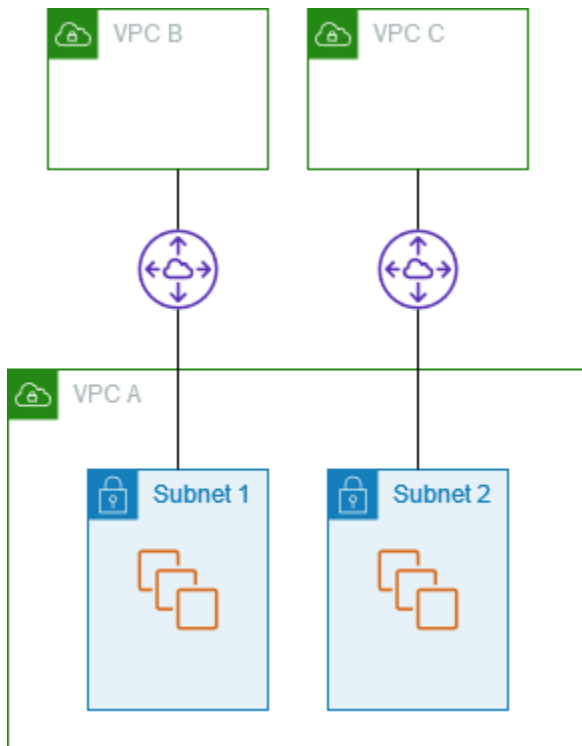
Configurazioni

- [Due VPCs che accedono a sottoreti specifiche in un VPC](#)
- [Due VPCs che accedono a blocchi CIDR specifici in un VPC](#)
- [Un VPC che accede a sottoreti specifiche in due VPCs](#)
- [Istanze in un VPC che accedono a istanze specifiche in due VPCs](#)
- [Un VPC che accede a due VPCs utilizzando le corrispondenze di prefisso più lunghe](#)

- [Configurazioni VPC multiple](#)

Due VPCs 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)	<i>VPC A CIDR</i>	Locale
	<i>VPC B CIDR</i>	pcx-aaaabbbb

Tabella di routing	Destinazione	Target
Sottorete 2 (VPC A)	<i>VPC A CIDR</i>	Locale
	<i>VPC C CIDR</i>	pcx-aaaacccc
VPC B	<i>VPC B CIDR</i>	Locale
	<i>Subnet 1 CIDR</i>	pcx-aaaabbbb
VPC C	<i>VPC C CIDR</i>	Locale
	<i>Subnet 2 CIDR</i>	pcx-aaaacccc

È possibile estendere questa configurazione a più blocchi CIDR. Supponiamo che VPC A e VPC B abbiano IPv4 entrambi i blocchi CIDR IPv6 e che la sottorete 1 abbia un blocco CIDR associato. IPv6 È possibile consentire a VPC B di comunicare con la sottorete 1 nel VPC A tramite IPv6 la connessione peering VPC. A tale scopo, aggiungi una route alla tabella di routing per VPC A con una destinazione del blocco IPv6 CIDR per VPC B e una route alla tabella di route per VPC B con una destinazione del IPv6 CIDR della sottorete 1 in VPC A.

Tabella di routing	Destinazione	Target	Note
Sottorete 1 in VPC A	<i>VPC A IPv4 CIDR</i>	Locale	
	<i>VPC A IPv6 CIDR</i>	Locale	Percorso locale che viene aggiunto automaticamente per la IPv6 comunicazione all'interno del VPC.
	<i>VPC B IPv4 CIDR</i>	pcx-aaaabbbb	
	<i>VPC B IPv6 CIDR</i>	pcx-aaaabbbb	Instradamento verso il blocco IPv6 CIDR di VPC B.

Tabella di routing	Destinazione	Target	Note
Sottorete 2 in VPC A	<i>VPC A IPv4 CIDR</i>	Locale	
	<i>VPC A IPv6 CIDR</i>	Locale	Percorso locale che viene aggiunto automaticamente per la IPv6 comunicazione all'interno del VPC.
	<i>VPC C IPv4 CIDR</i>	pcx-aaaacccc	
VPC B	<i>VPC B IPv4 CIDR</i>	Locale	
	<i>VPC B IPv6 CIDR</i>	Locale	Percorso locale che viene aggiunto automaticamente per la IPv6 comunicazione all'interno del VPC.
	<i>Subnet 1 IPv4 CIDR</i>	pcx-aaaabbbb	
	<i>Subnet 1 IPv6 CIDR</i>	pcx-aaaabbbb	Percorso verso il blocco IPv6 CIDR di VPC A.
VPC C	<i>VPC C IPv4 CIDR</i>	Locale	
	<i>Subnet 2 IPv4 CIDR</i>	pcx-aaaacccc	

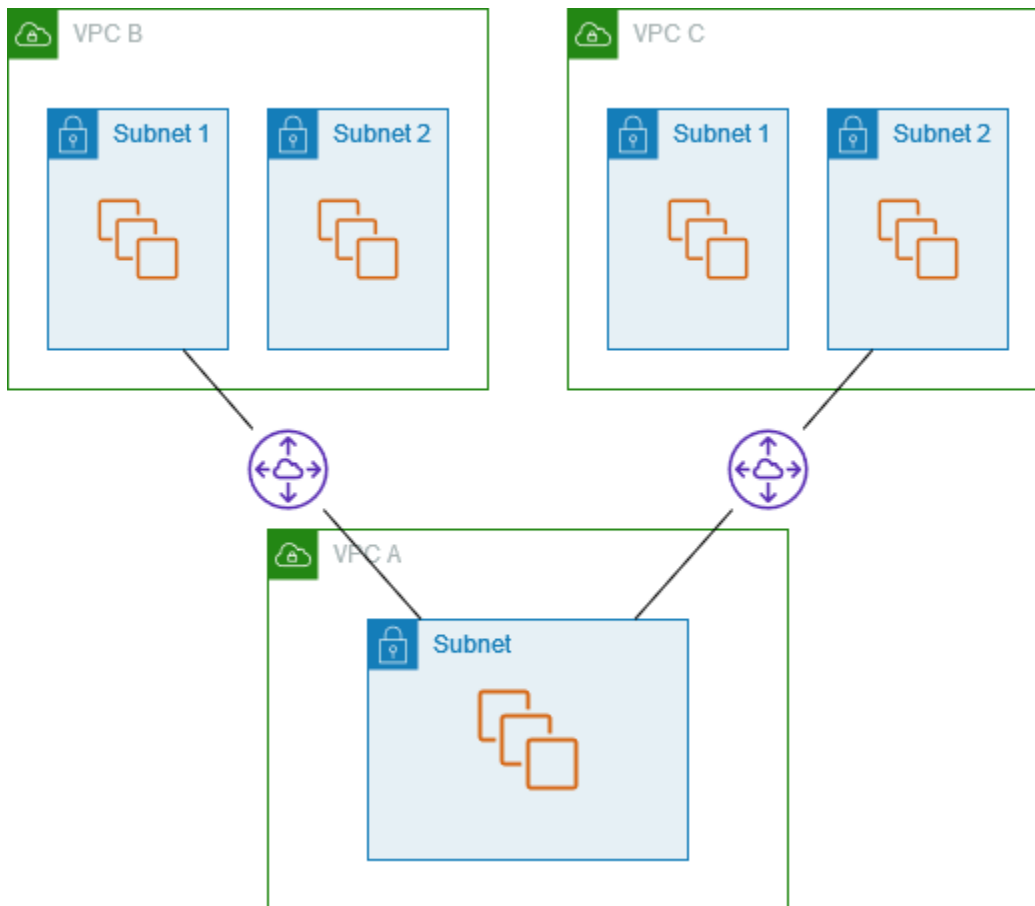
Due VPCs che accedono a blocchi CIDR specifici in un VPC

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	<i>VPC A CIDR 1</i>	Locale
	<i>VPC A CIDR 2</i>	Locale
	<i>VPC B CIDR</i>	pcx-aaaabbbb
	<i>VPC C CIDR</i>	pcx-aaaacccc
VPC B	<i>VPC B CIDR</i>	Locale
	<i>VPC A CIDR 1</i>	pcx-aaaabbbb
VPC C	<i>VPC C CIDR</i>	Locale
	<i>VPC A CIDR 2</i>	pcx-aaaacccc

Un VPC che accede a sottoreti specifiche in due VPCs

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.



Usa questa configurazione quando disponi di un VPC centrale con un unico set di risorse, come i servizi Active Directory, a cui altri VPCs devono accedere. Il VPC centrale non richiede l'accesso completo al VPC con VPCs cui è peering.

La tabella di routing per il VPC A utilizza le connessioni peering per accedere solo a sottoreti specifiche nel peered. VPCs 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	<i>VPC A CIDR</i>	Locale
	<i>Subnet 1 CIDR</i>	pcx-aaaabbbb
	<i>Subnet 2 CIDR</i>	pcx-aaaacccc
Sottorete 1 (VPC B)	<i>VPC B CIDR</i>	Locale

Tabella di routing	Destinazione	Target
	<i>Subnet in VPC A CIDR</i>	pcx-aaaabbbb
Sottorete 2 (VPC C)	<i>VPC C CIDR</i>	Locale
	<i>Subnet in VPC A CIDR</i>	pcx-aaaacccc

Routing per traffico di risposta

Se disponi di un VPC peering con più blocchi CIDR sovrapposti o corrispondenti, assicurati VPCs che le tabelle di routing siano configurate per evitare l'invio del traffico di risposta dal tuo VPC al VPC errato. AWS non 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.

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-aaaacccc.

Tabella di routing	Destinazione	Target
Sottorete 2 (VPC B)	<i>VPC B CIDR</i>	Locale
	<i>Subnet in VPC A CIDR</i>	pcx-aaaabbbb
VPC A	<i>VPC A CIDR</i>	Locale
	<i>VPC C CIDR</i>	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 2 in VPC B e con la sottorete 1 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'altra route per la sottorete specifica.

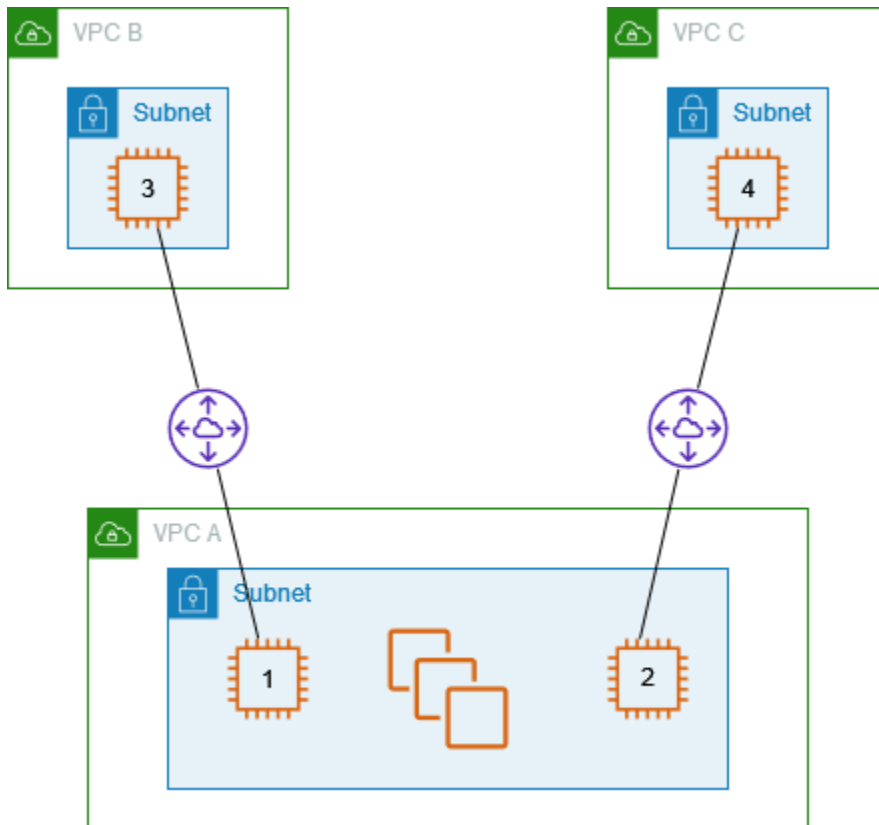
Destinazione	Target
<i>VPC A CIDR</i>	Locale
<i>Subnet 2 CIDR</i>	<code>pcx-aaaabbbb</code>
<i>Subnet 1 CIDR</i>	<code>pcx-aaaacccc</code>

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
<i>VPC A CIDR</i>	Locale
<i>Specific IP address in subnet 2</i>	<code>pcx-aaaabbbb</code>
<i>VPC B CIDR</i>	<code>pcx-aaaacccc</code>

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

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.



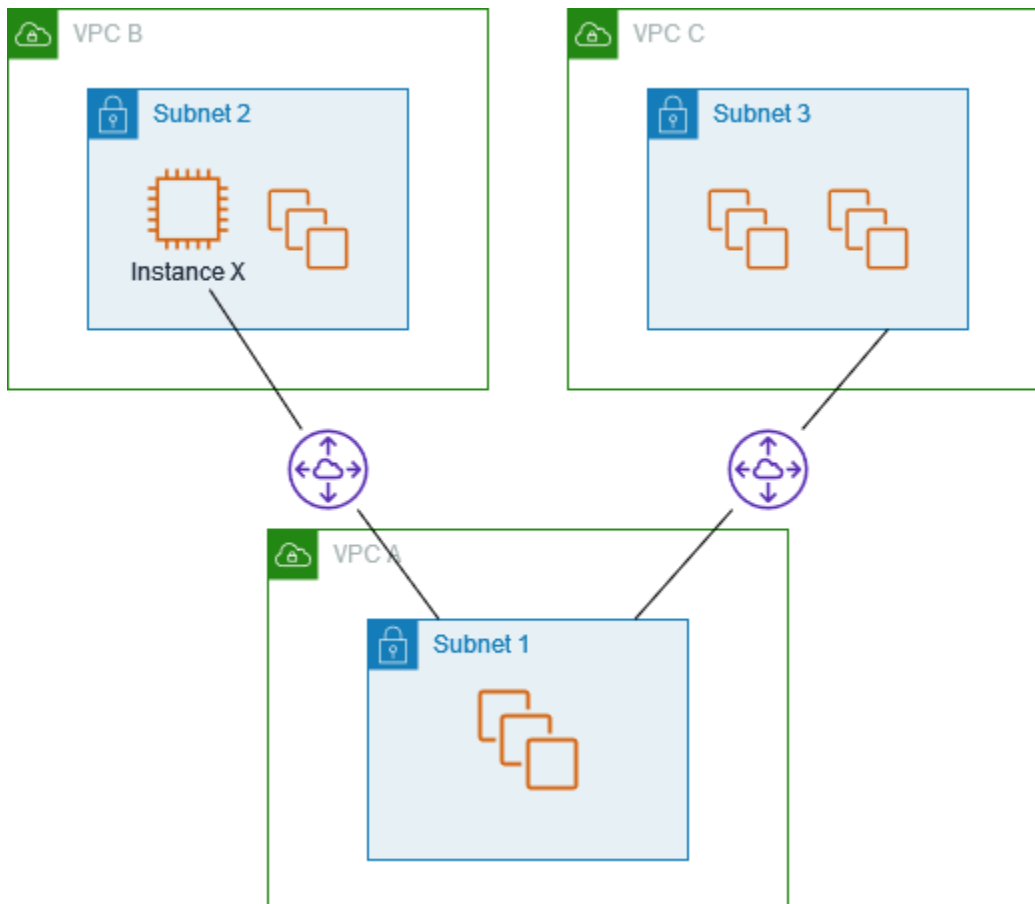
Ogni tabella di instradamento VPC punta alla connessione peering VPC pertinente per accedere a un singolo indirizzo IP (e pertanto un'istanza specifica) nel VPC in peering.

Tabella di routing	Destinazione	Target
VPC A	<i>VPC A CIDR</i>	Locale
	<i>Instance 3 IP address</i>	pcx-aaaabbbb
	<i>Instance 4 IP address</i>	pcx-aaaacccc
VPC B	<i>VPC B CIDR</i>	Locale

Tabella di routing	Destinazione	Target
	<i>Instance 1 IP address</i>	pcx-aaaabbbb
VPC C	<i>VPC C CIDR</i>	Locale
	<i>Instance 2 IP address</i>	pcx-aaaacccc

Un VPC che accede a due VPCs utilizzando le corrispondenze di prefisso più lunghe

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 instradato 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	<i>VPC A CIDR block</i>	Locale
	<i>Instance X IP address</i>	pcx-aaaabbbb
	<i>VPC C CIDR block</i>	pcx-aaaacccc
VPC B	<i>VPC B CIDR block</i>	Locale
	<i>VPC A CIDR block</i>	pcx-aaaabbbb
VPC C	<i>VPC C CIDR block</i>	Locale
	<i>VPC A CIDR block</i>	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](#).

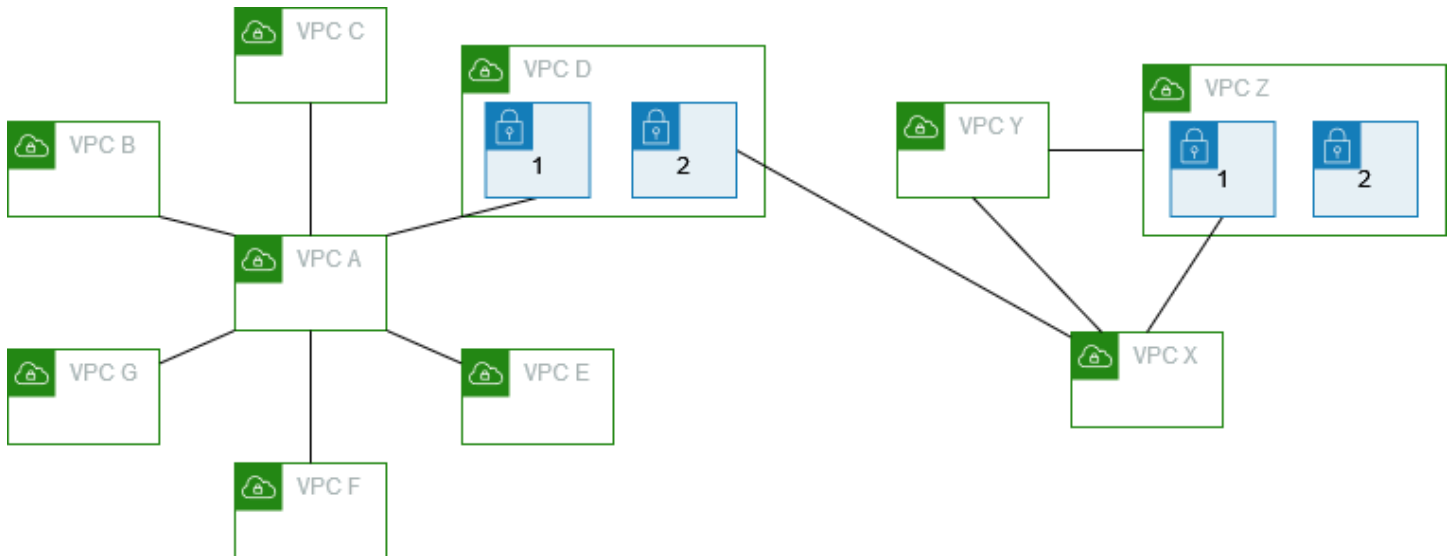
Configurazioni VPC multiple

In questa configurazione, è presente un VPC centrale (VPC A) peerizzato con più VPCs VPC in una configurazione a spoke. Sono inoltre disponibili tre VPCs peering (VPCs X, Y e Z) 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. AWS non 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 routing per VPCs B, C, E, F e G puntano alle connessioni peering pertinenti per accedere al blocco CIDR completo per VPC A, mentre la tabella di routing VPC A punta alle connessioni peering pertinenti per VPCs B, C, 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	<i>VPC A CIDR</i>	Locale

Tabella di routing	Destinazione	Target
	<i>VPC B CIDR</i>	pcx-aaaabbbb
	<i>VPC C CIDR</i>	pcx-aaaacccc
	<i>Subnet 1 CIDR in VPC D</i>	pcx-aaaadddd
	<i>VPC E CIDR</i>	pcx-aaaaeeee
	<i>VPC F CIDR</i>	pcx-aaaaffff
	<i>VPC G CIDR</i>	pcx-aaaagggg
VPC B	<i>VPC B CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaabbbb
VPC C	<i>VPC C CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaacccc
Sottorete 1 in VPC D	<i>VPC D CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaadddd
Sottorete 2 in VPC D	<i>VPC D CIDR</i>	Locale
	<i>VPC X CIDR</i>	pcx-ddddxxxx
VPC E	<i>VPC E CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaaeeee
VPC F	<i>VPC F CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaaffff
VPC G	<i>VPC G CIDR</i>	Locale
	<i>VPC A CIDR</i>	pcx-aaaagggg

Tabella di routing	Destinazione	Target
VPC X	<i>VPC X CIDR</i>	Locale
	<i>Subnet 2 CIDR in VPC D</i>	pcx-ddddxxxx
	<i>VPC Y CIDR</i>	pcx-xxxxyyyy
	<i>Subnet 1 CIDR in VPC Z</i>	pcx-xxxxzzzz
VPC Y	<i>VPC Y CIDR</i>	Locale
	<i>VPC X CIDR</i>	pcx-xxxxyyyy
	<i>VPC Z CIDR</i>	pcx-yyyyzzzz
VPC Z	<i>VPC Z CIDR</i>	Locale
	<i>VPC Y CIDR</i>	pcx-yyyyzzzz
	<i>VPC X CIDR</i>	pcx-xxxxzzzz

Scenari di rete di connessione peering VPC

Esistono diversi motivi per cui potresti dover configurare una connessione peering VPC tra il tuo VPC o tra un VPC di tua VPCs proprietà e un VPC di un altro account. AWS I seguenti scenari consentono di determinare quale configurazione è più idonea ai requisiti di rete.

Scenari

- [Peering di due o più risorse per fornire l'accesso completo VPCs alle risorse](#)
- [Collegamento in peering a un VPC per accedere a risorse centralizzate](#)

Peering di due o più risorse per fornire l'accesso completo VPCs alle risorse

In questo scenario, ne hai due o più VPCs che vuoi peer per consentire la condivisione completa delle risorse tra tutti. VPCs 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 si VPCs trovano all'interno dello stesso AWS account e altri in un AWS account diverso. Volete riunire tutti i reparti VPCs per consentire ai reparti IT di avere pieno accesso alle rispettive risorse.

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 [Connessioni in peering di VPC](#).

Collegamento in peering a un VPC per accedere a risorse centralizzate

In questo scenario, hai un VPC centrale che contiene risorse che desideri condividere con altri VPCs. Il VPC centrale può richiedere l'accesso totale o parziale al peer e VPCs, allo stesso modo, il peer VPCs può richiedere l'accesso totale o parziale al VPC centrale. Di seguito vengono mostrati alcuni esempi:

- Il reparto IT dell'azienda dispone di un VPC per la condivisione file. Vuoi che altri utenti accedano VPCs a quel VPC centrale, ma non vuoi che l'altro si invii traffico l'un l'altro VPCs.
- L'azienda dispone di un VPC che desideri condividere con altri clienti. Ogni cliente può creare una connessione peering VPC con il tuo VPC, tuttavia, i tuoi clienti non possono indirizzare il traffico verso altri VPCs che sono collegati al tuo, né sono a conoscenza dei percorsi degli altri clienti.
- Disponi di un VPC centrale che viene utilizzato per servizi Active Directory. Le istanze specifiche in peer VPCs inviano richieste ai server Active Directory e richiedono l'accesso completo al VPC centrale. Il VPC centrale non richiede l'accesso completo al peer VPCs; deve solo indirizzare il traffico di risposta verso istanze specifiche.

Per ulteriori informazioni sulla creazione e sull'utilizzo di connessioni peering VPC nella console Amazon VPC, consulta [Connessioni in peering di 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 seguente politica concede agli utenti l'autorizzazione a creare richieste di connessione peering VPC VPCs utilizzando quelle contrassegnate 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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*",
      "Condition": {
```

```

    "StringEquals": {
      "ec2:ResourceTag/Purpose": "Peering"
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:CreateVpcPeeringConnection",
    "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-connection/*"
  }
]
}

```

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

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:us-east-1:111122223333:vpc/vpc-1234567890abcdef0"
        }
      }
    }
  ]
}

```

Esempio: Accettazione di una connessione peering VPC

La seguente politica concede agli utenti l'autorizzazione ad accettare richieste di connessione peering VPC da un account specifico. AWS 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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:RequesterVpc": "arn:aws:ec2:us-east-1:111122223333:vpc/*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
    }
  ]
}
```

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

JSON

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

```

    "Effect": "Allow",
    "Action": "ec2:AcceptVpcPeeringConnection",
    "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-connection/*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:AcceptVpcPeeringConnection",
    "Resource": "arn:aws:ec2:us-east-1:123456789012: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.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2>DeleteVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-connection/*",
      "Condition": {
        "ArnNotEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-1234567890abcdef0",

```

```

        "ec2:RequesterVpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-0abcdef1234567890"
    }
}
]
}

```

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 le connessioni peering VPC, a condizione che siano 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 il permesso di creare connessioni peering VPC e l'accesso a VPCs tutti gli utenti dell'account specificato per farlo.

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 assicurano che le azioni possano essere eseguite solo su connessioni peering VPC VPCs che fanno 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.

JSON

```

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

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection"
      ],
      "Resource": "arn:aws:ec2:*:111122223333:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:*VpcPeeringConnection",
      "Resource": "arn:aws:ec2:*:111122223333:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AcceptorVpc": "arn:aws:ec2:*:111122223333:vpc/*",
          "ec2:RequesterVpc": "arn:aws:ec2:*:111122223333: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.

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-1234567890abcdef0",
        "arn:aws:ec2:*:*:vpc-peering-connection/*"
      ]
    }
  ]
}
```

Quote delle connessioni peering VPC per un account

Il peering VPC permette di connettere due VPC. Ciò consente alle risorse di un VPC di comunicare con quelle dell'altro VPC come se si trovassero nella stessa rete. Il peering VPC è una funzionalità utile per connettere i VPC, indipendentemente dal fatto che si trovino nella stessa Regione AWS o in Regioni diverse. Questa sezione descrive le quote di cui dovresti essere a conoscenza quando utilizzi le 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.

Se ritieni che i tuoi attuali requisiti di connessione peering VPC superino le quote predefinite, ti consigliamo di inviare una richiesta di aumento del limite di servizio. Esamineremo il tuo caso d'uso e collaboreremo con te per modificare le quote di conseguenza, assicurandoci che il l'ambiente VPC sia in grado di supportare le tue crescenti esigenze aziendali.

Nome	Predefinita	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 ulteriori informazioni sulle quote di 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-Classik 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 e 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.