Guida per l'utente

AWS Direct Connect

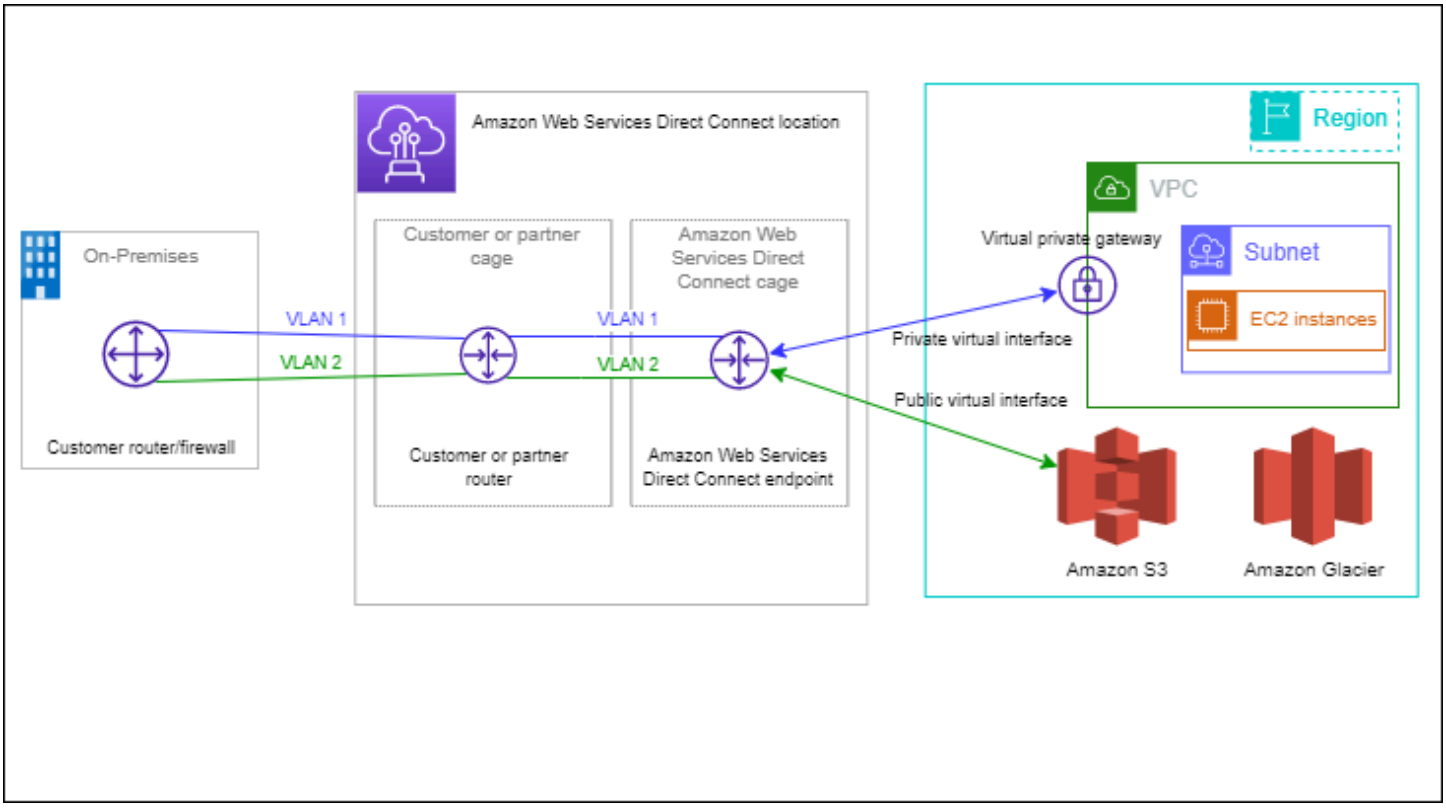
AWS Direct Connect: Guida per l'utente

Table of Contents

Che cos'è AWS Direct Connect?

AWS Direct Connect collega la rete interna a una AWS Direct Connect posizione tramite un cavo Ethernet standard in fibra ottica. Un'estremità del cavo è collegata al tuo router e l'altra estremità a un router di AWS Direct Connect . Con questa connessione, puoi creare interfacce virtuali direttamente verso AWS i servizi pubblici (ad esempio, Amazon S3) o Amazon VPC, aggirando i provider di servizi Internet nel tuo percorso di rete. Una AWS Direct Connect posizione consente l'accesso AWS nella regione a cui è associata. È possibile utilizzare una singola connessione in una regione pubblica o accedere AWS GovCloud (US) ai AWS servizi pubblici in tutte le altre regioni pubbliche.

Il diagramma seguente mostra una panoramica di alto livello del modo in cui si AWS Direct Connect interfaccia con la rete.



Indice

- Accesso a una regione AWS remota
- Policy di instradamento e comunità BGP

AWS Direct Connect componenti

Di seguito sono riportati i componenti chiave utilizzati per AWS Direct Connect:

Connessioni

Crea una connessione in una AWS Direct Connect posizione per stabilire una connessione di rete dalla tua sede a una AWS regione. Per ulteriori informazioni, consulta AWS Direct Connect connessioni.

Interfacce virtuali

Crea un'interfaccia virtuale per abilitare l'accesso ai AWS servizi. Un'interfaccia virtuale pubblica consente l'accesso ai servizi rivolti al pubblico, come Amazon S3. Un'interfaccia virtuale privata consente l'accesso al VPC. Per ulteriori informazioni, consulta AWS Direct Connect interfacce virtuali e Prerequisiti per le interfacce virtuali.

Requisiti di rete

Per essere utilizzata AWS Direct Connect in un AWS Direct Connect luogo, la rete deve soddisfare una delle seguenti condizioni:

- La rete è collocata in una posizione condivisa con una posizione esistente AWS Direct Connect . Per ulteriori informazioni sulle AWS Direct Connect località disponibili, consulta i dettagli del prodotto AWS Direct Connect.
- Stai lavorando con un AWS Direct Connect partner membro del AWS Partner Network (APN). Per informazioni, consulta la sezione Partner APN che supportano AWS Direct Connect.
- Lavori con un provider di servizi indipendente per la connessione a AWS Direct Connect.

Inoltre, la tua rete deve soddisfare le seguenti condizioni:

- La rete deve utilizzare la fibra monomodale con un ricetrasmettitore 1000BASE-LX (1310 nm) per 1 gigabit Ethernet, un ricetrasmettitore 10GBASE-LR (1310 nm) per 10 gigabit o un 100GBASE-LR4 per 100 gigabit Ethernet.

- La negoziazione automatica per una porta deve essere disabilitata per una connessione con una velocità di porta superiore a 1 Gbps. Tuttavia, a seconda dell'endpoint AWS Direct Connect che serve la connessione, potrebbe essere necessario abilitare o disabilitare la negoziazione automatica per le connessioni da 1 Gbps. Se l'interfaccia virtuale rimane inattiva, consulta Risoluzione dei problemi di livello 2 (collegamento dati).
- L'incapsulamento VLAN 802.1Q deve essere supportato su tutta la connessione, compresi i dispositivi intermedi.
- Il dispositivo deve supportare l'autenticazione Border Gateway Protocol (BGP) e BGP MD5.
- (Facoltativo) È possibile configurare il rilevamento bidirezionale di inoltro (BFD) sulla rete. Il BFD asincrono viene abilitato automaticamente per ogni interfaccia virtuale. AWS Direct Connect È abilitato automaticamente per le interfacce virtuali Direct Connect, ma non ha effetto finché non lo configuri sul router. Per ulteriori informazioni, consulta Abilitare BFD per una connessione Direct Connect.

AWS Direct Connect supporta entrambi i protocolli di comunicazione IPv4 e IPv6. Gli indirizzi IPv6 forniti dai AWS servizi pubblici sono accessibili tramite interfacce virtuali pubbliche. AWS Direct Connect

AWS Direct Connect supporta una dimensione frame Ethernet di 1522 o 9023 byte (14 byte intestazione Ethernet + 4 byte tag VLAN + byte per il datagramma IP + 4 byte FCS) a livello di layer di collegamento. Puoi impostare la MTU delle interfacce virtuali private. Per ulteriori informazioni, consulta Impostazione di MTU di rete per interfacce virtuali private o di transito.

Prezzi per AWS Direct Connect

AWS Direct Connect prevede due elementi di fatturazione: orari di porta e trasferimento dati in uscita. La tariffa oraria per l'utilizzo di una porta è determinata dal tipo di connessione (dedicata o ospitata) e dalla capacità.

I costi di trasferimento dei dati in uscita per le interfacce private e le interfacce virtuali di transito vengono assegnati all' AWS account responsabile del trasferimento dei dati. Non sono previsti costi aggiuntivi per l'utilizzo di un gateway AWS Direct Connect con più account.

Per AWS le risorse indirizzabili pubblicamente (ad esempio, bucket Amazon S3, istanze EC2 Classic o traffico EC2 che passa attraverso un gateway Internet), se il traffico in uscita è destinato a prefissi pubblici di proprietà AWS dello stesso account di pagamento e pubblicizzato attivamente tramite AWS Direct Connect un'interfaccia virtuale pubblica, l'utilizzo del Data Transfer Out (DTO) viene

misurato AWS verso il proprietario della risorsa alla velocità di trasferimento dei dati. AWS Direct Connect

Per ulteriori informazioni, consulta Prezzi di AWS Direct Connect.

AWS Direct Connect manutenzione

AWS Direct Connect è un servizio completamente gestito in cui, periodicamente, Direct Connect esegue attività di manutenzione su un parco hardware che supporta il servizio. Le connessioni Direct Connect vengono fornite su dispositivi hardware autonomi che consentono di creare connessioni di rete altamente resilienti tra Amazon Virtual Private Cloud e l'infrastruttura locale. Questa funzionalità consente di accedere alle AWS risorse in modo affidabile, scalabile ed economico. Per ulteriori informazioni, consulta Raccomandazioni per la resilienza di AWS Direct Connect.

Esistono due tipi di manutenzione Direct Connect: pianificata e di emergenza:

- Manutenzione pianificata. La manutenzione pianificata è programmata in anticipo per migliorare la disponibilità e fornire nuove funzionalità. Questo tipo di manutenzione viene pianificata durante una finestra di manutenzione in cui forniamo tre notifiche: 14 giorni di calendario, 7 giorni di calendario e 1 giorno di calendario.

  > **Note**
  >
  > I giorni di calendario includono giorni non lavorativi e festività locali.

- Manutenzione di emergenza. La manutenzione di emergenza viene avviata in modo critico a causa di un guasto del servizio che richiede un intervento immediato da parte di AWS per ripristinare i servizi. Questo tipo di manutenzione non è pianificato in anticipo. I clienti interessati vengono avvisati della manutenzione di emergenza fino a 60 minuti prima della manutenzione.

Ti consigliamo di seguire le indicazioni in AWS Direct Connect Resiliency Recommendations in modo da poter spostare in modo corretto e proattivo il traffico verso la connessione Direct Connect ridondante durante la manutenzione. Ti consigliamo inoltre di testare in modo proattivo la resilienza delle connessioni ridondanti su base regolare per verificare che il failover funzioni come previsto. Utilizzando questa the section called “Test di failover AWS Direct Connect” funzionalità, è possibile verificare le rotte del traffico tramite una delle interfacce virtuali ridondanti.

Per indicazioni sui criteri di idoneità per avviare una richiesta di annullamento della manutenzione pianificata, vedi Come posso annullare un evento di manutenzione Direct Connect?.

> **Note**
>
> Le richieste di manutenzione di emergenza non possono essere annullate, in quanto è AWS necessario agire immediatamente per ripristinare il servizio.

Per ulteriori informazioni sugli eventi di manutenzione, consulta Eventi di manutenzione nelle Domande frequenti.AWS Direct Connect

Accesso a una regione AWS remota

Le sedi AWS Direct Connect in AWS GovCloud (US) o nelle regioni pubbliche possono accedere ai servizi pubblici di qualsiasi altra regione pubblica (a esclusione della Cina (Pechino e Ningxia)). Inoltre, è possibile configurare le connessioni AWS Direct Connect in AWS GovCloud (US) o nelle regioni pubbliche per l'accesso a un VPC dell'account in qualsiasi altra regione pubblica (a esclusione di Cina (Pechino e Ningxia)). Puoi quindi utilizzare una singola connessione AWS Direct Connect per creare servizi in più regioni. Tutto il traffico di rete rimane sulla dorsale di rete globale di AWS, indipendentemente dal fatto che tu acceda ai servizi AWS pubblici o a un VPC in un'altra regione.

L'eventuale trasferimento di dati in uscita da una regione remota viene fatturato secondo la velocità di trasferimento dati di tale regione. Per ulteriori informazioni sui prezzi del trasferimento dati, consulta la sezione relativa ai Prezzi nella pagina degli approfondimenti su AWS Direct Connect.

Per ulteriori informazioni sulle policy di routing e sulle community BGP supportate per una connessione AWS Direct Connect, consulta Policy di instradamento e comunità BGP.

Accesso a servizi pubblici in una regione remota

Per accedere alle risorse pubbliche in una regione remota, è necessario impostare un'interfaccia virtuale pubblica e stabilire una sessione BGP (Border Gateway Protocol). Per ulteriori informazioni, consulta AWS Direct Connect interfacce virtuali.

Dopo aver creato un'interfaccia virtuale pubblica e aver stabilito una sessione BGP, il router apprende gli instradamenti delle altre regioni AWS pubbliche. Per ulteriori informazioni sui prefissi attualmente pubblicizzati da AWS, consulta Intervalli di indirizzi IP AWS nella Riferimenti generali di Amazon Web Services.

Accesso ai VPC in una regione remota

È possibile creare un gateway Direct Connect in qualsiasi regione pubblica. Utilizzalo per collegare la connessione AWS Direct Connect tramite un'interfaccia virtuale privata ai VPC nell'account che si trovano in regioni differenti o a un gateway di transito. Per ulteriori informazioni, consulta Utilizzo dei gateway Direct Connect.

In alternativa, puoi creare un'interfaccia virtuale pubblica per la tua connessione AWS Direct Connect e quindi stabilire una connessione VPN al VPC nella regione remota. Per ulteriori informazioni sulla configurazione di una connessione VPN a un VPC, consulta la sezione relativa agli Scenari di utilizzo per utilizzare Amazon Virtual Private Cloud nella Guida per l'utente di Amazon VPC.

Opzioni di connettività da rete ad Amazon VPC

La seguente configurazione può essere utilizzata per connettere reti remote con il tuo ambiente Amazon VPC. Queste opzioni sono utili per integrare le risorse AWS con i servizi in loco esistenti:

- Opzioni di connettività di Amazon Virtual Private Cloud

Policy di instradamento e comunità BGP

AWS Direct Connect applica le politiche di routing in entrata (dal data center locale) e in uscita (dalla tua AWS regione) per una connessione pubblica. AWS Direct Connect Puoi inoltre utilizzare i tag della community Border Gateway Protocol (BGP) sugli instradamenti Amazon pubblicizzati e applicare tali tag agli instradamenti che pubblicizzi per Amazon.

Policy di instradamento dell'interfaccia virtuale pubblica

Se lo utilizzi AWS Direct Connect per accedere a AWS servizi pubblici, devi specificare i prefissi IPv4 o IPv6 pubblici per fare pubblicità tramite BGP.

Si applicano le seguenti policy di instradamento in entrata:

- Devi possedere i prefissi pubblici e devono essere registrati come tali nel registro internet regionale di pertinenza.
- Il traffico deve essere destinato ai prefissi pubblici Amazon. L'instradamento transitivo tra le connessioni non è supportato.
- AWS Direct Connect esegue il filtraggio dei pacchetti in entrata per verificare che la fonte del traffico provenga dal prefisso pubblicizzato.

Si applicano le seguenti policy di instradamento in uscita:

- AS_PATH e Longest Prefix Match vengono utilizzati per determinare il percorso di routing. AWS consiglia di pubblicizzare percorsi più specifici utilizzando AWS Direct Connect se lo stesso prefisso viene pubblicizzato sia su Internet che su un'interfaccia virtuale pubblica.
- AWS Direct Connect pubblicizza tutti i prefissi AWS regionali locali e remoti, ove disponibili, e include prefissi in rete provenienti da altri punti di presenza (PoP) AWS non regionali, ove disponibili, come ad esempio Route 53. CloudFront

  > **Note**
  >
  > - I prefissi elencati nel file JSON degli intervalli di indirizzi AWS IP, ip-ranges.json, per le regioni cinesi sono pubblicizzati solo nelle regioni cinesi. AWS AWS
  > - I prefissi elencati nel file JSON degli intervalli di indirizzi AWS IP, ip-ranges.json, per le aree commerciali sono pubblicizzati solo nelle aree commerciali. AWS AWS
  >
  > Per ulteriori informazioni sul file ip-ranges.json, consulta Intervalli di indirizzi IP AWS nella Riferimenti generali di AWS

- AWS Direct Connect pubblicizza prefissi con una lunghezza minima del percorso di 3.
- AWS Direct Connect pubblicizza tutti i prefissi pubblici con la nota comunità BGP. `NO_EXPORT`
- Se pubblicizzi gli stessi prefissi di due regioni diverse utilizzando due diverse interfacce virtuali pubbliche ed entrambi hanno gli stessi attributi BGP e la lunghezza del prefisso più lunga, darà la priorità alla regione principale per il traffico in uscita. AWS
- Se disponi di più AWS Direct Connect connessioni, puoi regolare la condivisione del carico del traffico in entrata pubblicizzando prefissi con gli stessi attributi di percorso.
- I prefissi pubblicizzati da non AWS Direct Connect devono essere pubblicizzati oltre i confini di rete della connessione. Ad esempio, questi prefissi non devono essere inclusi in nessuna tabella di instradamento Internet pubblica.
- AWS Direct Connect mantiene i prefissi pubblicizzati dai clienti all'interno della rete Amazon. Non pubblicizziamo nuovamente i prefissi dei clienti acquisiti da un file VIF pubblico con uno dei seguenti prefissi:
  - Altri clienti AWS Direct Connect
  - Reti che collaborano con la rete AWS globale
  - I fornitori di servizi di trasporto di Amazon

Comunità BGP dell'interfaccia virtuale pubblica

AWS Direct Connect supporta i tag della community scope BGP per aiutare a controllare l'ambito (regionale o globale) e le preferenze di indirizzamento del traffico sulle interfacce virtuali pubbliche. AWS tratta tutte le rotte ricevute da un VIF pubblico come se fossero etichettate con il tag della community BGP NO_EXPORT, il che significa che solo la rete utilizzerà tali informazioni di routing. AWS

Comunità di ambito BGP

Puoi applicare i tag per le comunità BGP sui prefissi pubblici pubblicizzati per Amazon per indicare la propagazione dei prefissi sulla rete Amazon solo per la regione AWS locale, per tutte le regioni all'interno di un continente o per tutte le regioni pubbliche.

Regione AWS comunità

Per le policy di instradamento in entrata, puoi utilizzare le seguenti comunità BGP per i tuoi prefissi:

- `7224:9100`—Locale Regioni AWS
- `7224:9200`—Tutto Regioni AWS per un continente:
  - In tutto il Nord America
  - Asia Pacifico
  - Europa, Medio Oriente e Africa
- `7224:9300`—Globale (tutte le regioni pubbliche) AWS

> **Note**
>
> Se non applichi alcun tag di community, per impostazione predefinita i prefissi vengono pubblicizzati in tutte le AWS regioni pubbliche (globali).
> I prefissi marcati con le stesse comunità e con identici attributi AS_PATH sono indicati per il multi-pathing.

Le comunità `7224:1` - `7224:65535` sono riservate da AWS Direct Connect.

Per quanto riguarda le politiche di routing in uscita, AWS Direct Connect applica le seguenti community BGP ai percorsi pubblicizzati:

- `7224:8100`—Percorsi che provengono dalla stessa AWS regione a cui è associato il punto di presenza. AWS Direct Connect
- `7224:8200`—Rotte che provengono dallo stesso continente a cui è associato il AWS Direct Connect punto di presenza.
- Nessun tag: rotte che provengono da altri continenti.

> **Note**
>
> Per ricevere tutti i prefissi AWS pubblici non è necessario applicare alcun filtro.

Le comunità che non sono supportate per una connessione AWS Direct Connect pubblica vengono rimosse.

Comunità BGP **`NO_EXPORT`**

Per le policy di instradamento in uscita, il tag di community `NO_EXPORT` BGP è supportato per le interfacce virtuali pubbliche.

AWS Direct Connect fornisce anche tag della community BGP sui percorsi Amazon pubblicizzati. Se lo utilizzi AWS Direct Connect per accedere ai AWS servizi pubblici, puoi creare filtri basati su questi tag della community.

Per le interfacce virtuali pubbliche, tutti i percorsi che AWS Direct Connect pubblicizzano annunci ai clienti sono etichettati con il tag di community NO_EXPORT.

Policy di instradamento dell'interfaccia virtuale privata e dell'interfaccia virtuale di transito

Se lo utilizzi AWS Direct Connect per accedere alle tue AWS risorse private, devi specificare i prefissi IPv4 o IPv6 per fare pubblicità tramite BGP. Questi prefissi possono essere pubblici o privati.

Le seguenti regole di routing in uscita si applicano in base ai prefissi pubblicizzati:

- AWS valuta prima la lunghezza del prefisso più lunga. AWS consiglia di pubblicizzare percorsi più specifici utilizzando più interfacce virtuali Direct Connect se i percorsi di routing desiderati sono destinati a connessioni attive/passive. Per ulteriori informazioni, consulta Influenzare il traffico sulle reti ibride utilizzando Longest Prefix Match.

- La preferenza locale è l'attributo BGP consigliato da utilizzare quando i percorsi di routing desiderati sono destinati a connessioni attive/passive e le lunghezze dei prefissi pubblicizzate sono le stesse. Questo valore viene impostato per regione in modo da preferire le AWS Direct Connect località a cui sono associate Regione AWS le stesse utilizzando il valore della comunità di preferenza locale —Medium. `7224:7200` Se la regione locale non è associata alla posizione Direct Connect, è impostata su un valore inferiore. Questo vale solo se non viene assegnato alcun tag di comunità con preferenza locale.
- La lunghezza AS_PATH può essere utilizzata per determinare il percorso di routing quando la lunghezza del prefisso e la preferenza locale coincidono.
- È possibile utilizzare Multi-Exit Discriminator (MED) per determinare il percorso di routing quando la lunghezza del prefisso, la preferenza locale e AS_PATH coincidono. AWS non consiglia di utilizzare i valori MED data la loro priorità inferiore nella valutazione.
- AWS condividerà il caricamento su più interfacce virtuali private o di transito quando i prefissi hanno la stessa lunghezza e gli stessi attributi BGP.

Comunità BGP dell'interfaccia virtuale privata e dell'interfaccia virtuale di transito

Quando un indirizzamento del Regione AWS traffico verso le sedi locali tramite interfacce private o virtuali di transito di Direct Connect, la posizione Direct Connect associata influisce sulla capacità Regione AWS di utilizzare il routing multipercorso (ECMP) a costo equo. Regioni AWS per impostazione predefinita, preferisce le sedi Direct Connect nelle stesse associate Regione AWS . Vedi AWS Direct Connect Sedi per identificare le sedi associate a Regione AWS qualsiasi posizione Direct Connect.

Quando non vengono applicati tag di comunità con preferenze locali, Direct Connect supporta ECMP su interfacce virtuali private o di transito per prefissi con la stessa lunghezza, lunghezza AS_PATH e valore MED su due o più percorsi nei seguenti scenari:

- Il traffico di Regione AWS invio ha due o più percorsi di interfaccia virtuali da postazioni nella stessa area associata Regione AWS, situate nelle stesse strutture di colocation o in strutture di colocation diverse.
- Il traffico di Regione AWS invio ha due o più percorsi di interfaccia virtuale da località diverse dalla stessa regione.

Per ulteriori informazioni, vedi Come si configura una connessione Direct Connect Active/Active o Active/Passive Direct Connect AWS da un'interfaccia virtuale privata o di transito?

> **Note**
>
> Ciò non ha alcun effetto sull'ECMP da e verso le postazioni locali. Regione AWS

Per controllare le preferenze di percorso, Direct Connect supporta i tag di comunità BGP con preferenza locale per interfacce virtuali private e interfacce virtuali di transito.

Comunità BGP di preferenza locale

Puoi usare i tag per le comunità BGP di preferenza locale per raggiungere il bilanciamento del carico e instradare la preferenza per il traffico in entrata verso la rete. Per ogni prefisso che pubblicizzi su una sessione BGP, puoi applicare un tag per la comunità per indicare la priorità del percorso associato al traffico restituito.

I seguenti tag per le comunità BGP di preferenza locale sono supportati:

- `7224:7100` - Bassa preferenza
- `7224:7200` - Media preferenza
- `7224:7300` - Alta preferenza

I tag per le comunità BGP di preferenza locale sono reciprocamente esclusivi. Per bilanciare il carico del traffico su più AWS Direct Connect connessioni (attive/attive) situate nella stessa regione o in AWS regioni diverse, applica lo stesso tag di community, ad esempio `7224:7200` (preferenza media) tra i prefissi delle connessioni. Se una delle connessioni fallisce, il traffico verrà quindi bilanciato utilizzando ECMP tra le connessioni attive rimanenti, indipendentemente dalle associazioni delle rispettive regioni di origine. Per supportare il failover su più connessioni AWS Direct Connect (attive/attive), applica un tag per le comunità con una preferenza maggiore ai prefissi per l'interfaccia virtuale primaria o attiva e una preferenza minore ai prefissi per il backup o le interfacce virtuali passive. Ad esempio, imposta i tag della community BGP per le interfacce virtuali primarie o attive su `7224:7300` (preferenza alta) e `7224:7100` (preferenza bassa) per le interfacce virtuali passive.

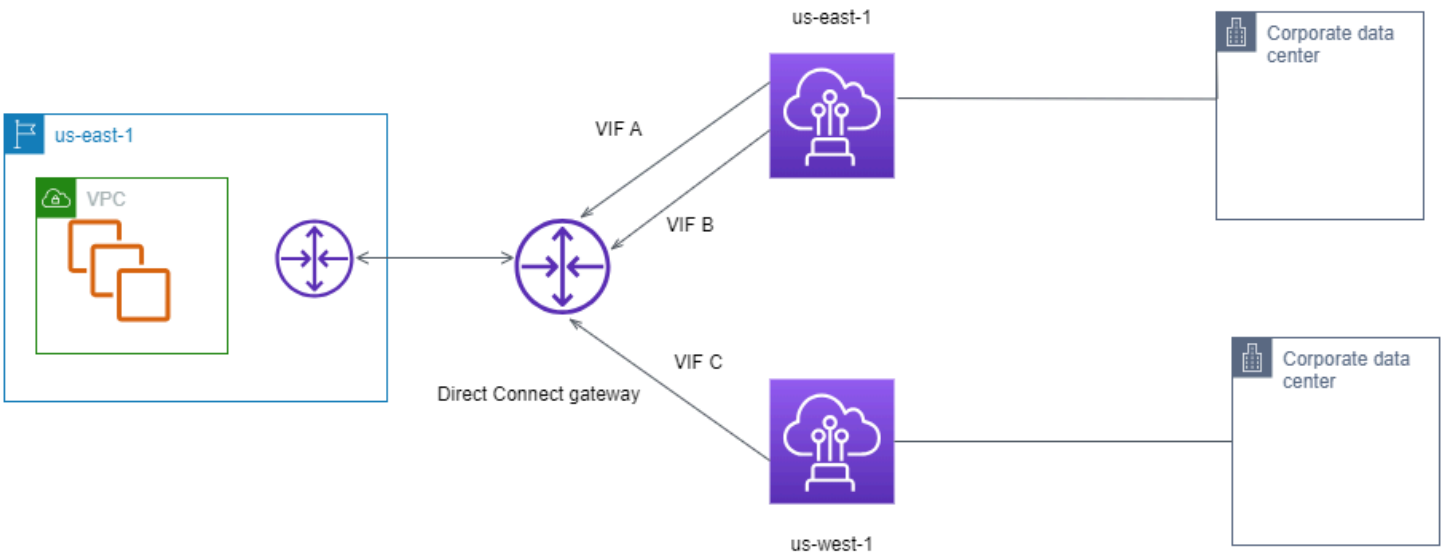
I tag per le comunità BGP di preferenza locale vengono valutati prima di qualsiasi attributo AS_PATH e secondo l'ordine che va dalla preferenza più bassa a quella più alta (è consigliata la preferenza più alta).

Esempio di instradamento di interfacce virtuali private

Considera la configurazione in cui la regione principale della AWS Direct Connect posizione 1 è la stessa della regione principale del VPC. Esiste una AWS Direct Connect posizione ridondante in una regione diversa. Esistono due VIF privati (VIF A e VIF B) dalla posizione AWS Direct Connect 1 (us-east-1) al gateway Direct Connect. Esiste un VIF privato (VIF C) dalla AWS Direct Connect posizione (us-west-1) al gateway Direct Connect. Per fare in modo che il traffico di AWS routing su VIF B sia precedente a VIF A, impostate l'attributo AS_PATH di VIF B in modo che sia più corto dell'attributo VIF A AS_PATH.

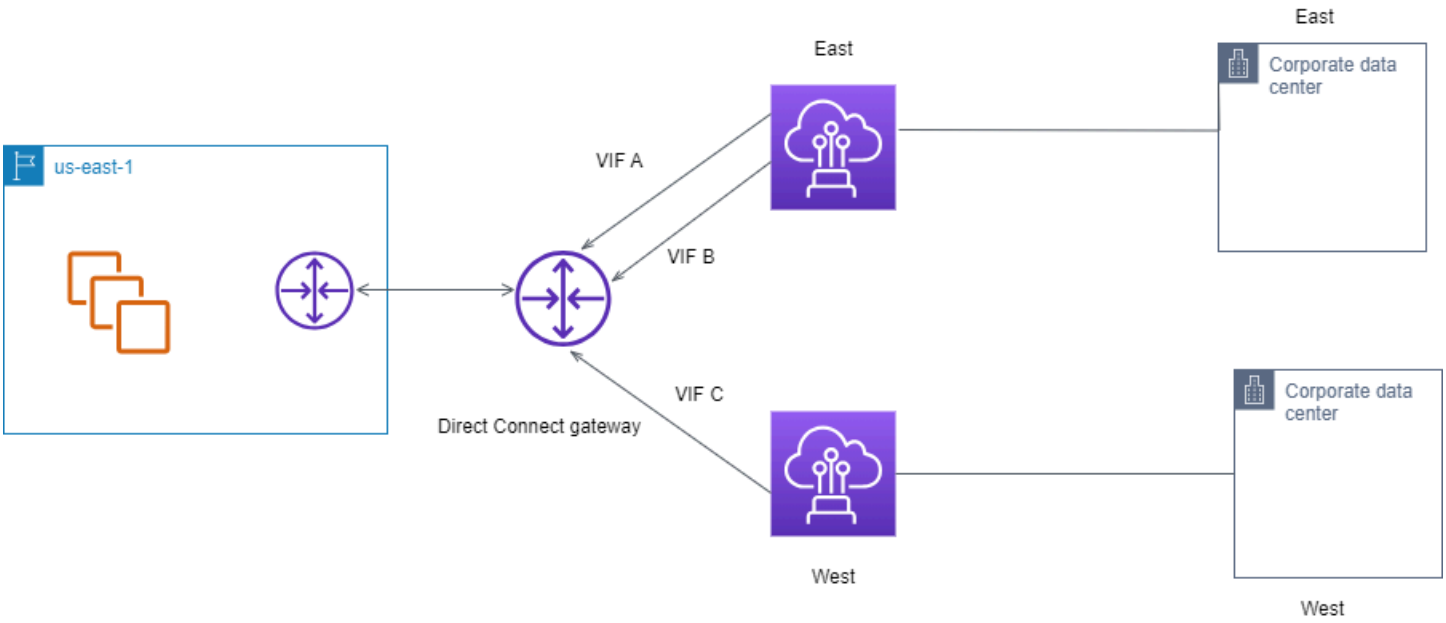
Le VIF hanno il seguente comportamento:

- VIF A (in us-east-1) pubblicizza 172.16.0.0/16 e ha un attributo AS_PATH di 65001, 65001, 65001
- VIF B (in us-east-1) pubblicizza 172.16.0.0/16 e ha un attributo AS_PATH di 65001, 65001
- VIF C (in us-east-1) pubblicizza 172.16.0.0/16 e ha un attributo AS_PATH di 65001



Se modificate la configurazione dell'intervallo CIDR di VIF C, le route che rientrano nell'intervallo CIDR VIF C utilizzano VIF C perché ha la lunghezza del prefisso più lunga.

- VIF C (in us-east-1) pubblicizza 172.16.0.0/24 e ha un attributo AS_PATH di 65001


East
East
Corporate data center
us-east-1
VIF A
VIF B
VIF C
Direct Connect gateway
Corporate data center
West
West

Utilizzo del AWS Direct Connect Resiliency Toolkit per iniziare

AWS offre ai clienti la possibilità di ottenere connessioni di rete altamente resilienti tra Amazon Virtual Private Cloud (Amazon VPC) e la loro infrastruttura locale. Il AWS Direct Connect Resiliency Toolkit fornisce una procedura guidata di connessione con più modelli di resilienza. Questi modelli consentono di determinare, e quindi di effettuare, un ordine per il numero di connessioni dedicate per raggiungere l'obiettivo SLA. Si seleziona un modello di resilienza, quindi il AWS Direct Connect Resiliency Toolkit guida l'utente attraverso il processo di ordinazione delle connessioni dedicato. I modelli di resilienza sono progettati per garantire il numero appropriato di connessioni dedicate in più posizioni.

Il AWS Direct Connect Resiliency Toolkit offre i seguenti vantaggi:

- Permette di capire come determinare e successivamente ordinare connessioni dedicate AWS Direct Connect che siano ridondanti e adatte allo scopo.
- Garantisce che le connessioni dedicate ridondanti abbiano la stessa velocità.
- Configura automaticamente i nomi di connessione dedicate.
- Approva automaticamente le connessioni dedicate quando disponi di un AWS account esistente e selezioni un partner noto. AWS Direct Connect La Letter of Authority (LOA) è disponibile per il download immediato.
- Crea automaticamente un ticket di supporto per l'approvazione della connessione dedicata quando sei un nuovo AWS cliente o selezioni un partner sconosciuto (Altro).
- Fornisce un riepilogo dell'ordine per le connessioni dedicate, con il contratto sul livello di servizio (SLA) che è possibile ottenere e il costo orario della porta per le connessioni dedicate ordinate.
- Crea Link Aggregation group (LAG) e aggiunge il numero appropriato di connessioni dedicate ai LAG quando scegli una velocità diversa da 1 Gbps, 10 Gbps o 100 Gbps.
- Fornisce un riepilogo del LAG con il contratto sul livello di servizio di connessione dedicata che è possibile ottenere e il costo orario di porta totale per ogni connessione dedicata ordinata come parte del LAG.
- Impedisce di terminare le connessioni dedicate sullo stesso dispositivo AWS Direct Connect .
- Fornisce un modo per verificare la resilienza della configurazione. Si lavora con AWS per abbattere la sessione di peering BGP al fine di verificare che il traffico sia indirizzato a una delle interfacce

virtuali ridondanti. Per ulteriori informazioni, consulta the section called “Test di failover AWS Direct Connect”.

- Fornisce CloudWatch parametri Amazon per connessioni e interfacce virtuali. Per ulteriori informazioni, consulta Monitoraggio.

I seguenti modelli di resilienza sono disponibili nel Resiliency Toolkit: AWS Direct Connect

- Resilienza massima: questo modello fornisce un modo per ordinare le connessioni dedicate per ottenere un contratto sul livello di servizio del 99,99%. Richiede di soddisfare tutti i requisiti per ottenere il contratto sul livello di servizio specificati in Contratto sul livello di servizio AWS Direct Connect.
- High Resiliency (Elevata resilienza): questo modello fornisce un modo per ordinare le connessioni dedicate per ottenere un contratto sul livello di servizio del 99,9%. Richiede di soddisfare tutti i requisiti per ottenere il contratto sul livello di servizio specificati in Contratto sul livello di servizio AWS Direct Connect.
- Development and Test (Sviluppo e test): questo modello fornisce un modo per ottenere la resilienza di sviluppo e test per carichi di lavoro non critici utilizzando connessioni separate che terminano su dispositivi separati in un'unica posizione.
- Classic. Questo modello è destinato agli utenti che dispongono di connessioni già esistenti e che desiderano aggiungerne di nuove. Questo modello non fornisce un contratto sul livello di servizio.

La migliore pratica consiste nell'utilizzare la procedura guidata di connessione nel AWS Direct Connect Resiliency Toolkit per ordinare le connessioni dedicate in modo da raggiungere l'obiettivo SLA.

Dopo aver selezionato il modello di resilienza, AWS Direct Connect Resiliency Toolkit illustra le seguenti procedure:

- Selezione del numero di connessioni dedicate
- Selezione della capacità di connessione e della posizione della connessione dedicata
- Ordinamento delle connessioni dedicate
- Verifica che le connessioni dedicate siano pronte per l'uso
- Download della Letter of Authority (LOA-CFA) per ogni connessione dedicata
- Verifica che la configurazione soddisfi i requisiti di resilienza

Prerequisiti

AWS Direct Connect supporta le seguenti velocità di porta su fibra monomodale: ricetrasmettitore 1000BASE-LX (1310 nm) per 1 gigabit Ethernet, ricetrasmettitore 10GBASE-LR (1310 nm) per 10 gigabit o 100GBASE-LR4 per 100 gigabit Ethernet.

È possibile configurare una connessione in uno dei seguenti modi: AWS Direct Connect

Modello	Larghezza di banda	Metodo
Connessione dedicata	1 Gbps, 10 Gbps e 100 Gbps	Collabora con un AWS Direct Connect partner o un provider di rete per connettere un router dal tuo data center, ufficio o ambiente di colocatio n a una AWS Direct Connect posizione. Il provider di rete non deve essere un Partner AWS Direct Connect affinché sia possibile collegarsi a una connessione dedicata. Le connessioni dedicate AWS Direct Connect supportano queste velocità di porta su fibra monomodale: 1 Gbps: 1000BASE-LX (1310 nm), 10 Gbps: 10GBASE-LR (1310 nm) e 100Gbps: 100GBASE-LR4.
Connessione ospitata	50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps e 10 Gbps	Collabora con un AWS Direct Connect partner del Partner Program per connettere un router dal tuo data center, ufficio o ambiente di colocatio n a un'ubicazione. AWS Direct Connect

Modello	Larghezza di banda	Metodo
		Solo alcuni partner forniscono connessioni di maggiore capacità.

Per connessioni AWS Direct Connect con larghezze di banda pari o superiori a 1 Gbps, assicurati che la rete soddisfi i seguenti requisiti:

- La rete deve utilizzare la fibra monomodale con un ricetrasmettitore 1000BASE-LX (1310 nm) per 1 gigabit Ethernet, un ricetrasmettitore 10GBASE-LR (1310 nm) per 10 gigabit o un 100GBASE-LR4 per 100 gigabit Ethernet.
- La negoziazione automatica per una porta deve essere disabilitata per una connessione con una velocità di porta superiore a 1 Gbps. Tuttavia, a seconda dell'endpoint AWS Direct Connect che serve la connessione, potrebbe essere necessario abilitare o disabilitare la negoziazione automatica per le connessioni da 1 Gbps. Se l'interfaccia virtuale rimane inattiva, consulta Risoluzione dei problemi di livello 2 (collegamento dati).
- L'incapsulamento VLAN 802.1Q deve essere supportato su tutta la connessione, compresi i dispositivi intermedi.
- Il dispositivo deve supportare l'autenticazione Border Gateway Protocol (BGP) e BGP MD5.
- (Facoltativo) È possibile configurare il rilevamento bidirezionale di inoltro (BFD) sulla rete. Il BFD asincrono viene abilitato automaticamente per ogni interfaccia virtuale. AWS Direct Connect È abilitato automaticamente per le interfacce virtuali Direct Connect, ma non ha effetto finché non lo configuri sul router. Per ulteriori informazioni, consulta Abilitare BFD per una connessione Direct Connect.

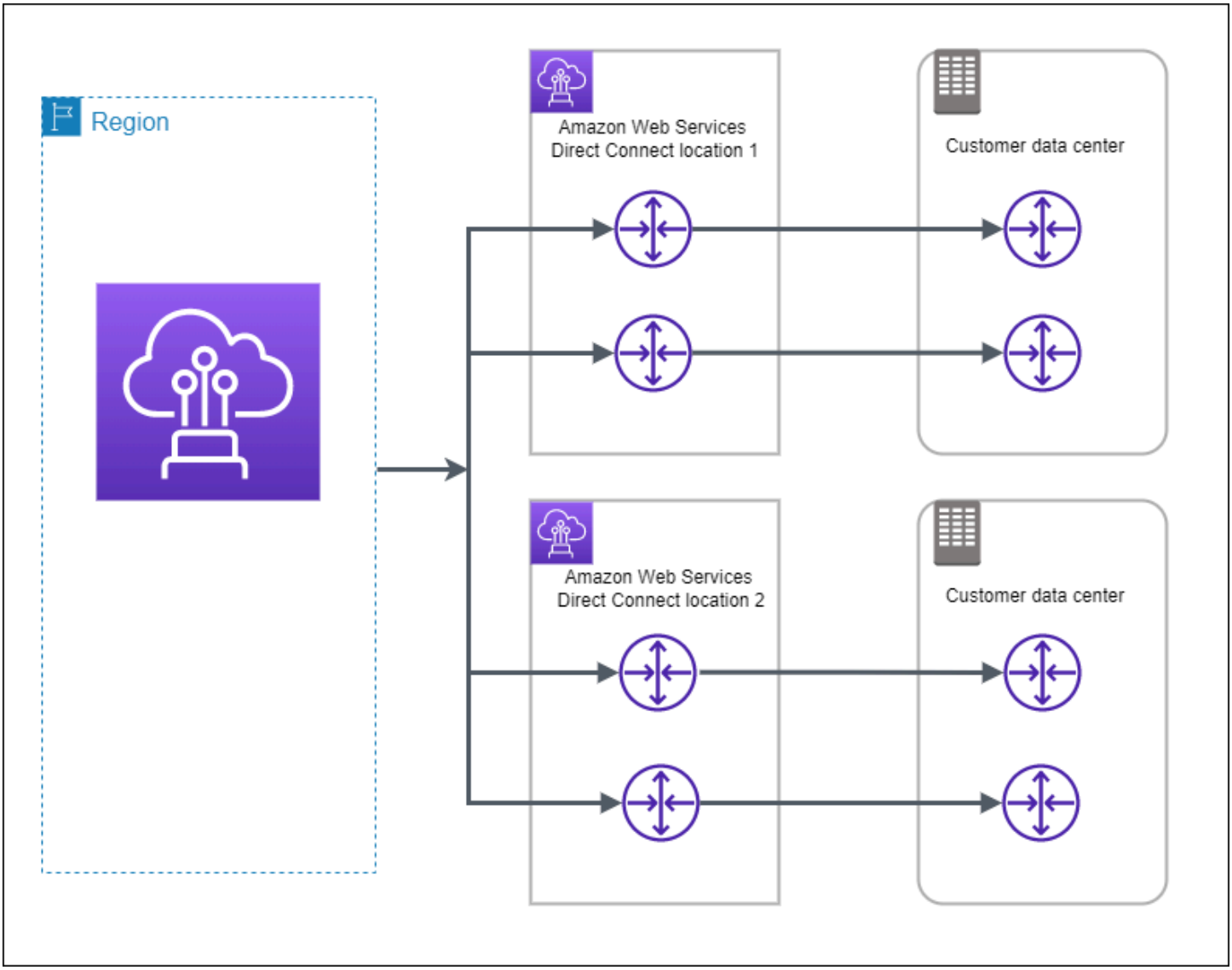
Assicurati di disporre delle informazioni seguenti prima di iniziare la configurazione:

- Il modello di resilienza che desideri utilizzare.
- La velocità, la posizione e il partner per tutte le connessioni.

  È necessaria solo la velocità per una connessione.

Resilienza massima

È possibile ottenere la massima resilienza per carichi di lavoro critici utilizzando connessioni separate che terminano su dispositivi separati in più di una posizione (come mostrato nella figura seguente). Questo modello fornisce resilienza contro i guasti del dispositivo, della connettività e della posizione completa. La figura seguente mostra entrambe le connessioni da ogni data center del cliente che si dirigono verso le stesse posizioni. AWS Direct Connect Facoltativamente, puoi fare in modo che ogni connessione da un data center del cliente vada a località diverse.



Le seguenti procedure mostrano come utilizzare il AWS Direct Connect Resiliency Toolkit per configurare un modello di massima resilienza.

Argomenti

Passaggio 1: iscriviti a AWS

Per utilizzarlo AWS Direct Connect, hai bisogno di un AWS account se non ne hai già uno.

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Fase 2: configurazione del modello di resilienza

Per configurare un modello di resilienza massima

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Connessioni, quindi Crea connessione.
3. In Connection ordering type (Tipo di ordinamento connessione), scegliere Connection wizard (Procedura guidata di connessione).
4. In Resiliency level (Livello di resilienza), scegliere Maximum Resiliency (Resilienza massima), quindi Next (Avanti).
5. Nel riquadro Configure connections (Configura connessioni), in Connection settings (Impostazioni connessione), procedere come segue:

   a. Per Bandwidth (Larghezza di banda), scegliere la larghezza di banda della connessione dedicata.

      Questa larghezza di banda si applica a tutte le connessioni create.

   b. Per il primo fornitore di servizi di localizzazione, seleziona la AWS Direct Connect posizione appropriata per la connessione dedicata.

   c. Se applicabile, per First Sub Location (Sede secondaria principale), scegliere il piano più vicino a te o al provider di rete. Questa opzione è disponibile soltanto se nella sede scelta sono presenti stanze meet-me (MMR, Meet-Me Room) su più piani dell'edificio.

   d. Se hai selezionato Other (Altro) per First location service provider (Provider di servizi sede principale), per Name of other provider (Nome di altro provider), immetti il nome del partner utilizzato.

   e. Per Provider di servizi di seconda localizzazione, seleziona la AWS Direct Connect località appropriata.

f. Se applicabile, per Second Sub location (Seconda sede secondaria), scegliere il piano più vicino a te o al provider di rete. Questa opzione è disponibile soltanto se nella sede scelta sono presenti stanze meet-me (MMR, Meet-Me Room) su più piani dell'edificio.

g. Se si seleziona Other (Altro) per Second location service provider (Provider di servizi di seconda sede), per Name of other provider (Nome di altro provider), immettere il nome del partner utilizzato.

h. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

6. Seleziona Successivo.
7. Esaminare le connessioni, quindi scegliere Continue (Continua).

Se i LOA sono pronti, è possibile scegliere Download LOA (Scarica LOA), quindi fare clic su Continue (Continua).

Possono essere necessarie fino a 72 ore AWS per esaminare la richiesta e fornire una porta per la connessione. Durante questo intervallo di tempo, potresti ricevere un'e-mail con una richiesta di ulteriori informazioni sul caso d'uso o sulla sede specificata. L'e-mail viene inviata all'indirizzo e-mail che hai utilizzato al momento della registrazione AWS. Devi rispondere entro 7 giorni o la connessione verrà eliminata.

Fase 3: creazione delle interfacce virtuali

È possibile creare un'interfaccia virtuale privata per connettersi al tuo VPC. In alternativa, puoi creare un'interfaccia virtuale pubblica per connetterti a AWS servizi pubblici che non si trovano in un VPC. Quando crei un'interfaccia virtuale privata su un VPC, ti servirà un'interfaccia virtuale privata per ogni VPC a cui ti connetti. Ad esempio, ti serviranno tre interfacce virtuali private per connetterti a tre VPC.

Prima di iniziare, assicurati di disporre delle informazioni riportate di seguito:

Risorsa	Informazioni obbligatorie
Connessione	La AWS Direct Connect connessione o il gruppo di aggregazione dei link (LAG) per cui stai creando l'interfaccia virtuale.
Nome dell'interfaccia virtuale	Un nome per l'interfaccia virtuale.
Proprietario dell'interfaccia virtuale	Se stai creando l'interfaccia virtuale per un altro account, hai bisogno dell'ID dell'altro AWS account.
(Solo interfaccia virtuale privata) Connessione	Per connetterti a un VPC nella stessa AWS regione, è necessario il gateway privato virtuale per il tuo VPC. L'ASN per il lato Amazon della sessione BGP viene ereditato dal gateway virtuale privato. Quando crei un gateway privato virtuale, puoi specificare il tuo ASN privato. Altrimenti, Amazon fornisce un ASN predefinito. Per ulteriori informazioni, consulta l'articolo relativo alla Creare un gateway virtuale privato nella Guida dell'utente di Amazon VPC. Per la connessione a un VPC tramite un gateway Direct Connect, è necessari o il gateway Direct Connect. Per ulteriori informazioni, consulta Gateway Direct Connect.
VLAN	Un tag Rete dell'area locale virtuale (VLAN) univoco che non è già in uso sulla tua connessione. Il valore deve essere compreso tra 1 e 4094 e deve essere conforme allo standard Ethernet 802.1Q. Questo tag è necessario per tutto il traffico che attraversa la connessione AWS Direct Connect . Se disponi di una connessione ospitata, il tuo AWS Direct Connect partner offre questo valore. Non è possibile modificare il valore dopo aver creato l'interfaccia virtuale.
Indirizzi IP peer	Un'interfaccia virtuale può supportare una sessione di peering BGP per IPv4, IPv6 o una di ciascuna (dual-stack). Non utilizzare IP elastici (EIP) o Bring your own IP address (BYOIP) dal pool Amazon per creare un'interfaccia virtuale pubblica. Non puoi creare più sessioni BGP per la stessa famiglia di indirizzi IP sulla stessa interfaccia virtuale. Gli intervalli di indirizzi IP vengono assegnati a ciascuna estremità dell'interfaccia virtuale per la sessione di peering BGP.

Risorsa	Informazioni obbligatorie

	• IPv4:
	  • (Solo interfaccia virtuale pubblica) È necessario specificare indirizzi IPv4 pubblici univoci di cui si è proprietari. Il valore può essere uno dei seguenti:
	  • Un CIDR IPv4 di proprietà del cliente
	
	Questi possono essere qualsiasi IP pubblico (di proprietà del cliente o fornito da AWS), ma è necessario utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del router. AWS Ad esempio, se si assegna un `/31` intervallo, ad esempio, è possibile utilizzarlo per l'IP peer e `203.0.113.0` per l'IP peer. `203.0.113.0/31` `203.0.113.1` AWS Oppure, se allocate un `/24` intervallo, ad esempio, potreste utilizzarlo `198.51.100.10` per il vostro IP peer e `198.51.100.20` per l'IP peer. `198.51.100.0/24` AWS
	  • Un intervallo IP di proprietà del AWS Direct Connect partner o dell'ISP, insieme a un'autorizzazione LOA-CFA
	  • Un AWS CIDR /31 fornito. In caso contrario, contatta AWS Support per richiedere un CIDR IPv4 pubblico (e fornire un caso d'uso nella richiesta).
	
	Note
	Non possiamo garantire che saremo in grado di soddisfare tutte le richieste di indirizzi IPv4 pubblici AWS forniti.
	  • (Solo interfaccia virtuale privata) Amazon può generare indirizzi IPv4 privati per te. Se ne specifichi uno personalizzato, assicurati di specifica re i CIDR privati solo per l'interfaccia del router e l'interfaccia AWS Direct Connect. Ad esempio, non specificare altri indirizzi IP dalla rete locale. Analogamente a un'interfaccia virtuale pubblica, è necessari o utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del AWS router. Ad esempio, se si assegna un `/30` intervallo, ad esempio`192.168.0.0/30` , è possibile utilizzarlo per l'IP peer e `192.168.0.1` `192.168.0.2` per l'IP peer. AWS

Risorsa	Informazioni obbligatorie
	• IPv6: Amazon alloca automaticamente un CIDR IPv6 /125. Non puoi specificare indirizzi IPv6 peer personali.
Famiglia di indirizzi	Se la sessione di peering BGP sarà su IPv4 o IPv6.
Informazioni BGP	• Un numero di sistema autonomo (ASN) del Border Gateway Protocol (BGP) pubblico o privato per il lato della sessione BGP. Se utilizzi un ASN pubblico, devi esserne proprietario. Se utilizzi un ASN privato, puoi impostare un valore ASN personalizzato. Per un ASN a 16 bit, il valore deve Esser compreso nell'intervallo da 64512 a 65534. Per un ASN a 32 bit, il valore deve essere compreso nell'intervallo da 1 a 2147483647. La prependenza del sistema autonomo (AS) non funziona se utilizzi un ASN privato per un'interfaccia virtuale pubblica. • AWS abilita MD5 per impostazione predefinita. Tale opzione non è modificabile. • Una chiave di autenticazione MD5 BGP. Puoi fornire il tuo oppure lasciare che Amazon ne generi uno per te.

Risorsa	Informazioni obbligatorie

(Solo interfaccia virtuale pubblica) Prefissi che desideri pubblicizzare	Percorsi IPv4 pubblici o percorsi IPv6 per la pubblicità tramite BGP. Devi pubblicizzare almeno un prefisso utilizzando BGP, fino a un massimo di 1.000 prefissi.
	• IPv4: il CIDR IPv4 può sovrapporsi a un altro CIDR IPv4 pubblico annunciato o utilizzando quando una delle seguenti condizioni è vera: AWS Direct Connect
	  • I CIDR AWS provengono da diverse regioni. Assicurati di applicare i tag della community BGP ai prefissi pubblici.
	  • Utilizzi AS_PATH quando disponi di un ASN pubblico in una configurazione attiva/passiva.
	  Per ulteriori informazioni, consulta la Policy di routing e community BGP.
	• IPv6: specificare una lunghezza di prefisso di /64 o inferiore.
	• È possibile aggiungere prefissi aggiuntivi a un file VIF pubblico esistente e pubblicizzarli contattando AWS support. Nel caso di supporto, fornisci un elenco di prefissi CIDR aggiuntivi che desideri aggiungere al file VIF pubblico e pubblicizzare.
	• Puoi specificare qualsiasi lunghezza del prefisso su un'interfaccia virtuale pubblica Direct Connect. IPv4 dovrebbe supportare qualsiasi cosa compresa tra /1 e /32 e IPv6 dovrebbe supportare qualsiasi cosa compresa tra /1 - /64.

Risorsa	Informazioni obbligatorie
(Solo interfaccia virtuale privata) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti in eccesso. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 9001 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettività di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I jumbo frame si applicano solo ai percorsi propagati da. AWS Direct Connect Se aggiungi route statiche a una tabella di routing che punta al gateway privato virtuale, il traffico instradato attraverso le route statiche viene inviato utilizzando 1500 MTU. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.
(Solo interfaccia virtuale Transit) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti superati. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 8500 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettiv ità di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I frame jumbo sono supportati fino a 8500 MTU per Direct Connect. Le route statiche e le rotte propagate configurate nella tabella di routing di Transit Gateway supporteranno i frame jumbo, incluse le istanze EC2 con voci della tabella di routing statica VPC al collegamento del gateway di transito alla VPN. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.

Se i prefissi pubblici o gli ASN appartengono a un ISP o a un operatore di rete, richiederemo ulteriori informazioni. Potrebbe trattarsi di un documento con l'intestazione ufficiale dell'azienda o di un'e-mail inviata dal nome di dominio aziendale per verificare che il prefisso di rete/ASN possa essere utilizzato da te.

Quando si crea un'interfaccia virtuale pubblica, possono essere necessarie fino a 72 ore per AWS esaminare e approvare la richiesta.

Per effettuare il provisioning di un'interfaccia virtuale pubblica su servizi non-VPC

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Virtual interface type (Tipo di interfaccia virtuale), per Type (Tipo) scegliere Public (Pubblico).
5. In Public virtual interface settings (Impostazioni interfaccia virtuale pubblica), procedere come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

   b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

   c. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

   d. In BGP ASN, immettere il Border Gateway Protocol (BGP) Autonomous System Number (ASN) del gateway.

      I valori validi sono 1-2147483647.
6. In Additional settings (Impostazioni aggiuntive), procedere come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

      [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

      - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
      - In Amazon router peer IP (IP peer del router Amazon), immettere l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

      [IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

   b. Per fornire la propria chiave BGP, immettere la chiave MD5 del BGP.

Se non si inserisce un valore, procederemo a generare una chiave BGP.

c. Per pubblicizzare prefissi per Amazon, in Prefissi da pubblicizzare, immetti gli indirizzi CIDR IPv4 di destinazione (separati da virgole) a cui instradare il traffico tramite l'interfaccia virtuale.

d. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).

Per effettuare il provisioning di un'interfaccia virtuale privata su un VPC

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Tipo di interfaccia virtuale, per Tipo scegli Pubblico.
5. In Impostazioni dell'interfaccia virtuale pubblica, procedi come segue:

a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

c. Per il Tipo di gateway, scegli Gateway privato virtuale oGateway Direct Connect.

d. Per Proprietario dell'interfaccia virtuale, scegli Altro AWS account, quindi inserisci l' AWS account.

e. Per Gateway virtuale privato, scegli il gateway virtuale privato da usare per l'interfaccia.

f. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

g. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

I valori validi sono compresi tra 1 e 2147483647.

6. In Impostazioni aggiuntive, procedi come segue:

a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

   [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

   - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
   - In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

   > **Important**
   >
   > Se consenti l' AWS assegnazione automatica degli indirizzi IPv4, verrà allocato un CIDR /29 da 169.254.0.0/16 IPv4 Link-Local secondo RFC 3927 per la connettività. point-to-point AWS non consiglia questa opzione se si intende utilizzare l'indirizzo IP peer del router del cliente come origine e/o destinazione per il traffico VPC. Ti consigliamo invece di utilizzare RFC 1918 o un altro indirizzo e di specificare manualmente l'indirizzo.
   >
   > - Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.
   > - Per ulteriori informazioni su RFC 3927, consulta Dynamic Configuration of IPv4 Link-Local Addresses.

   [IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

b. Per modificare l'unità di trasmissione massima (MTU) da 1500 (predefinito) a 9001 (frame jumbo), seleziona Jumbo MTU (MTU size 9001) (MTU jumbo - dimensione della MTU 9001).

c. (Facoltativo) In Abilita SiteLink, scegli Abilitato per abilitare la connettività diretta tra i punti di presenza Direct Connect.

d. (Facoltativo) Aggiunta o rimozione di un tag.

   [Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).

Passaggio 4: Verificare la configurazione di resilienza dell'interfaccia virtuale

Dopo aver stabilito le interfacce virtuali verso il AWS Cloud o Amazon VPC, esegui un test di failover dell'interfaccia virtuale per verificare che la configurazione soddisfi i requisiti di resilienza. Per ulteriori informazioni, consulta the section called “Test di failover AWS Direct Connect”.

Passaggio 5: Verificare la connettività delle interfacce virtuali

Dopo aver stabilito le interfacce virtuali verso il AWS Cloud o Amazon VPC, puoi verificare AWS Direct Connect la connessione utilizzando le seguenti procedure.

Per verificare la connessione dell'interfaccia virtuale al Cloud AWS

- Esegui `traceroute` e verifica che l' AWS Direct Connect identificatore sia presente nella traccia di rete.

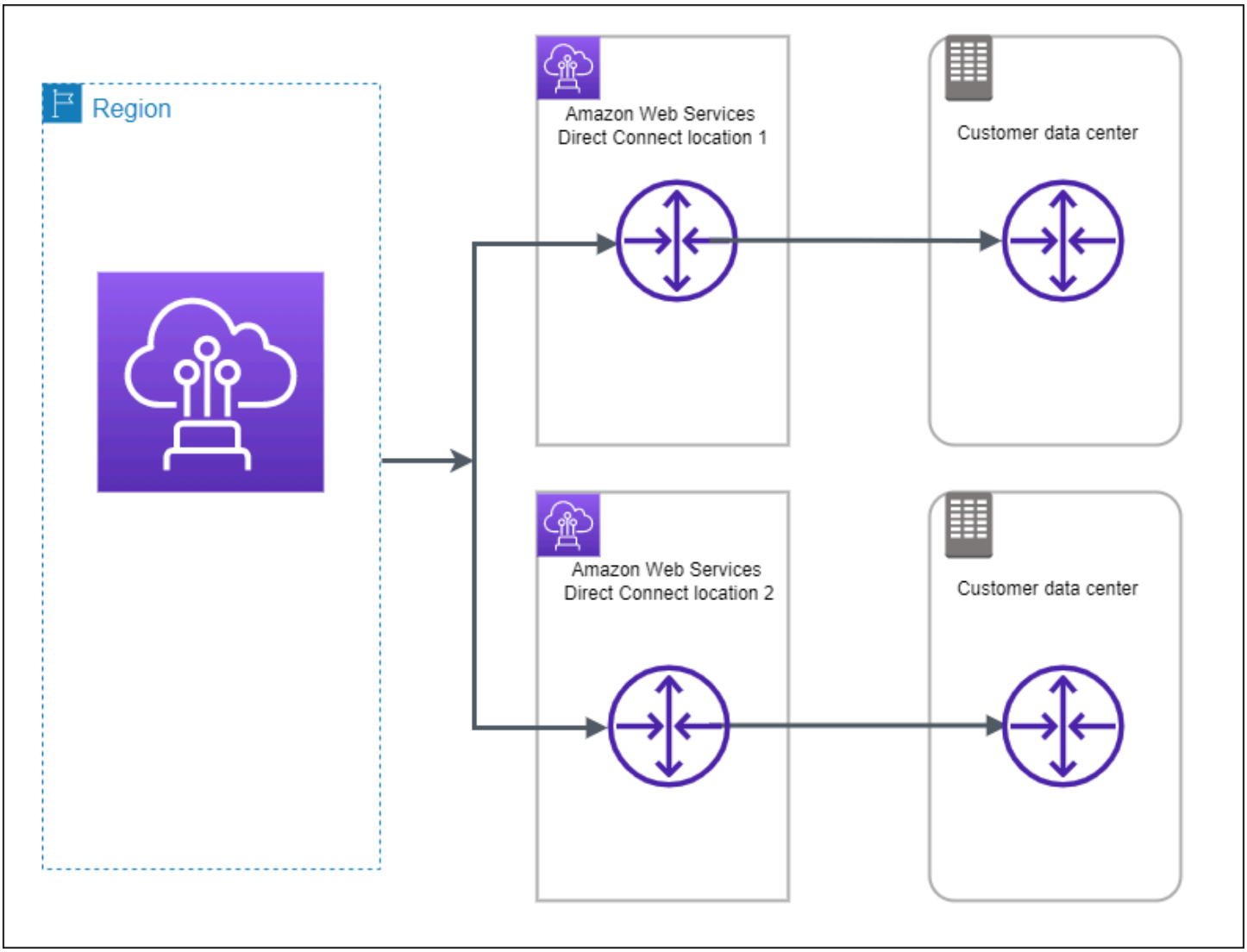
Verificare la connessione dell'interfaccia virtuale su Amazon VPC

1. Tramite un AMI per cui è possibile effettuare il ping, ad esempio un AMI di Amazon Linux, avvia un'istanza EC2 nel VPC associato al gateway virtuale privato. Le AMI di Amazon Linux sono disponibili nel menu Avvio rapido quando si utilizza la procedura guidata per avviare le istanze nella console Amazon EC2. Per ulteriori informazioni, consulta Launch an Instance nella Amazon EC2 User Guide. Assicurati che il gruppo di sicurezza associato all'istanza includa una regola che consenta il traffico ICMP in entrata (per la richiesta di ping).
2. Dopo che l'istanza è in esecuzione, recupera l'indirizzo IPv4 privato corrispondente (per esempio, 10.0.0.4). La console Amazon EC2 visualizza l'indirizzo come parte dei dettagli dell'istanza.
3. Effettua il ping dell'indirizzo IPv4 privato e ricevi una risposta.

Elevata resilienza

È possibile ottenere un'elevata resilienza per carichi di lavoro critici utilizzando due connessioni singole a più posizioni (come illustrato nella figura seguente). Questo modello fornisce resilienza

agli errori di connettività causati da un taglio di fibra o da un guasto del dispositivo. Inoltre, aiuta a prevenire un errore di percorso completo.



Le seguenti procedure mostrano come utilizzare il AWS Direct Connect Resiliency Toolkit per configurare un modello ad alta resilienza.

Argomenti

- Passaggio 1: iscriviti a AWS
- Fase 2: configurazione del modello di resilienza
- Fase 3: creazione delle interfacce virtuali
- Passaggio 4: Verificare la configurazione di resilienza dell'interfaccia virtuale
- Passaggio 5: Verificare la connettività delle interfacce virtuali

Passaggio 1: iscriviti a AWS

Per utilizzarlo AWS Direct Connect, hai bisogno di un AWS account se non ne hai già uno.

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Fase 2: configurazione del modello di resilienza

Per configurare un modello ad elevata resilienza

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Connessioni, quindi Crea connessione.
3. In Connection ordering type (Tipo di ordinamento connessione), scegliere Connection wizard (Procedura guidata di connessione).
4. In Resiliency level (Livello di resilienza), scegliere High Resiliency (Resilienza elevata), quindi Next (Avanti).
5. Nel riquadro Configure connections (Configura connessioni), in Connection settings (Impostazioni connessione), procedere come segue:

   a. Per bandwidth (Larghezza di banda), scegliere la larghezza di banda della connessione.

      Questa larghezza di banda si applica a tutte le connessioni create.

   b. Per il primo fornitore di servizi di localizzazione, seleziona la AWS Direct Connect posizione appropriata.

   c. Se applicabile, per First Sub Location (Sede secondaria principale), scegliere il piano più vicino a te o al provider di rete. Questa opzione è disponibile soltanto se nella sede scelta sono presenti stanze meet-me (MMR, Meet-Me Room) su più piani dell'edificio.

   d. Se hai selezionato Other (Altro) per First location service provider (Provider di servizi sede principale), per Name of other provider (Nome di altro provider), immetti il nome del partner utilizzato.

   e. Per Provider di servizi di seconda localizzazione, seleziona la AWS Direct Connect località appropriata.

   f. Se applicabile, per Second Sub location (Seconda sede secondaria), scegliere il piano più vicino a te o al provider di rete. Questa opzione è disponibile soltanto se nella sede scelta sono presenti stanze meet-me (MMR, Meet-Me Room) su più piani dell'edificio.

   g. Se si seleziona Other (Altro) per Second location service provider (Provider di servizi di seconda sede), per Name of other provider (Nome di altro provider), immettere il nome del partner utilizzato.

   h. (Facoltativo) Aggiunta o rimozione di un tag.

      [Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

6. Seleziona Successivo.
7. Esaminare le connessioni, quindi scegliere Continue (Continua).

   Se i LOA sono pronti, è possibile scegliere Download LOA (Scarica LOA), quindi fare clic su Continue (Continua).

   Possono essere necessarie fino a 72 ore AWS per esaminare la richiesta e fornire una porta per la connessione. Durante questo intervallo di tempo, potresti ricevere un'e-mail con una richiesta di ulteriori informazioni sul caso d'uso o sulla sede specificata. L'e-mail viene inviata all'indirizzo e-mail che hai utilizzato al momento della registrazione AWS. Devi rispondere entro 7 giorni o la connessione verrà eliminata.

Fase 3: creazione delle interfacce virtuali

È possibile creare un'interfaccia virtuale privata per connettersi al tuo VPC. In alternativa, puoi creare un'interfaccia virtuale pubblica per connetterti a AWS servizi pubblici che non si trovano in un VPC. Quando crei un'interfaccia virtuale privata su un VPC, ti servirà un'interfaccia virtuale privata per ogni VPC a cui ti connetti. Ad esempio, ti serviranno tre interfacce virtuali private per connetterti a tre VPC.

Prima di iniziare, assicurati di disporre delle informazioni riportate di seguito:

Risorsa	Informazioni obbligatorie
Connessione	La AWS Direct Connect connessione o il gruppo di aggregazione dei link (LAG) per cui stai creando l'interfaccia virtuale.
Nome dell'interfaccia virtuale	Un nome per l'interfaccia virtuale.
Proprietario dell'interfaccia virtuale	Se stai creando l'interfaccia virtuale per un altro account, hai bisogno dell'ID dell'altro AWS account.

Risorsa	Informazioni obbligatorie
(Solo interfaccia virtuale privata) Connessione	Per connetterti a un VPC nella stessa AWS regione, è necessario il gateway privato virtuale per il tuo VPC. L'ASN per il lato Amazon della sessione BGP viene ereditato dal gateway virtuale privato. Quando crei un gateway privato virtuale, puoi specificare il tuo ASN privato. Altrimenti, Amazon fornisce un ASN predefinito. Per ulteriori informazioni, consulta l'articolo relativo alla Creare un gateway virtuale privato nella Guida dell'utente di Amazon VPC. Per la connessione a un VPC tramite un gateway Direct Connect, è necessari o il gateway Direct Connect. Per ulteriori informazioni, consulta Gateway Direct Connect.
VLAN	Un tag Rete dell'area locale virtuale (VLAN) univoco che non è già in uso sulla tua connessione. Il valore deve essere compreso tra 1 e 4094 e deve essere conforme allo standard Ethernet 802.1Q. Questo tag è necessario per tutto il traffico che attraversa la connessione AWS Direct Connect . Se disponi di una connessione ospitata, il tuo AWS Direct Connect partner offre questo valore. Non è possibile modificare il valore dopo aver creato l'interfaccia virtuale.

Risorsa	Informazioni obbligatorie
Indirizzi IP peer	Un'interfaccia virtuale può supportare una sessione di peering BGP per IPv4, IPv6 o una di ciascuna (dual-stack). Non utilizzare IP elastici (EIP) o Bring your own IP address (BYOIP) dal pool Amazon per creare un'interfaccia virtuale pubblica. Non puoi creare più sessioni BGP per la stessa famiglia di indirizzi IP sulla stessa interfaccia virtuale. Gli intervalli di indirizzi IP vengono assegnati a ciascuna estremità dell'interfaccia virtuale per la sessione di peering BGP. • IPv4: • (Solo interfaccia virtuale pubblica) È necessario specificare indirizzi IPv4 pubblici univoci di cui si è proprietari. Il valore può essere uno dei seguenti: • Un CIDR IPv4 di proprietà del cliente Questi possono essere qualsiasi IP pubblico (di proprietà del cliente o fornito da AWS), ma è necessario utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del router. AWS Ad esempio, se si assegna un `/31` intervallo, ad esempio, è possibile utilizzarlo per l'IP peer e `203.0.113.0` per l'IP peer. `203.0.113.0/31` `203.0.113.1` AWS Oppure, se allocate un `/24` intervallo, ad esempio, potreste utilizzarlo `198.51.100.10` per il vostro IP peer e `198.51.100.20` per l'IP peer. `198.51.100.0/24` AWS • Un intervallo IP di proprietà del AWS Direct Connect partner o dell'ISP, insieme a un'autorizzazione LOA-CFA • Un AWS CIDR /31 fornito. In caso contrario, contatta AWS Support per richiedere un CIDR IPv4 pubblico (e fornire un caso d'uso nella richiesta). **Note** Non possiamo garantire che saremo in grado di soddisfare tutte le richieste di indirizzi IPv4 pubblici AWS forniti. • (Solo interfaccia virtuale privata) Amazon può generare indirizzi IPv4 privati per te. Se ne specifichi uno personalizzato, assicurati di specifica

Risorsa	Informazioni obbligatorie
	re i CIDR privati solo per l'interfaccia del router e l'interfaccia AWS Direct Connect. Ad esempio, non specificare altri indirizzi IP dalla rete locale. Analogamente a un'interfaccia virtuale pubblica, è necessari o utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del AWS router. Ad esempio, se si assegna un `/30` intervallo, ad esempio`192.168.0.0/30` , è possibile utilizzarlo per l'IP peer e `192.168.0.1` `192.168.0.2` per l'IP peer. AWS • IPv6: Amazon alloca automaticamente un CIDR IPv6 /125. Non puoi specificare indirizzi IPv6 peer personali.
Famiglia di indirizzi	Se la sessione di peering BGP sarà su IPv4 o IPv6.
Informazioni BGP	• Un numero di sistema autonomo (ASN) del Border Gateway Protocol (BGP) pubblico o privato per il lato della sessione BGP. Se utilizzi un ASN pubblico, devi esserne proprietario. Se utilizzi un ASN privato, puoi impostare un valore ASN personalizzato. Per un ASN a 16 bit, il valore deve Esser compreso nell'intervallo da 64512 a 65534. Per un ASN a 32 bit, il valore deve essere compreso nell'intervallo da 1 a 2147483647. La prependenza del sistema autonomo (AS) non funziona se utilizzi un ASN privato per un'interfaccia virtuale pubblica. • AWS abilita MD5 per impostazione predefinita. Tale opzione non è modificabile. • Una chiave di autenticazione MD5 BGP. Puoi fornire il tuo oppure lasciare che Amazon ne generi uno per te.

Risorsa	Informazioni obbligatorie

(Solo interfaccia virtuale pubblica) Prefissi che desideri pubblicizzare	Percorsi IPv4 pubblici o percorsi IPv6 per la pubblicità tramite BGP. Devi pubblicizzare almeno un prefisso utilizzando BGP, fino a un massimo di 1.000 prefissi.
	• IPv4: il CIDR IPv4 può sovrapporsi a un altro CIDR IPv4 pubblico annunciato o utilizzando quando una delle seguenti condizioni è vera: AWS Direct Connect
	  • I CIDR AWS provengono da diverse regioni. Assicurati di applicare i tag della community BGP ai prefissi pubblici.
	  • Utilizzi AS_PATH quando disponi di un ASN pubblico in una configurazione attiva/passiva.
	  Per ulteriori informazioni, consulta la Policy di routing e community BGP.
	• IPv6: specificare una lunghezza di prefisso di /64 o inferiore.
	• È possibile aggiungere prefissi aggiuntivi a un file VIF pubblico esistente e pubblicizzarli contattando AWS support. Nel caso di supporto, fornisci un elenco di prefissi CIDR aggiuntivi che desideri aggiungere al file VIF pubblico e pubblicizzare.
	• Puoi specificare qualsiasi lunghezza del prefisso su un'interfaccia virtuale pubblica Direct Connect. IPv4 dovrebbe supportare qualsiasi cosa compresa tra /1 e /32 e IPv6 dovrebbe supportare qualsiasi cosa compresa tra /1 - /64.

Risorsa	Informazioni obbligatorie
(Solo interfaccia virtuale privata) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti in eccesso. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 9001 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettività di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I jumbo frame si applicano solo ai percorsi propagati da. AWS Direct Connect Se aggiungi route statiche a una tabella di routing che punta al gateway privato virtuale, il traffico instradato attraverso le route statiche viene inviato utilizzando 1500 MTU. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.
(Solo interfaccia virtuale Transit) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti superati. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 8500 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettiv ità di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I frame jumbo sono supportati fino a 8500 MTU per Direct Connect. Le route statiche e le rotte propagate configurate nella tabella di routing di Transit Gateway supporteranno i frame jumbo, incluse le istanze EC2 con voci della tabella di routing statica VPC al collegamento del gateway di transito alla VPN. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.

Se i tuoi prefissi o ASN pubblici appartengono a un ISP o a un gestore di rete, AWS ti richiede informazioni aggiuntive. Potrebbe trattarsi di un documento con l'intestazione ufficiale dell'azienda o di un'e-mail inviata dal nome di dominio aziendale per verificare che il prefisso di rete/ASN possa essere utilizzato da te.

Quando crei un'interfaccia virtuale pubblica, possono essere necessarie fino a 72 ore per esaminare e AWS approvare la richiesta.

Per effettuare il provisioning di un'interfaccia virtuale pubblica su servizi non-VPC

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Virtual interface type (Tipo di interfaccia virtuale), per Type (Tipo) scegliere Public (Pubblico).
5. In Public virtual interface settings (Impostazioni interfaccia virtuale pubblica), procedere come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

   b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

   c. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

   d. In BGP ASN, immettere il Border Gateway Protocol (BGP) Autonomous System Number (ASN) del gateway.

      I valori validi sono 1-2147483647.
6. In Additional settings (Impostazioni aggiuntive), procedere come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

      [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

      - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
      - In Amazon router peer IP (IP peer del router Amazon), immettere l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

      [IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

   b. Per fornire la propria chiave BGP, immettere la chiave MD5 del BGP.

Se non si inserisce un valore, procederemo a generare una chiave BGP.

c. Per pubblicizzare prefissi per Amazon, in Prefissi da pubblicizzare, immetti gli indirizzi CIDR IPv4 di destinazione (separati da virgole) a cui instradare il traffico tramite l'interfaccia virtuale.

d. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).

Per effettuare il provisioning di un'interfaccia virtuale privata su un VPC

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Tipo di interfaccia virtuale, per Tipo scegli Pubblico.
5. In Impostazioni dell'interfaccia virtuale pubblica, procedi come segue:

a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

c. Per il Tipo di gateway, scegli Gateway privato virtuale oGateway Direct Connect.

d. Per Proprietario dell'interfaccia virtuale, scegli Altro AWS account, quindi inserisci l' AWS account.

e. Per Gateway virtuale privato, scegli il gateway virtuale privato da usare per l'interfaccia.

f. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

g. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

I valori validi sono compresi tra 1 e 2147483647.

6. In Impostazioni aggiuntive, procedi come segue:

a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

   [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

   - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
   - In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

   > **Important**
   >
   > Se consenti l' AWS assegnazione automatica degli indirizzi IPv4, verrà allocato un CIDR /29 da 169.254.0.0/16 IPv4 Link-Local secondo RFC 3927 per la connettività. point-to-point AWS non consiglia questa opzione se si intende utilizzare l'indirizzo IP peer del router del cliente come origine e/o destinazione per il traffico VPC. Ti consigliamo invece di utilizzare RFC 1918 o un altro indirizzo e di specificare manualmente l'indirizzo.
   >
   > - Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.
   > - Per ulteriori informazioni su RFC 3927, consulta Dynamic Configuration of IPv4 Link-Local Addresses.

   [IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

b. Per modificare l'unità di trasmissione massima (MTU) da 1500 (predefinito) a 9001 (frame jumbo), seleziona Jumbo MTU (MTU size 9001) (MTU jumbo - dimensione della MTU 9001).

c. (Facoltativo) In Abilita SiteLink, scegli Abilitato per abilitare la connettività diretta tra i punti di presenza Direct Connect.

d. (Facoltativo) Aggiunta o rimozione di un tag.

   [Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).

Passaggio 4: Verificare la configurazione di resilienza dell'interfaccia virtuale

Dopo aver stabilito le interfacce virtuali verso il AWS Cloud o Amazon VPC, esegui un test di failover dell'interfaccia virtuale per verificare che la configurazione soddisfi i requisiti di resilienza. Per ulteriori informazioni, consulta the section called “Test di failover AWS Direct Connect”.

Passaggio 5: Verificare la connettività delle interfacce virtuali

Dopo aver stabilito le interfacce virtuali verso il AWS Cloud o Amazon VPC, puoi verificare AWS Direct Connect la connessione utilizzando le seguenti procedure.

Per verificare la connessione dell'interfaccia virtuale al Cloud AWS

- Esegui `traceroute` e verifica che l' AWS Direct Connect identificatore sia presente nella traccia di rete.

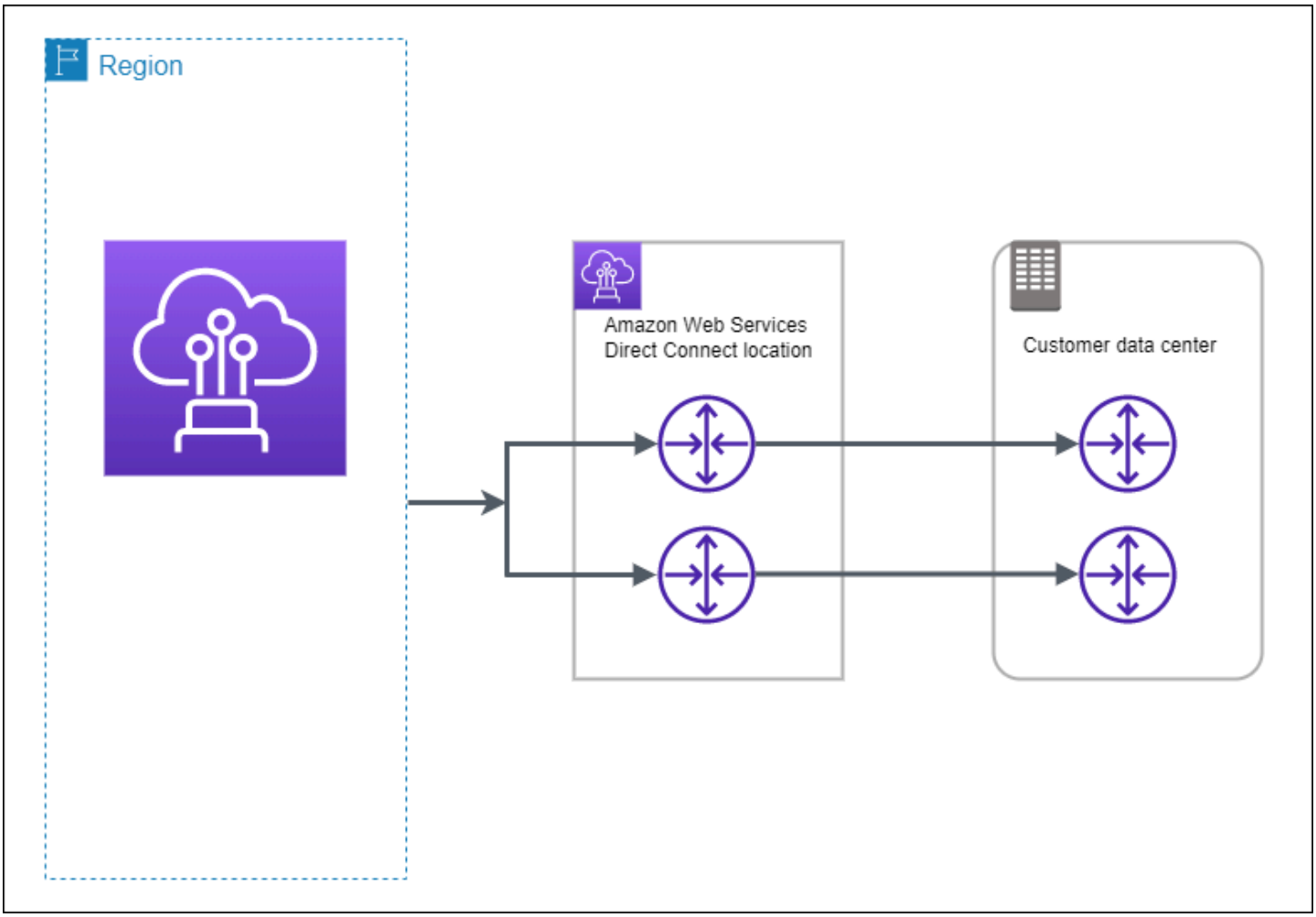
Verificare la connessione dell'interfaccia virtuale su Amazon VPC

1. Tramite un AMI per cui è possibile effettuare il ping, ad esempio un AMI di Amazon Linux, avvia un'istanza EC2 nel VPC associato al gateway virtuale privato. Le AMI di Amazon Linux sono disponibili nel menu Avvio rapido quando si utilizza la procedura guidata per avviare le istanze nella console Amazon EC2. Per ulteriori informazioni, consulta Launch an Instance nella Amazon EC2 User Guide. Assicurati che il gruppo di sicurezza associato all'istanza includa una regola che consenta il traffico ICMP in entrata (per la richiesta di ping).
2. Dopo che l'istanza è in esecuzione, recupera l'indirizzo IPv4 privato corrispondente (per esempio, 10.0.0.4). La console Amazon EC2 visualizza l'indirizzo come parte dei dettagli dell'istanza.
3. Effettua il ping dell'indirizzo IPv4 privato e ricevi una risposta.

Sviluppo e test

È possibile ottenere la resilienza di sviluppo e test per carichi di lavoro non critici utilizzando connessioni separate che terminano su dispositivi separati in un'unica posizione (come mostrato

nella figura seguente). Questo modello fornisce resilienza ai guasti del dispositivo, ma non fornisce resilienza ai guasti della posizione.



Le seguenti procedure mostrano come utilizzare il AWS Direct Connect Resiliency Toolkit per configurare un modello di resilienza per lo sviluppo e il test.

Argomenti

- Fase 1: Iscriviti a AWS
- Fase 2: configurazione del modello di resilienza
- Fase 3: Creazione di un'interfaccia virtuale
- Passaggio 4: Verificare la configurazione di resilienza dell'interfaccia virtuale
- Fase 5: Verifica dell'interfaccia virtuale

Fase 1: Iscriviti a AWS

Per utilizzarlo AWS Direct Connect, hai bisogno di un AWS account se non ne hai già uno.

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Fase 2: configurazione del modello di resilienza

Per configurare il modello di resilienza

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Connessioni, quindi Crea connessione.

3. In Connection ordering type (Tipo di ordinamento connessione), scegliere Connection wizard (Procedura guidata di connessione).
4. In Resiliency level (Livello di resilienza), scegliere Development and test (Sviluppo e test), quindi Next (Avanti).
5. Nel riquadro Configure connections (Configura connessioni), in Connection settings (Impostazioni connessione), procedere come segue:

   a. Per bandwidth (Larghezza di banda), scegliere la larghezza di banda della connessione.

      Questa larghezza di banda si applica a tutte le connessioni create.

   b. Per il primo fornitore di servizi di localizzazione, seleziona la AWS Direct Connect posizione appropriata.

   c. Se applicabile, per First Sub Location (Sede secondaria principale), scegliere il piano più vicino a te o al provider di rete. Questa opzione è disponibile soltanto se nella sede scelta sono presenti stanze meet-me (MMR, Meet-Me Room) su più piani dell'edificio.

   d. Se hai selezionato Other (Altro) per First location service provider (Provider di servizi sede principale), per Name of other provider (Nome di altro provider), immetti il nome del partner utilizzato.

   e. (Facoltativo) Aggiunta o rimozione di un tag.

      [Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

      - In Chiave, immetti il nome della chiave.
      - In Valore, immetti il valore della chiave.

      [Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).
6. Seleziona Successivo.
7. Esaminare le connessioni, quindi scegliere Continue (Continua).

   Se i LOA sono pronti, è possibile scegliere Download LOA (Scarica LOA), quindi fare clic su Continue (Continua).

   Possono essere necessarie fino a 72 ore AWS per esaminare la richiesta e fornire una porta per la connessione. Durante questo intervallo di tempo, potresti ricevere un'e-mail con una richiesta di ulteriori informazioni sul caso d'uso o sulla sede specificata. L'e-mail viene inviata all'indirizzo e-mail che hai utilizzato al momento della registrazione AWS. Devi rispondere entro 7 giorni o la connessione verrà eliminata.

Fase 3: Creazione di un'interfaccia virtuale

Per iniziare a utilizzare la AWS Direct Connect connessione, è necessario creare un'interfaccia virtuale. È possibile creare un'interfaccia virtuale privata per connettersi al tuo VPC. In alternativa, puoi creare un'interfaccia virtuale pubblica per connetterti a AWS servizi pubblici che non si trovano in un VPC. Quando crei un'interfaccia virtuale privata su un VPC, ti servirà un'interfaccia virtuale privata per ogni VPC a cui ti connetti. Ad esempio, ti serviranno tre interfacce virtuali private per connetterti a tre VPC.

Prima di iniziare, assicurati di disporre delle informazioni riportate di seguito:

Risorsa	Informazioni obbligatorie
Connessione	La AWS Direct Connect connessione o il gruppo di aggregazione dei link (LAG) per cui stai creando l'interfaccia virtuale.
Nome dell'interfaccia virtuale	Un nome per l'interfaccia virtuale.
Proprietario dell'interfaccia virtuale	Se stai creando l'interfaccia virtuale per un altro account, hai bisogno dell'ID dell'altro AWS account.
(Solo interfaccia virtuale privata) Connessione	Per connetterti a un VPC nella stessa AWS regione, è necessario il gateway privato virtuale per il tuo VPC. L'ASN per il lato Amazon della sessione BGP viene ereditato dal gateway virtuale privato. Quando crei un gateway privato virtuale, puoi specificare il tuo ASN privato. Altrimenti, Amazon fornisce un ASN predefinito. Per ulteriori informazioni, consulta l'articolo relativo alla Creare un gateway virtuale privato nella Guida dell'utente di Amazon VPC. Per la connessione a un VPC tramite un gateway Direct Connect, è necessari o il gateway Direct Connect. Per ulteriori informazioni, consulta Gateway Direct Connect.
VLAN	Un tag Rete dell'area locale virtuale (VLAN) univoco che non è già in uso sulla tua connessione. Il valore deve essere compreso tra 1 e 4094 e deve essere conforme allo standard Ethernet 802.1Q. Questo tag è necessario per tutto il traffico che attraversa la connessione AWS Direct Connect .

Risorsa	Informazioni obbligatorie
	Se disponi di una connessione ospitata, il tuo AWS Direct Connect partner offre questo valore. Non è possibile modificare il valore dopo aver creato l'interfaccia virtuale.

Risorsa	Informazioni obbligatorie

Indirizzi IP peer	Un'interfaccia virtuale può supportare una sessione di peering BGP per IPv4, IPv6 o una di ciascuna (dual-stack). Non utilizzare IP elastici (EIP) o Bring your own IP address (BYOIP) dal pool Amazon per creare un'interfaccia virtuale pubblica. Non puoi creare più sessioni BGP per la stessa famiglia di indirizzi IP sulla stessa interfaccia virtuale. Gli intervalli di indirizzi IP vengono assegnati a ciascuna estremità dell'interfaccia virtuale per la sessione di peering BGP.
	
	• IPv4:
	  • (Solo interfaccia virtuale pubblica) È necessario specificare indirizzi IPv4 pubblici univoci di cui si è proprietari. Il valore può essere uno dei seguenti:
	  • Un CIDR IPv4 di proprietà del cliente
	
	Questi possono essere qualsiasi IP pubblico (di proprietà del cliente o fornito da AWS), ma è necessario utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del router. AWS Ad esempio, se si assegna un `/31` intervallo, ad esempio, è possibile utilizzarlo per l'IP peer e `203.0.113.0` per l'IP peer. `203.0.113.0/31` `203.0.113.1` AWS Oppure, se allocate un `/24` intervallo, ad esempio, potreste utilizzarlo `198.51.100.10` per il vostro IP peer e `198.51.100.20` per l'IP peer. `198.51.100.0/24` AWS
	  • Un intervallo IP di proprietà del AWS Direct Connect partner o dell'ISP, insieme a un'autorizzazione LOA-CFA
	  • Un AWS CIDR /31 fornito. In caso contrario, contatta AWS Support per richiedere un CIDR IPv4 pubblico (e fornire un caso d'uso nella richiesta).
	
	Note
	Non possiamo garantire che saremo in grado di soddisfare tutte le richieste di indirizzi IPv4 pubblici AWS forniti.
	  • (Solo interfaccia virtuale privata) Amazon può generare indirizzi IPv4 privati per te. Se ne specifichi uno personalizzato, assicurati di specifica

Risorsa	Informazioni obbligatorie
	re i CIDR privati solo per l'interfaccia del router e l'interfaccia AWS Direct Connect. Ad esempio, non specificare altri indirizzi IP dalla rete locale. Analogamente a un'interfaccia virtuale pubblica, è necessari o utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del AWS router. Ad esempio, se si assegna un `/30` intervallo, ad esempio`192.168.0.0/30` , è possibile utilizzarlo per l'IP peer e `192.168.0.1` `192.168.0.2` per l'IP peer. AWS • IPv6: Amazon alloca automaticamente un CIDR IPv6 /125. Non puoi specificare indirizzi IPv6 peer personali.
Famiglia di indirizzi	Se la sessione di peering BGP sarà su IPv4 o IPv6.
Informazioni BGP	• Un numero di sistema autonomo (ASN) del Border Gateway Protocol (BGP) pubblico o privato per il lato della sessione BGP. Se utilizzi un ASN pubblico, devi esserne proprietario. Se utilizzi un ASN privato, puoi impostare un valore ASN personalizzato. Per un ASN a 16 bit, il valore deve Esser compreso nell'intervallo da 64512 a 65534. Per un ASN a 32 bit, il valore deve essere compreso nell'intervallo da 1 a 2147483647. La prependenza del sistema autonomo (AS) non funziona se utilizzi un ASN privato per un'interfaccia virtuale pubblica. • AWS abilita MD5 per impostazione predefinita. Tale opzione non è modificabile. • Una chiave di autenticazione MD5 BGP. Puoi fornire il tuo oppure lasciare che Amazon ne generi uno per te.

Risorsa	Informazioni obbligatorie

(Solo interfaccia virtuale pubblica) Prefissi che desideri pubblicizzare	Percorsi IPv4 pubblici o percorsi IPv6 per la pubblicità tramite BGP. Devi pubblicizzare almeno un prefisso utilizzando BGP, fino a un massimo di 1.000 prefissi.
	• IPv4: il CIDR IPv4 può sovrapporsi a un altro CIDR IPv4 pubblico annunciato utilizzando quando una delle seguenti condizioni è vera: AWS Direct Connect
	  • I CIDR AWS provengono da diverse regioni. Assicurati di applicare i tag della community BGP ai prefissi pubblici.
	  • Utilizzi AS_PATH quando disponi di un ASN pubblico in una configurazione attiva/passiva.
	  Per ulteriori informazioni, consulta la Policy di routing e community BGP.
	• IPv6: specificare una lunghezza di prefisso di /64 o inferiore.
	• È possibile aggiungere prefissi aggiuntivi a un file VIF pubblico esistente e pubblicizzarli contattando AWS support. Nel caso di supporto, fornisci un elenco di prefissi CIDR aggiuntivi che desideri aggiungere al file VIF pubblico e pubblicizzare.
	• Puoi specificare qualsiasi lunghezza del prefisso su un'interfaccia virtuale pubblica Direct Connect. IPv4 dovrebbe supportare qualsiasi cosa compresa tra /1 e /32 e IPv6 dovrebbe supportare qualsiasi cosa compresa tra /1 - /64.

Risorsa	Informazioni obbligatorie
(Solo interfaccia virtuale privata) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti in eccesso. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 9001 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettività di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I jumbo frame si applicano solo ai percorsi propagati da. AWS Direct Connect Se aggiungi route statiche a una tabella di routing che punta al gateway privato virtuale, il traffico instradato attraverso le route statiche viene inviato utilizzando 1500 MTU. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.
(Solo interfaccia virtuale Transit) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti superati. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 8500 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettiv ità di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I frame jumbo sono supportati fino a 8500 MTU per Direct Connect. Le route statiche e le rotte propagate configurate nella tabella di routing di Transit Gateway supporteranno i frame jumbo, incluse le istanze EC2 con voci della tabella di routing statica VPC al collegamento del gateway di transito alla VPN. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.

Se i prefissi pubblici o gli ASN appartengono a un ISP o a un operatore di rete, richiederemo ulteriori informazioni. Potrebbe trattarsi di un documento con l'intestazione ufficiale dell'azienda o di un'e-mail inviata dal nome di dominio aziendale per verificare che il prefisso di rete/ASN possa essere utilizzato da te.

Quando crei un'interfaccia virtuale pubblica, possono essere necessarie fino a 72 ore affinché AWS riveda e approvi la tua richiesta.

Per effettuare il provisioning di un'interfaccia virtuale pubblica su servizi non-VPC

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Virtual interface type (Tipo di interfaccia virtuale), per Type (Tipo) scegliere Public (Pubblico).
5. In Public virtual interface settings (Impostazioni interfaccia virtuale pubblica), procedere come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

   b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

   c. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

   d. In BGP ASN, immettere il Border Gateway Protocol (BGP) Autonomous System Number (ASN) del gateway.

      I valori validi sono 1-2147483647.
6. In Additional settings (Impostazioni aggiuntive), procedere come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

      [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

      - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
      - In Amazon router peer IP (IP peer del router Amazon), immettere l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

      [IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

   b. Per fornire la propria chiave BGP, immettere la chiave MD5 del BGP.

Se non si inserisce un valore, procederemo a generare una chiave BGP.

c. Per pubblicizzare prefissi per Amazon, in Prefissi da pubblicizzare, immetti gli indirizzi CIDR IPv4 di destinazione (separati da virgole) a cui instradare il traffico tramite l'interfaccia virtuale.

d. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).

Per effettuare il provisioning di un'interfaccia virtuale privata su un VPC

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Tipo di interfaccia virtuale, per Tipo scegli Pubblico.
5. In Impostazioni dell'interfaccia virtuale pubblica, procedi come segue:

a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

c. Per il Tipo di gateway, scegli Gateway privato virtuale oGateway Direct Connect.

d. Per Proprietario dell'interfaccia virtuale, scegli Altro AWS account, quindi inserisci l' AWS account.

e. Per Gateway virtuale privato, scegli il gateway virtuale privato da usare per l'interfaccia.

f. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

g. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

I valori validi sono compresi tra 1 e 2147483647.

6. In Impostazioni aggiuntive, procedi come segue:

a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

   [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

   - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
   - In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

   > **Important**
   >
   > Se consenti l' AWS assegnazione automatica degli indirizzi IPv4, verrà allocato un CIDR /29 da 169.254.0.0/16 IPv4 Link-Local secondo RFC 3927 per la connettività. point-to-point AWS non consiglia questa opzione se si intende utilizzare l'indirizzo IP peer del router del cliente come origine e/o destinazione per il traffico VPC. Ti consigliamo invece di utilizzare RFC 1918 o un altro indirizzo e di specificare manualmente l'indirizzo.
   >
   > - Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.
   > - Per ulteriori informazioni su RFC 3927, consulta Dynamic Configuration of IPv4 Link-Local Addresses.

   [IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

b. Per modificare l'unità di trasmissione massima (MTU) da 1500 (predefinito) a 9001 (frame jumbo), seleziona Jumbo MTU (MTU size 9001) (MTU jumbo - dimensione della MTU 9001).

c. (Facoltativo) In Abilita SiteLink, scegli Abilitato per abilitare la connettività diretta tra i punti di presenza Direct Connect.

d. (Facoltativo) Aggiunta o rimozione di un tag.

   [Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).

Passaggio 4: Verificare la configurazione di resilienza dell'interfaccia virtuale

Dopo aver stabilito le interfacce virtuali verso il AWS Cloud o Amazon VPC, esegui un test di failover dell'interfaccia virtuale per verificare che la configurazione soddisfi i requisiti di resilienza. Per ulteriori informazioni, consulta the section called “Test di failover AWS Direct Connect”.

Fase 5: Verifica dell'interfaccia virtuale

Dopo aver stabilito le interfacce virtuali verso il AWS Cloud o Amazon VPC, puoi verificare AWS Direct Connect la connessione utilizzando le seguenti procedure.

Per verificare la connessione dell'interfaccia virtuale al Cloud AWS

- Esegui `traceroute` e verifica che l' AWS Direct Connect identificatore sia presente nella traccia di rete.

Verificare la connessione dell'interfaccia virtuale su Amazon VPC

1. Tramite un AMI per cui è possibile effettuare il ping, ad esempio un AMI di Amazon Linux, avvia un'istanza EC2 nel VPC associato al gateway virtuale privato. Le AMI di Amazon Linux sono disponibili nel menu Avvio rapido quando si utilizza la procedura guidata per avviare le istanze nella console Amazon EC2. Per ulteriori informazioni, consulta Launch an Instance nella Amazon EC2 User Guide. Assicurati che il gruppo di sicurezza associato all'istanza includa una regola che consenta il traffico ICMP in entrata (per la richiesta di ping).
2. Dopo che l'istanza è in esecuzione, recupera l'indirizzo IPv4 privato corrispondente (per esempio, 10.0.0.4). La console Amazon EC2 visualizza l'indirizzo come parte dei dettagli dell'istanza.
3. Effettua il ping dell'indirizzo IPv4 privato e ricevi una risposta.

Classic

Selezionare Classic quando si dispone di connessioni esistenti.

Le procedure seguenti illustrano gli scenari comuni per configurare una connessione AWS Direct Connect .

Indice

Prerequisiti

Per connessioni AWS Direct Connect con velocità di porta pari o superiori a 1 Gbps, assicurati che la rete soddisfi i seguenti requisiti:

- La rete deve utilizzare la fibra monomodale con un ricetrasmettitore 1000BASE-LX (1310 nm) per 1 gigabit Ethernet, un ricetrasmettitore 10GBASE-LR (1310 nm) per 10 gigabit o un 100GBASE-LR4 per 100 gigabit Ethernet.
- La negoziazione automatica per una porta deve essere disabilitata per una connessione con una velocità di porta superiore a 1 Gbps. Tuttavia, a seconda dell'endpoint AWS Direct Connect che serve la connessione, potrebbe essere necessario abilitare o disabilitare la negoziazione automatica per le connessioni da 1 Gbps. Se l'interfaccia virtuale rimane inattiva, consulta Risoluzione dei problemi di livello 2 (collegamento dati).
- L'incapsulamento VLAN 802.1Q deve essere supportato su tutta la connessione, compresi i dispositivi intermedi.
- Il dispositivo deve supportare l'autenticazione Border Gateway Protocol (BGP) e BGP MD5.
- (Facoltativo) È possibile configurare il rilevamento bidirezionale di inoltro (BFD) sulla rete. Il BFD asincrono viene abilitato automaticamente per ogni interfaccia virtuale. AWS Direct Connect È abilitato automaticamente per le interfacce virtuali Direct Connect, ma non ha effetto finché non lo configuri sul router. Per ulteriori informazioni, consulta Abilitare BFD per una connessione Direct Connect.

Passaggio 1: iscriviti a AWS

Per utilizzarlo AWS Direct Connect, hai bisogno di un account se non ne hai già uno.

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Fase 2: Richiedere una connessione AWS Direct Connect dedicata

Per le connessioni dedicate, puoi inviare una richiesta di connessione utilizzando la AWS Direct Connect console. Per le connessioni ospitate, collabora con un AWS Direct Connect partner per richiedere una connessione ospitata. Assicurati di disporre delle informazioni riportate di seguito:

- La velocità di porta richiesta. Dopo aver creato la richiesta di connessione, non potrai modificare la velocità della porta.
- La AWS Direct Connect posizione in cui deve essere interrotta la connessione.

> **Note**
>
> Non è possibile utilizzare la AWS Direct Connect console per richiedere una connessione ospitata. Contatta invece un AWS Direct Connect partner, che può creare per te una connessione ospitata, che poi accetti. Ignora la procedura seguente e vai a Accettare una connessione ospitata.

Per creare una nuova AWS Direct Connect connessione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Connessioni, quindi Crea connessione.
3. Scegliere Classic.
4. Nel riquadro Create connection (Crea connessione), in Connection settings (Impostazioni di connessione), procedere come segue:
   a. In Name (Nome), immettere un nome per la connessione.
   b. Per Location (Sede), selezionare la località AWS Direct Connect appropriata.
   c. Se applicabile, per Sub Location (Sede secondaria), scegliere il piano più vicino a te o al provider di rete. Questa opzione è disponibile soltanto se nella sede scelta sono presenti delle stanze meet-me (MMR, Meet-Me Room) su più piani dell'edificio.
   d. In Port Speed (Velocità porta), scegliere la larghezza di banda per la connessione.
   e. Per On-premise, seleziona Connetti tramite un AWS Direct Connect partner quando usi questa connessione per connetterti al tuo data center.

f. Per Service provider, seleziona il AWS Direct Connect Partner. Se utilizzi un partner non presente nell'elenco, seleziona Altro.

g. Se hai selezionato Altro per Provider di servizi, perNome dell'altro provider, immetti il nome del partner utilizzato.

h. (Facoltativo) Aggiunta o rimozione di un tag.

   [Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.

   [Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

5. Scegli Crea connessione.

Possono essere necessarie fino a 72 ore AWS per esaminare la richiesta e fornire una porta per la connessione. Durante questo intervallo di tempo, potresti ricevere un'e-mail con una richiesta di ulteriori informazioni sul caso d'uso o sulla sede specificata. L'e-mail viene inviata all'indirizzo e-mail che hai utilizzato al momento della registrazione AWS. Devi rispondere entro 7 giorni o la connessione verrà eliminata.

Per ulteriori informazioni, consulta AWS Direct Connect connessioni.

Accettare una connessione ospitata

È necessario accettare la connessione ospitata nella AWS Direct Connect console prima di poter creare un'interfaccia virtuale. Questo passaggio si applica solo alle connessioni ospitate.

Per accettare un'interfaccia virtuale in hosting

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Connections (Connessioni).
3. Seleziona la connessione ospitata, quindi scegli Accetta.

   Scegliere Accept (Accetta).

(Connessione dedicata) Fase 3: download di LOA-CFA

Dopo aver richiesto una connessione, creiamo una LOA-CFA (Letter of Authorization and Connecting Facility Assignment), disponibile per il download, o ti invieremo un'e-mail con una richiesta di ulteriori informazioni. Il LOA-CFA è l'autorizzazione alla AWS connessione ed è richiesto dal provider di colocation o dal provider di rete per stabilire la connessione tra reti (cross-connect).

Per scaricare la LOA-CFA

1. Apri AWS Direct Connectla console all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Connections (Connessioni).
3. Selezionare la connessione e scegliere View Details (Visualizza dettagli).
4. Scegliere Download LOA-CFA (Scarica LOA-CFA).

   La LOA-CFA viene scaricata sul tuo computer come file PDF.

   > **Note**
   >
   > Se il collegamento non è abilitato, vuol dire che la LOA-CFA non è ancora disponibile per il download. Controlla l'e-mail per verificare se hai ricevuto una richiesta di ulteriori informazioni. Se non è ancora disponibile, o se non hai ricevuto alcuna e-mail dopo 72 ore, contatta AWS Support.

5. Dopo aver scaricato la LOA-CFA, procedere in uno dei seguenti modi:

   - Se lavori con un AWS Direct Connect partner o un provider di rete, inviagli il LOA-CFA in modo che possano ordinare una connessione incrociata per te presso la sede. AWS Direct Connect Se non riescono a configurare l'interconnessione per tuo conto, puoi contattare direttamente il provider di co-location.
   - Se disponi di apparecchiature in loco, contatta il AWS Direct Connect provider di colocation per richiedere una connessione transrete. È necessario essere un cliente del provider co-location. È inoltre necessario presentare loro il LOA-CFA che autorizza la connessione al AWS router e le informazioni necessarie per connettersi alla rete.

AWS Direct Connect le sedi elencate come siti multipli (ad esempio, Equinix DC1-DC6 e DC10-DC11) sono configurate come campus. Se le tue apparecchiature o quelle del tuo provider di rete si

trovano in uno di questi siti, potrai richiedere un'interconnessione alla porta assegnata anche se si trova in un altro edificio del campus.

> **Important**
>
> Un campus viene considerato come un'unica sede. AWS Direct Connect Per ottenere un'elevata disponibilità, configurare le connessioni su diverse aree geografiche AWS Direct Connect .

Se tu o il tuo provider di rete riscontrate dei problemi durante la creazione di una connessione fisica, consulta Risoluzione dei problemi di livello 1 (fisico).

Fase 4: Creazione di un'interfaccia virtuale

Per iniziare a utilizzare la AWS Direct Connect connessione, è necessario creare un'interfaccia virtuale. È possibile creare un'interfaccia virtuale privata per connettersi al tuo VPC. In alternativa, puoi creare un'interfaccia virtuale pubblica per connetterti a AWS servizi pubblici che non si trovano in un VPC. Quando crei un'interfaccia virtuale privata su un VPC, ti servirà un'interfaccia virtuale privata per ogni VPC a cui connetterti. Ad esempio, ti serviranno tre interfacce virtuali private per connetterti a tre VPC.

Prima di iniziare, assicurati di disporre delle informazioni riportate di seguito:

Risorsa	Informazioni obbligatorie
Connessione	La AWS Direct Connect connessione o il gruppo di aggregazione dei link (LAG) per cui stai creando l'interfaccia virtuale.
Nome dell'interfaccia virtuale	Un nome per l'interfaccia virtuale.
Proprietario dell'interfaccia virtuale	Se stai creando l'interfaccia virtuale per un altro account, hai bisogno dell'ID dell'altro AWS account.
(Solo interfaccia virtuale privata) Connessione	Per connetterti a un VPC nella stessa AWS regione, è necessario il gateway privato virtuale per il tuo VPC. L'ASN per il lato Amazon della sessione BGP viene ereditato dal gateway virtuale privato. Quando crei un gateway privato

Risorsa	Informazioni obbligatorie
	virtuale, puoi specificare il tuo ASN privato. Altrimenti, Amazon fornisce un ASN predefinito. Per ulteriori informazioni, consulta l'articolo relativo alla Creare un gateway virtuale privato nella Guida dell'utente di Amazon VPC. Per la connessione a un VPC tramite un gateway Direct Connect, è necessari o il gateway Direct Connect. Per ulteriori informazioni, consulta Gateway Direct Connect.
VLAN	Un tag Rete dell'area locale virtuale (VLAN) univoco che non è già in uso sulla tua connessione. Il valore deve essere compreso tra 1 e 4094 e deve essere conforme allo standard Ethernet 802.1Q. Questo tag è necessario per tutto il traffico che attraversa la connessione AWS Direct Connect . Se disponi di una connessione ospitata, il tuo AWS Direct Connect partner offre questo valore. Non è possibile modificare il valore dopo aver creato l'interfaccia virtuale.

Risorsa	Informazioni obbligatorie

Indirizzi IP peer	Un'interfaccia virtuale può supportare una sessione di peering BGP per IPv4, IPv6 o una di ciascuna (dual-stack). Non utilizzare IP elastici (EIP) o Bring your own IP address (BYOIP) dal pool Amazon per creare un'interfaccia virtuale pubblica. Non puoi creare più sessioni BGP per la stessa famiglia di indirizzi IP sulla stessa interfaccia virtuale. Gli intervalli di indirizzi IP vengono assegnati a ciascuna estremità dell'interfaccia virtuale per la sessione di peering BGP.
	
	• IPv4:
	  • (Solo interfaccia virtuale pubblica) È necessario specificare indirizzi IPv4 pubblici univoci di cui si è proprietari. Il valore può essere uno dei seguenti:
	  • Un CIDR IPv4 di proprietà del cliente
	
	Questi possono essere qualsiasi IP pubblico (di proprietà del cliente o fornito da AWS), ma è necessario utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del router. AWS Ad esempio, se si assegna un `/31` intervallo, ad esempio, è possibile utilizzarlo per l'IP peer e `203.0.113.0` per l'IP peer. `203.0.113.0/31` `203.0.113.1` AWS Oppure, se allocate un `/24` intervallo, ad esempio, potreste utilizzarlo `198.51.100.10` per il vostro IP peer e `198.51.100.20` per l'IP peer. `198.51.100.0/24` AWS
	  • Un intervallo IP di proprietà del AWS Direct Connect partner o dell'ISP, insieme a un'autorizzazione LOA-CFA
	  • Un AWS CIDR /31 fornito. In caso contrario, contatta AWS Support per richiedere un CIDR IPv4 pubblico (e fornire un caso d'uso nella richiesta).
	
	Note
	Non possiamo garantire che saremo in grado di soddisfare tutte le richieste di indirizzi IPv4 pubblici AWS forniti.
	  • (Solo interfaccia virtuale privata) Amazon può generare indirizzi IPv4 privati per te. Se ne specifichi uno personalizzato, assicurati di specifica

Risorsa	Informazioni obbligatorie
	re i CIDR privati solo per l'interfaccia del router e l'interfaccia AWS Direct Connect. Ad esempio, non specificare altri indirizzi IP dalla rete locale. Analogamente a un'interfaccia virtuale pubblica, è necessari o utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del AWS router. Ad esempio, se si assegna un `/30` intervallo, ad esempio`192.168.0.0/30` , è possibile utilizzarlo per l'IP peer e `192.168.0.1` `192.168.0.2` per l'IP peer. AWS • IPv6: Amazon alloca automaticamente un CIDR IPv6 /125. Non puoi specificare indirizzi IPv6 peer personali.
Famiglia di indirizzi	Se la sessione di peering BGP sarà su IPv4 o IPv6.
Informazioni BGP	• Un numero di sistema autonomo (ASN) del Border Gateway Protocol (BGP) pubblico o privato per il lato della sessione BGP. Se utilizzi un ASN pubblico, devi esserne proprietario. Se utilizzi un ASN privato, puoi impostare un valore ASN personalizzato. Per un ASN a 16 bit, il valore deve Esser compreso nell'intervallo da 64512 a 65534. Per un ASN a 32 bit, il valore deve essere compreso nell'intervallo da 1 a 2147483647. La prependenza del sistema autonomo (AS) non funziona se utilizzi un ASN privato per un'interfaccia virtuale pubblica. • AWS abilita MD5 per impostazione predefinita. Tale opzione non è modificabile. • Una chiave di autenticazione MD5 BGP. Puoi fornire il tuo oppure lasciare che Amazon ne generi uno per te.

Risorsa	Informazioni obbligatorie

(Solo interfaccia virtuale pubblica) Prefissi che desideri pubblicizzare	Percorsi IPv4 pubblici o percorsi IPv6 per la pubblicità tramite BGP. Devi pubblicizzare almeno un prefisso utilizzando BGP, fino a un massimo di 1.000 prefissi.
	• IPv4: il CIDR IPv4 può sovrapporsi a un altro CIDR IPv4 pubblico annunciato utilizzando quando una delle seguenti condizioni è vera: AWS Direct Connect
	  • I CIDR AWS provengono da diverse regioni. Assicurati di applicare i tag della community BGP ai prefissi pubblici.
	  • Utilizzi AS_PATH quando disponi di un ASN pubblico in una configurazione attiva/passiva.
	  Per ulteriori informazioni, consulta la Policy di routing e community BGP.
	• IPv6: specificare una lunghezza di prefisso di /64 o inferiore.
	• È possibile aggiungere prefissi aggiuntivi a un file VIF pubblico esistente e pubblicizzarli contattando AWS support. Nel caso di supporto, fornisci un elenco di prefissi CIDR aggiuntivi che desideri aggiungere al file VIF pubblico e pubblicizzare.
	• Puoi specificare qualsiasi lunghezza del prefisso su un'interfaccia virtuale pubblica Direct Connect. IPv4 dovrebbe supportare qualsiasi cosa compresa tra /1 e /32 e IPv6 dovrebbe supportare qualsiasi cosa compresa tra /1 - /64.

Risorsa	Informazioni obbligatorie
(Solo interfaccia virtuale privata) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti in eccesso. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 9001 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettività di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I jumbo frame si applicano solo ai percorsi propagati da. AWS Direct Connect Se aggiungi route statiche a una tabella di routing che punta al gateway privato virtuale, il traffico instradato attraverso le route statiche viene inviato utilizzando 1500 MTU. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.
(Solo interfaccia virtuale Transit) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti superati. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 8500 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettiv ità di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I frame jumbo sono supportati fino a 8500 MTU per Direct Connect. Le route statiche e le rotte propagate configurate nella tabella di routing di Transit Gateway supporteranno i frame jumbo, incluse le istanze EC2 con voci della tabella di routing statica VPC al collegamento del gateway di transito alla VPN. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.

Ti richiederemo ulteriori informazioni se i prefissi pubblici o gli ASN appartengono a un ISP o a un operatore di rete. Potrebbe trattarsi di un documento con l'intestazione ufficiale dell'azienda o di un'e-mail inviata dal nome di dominio aziendale per verificare che il prefisso di rete/ASN possa essere utilizzato da te.

Per l'interfaccia virtuale privata e le interfacce virtuali pubbliche, l'unità di trasmissione massima (MTU) di una connessione di rete è la dimensione, espressa in byte, del pacchetto più grande ammissibile che può essere passato sulla connessione. La MTU di un'interfaccia virtuale privata può essere 1500 o 9001 (frame jumbo). La MTU di un'interfaccia virtuale di transito può essere 1500 o 8500 (frame jumbo). Puoi specificare la MTU quando crei l'interfaccia o la aggiorni dopo la creazione. L'impostazione della MTU di un'interfaccia virtuale su 8500 (frame jumbo) o 9001 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettività di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova Jumbo Frame Capable nella scheda Riepilogo.

Quando crei un'interfaccia virtuale pubblica, possono essere necessarie fino a 72 ore per AWS esaminare e approvare la richiesta.

Per effettuare il provisioning di un'interfaccia virtuale pubblica su servizi non-VPC

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Virtual interface type (Tipo di interfaccia virtuale), per Type (Tipo) scegliere Public (Pubblico).
5. In Public virtual interface settings (Impostazioni interfaccia virtuale pubblica), procedere come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

   b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

   c. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

   d. Per BGP ASN, immettere il Border Gateway Protocol Autonomous System Number del router peer locale per la nuova interfaccia virtuale.

      I valori validi sono 1-2147483647.
6. In Additional settings (Impostazioni aggiuntive), procedere come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

[IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

- Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
- In Amazon router peer IP (IP peer del router Amazon), immettere l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

[IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

b. Per fornire la propria chiave BGP, immettere la chiave MD5 del BGP.

   Se non si inserisce un valore, procederemo a generare una chiave BGP.

c. Per pubblicizzare prefissi per Amazon, in Prefissi da pubblicizzare, immetti gli indirizzi CIDR IPv4 di destinazione (separati da virgole) a cui instradare il traffico tramite l'interfaccia virtuale.

d. (Facoltativo) Aggiunta o rimozione di un tag.

   [Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.

   [Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).

Per effettuare il provisioning di un'interfaccia virtuale privata su un VPC

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Tipo di interfaccia virtuale, per Tipo scegli Pubblico.
5. In Impostazioni dell'interfaccia virtuale pubblica, procedi come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

c. Per il Tipo di gateway, scegli Gateway privato virtuale oGateway Direct Connect.

d. Per Proprietario dell'interfaccia virtuale, scegli Altro AWS account, quindi inserisci l' AWS account.

e. Per Gateway virtuale privato, scegli il gateway virtuale privato da usare per l'interfaccia.

f. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

g. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

   I valori validi sono compresi tra 1 e 2147483647.

6. In Impostazioni aggiuntive, procedi come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

      [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

      - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
      - In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

      > **Important**
      >
      > Se consenti l' AWS assegnazione automatica degli indirizzi IPv4, verrà allocato un CIDR /29 da 169.254.0.0/16 IPv4 Link-Local secondo RFC 3927 per la connettività. point-to-point AWS non consiglia questa opzione se si intende utilizzare l'indirizzo IP peer del router del cliente come origine e/o destinazione per il traffico VPC. Ti consigliamo invece di utilizzare RFC 1918 o un altro indirizzo e di specificare manualmente l'indirizzo.
      >
      > - Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.
      > - Per ulteriori informazioni su RFC 3927, consulta Dynamic Configuration of IPv4 Link-Local Addresses.

[IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

b. Per modificare l'unità di trasmissione massima (MTU) da 1500 (predefinito) a 9001 (frame jumbo), seleziona Jumbo MTU (MTU size 9001) (MTU jumbo - dimensione della MTU 9001).

c. (Facoltativo) In Abilita SiteLink, scegli Abilitato per abilitare la connettività diretta tra i punti di presenza Direct Connect.

d. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).
8. È necessario utilizzare il dispositivo BGP per pubblicizzare la rete utilizzata per la connessione VIF pubblica.

Fase 5: Download della configurazione del router

Dopo aver creato un'interfaccia virtuale per la AWS Direct Connect connessione, puoi scaricare il file di configurazione del router. Il file contiene i comandi necessari per configurare il router per l'uso con l'interfaccia virtuale privata o pubblica.

Per scaricare la configurazione di un router

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Selezionare la connessione e scegliere View Details (Visualizza dettagli).
4. Scegliere Download router configuration (Scarica configurazione router).
5. In Download Router Configuration (Scarica configurazione router), procedere come segue:

   a. Per Vendor (Fornitore), selezionare il produttore del router.

   b. Per Platform (Piattaforma), selezionare il modello del router.

c. Per Software, selezionare la versione software del router.

6. Scegliere Download (Scarica), quindi utilizzare la configurazione del router appropriata per assicurare la connettività ad AWS Direct Connect.

Per i file di configurazione di esempio, consulta la sezione File di configurazione del router di esempio.

Dopo aver configurato il router, lo stato dell'interfaccia virtuale passa su UP. Se l'interfaccia virtuale rimane inattiva e non è possibile eseguire il ping dell'indirizzo IP peer del AWS Direct Connect dispositivo, consultaRisoluzione dei problemi di livello 2 (collegamento dati). Se riesci a effettuare il ping dell'indirizzo IP peer, consulta Risoluzione dei problemi di livello 3/4 (rete/trasporto). Se la sessione di peering BGP viene stabilita, ma non riesci a instradare il traffico, consulta Risoluzione dei problemi di instradamento.

Fase 6: Verifica dell'interfaccia virtuale

Dopo aver stabilito le interfacce virtuali verso il AWS Cloud o Amazon VPC, puoi verificare AWS Direct Connect la connessione utilizzando le seguenti procedure.

Per verificare la connessione dell'interfaccia virtuale al Cloud AWS

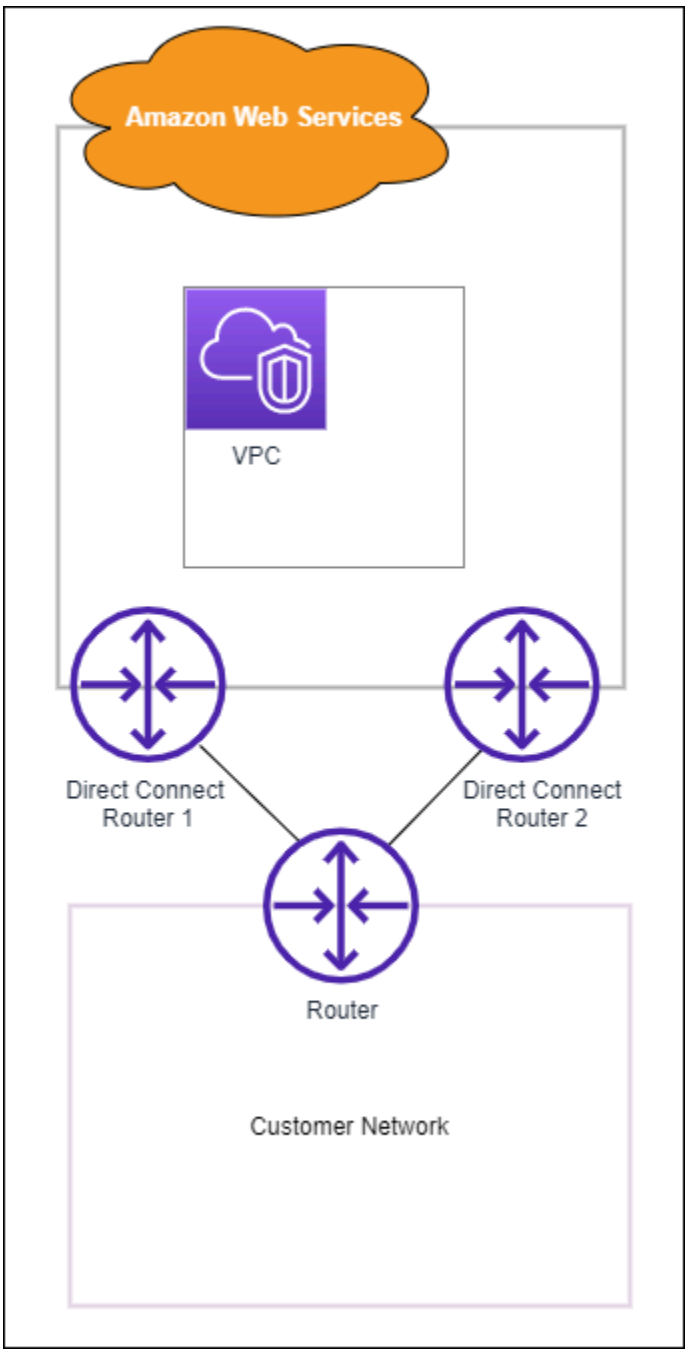
- Esegui `traceroute` e verifica che l' AWS Direct Connect identificatore sia presente nella traccia di rete.

Verificare la connessione dell'interfaccia virtuale su Amazon VPC

1. Tramite un AMI per cui è possibile effettuare il ping, ad esempio un AMI di Amazon Linux, avvia un'istanza EC2 nel VPC associato al gateway virtuale privato. Le AMI di Amazon Linux sono disponibili nel menu Avvio rapido quando si utilizza la procedura guidata per avviare le istanze nella console Amazon EC2. Per ulteriori informazioni, consulta Launch an Instance nella Amazon EC2 User Guide. Assicurati che il gruppo di sicurezza associato all'istanza includa una regola che consenta il traffico ICMP in entrata (per la richiesta di ping).
2. Dopo che l'istanza è in esecuzione, recupera l'indirizzo IPv4 privato corrispondente (per esempio, 10.0.0.4). La console Amazon EC2 visualizza l'indirizzo come parte dei dettagli dell'istanza.
3. Effettua il ping dell'indirizzo IPv4 privato e ricevi una risposta.

(Consigliato) Passaggio 7: Configurare le connessioni ridondanti

Per provvedere al failover, consigliamo di richiedere e configurare due connessioni dedicate a AWS, come illustrato nella figura seguente. Queste connessioni possono terminare su uno o due router nella tua rete.



Puoi scegliere tra diverse opzioni di configurazione quando effettui il provisioning di due connessioni dedicate:

- Attiva/Attiva (percorso multiplo BGP). Questa è la configurazione predefinita, in cui entrambe le connessioni sono attive. AWS Direct Connect supporta percorsi multipli verso più interfacce virtuali all'interno della stessa posizione e il traffico viene condiviso tra le interfacce in base al flusso. Se una connessione non è più disponibile, tutto il traffico viene instradato attraverso l'altra connessione.
- Attiva/Passiva (failover). Una connessione gestisce il traffico e l'altra è in standby. Se la connessione attiva non è più disponibile, tutto il traffico viene instradato attraverso la connessione passiva. Occorre anteporre il percorso AS agli instradamenti su uno dei collegamenti per rendere passivo il collegamento selezionato.

La modalità di configurazione delle connessioni non influisce sulla ridondanza, ma pregiudica le policy che determinano la modalità di instradamento dei dati su entrambe le connessioni. Ti consigliamo di configurare entrambe le connessioni come attive.

Se utilizzi una connessione VPN per la ridondanza, assicurati di implementare un meccanismo di controllo dello stato e di failover. Se utilizzi una delle seguenti configurazioni, devi controllare il routing della tabella di routing per l'instradamento alla nuova interfaccia di rete.

- Puoi utilizzare le tue istanze per l'instradamento, ad esempio il firewall.
- Puoi utilizzare la tua istanza che termina una connessione VPN.

Per ottenere un'elevata disponibilità, consigliamo vivamente di configurare le connessioni verso posizioni diverse. AWS Direct Connect

Per ulteriori informazioni sulla AWS Direct Connect resilienza, consulta Raccomandazioni sulla AWS Direct Connect resilienza.

Test di failover AWS Direct Connect

L'AWS Direct Connect Resiliency Toolkit è progettato per garantire il numero appropriato di connessioni alle interfacce virtuali in molteplici località. Dopo aver completato la procedura guidata, utilizzare il test di failover AWS Direct Connect Resiliency Toolkit per abbassare la sessione di peering BGP e verificare che il traffico sia indirizzato a una delle interfacce virtuali ridondanti e soddisfi i requisiti di resilienza.

Utilizzare il test per assicurarsi che il traffico venga instradato su interfacce virtuali ridondanti quando un'interfaccia virtuale è fuori servizio. È possibile avviare il test selezionando un'interfaccia virtuale,

una sessione di peering BGP e per quanto tempo eseguire il test. AWS posiziona la sessione di peering BGP dell'interfaccia virtuale selezionata nello stato inattivo. Quando l'interfaccia è in questo stato, il traffico dovrebbe passare su un'interfaccia virtuale ridondante. Se la configurazione non contiene le connessioni ridondanti appropriate, la sessione di peering BGP non riesce e il traffico non viene instradato. Al termine del test, o se si interrompe manualmente il test, AWS ripristina la sessione BGP. Al termine del test, è possibile utilizzare l'AWS Direct Connect Resiliency Toolkit per regolare la configurazione.

> **Note**
>
> Non utilizzare questa funzione durante un periodo di manutenzione di Direct Connect poiché la sessione BGP potrebbe essere ripristinata prematuramente durante o dopo la manutenzione.

Cronologia dei test

AWS elimina la cronologia dei test dopo 365 giorni. La cronologia dei test include lo stato dei test eseguiti su tutti i peer BGP. La cronologia include quali sessioni di peering BGP sono state testate, l'ora di inizio e di fine e lo stato del test, che può essere uno dei seguenti valori:

- In corso - Il test è attualmente in esecuzione.
- Completato : il test è stato eseguito per il tempo specificato.
- Annullato - Il test è stato annullato prima dell'ora specificata.
- Non riuscito : il test non è stato eseguito per il tempo specificato. Questo può accadere quando c'è un problema con il router.

Per ulteriori informazioni, consulta the section called “Visualizzazione della cronologia dei test di failover dell'interfaccia virtuale”.

Autorizzazioni di convalida

L'unico account che dispone dell'autorizzazione per eseguire il test di failover è l'account proprietario dell'interfaccia virtuale. Il proprietario dell'account riceve un'indicazione attraverso AWS CloudTrail che un test è stato eseguito su un'interfaccia virtuale.

Avvio del test di failover dell'interfaccia virtuale

È possibile avviare il test di failover dell'interfaccia virtuale utilizzando la console AWS Direct Connect o AWS CLI.

Per avviare il test di failover dell'interfaccia virtuale dalla console AWS Direct Connect

1. Apri la console all'indirizzo https://console.aws.amazon.com/directconnect/v2/home AWS Direct Connect.
2. Scegliere Interfacce virtuali.
3. Selezionare le interfacce virtuali e quindi scegliere Azioni, Abbassare BGP.

   È possibile eseguire il test su un'interfaccia virtuale pubblica, privata o di transito.
4. Nella finestra di dialogo Avvia test errore eseguire le operazioni seguenti:

   a. Per abbassare i peering da testare, scegliere le sessioni di peering da testare, ad esempio IPv4.

   b. In Tempo massimo test, immettere il numero di minuti di durata del test.

      Il valore massimo è 4.320 minuti (72 ore).

      Il valore predefinito è 180 minuti (3 ore).

   c. In Confermare il test, immettere Conferma.

   d. Scegli Conferma.

   La sessione di peering BGP viene posizionata nello stato DOWN. È possibile inviare traffico per verificare che non vi siano interruzioni. Se necessario, è possibile interrompere immediatamente il test.

Per avviare il test di failover dell'interfaccia virtuale utilizzando l'opzione AWS CLI

Usa StartBgpFailoverTest.

Visualizzazione della cronologia dei test di failover dell'interfaccia virtuale

È possibile visualizzare la cronologia dei test di failover dell'interfaccia virtuale utilizzando la console AWS Direct Connect o AWS CLI.

Per visualizzare la cronologia dei test di failover dell'interfaccia virtuale dalla console AWS Direct Connect

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Scegliere Interfacce virtuali.
3. Selezionare l'interfaccia virtuale,quindi scegliere View details (Visualizza dettagli).
4. Scegliere Cronologia test.

   Nella console vengono visualizzati i test dell'interfaccia virtuale eseguiti per l'interfaccia virtuale.
5. Per visualizzare i dettagli di un test specifico, selezionare l'id del test.

Per visualizzare la cronologia dei test di failover dell'interfaccia virtuale utilizzando l'opzione AWS CLI

Usa ListVirtualInterfaceTestHistory.

Arresto del test di failover dell'interfaccia virtuale

È possibile interrompere il test di failover dell'interfaccia virtuale utilizzando la console AWS Direct Connect o AWS CLI.

Per interrompere il test di failover dell'interfaccia virtuale dalla console AWS Direct Connect

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Scegliere Interfacce virtuali.
3. Selezionare l'interfaccia virtuale, quindi scegliere Azioni, Annulla test.
4. Scegli Conferma.

AWS ripristina la sessione di peering BGP. La cronologia dei test visualizza “annullato” per il test.

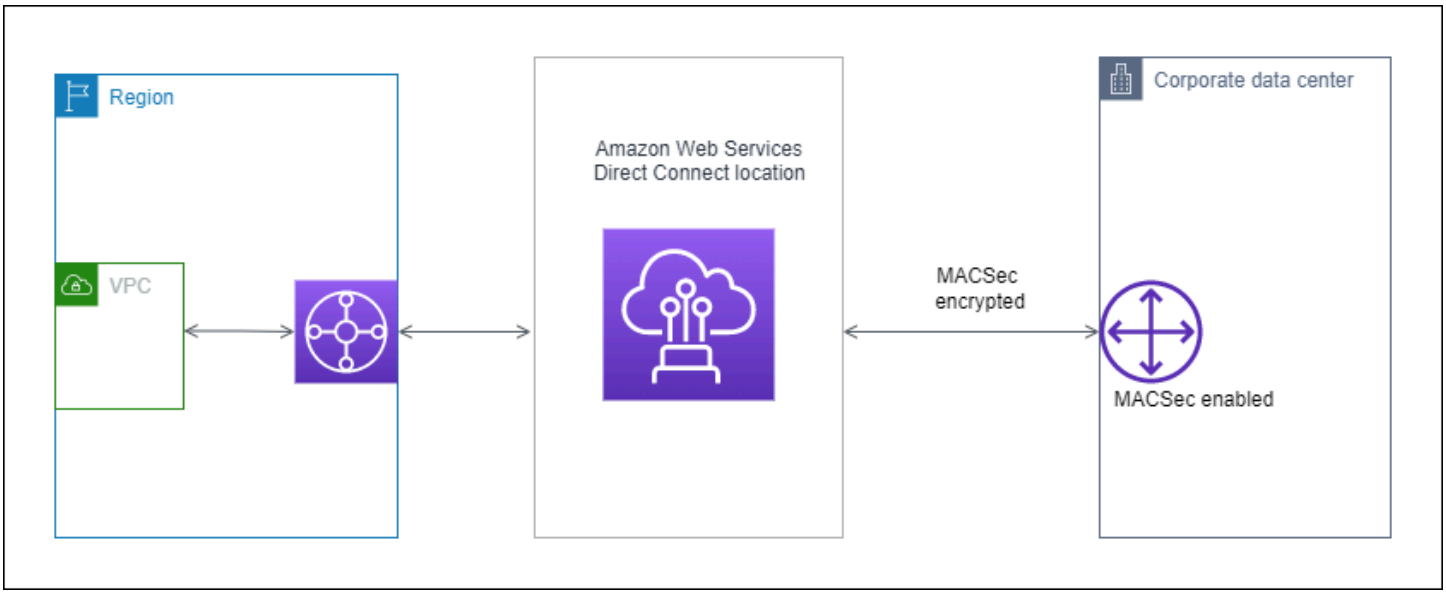
Per arrestare il test di failover dell'interfaccia virtuale utilizzando l'opzione AWS CLI

Usa StopBgpFailoverTest.

MAC Security

MAC Security (MACsec) è uno standard IEEE che garantisce la riservatezza dei dati, l'integrità dei dati e l'autenticità dell'origine dei dati. MacSec fornisce la point-to-point crittografia di livello 2 sulla connessione incrociata a. AWS MacSec opera a livello 2 tra due router di livello 3 e fornisce la crittografia sul dominio di livello 2. Tutti i dati che fluiscono attraverso la rete AWS globale che si interconnette con i data center e le regioni vengono automaticamente crittografati a livello fisico prima di lasciare il data center.

Nel diagramma seguente, sia la connessione dedicata che le risorse on-premise devono supportare MACsec. Il traffico di livello 2 che viaggia attraverso la connessione dedicata da o verso il data center è crittografato.



Concetti di MACsec

Di seguito sono elencati i concetti fondamentali per :

- MAC Security (MACsec): uno standard IEEE 802.1 di Livello 2 che garantisce la riservatezza, l'integrità e l'autenticità dell'origine dei dati. Per ulteriori informazioni sul protocollo, consulta 802.1AE: MAC Security (MacSec).
- Chiave segreta MacSec: una chiave precondivisa che stabilisce la connettività MacSec tra il router locale del cliente e la porta di connessione presso la sede. AWS Direct Connect La chiave viene generata dai dispositivi alle estremità della connessione utilizzando la coppia CKN/CAK fornita dall'utente e fornita anche sul dispositivo. AWS

- Connection Key Name (CKN) e Connectivity Association Key (CAK): i valori in questa coppia vengono utilizzati per generare la chiave segreta MACsec. I valori della coppia vengono generati, associati a una AWS Direct Connect connessione e forniti sul dispositivo perimetrale alla fine della connessione. AWS Direct Connect

Connessioni supportate

MACsec è disponibile su connessioni dedicate. Per informazioni su come ordinare connessioni che supportano MACsec, consulta AWS Direct Connect.

Inizia a usare MACsec su connessioni dedicate

Le seguenti attività consentono di acquisire familiarità con MacSec su connessioni AWS Direct Connect dedicate. Non sono previsti costi aggiuntivi per l'utilizzo di MacSec.

Prima di configurare MacSec su una connessione dedicata, tieni presente quanto segue:

- MACSec è supportato su connessioni Direct Connect dedicate da 10 Gbps e 100 Gbps in determinati punti di presenza. Per queste connessioni, sono supportate le seguenti suite di crittografia MacSec:
  - Per connessioni a 10 Gbps, GCM-AES-256 e GCM-AES-XPN-256.
  - Per connessioni a 100 Gbps, GCM-AES-XPN-256.

- Sono supportate solo chiavi MacSec a 256 bit.
- La numerazione estesa dei pacchetti (XPN) è richiesta per le connessioni a 100 Gbps. Per connessioni a 10 Gbps, Direct Connect supporta sia GCM-AES-256 che GCM-AES-XPN-256. Le connessioni ad alta velocità, come le connessioni dedicate da 100 Gbps, possono esaurire rapidamente lo spazio di numerazione dei pacchetti originale a 32 bit di MacSec, il che richiederebbe la rotazione delle chiavi di crittografia ogni pochi minuti per creare una nuova Connectivity Association. Per evitare questa situazione, l'emendamento IEEE Std 802.1AEBW-2013 ha introdotto la numerazione estesa dei pacchetti, aumentando lo spazio di numerazione a 64 bit, semplificando il requisito di tempestività per la rotazione dei tasti.
- Il Secure Channel Identifier (SCI) è obbligatorio e deve essere attivato. Questa impostazione non può essere modificata.
- Il tag IEEE 802.1Q (dot1Q/VLAN) offset/dot1 non q-in-clear è supportato per lo spostamento di un tag VLAN all'esterno di un payload crittografato.

Per ulteriori informazioni su Direct Connect e MacSec, consulta la sezione MacSec delle AWS Direct Connect domande frequenti.

Argomenti

Prerequisiti MACsec

Completa le seguenti attività prima di configurare MACsec su una connessione dedicata.

- Crea una coppia CKN/CAK per la chiave segreta MACsec.

  È possibile creare la coppia utilizzando uno strumento standard aperto. L'AMI specificato nel modello deve soddisfare i requisiti in the section called “Fase 4: configurazione del router on-premise”.
- È necessario disporre di un dispositivo all'estremità della connessione che supporti MACsec.
- Il Secure Channel Identifier (SCI) deve essere attivato.
- Sono supportate solo chiavi MacSec a 256 bit, che forniscono la più recente protezione avanzata dei dati.

Ruoli collegati ai servizi

AWS Direct Connect utilizza ruoli collegati ai AWS Identity and Access Management servizi (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS Direct Connect I ruoli collegati ai servizi sono predefiniti AWS Direct Connect e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS Un ruolo collegato al servizio semplifica la configurazione AWS Direct Connect perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Direct Connect definisce le autorizzazioni dei ruoli

collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS Direct Connect Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM. Per ulteriori informazioni, consulta the section called “Ruoli collegati ai servizi”.

Considerazioni chiave CKN/CAK precondivise da MACSec

AWS Direct Connect utilizza CMK AWS gestiti per le chiavi già condivise associate a connessioni o LAG. Secrets Manager archivia le coppie CKN e CAK precondivise come un segreto che viene crittografato dalla chiave principale di Secrets Manager. Per ulteriori informazioni, consulta CMK gestiti da AWS nella Guida per gli sviluppatori di AWS Key Management Service .

La chiave memorizzata è di sola lettura in base alla progettazione, ma è possibile pianificare un'eliminazione da sette a trenta giorni utilizzando la console o l'API AWS Secrets Manager. Non è possibile leggere il CKN mentre si pianifica un'eliminazione, e ciò potrebbe influire sulla connettività di rete. In tale eventualità, applichiamo le seguenti regole:

- Se la connessione è in sospeso, dissociamo il CKN dalla connessione.
- Se la connessione è disponibile, informiamo il proprietario della connessione tramite e-mail. Se non intraprendi alcuna azione entro 30 giorni, procederemo a disassociare il CKN dalla tua connessione.

Quando disassociamo l'ultimo CKN dalla tua connessione e la modalità di crittografia della connessione è impostata su «must encrypt», impostiamo la modalità su «should_encrypt» per prevenire la perdita improvvisa di pacchetti.

Fase 1: creazione di una connessione

Per iniziare a utilizzare MACSec, è necessario attivare la funzionalità quando si crea una connessione dedicata. Per ulteriori informazioni, consulta the section called “Creare una connessione utilizzando la procedura guidata di connessione”.

(Facoltativo) Fase 2: creazione di un gruppo di aggregazione dei collegamenti (LAG)

Se utilizzi più connessioni per la ridondanza, puoi creare un LAG che supporti MACSec. Per ulteriori informazioni, consultare the section called “Considerazioni relative a MACsec” e the section called “Creazione di un LAG”.

Fase 3: associazione del CKN/CAK alla connessione o al LAG

Dopo aver creato la connessione o il LAG che supporta MacSec, è necessario associare un CKN/CAK alla connessione. Per ulteriori informazioni, consultare uno dei seguenti argomenti:

- the section called “Associa un MACsec CKN/CAK a una connessione”
- the section called “Associa un MACsec CKN/CAK a un LAG”

Fase 4: configurazione del router on-premise

Aggiorna il router on-premise con la chiave segreta MACsec. La chiave segreta MacSec sul router locale e nella posizione deve corrispondere. AWS Direct Connect Per ulteriori informazioni, consulta the section called “Download del file di configurazione del router”.

Fase 5: (Facoltativo) rimuovere l'associazione tra CKN/CAK e la connessione o il LAG

Se devi rimuovere l'associazione tra la chiave MACSec e la connessione o il LAG, consulta una delle operazioni seguenti:

- the section called “Rimozione dell'associazione tra una chiave segreta MACsec e una connessione”
- the section called “Rimozione dell'associazione tra una chiave segreta MACsec e un LAG”

AWS Direct Connect connessioni

AWS Direct Connect consente di stabilire una connessione di rete dedicata tra la rete e una delle AWS Direct Connect sedi.

Esistono due tipi di connessioni:

- Connessione dedicata: una connessione fisica Ethernet associata a un singolo cliente. I clienti possono richiedere una connessione dedicata tramite la AWS Direct Connect console, la CLI o l'API. Per ulteriori informazioni, consulta the section called “Connessioni dedicate”.
- Connessione ospitata: una connessione Ethernet fisica fornita da un AWS Direct Connect partner per conto di un cliente. I clienti possono richiedere una connessione ospitata contattando il partner del Programma di partner AWS Direct Connect , che effettua il provisioning della connessione. Per ulteriori informazioni, consulta the section called “Connessioni ospitate”.

Connessioni dedicate

Per creare una connessione AWS Direct Connect dedicata, è necessario disporre delle informazioni seguenti:

AWS Direct Connect posizione

Collabora con un AWS Direct Connect partner del Partner Program per aiutarti a stabilire circuiti di rete tra una AWS Direct Connect sede e il tuo data center, ufficio o ambiente di colocation. I partner APN possono anche fornire uno spazio di co-location nella stessa struttura della sede. Per ulteriori informazioni, consulta Partner APN che supportano AWS Direct Connect.

Velocità porta

I valori possibili sono 1 Gbps, 10 Gbps e 100 Gbps.

Dopo aver creato la richiesta di connessione, non potrai modificare la velocità della porta. Per modificare la velocità della porta, devi creare e configurare una nuova connessione.

Puoi creare una connessione utilizzando la procedura guidata di connessione oppure creando una connessione classica. La procedura guidata di connessione ti permette di configurare le connessioni utilizzando i consigli di resilienza. La procedura guidata è consigliata se è la prima volta che configuri

una connessione. Se preferisci, puoi usare Classic per creare connessioni. one-at-a-time La versione classica è consigliata se hai già una configurazione esistente a cui desideri aggiungere connessioni. Puoi creare una connessione autonoma o una connessione da associare a un LAG nel tuo account. Se associata a un LAG, la connessione viene creata con la stessa velocità della porta e la stessa sede specificate nel LAG.

Dopo aver richiesto la connessione, creiamo una LOA-CFA (Letter of Authorization and Connecting Facility Assignment), disponibile per il download, o ti invierà un'e-mail con una richiesta di ulteriori informazioni. Se ricevi una richiesta di ulteriori informazioni, dovrai rispondere entro 7 giorni o la connessione verrà eliminata. Il LOA-CFA è l'autorizzazione alla AWS connessione ed è richiesto dal provider di rete per ordinare una connessione incrociata. Se non disponete di apparecchiature in AWS Direct Connect loco, non potete ordinare una connessione incrociata per conto vostro.

Di seguito sono elencate le operazioni disponibili per le connessioni dedicate:

- the section called “Creare una connessione utilizzando la procedura guidata di connessione”
- the section called “Crea una connessione classica”
- the section called “Visualizzare i dettagli di connessione”
- the section called “Aggiornamento di una connessione”
- the section called “Associa un MACsec CKN/CAK a una connessione”
- the section called “Rimozione dell'associazione tra una chiave segreta MACsec e una connessione”
- the section called “Elimina connessioni”

Puoi aggiungere una connessione dedicata a un Gruppo di aggregazione collegamenti (LAG) che consente di gestire più connessioni come fosse una sola. Per informazioni, consulta Associazione di una connessione a un LAG..

Dopo aver creato una connessione, crea un'interfaccia virtuale da connettere alle risorse AWS pubbliche e private. Per ulteriori informazioni, consulta AWS Direct Connect interfacce virtuali.

Se non disponi di apparecchiature in una AWS Direct Connect sede, contatta innanzitutto un AWS Direct Connect AWS Direct Connect partner del Partner Program. Per ulteriori informazioni, consulta Partner APN che supportano AWS Direct Connect.

Se desideri creare una connessione che utilizzi MAC Security (MACsec), esamina i prerequisiti prima di creare la connessione. Per ulteriori informazioni, consulta the section called “Prerequisiti MACsec ”.

Creare una connessione utilizzando la procedura guidata di connessione

Questa sezione descrive la creazione di una connessione utilizzando la procedura guidata di connessione. Se preferisci creare una connessione classica, consulta la procedura riportata in the section called “Fase 2: Richiedere una connessione AWS Direct Connect dedicata”.

Per creare una connesione Procedura guidata di connessione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Connessioni, quindi Crea connessione.
3. Nella pagina Crea connessione, in Tipo di ordine della connessione, scegli Procedura guidata di connessione.
4. Scegli un Livello di resilienza per le tue connessioni di rete. Un livello di resilienza può essere uno dei seguenti:

   - Resilienza massima
   - Resilienza elevata
   - Sviluppo e test

   Per descrizioni e informazioni più dettagliate su questi livelli di resilienza, consulta Utilizzo del AWS Direct Connect Resiliency Toolkit per iniziare.
5. Seleziona Successivo.
6. Nella pagina Configura connessioni, fornisci i seguenti dettagli.

   a. Dall'elenco a discesa Larghezza di banda, scegli la larghezza di banda richiesta per la connessione. Può variare da 1 Gbps a 100 Gbps.

   b. Per Posizione, scegli la AWS Direct Connect posizione appropriata, quindi scegli il primo fornitore di servizi di localizzazione, seleziona il provider di servizi che fornisce la connettività per la connessione in questa posizione.

   c. Per Seconda posizione, scegli la posizione appropriata AWS Direct Connect nella seconda posizione, quindi scegli Provider di servizi di seconda posizione, seleziona il fornitore di servizi che fornisce la connettività per la connessione in questa seconda posizione.

   d. (Facoltativo) Configura la sicurezza MAC (MACsec) per la connessione. In Impostazioni aggiuntive, seleziona Richiedi una porta compatibile con MACsec.

MACsec è disponibile solo su connessioni dedicate.

e. (Facoltativo) Scegli Aggiungi tag per aggiungere coppie chiave/valore per identificare ulteriormente questa connessione.

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

Per rimuovere un tag esistente, scegli il tag, quindi Rimuovi tag. Non è possibile avere tag vuoti.

7. Seleziona Successivo.
8. Verifica la connessione nella pagina Verifica e crea. Questa pagina mostra anche i costi stimati per l'utilizzo delle porte e i costi aggiuntivi per il trasferimento dei dati.
9. Scegli Crea.
10. Scarica la lettera di autorizzazione e assegnazione della struttura di collegamento (LOA-CFA). Per ulteriori informazioni, consulta the section called “Scaricare la LOA-CFA”.

Utilizzare uno dei seguenti comandi.

- create-connection (AWS CLI)
- CreateConnection(AWS Direct Connect API)

Crea una connessione classica

Per le connessioni dedicate, puoi inviare una richiesta di connessione utilizzando la AWS Direct Connect console. Per le connessioni ospitate, collabora con un AWS Direct Connect partner per richiedere una connessione ospitata. Assicurati di disporre delle informazioni riportate di seguito:

- La velocità di porta richiesta. Per le connessioni dedicate, una volta creata la richiesta di connessione, non potrai modificare la velocità della porta. Per le connessioni ospitate, il Partner AWS Direct Connect può modificare la velocità.
- La AWS Direct Connect posizione in cui deve essere interrotta la connessione.

> **Note**
>
> Non è possibile utilizzare la AWS Direct Connect console per richiedere una connessione ospitata. Contatta invece un AWS Direct Connect partner, che può creare per te una connessione ospitata, che poi accetti. Ignora la procedura seguente e vai a Accettare una connessione ospitata.

Per creare una nuova AWS Direct Connect connessione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nella schermata AWS Direct Connect, in Get started (Inizia), selezionare Create a connection (Crea una connessione).
3. Scegliere Classic.
4. In Name (Nome), immettere un nome per la connessione.
5. Per Location (Sede), selezionare la località AWS Direct Connect appropriata.
6. Se applicabile, per Sub Location (Sede secondaria), scegliere il piano più vicino a te o al provider di rete. Questa opzione è disponibile soltanto se nella sede scelta sono presenti delle stanze meet-me (MMR, Meet-Me Room) su più piani dell'edificio.
7. In Port Speed (Velocità porta), scegliere la larghezza di banda per la connessione.
8. Per On-premise, seleziona Connetti tramite un partner AWS Direct Connect quando utilizzi questa connessione per connetterti al data center.
9. Per Service provider, seleziona il AWS Direct Connect Partner. Se utilizzi un partner non presente nell'elenco, seleziona Altro.
10. Se hai selezionato Altro per Provider di servizi, perNome dell'altro provider, immetti il nome del partner utilizzato.
11. (Facoltativo) Scegli Aggiungi tag per aggiungere coppie chiave/valore per identificare ulteriormente questa connessione.

    - In Chiave, immetti il nome della chiave.
    - In Valore, immetti il valore della chiave.

    Per rimuovere un tag esistente, scegli il tag, quindi Rimuovi tag. Non è possibile avere tag vuoti.

12. Scegli Crea connessione.

Possono essere necessarie fino a 72 ore AWS per esaminare la richiesta e fornire una porta per la connessione. Durante questo intervallo di tempo, potresti ricevere un'e-mail con una richiesta di ulteriori informazioni sul caso d'uso o sulla sede specificata. L'e-mail viene inviata all'indirizzo e-mail che hai utilizzato al momento della registrazione AWS. Devi rispondere entro 7 giorni o la connessione verrà eliminata.

Per ulteriori informazioni, consulta AWS Direct Connect connessioni.

Scaricare la LOA-CFA

Dopo che abbiamo elaborato la tua richiesta di connessione, puoi scaricare la LOA-CFA. Se il collegamento non è abilitato, vuol dire che la LOA-CFA non è ancora disponibile per il download. Controlla l'e-mail per una richiesta di informazioni.

La fatturazione inizia automaticamente quando la porta è attiva o 90 giorni dopo l'emissione del LOA, a seconda dell'evento che si verifica per primo. È possibile evitare i costi di fatturazione eliminando la porta prima dell'attivazione o entro 90 giorni dall'emissione del LOA.

Se la connessione non è attiva dopo 90 giorni e il LOA-CFA non è stato emesso, ti invieremo un'e-mail per avvisarti che la porta verrà eliminata entro 10 giorni. Se non riesci ad attivare la porta entro il periodo aggiuntivo di 10 giorni, la porta verrà automaticamente eliminata e dovrai riavviare il processo di creazione della porta.

> **Note**
>
> Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS Direct Connect. Se non desideri più utilizzare la connessione dopo aver emesso nuovamente la LOA-CFA, dovrai essere tu a eliminarla. Per ulteriori informazioni, consulta Elimina connessioni.

Console

Per scaricare la LOA-CFA

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Connections (Connessioni).

3. Seleziona la connessione e scegli Visualizza dettagli.
4. Scegliere Download LOA-CFA (Scarica LOA-CFA).

> **Note**
>
> Se il collegamento non è abilitato, vuol dire che la LOA-CFA non è ancora disponibile per il download. Verrà creato un caso Support per richiedere informazioni aggiuntive. Dopo aver risposto alla richiesta e averla elaborata, il LOA-CFA sarà disponibile per il download. Se non è ancora disponibile, contatta AWS Support.

5. Invia la LOA-CFA al tuo provider di rete o di co-location in modo che possa ordinare un'interconnessione per te. Le modalità di contatto possono variare in base al provider di co-location. Per ulteriori informazioni, consulta Richiesta di connessioni incrociate presso AWS Direct Connect le sedi.

Command line

Per scaricare il documento LOA-CFA utilizzando l'API o la riga di comando

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct Connect API)

Aggiornamento di una connessione

Puoi aggiornare i seguenti attributi di connessione:

- Il nome della connessione.
- La modalità di crittografia MACsec della connessione.

> **Note**
>
> MACsec è disponibile solo su connessioni dedicate.

I valori validi sono:

- `should_encrypt`
- `must_encrypt`

Quando si imposta la modalità di crittografia su questo valore, la connessione si interrompe quando la crittografia non è attiva.

- `no_encrypt`

Console

Per aggiornare una connessione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Connections (Connessioni).
3. Seleziona la connessione, quindi scegli Modifica.
4. Modificare la connessione:

   [Modificare il nome] Per Name (Nome), immettere un nuovo nome per la connessione.

   [Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.

   [Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).
5. Scegliere Edit connection (Modifica connessione).

Command line

Per aggiungere e rimuovere i tag utilizzando la riga di comando

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Per eliminare una connessione utilizzando l'API o la riga di comando

- update-connection (AWS CLI)
- UpdateConnection(AWS Direct Connect API)

Associa un MACsec CKN/CAK a una connessione

Dopo aver creato la connessione che supporta MACsec, puoi procedere ad associare un CKN/CAK alla connessione.

> **Note**
>
> Non è possibile modificare una chiave segreta MACsec dopo averla associata a una connessione. Se è necessario modificare la chiave, dissocia la chiave dalla connessione e quindi associa una nuova chiave alla connessione. Per ulteriori informazioni sulla rimozione di un'associazione, consulta the section called “Rimozione dell'associazione tra una chiave segreta MACsec e una connessione”.

Console

Per associare una connessione a una chiave MACsec

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di sinistra, scegli Connections (Connessioni).
3. Seleziona una connessione e scegli Visualizza dettagli.
4. Selezionare Associa chiave.
5. Immettere la chiave MACsec.

   [Usa la coppia CAK/CKN] Scegli Coppia di chiavi, quindi procedi come segue:

   - Per Connectivity Association Key (CAK), inserisci il CAK.
   - Per Connectivity Association Key Name (CKN), inserisci il CKN.

   [Usa il segreto] Scegli il segreto di Segreto di Segret Manager esistente, quindi per Segreto, seleziona la chiave segreta MACsec.
6. Selezionare Associa chiave.

Command line

Per associare una connessione a una chiave MACsec

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(AWS Direct Connect API)

Rimozione dell'associazione tra una chiave segreta MACsec e una connessione

Puoi rimuovere l'associazione tra la chiave segreta MACsec e la connessione.

Console

Rimuovere un'associazione tra una connessione e una chiave MACsec

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2.
3. Nel riquadro di sinistra, scegli Connections (Connessioni).
4. Seleziona una connessione e scegli Visualizza dettagli.
5. Seleziona il segreto MacSec da rimuovere, quindi scegli Annulla associazione chiave.
6. Nella finestra di dialogo di conferma immetti annulla associazione, quindi scegli Annulla associazione.

Command line

Rimuovere un'associazione tra una connessione e una chiave MACsec

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct Connect API)

Connessioni ospitate

Per creare una connessione AWS Direct Connect ospitata, sono necessarie le seguenti informazioni:

AWS Direct Connect posizione

Collabora con un AWS Direct Connect AWS Direct Connect partner del Partner Program per aiutarti a stabilire circuiti di rete tra una AWS Direct Connect sede e il tuo data center, ufficio o ambiente di colocation. I partner APN possono anche fornire uno spazio di co-location nella stessa struttura della sede. Per ulteriori informazioni, consulta Deliver partner AWS Direct Connect.

> **Note**
>
> Non puoi richiedere una connessione ospitata tramite la console. AWS Direct Connect Tuttavia, un AWS Direct Connect partner può creare e configurare una connessione ospitata per te. Una volta configurata, la connessione viene visualizzata nel riquadro Connessioni della console.
> Prima di iniziare a utilizzare una connessione ospitata, devi accettarla. Per ulteriori informazioni, consulta the section called “Accettare una connessione ospitata”.

Velocità porta

Per le connessioni ospitate, i valori possibili sono 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps e 25 Gbps. Tieni presente che solo AWS Direct Connect i partner che hanno soddisfatto requisiti specifici possono creare una connessione ospitata da 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps o 25 Gbps. Le connessioni a 25 Gbps sono disponibili solo nelle località Direct Connect in cui sono disponibili velocità di porta di 100 Gbps.

Tieni presente quanto segue:

- La velocità delle porte di connessione può essere modificata solo dal partner AWS Direct Connect . Non è più necessario eliminare e quindi ricreare una connessione per aggiornare o ridurre la larghezza di banda di una connessione ospitata esistente. Per modificare la velocità della porta, contatta il AWS Direct Connect partner che gestisce la connessione ospitata.
- AWS utilizza il controllo del traffico sulle connessioni ospitate, il che significa che quando la velocità di traffico raggiunge la velocità massima configurata, il traffico in eccesso viene eliminato. Ciò potrebbe comportare una velocità effettiva inferiore rispetto al traffico non velocizzato.
- Per le connessioni ospitate, i frame Jumbo possono essere abilitati solo se originariamente abilitati sulla connessione principale ospitata da AWS Direct Connect . Se i frame Jumbo non sono abilitati su quella connessione principale, non possono essere abilitati su nessuna connessione.

Le seguenti operazioni della console sono disponibili dopo aver richiesto e accettato una connessione ospitata:

- the section called “Visualizzare i dettagli di connessione”
- the section called “Aggiornamento di una connessione”
- the section called “Elimina connessioni”

Dopo aver accettato una connessione, crea un'interfaccia virtuale da connettere alle risorse AWS pubbliche e private. Per ulteriori informazioni, consulta AWS Direct Connect interfacce virtuali.

Accettare una connessione ospitata

Se sei interessato all'acquisto di una connessione ospitata, devi contattare un AWS Direct Connect AWS Direct Connect partner del Partner Program. Il partner effettua il provisioning della connessione per te. Una volta configurata, la connessione viene visualizzata nel riquadro Connessioni della console AWS Direct Connect .

Prima di iniziare a utilizzare una connessione in hosting, devi accettare la connessione.

Console

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Connections (Connessioni).
3. Seleziona la connessione ospitata e scegli Visualizza dettagli.
4. Seleziona la casella di controllo di conferma e scegli Accetta.

Command line

Per accettare una connessione in hosting utilizzando l'API o la riga di comando

- confirm-connection (AWS CLI)
- ConfirmConnection(AWS Direct Connect API)

Visualizzare i dettagli di connessione

Puoi visualizzare lo stato corrente della tua connessione. Puoi inoltre visualizzare l'ID della connessione (ad esempio, `dxcon-12nikabc`) e verificare che corrisponda all'ID della connessione riportato nella LOA-CFA che hai ricevuto o scaricato.

Per informazioni sul monitoraggio delle connessioni, consultare Monitoraggio.

Console

Per visualizzare i dettagli relativi a una connessione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di sinistra, scegli Connections (Connessioni).
3. Seleziona una connessione e scegli Visualizza dettagli.

Command line

Per descrivere una connessione utilizzando l'API o la riga di comando

- describe-connections (AWS CLI)
- DescribeConnections(AWS Direct Connect API)

Elimina connessioni

È possibile eliminare una connessione purché non vi siano collegate interfacce virtuali. L'eliminazione della connessione interrompe tutti i costi orari di porta per questa connessione, ma potrebbero comunque verificarsi addebiti per connessioni incrociate o addebiti per i circuiti di rete (vedi sotto). AWS Direct Connect i costi di trasferimento dei dati sono associati alle interfacce virtuali. Per ulteriori informazioni su come eliminare un'interfaccia virtuale, consulta Eliminazione di interfacce virtuali.

Prima di eliminare una connessione, scarica il LOA della connessione contenente le informazioni relative ai diversi account in modo da disporre delle informazioni pertinenti sui circuiti da disconnettere. Per i passaggi per scaricare la connessione LOA, consulta the section called “Scaricare la LOA-CFA”.

Quando elimini una connessione, AWS indicherà al provider di colocation di disconnettere il dispositivo di rete dal router Direct Connect rimuovendo il cavo di connessione incrociata in fibra ottica dal pannello di patch applicabile. AWS Tuttavia, il fornitore di circuiti o di colocation potrebbe comunque addebitarti i costi di connessione incrociata o dei circuiti di rete, poiché il cavo di connessione incrociata potrebbe essere ancora collegato al tuo dispositivo di rete. Questi addebiti per la connessione incrociata sono indipendenti da Direct Connect e devono essere annullati presso il fornitore della colocation o del circuito utilizzando le informazioni del LOA.

Se la connessione fa parte di un Link Aggregation Group (LAG), non puoi eliminarla se, così facendo, il numero minimo di connessioni operative nel LAG originale scende al di sotto della soglia impostata.

Console

Per eliminare una connessione

1. Apri la console all'indirizzo https://console.aws.amazon.com/directconnect/v2/home. AWS Direct Connect
2. Nel riquadro di navigazione, scegli Connections (Connessioni).
3. Selezionare le connessioni, quindi scegliere Delete (Elimina).
4. Nella finestra di dialogo di conferma Delete (Elimina), scegliere Delete (Elimina).

Command line

Per eliminare una connessione utilizzando l'API o la riga di comando

- delete-connection (AWS CLI)
- DeleteConnection(AWS Direct Connect API)

Richiesta di connessioni incrociate presso AWS Direct Connect le sedi

Dopo aver scaricato la Letter of Authorization e Connecting Facility Assignment (LOA-CFA), devi completare la tua connessione di rete incrociata, nota anche come interconnessione. Se disponi già di apparecchiature situate in una AWS Direct Connect località, contatta il provider appropriato per completare la connessione incrociata. Per le istruzioni specifiche per ogni fornitore, consulta la tabella seguente. Contatta il tuo fornitore per conoscere il prezzo delle interconnessioni. Una volta stabilita l'interconnessione, puoi creare le interfacce virtuali utilizzando la console AWS Direct Connect .

Alcune posizioni sono impostate come campus. Per ulteriori informazioni, incluse le velocità disponibili in ogni località, consulta Posizioni AWS Direct Connect.

Se non disponi già di apparecchiature in una AWS Direct Connect località, puoi collaborare con uno dei partner del AWS Partner Network (APN). Questi consentono di connettersi a una località AWS Direct Connect . Per ulteriori informazioni, consulta Supporto dei partner APN. AWS Direct Connect Devi condividere la LOA-CFA con il tuo fornitore selezionato per facilitare la tua richiesta di interconnessione.

Una AWS Direct Connect connessione può fornire l'accesso a risorse in altre regioni. Per ulteriori informazioni, consulta Accesso a una regione AWS remota.

> **Note**
>
> Se l'interconnessione non è completata entro 90 giorni, l'autorità concessa dalla LOA-CFA scade. Per rinnovare una LOA-CFA scaduta, puoi scaricarla nuovamente dalla console AWS Direct Connect . Per ulteriori informazioni, consulta Scaricare la LOA-CFA.

Co-locazioni

- Stati Uniti orientali (Ohio)
- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti occidentali (California settentrionale)
- US West (Oregon)
- Africa (Città del Capo)

- Asia Pacifico (Giacarta)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Seul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Canada (Centrale)
- Cina (Pechino)
- Cina (Ningxia)
- Europa (Francoforte)
- Europa (Irlanda)
- Europa (Milano)
- Europa (Londra)
- Europa (Parigi)
- Europa (Stoccolma)
- Europa (Zurigo)
- Israele (Tel Aviv)
- Medio Oriente (Bahrein)
- Medio Oriente (Emirati Arabi Uniti)
- Sud America (San Paolo)
- AWS GovCloud (Stati Uniti orientali)
- AWS GovCloud (Stati Uniti occidentali)

Stati Uniti orientali (Ohio)

Ubicazione	Come richiedere una connessione
Cologix COL2, Columbus	Contatta Cologix all'indirizzo sales@cologix.com.
Cologix MIN3, Minneapolis	Contatta Cologix all'indirizzo sales@cologix.com.
CyrusOne West III, Houston	Invia una richiesta utilizzando il portale del cliente

Ubicazione	Come richiedere una connessione
Equinix CH2, Chicago	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
QTS, Chicago	Contatta QTS all'indirizzo AConnect@qtsdatacenters.com.
Centri dati di neutralità, 1102 Grand, Kansas City	Contatta Netrality Data Centers all'indirizzo support@netrality.com.

Stati Uniti orientali (Virginia settentrionale)

Ubicazione	Come richiedere una connessione
165 Halsey Street, Newark	Contattare operations@165halsey.com.
CoreSite 32 km, New York	Effettua un ordine utilizzando il Portale CoreSite clienti. Dopo aver completato il modulo, rivedi l'ordine e quindi approvalo utilizzando il sito Web.
CoreSite VA1-VA2, Reston	Effettua un ordine nel Portale clienti. CoreSite Dopo aver completato il modulo, rivedi l'ordine e quindi approvalo utilizzan do il sito Web.
Digital Realty ATL1 e ATL2, Atlanta	Contatta Digital Realty all'indirizzo amazon.orders@digitalrealty.com.
Digital Realty IAD38, Ashburn	Contatta Digital Realty all'indirizzo amazon.orders@digitalrealty.com.
Equinix DC1-DC6 e DC10-D12, Ashburn	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix DAA1-DC3 e DC6, Dallas	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix MI1, Miami	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix NY5, Seacaucus	Contatta Equinix all'indirizzo awsdealreg@equinix.com.

Ubicazione	Come richiedere una connessione
KIO Networks QRO1, Querétaro, MX	Contatta KIO Networks».
Markley, One Summer Street, Boston	Per i clienti attuali, crea una richiesta utilizzando il portale clienti. Per nuove richieste contatta sales@markleygroup.com.
Netrality Data Center, 2° piano MMR, Philadelphia	Contatta Netrality Data Centers all'indirizzo support@netrality.com.
QTS ATL1, Atlanta	Contatta QTS all'indirizzo AConnect@qtsdatacenters.com.

Stati Uniti occidentali (California settentrionale)

Ubicazione	Come richiedere una connessione
CoreSite, LA 1, Los Angeles	Effettua un ordine utilizzando il Portale CoreSite clienti. Dopo aver completato il modulo, rivedi l'ordine e quindi approvalo utilizzando il sito Web.
CoreSite SV2, Milpitas	Effettua un ordine utilizzando il CoreSite Portale clienti. Dopo aver completato il modulo, rivedi l'ordine e quindi approvalo utilizzando il sito Web.
CoreSite SV4, Santa Clara	Effettua un ordine utilizzando il Portale CoreSite clienti. Dopo aver completato il modulo, verifica la correttezza dell'ordine, quindi approvalo utilizzando il MyCoreSite sito Web.
EdgeConneX, Fenice	Esegui un ordine utilizzando il portale del cliente EdgeOS. Dopo aver inviato il modulo, EdgeConne X fornirà un modulo di ordine di assistenza per l'approvazione. Puoi inviare domande all'indirizzo cloudaccess@edgeconnex.com.
Equinix LA3, El Segundo	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix SV1 e SV5, San Jose	Contatta Equinix all'indirizzo awsdealreg@equinix.com.

Ubicazione	Come richiedere una connessione
PhoenixNAP, Phoenix	Contatta phoenixNAP Provisioning all'indirizzo provisioning@phoenixnap.com.

US West (Oregon)

Ubicazione	Come richiedere una connessione
CoreSite DE 1, Denver	Effettua un ordine utilizzando il Portale CoreSite clienti. Dopo aver completato il modulo, rivedi l'ordine e quindi approvalo utilizzando il sito Web.
Digital Realty SEA10, Westin Building, Seattle	Contatta Digital Realty all'indirizzo amazon.orders@digitalrealty.com.
EdgeConneX, Portland	Esegui un ordine utilizzando il portale del cliente EdgeOS. Dopo aver inviato il modulo, EdgeConne X fornirà un modulo di ordine di assistenza per l'approvazione. Puoi inviare domande all'indirizzo cloudaccess@edgeconnex.com.
Equinix SE2, Seattle	Contatta Equinix all'indirizzo support@equinix.com.
Pittock Block, Portland	Invia le richieste tramite e-mail all'indirizzo crossconnect@pittock.com o telefonicamente al numero+1 503 226 6777.
Switch SUPERNAP 8, Las Vegas	Contatta Switch SUPERNAP all'indirizzo orders@supernap.com.
TierPoint Seattle	Contattaci TierPoint all'indirizzo sales@tierpoint.com.

Africa (Città del Capo)

Ubicazione	Come richiedere una connessione
Centro dati Teraco/Internet Exchange a Città del Capo	Contatta Teraco all'indirizzo support@teraco.co.za per clienti Teraco esistenti o connect@teraco.co.za per nuovi clienti.
Teraco JB1, Johannesburg, Sudafrica	Contatta Teraco all'indirizzo support@teraco.co.za per clienti Teraco esistenti o connect@teraco.co.za per nuovi clienti.

Asia Pacifico (Giacarta)

Ubicazione	Come richiedere una connessione
DCI JK3, Giacarta	Contatta DCI Indonesia all'indirizzo jessie.w@dci-indonesia.com.com.
Data center NTT 2, Giacarta	Contatta NTT all'indirizzo tps.cms.presales@global.ntt.

Asia Pacifico (Mumbai)

Ubicazione	Come richiedere una connessione
Equinix, Mumbai	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
NetMagic DC2, Bangalore	Contatta NetMagic Sales and Marketing al numero verde 18001033130 o all'indirizzo marketing@netmagicsolutions.com.
Sify Rabale, Mumbai	Contatta Sify all'indirizzo aws.directconnect@sifycorp.com.
STT Delhi DC2, Delhi	Contatta STT per richiedere informazioni. AWSDX@stt elemediagdc .it.
STT GDC Pvt. Ltd. VSB, Chennai	Contatta STT per richiedere informazioni. AWSDX@stt elemediagdc .it.

Ubicazione	Come richiedere una connessione
STT Hyderabad DC1, Hyderabad	Contatta STT per richiedere informazioni. AWSDX@stt elemediagdc .it.

Asia Pacifico (Seul)

Ubicazione	Come richiedere una connessione
Digital Realty ICN1, Seul	Contatta Digital Realty all'indirizzo amazon.orders@digitalrealty .com.
KINX Gasan Data Center, Seul	Contatta KINX all'indirizzo sales@kinx.net.
LG U+ Pyeong-Chon Mega Center, Seul	Invia il documento LOA all'indirizzo kidcadmin@lguplus.co.kr e center8@kidc.net.

Asia Pacifico (Singapore)

Ubicazione	Come richiedere una connessione
Equinix HK1, Tsuen Wan NT, RAS di Hong Kong	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix SG2, Singapore	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Global Switch, Singapore	Contatta Global Switch all'indirizzo salessingapore@glo balswitch.com.
GPX, Mumbai	Contatta GPX (Equinix) all'indirizzo awsdealreg@equinix.com.
iAdvantage Mega-i, Hong Kong	Contatta iAdvantage all'indirizzo cs@iadvantage.net oppure effettua un ordine utilizzando iAdvantage Cabling Order e-Form.
Menara AIMS, Kuala Lumpur	I clienti AIMS esistenti possono richiedere un ordine X-Connect tramite il portale del Servizio clienti compilando l'Engineering

Ubicazione	Come richiedere una connessione
	Work Order Request Form. Contattare service.delivery@aims.com.my per problemi di invio della richiesta.
Data center TCC, Bangkok	Contatta TCC Technology Co., Ltd all'indirizzo gateway.ne@tcc-technology.com.

Asia Pacifico (Sydney)

Ubicazione	Come richiedere una connessione
CDC Hume 2, Canberra	Accedi al portale clienti all'indirizzo CDC Customer Portal.
Datacom DH6, Auckland	Contatta Datacom presso Datacom Orbit —Auckland.
Equinix ME 2, Melbourne	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix SY3, Sydney	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Global Switch, Sydney	Contatta Global Switch all'indirizzo salessydney@globalswitch.com.
NEXTDC C1, Canberra	Contatta NEXTDC all'indirizzo nxtops@nextdc.com.
NEXTDC M1, Melbourne	Contatta NEXTDC all'indirizzo nxtops@nextdc.com.
NEXTDC P1, Perth	Contatta NEXTDC all'indirizzo nxtops@nextdc.com.
NEXTDC S2, Sydney	Contatta NEXTDC all'indirizzo nxtops@nextdc.com.

Asia Pacifico (Tokyo)

Ubicazione	Come richiedere una connessione
AT Tokyo Chuo Data Center, Tokyo	Contatta AT TOKYO all'indirizzo at-sales@attokyo.co.jp.

Ubicazione	Come richiedere una connessione
Chief Telecom LY, Taipei	Contattare Chief Telecom all'indirizzo vicky_chan@chief.com.tw.
Chunghwa Telecom, Taipei	Contatta CHT Taipei IDC NOC all'indirizzo taipei_idc@cht.com.tw.
Equinix OS1, Osaka	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix TY2, Tokyo	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
NEC Inzai, Inzai	Contatta NEC Inzai all'indirizzo connection_support@ices.jp.nec.com.

Canada (Centrale)

Ubicazione	Come richiedere una connessione
Allied 250 Front St W, Toronto	Contatta driches@alliedreit.com.
Cologix MTL3, Montreal	Contatta Cologix all'indirizzo sales@cologix.com.
Cologix VAN2, Vancouver	Contatta Cologix all'indirizzo sales@cologix.com.
eStruxture, Montreal	Contatta eStruxture all'indirizzo directconnect@estruxture.com.

Cina (Pechino)

Ubicazione	Come richiedere una connessione
CIDS Jiachuang IDC, Beijing	Contatta dx-order@sinnet.com.cn.
Sinnet Jiuxianqiao IDC, Pechino	Contatta dx-order@sinnet.com.cn.
GDS No. 3 Data Center, Shanghai	Contatta dx@nwcdcloud.cn.

Ubicazione	Come richiedere una connessione
GDS No. 3 Data Center, Shenzhen	Contatta dx@nwcdcloud.cn.

Cina (Ningxia)

Ubicazione	Come richiedere una connessione
Industrial Park IDC, Ningxia	Contatta dx@nwcdcloud.cn.
Shapotou IDC, Ningxia	Contatta dx@nwcdcloud.cn.

Europa (Francoforte)

Ubicazione	Come richiedere una connessione
CE Colo, Praga, Repubblica Ceca	Contatta CE Colo all'indirizzo info@cecolo.com.
DigiPlex Ulven, Oslo, Norvegia	Contattateci DigiPlex all'indirizzo helpme@digiplex.com.
Equinix AM3, Amsterdam, Paesi Bassi	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix FR5, Francoforte	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix HE6, Helsinki	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix MU1, Monaco	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix WA1, Varsavia	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Interxion AMS7, Amsterdam	Contatta Interxion all'indirizzo customer.services@interxion.com.
Interxion CPH2, Copenhagen	Contatta Interxion all'indirizzo customer.services@interxion.com.

Ubicazione	Come richiedere una connessione
Interxion FRA6, Francoforte	Contatta Interxion all'indirizzo customer.services@interxion.com.
Interxion MAD2, Madrid	Contatta Interxion all'indirizzo customer.services@interxion.com.
Interxion VIE2, Vienna	Contatta Interxion all'indirizzo customer.services@interxion.com.
Interxion ZUR1, Zurigo	Contatta Interxion all'indirizzo customer.services@interxion.com.
IPB, Berlino	Contatta IPB all'indirizzo kontakt@ipb.de.
Equinix ITConic MD2, Madrid	Contatta Equinix all'indirizzo awsdealreg@equinix.com.

Europa (Irlanda)

Ubicazione	Come richiedere una connessione
Digital Realty (UK), Docklands	Contatta Digital Realty (UK) all'indirizzo amazon.orders@digitalrealty.com.
Eircom Clonshaugh	Contatta Eircom all'indirizzo awsorders@eircom.ie.
Equinix DX1, Dublino	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix LD5, Londra (Slough)	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Interxion DUB2, Dublino	Contatta Interxion all'indirizzo customer.services@interxion.com.
Interxion MRS1, Marsiglia	Contatta Interxion all'indirizzo customer.services@interxion.com.

Europa (Milano)

Ubicazione	Come richiedere una connessione
CDLAN srl Via Caldera 21, Milano	Contatta CDLAN all'indirizzo sales@cdlan.it.

Ubicazione	Come richiedere una connessione
Equinix, ML2, Milano, Italia	Contatta Equinix all'indirizzo awsdealreg@equinix.com.

Europa (Londra)

Ubicazione	Come richiedere una connessione
Digital Realty (UK), Docklands	Contatta Digital Realty (UK) all'indirizzo amazon.orders@digitalrealty.com.
Equinix LD5, Londra (Slough)	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix MA3, Manchester	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Telehouse West, Londra	Contatta Telehouse UK all'indirizzo sales.support@uk.telehouse.net.

Europa (Parigi)

Ubicazione	Come richiedere una connessione
Equinix PA3, Parigi	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Interxion PAR7, Parigi	Contatta Interxion all'indirizzo customer.services@interxion.com.
Telehouse Voltaire, Parigi	Contatta Telehouse Paris Voltaire utilizzando la pagina Contattaci.

Europa (Stoccolma)

Ubicazione	Come richiedere una connessione
Interxion STO1, Stoccolma	Contatta Interxion all'indirizzo customer.services@interxion.com.

Europa (Zurigo)

Ubicazione	Come richiedere una connessione
Equinix ZRH51, Oberengstringen, Svizzera	Contatta Equinix all'indirizzo awsdealreg@equinix.com.

Israele (Tel Aviv)

Ubicazione	Come richiedere una connessione
MedOne, Haifa	Contatta MedOne all'indirizzo support@Medone.co.il
EdgeConnex, Herzliya	Contatta all'indirizzo info@edgeconnecx.com EdgeConnect

Medio Oriente (Bahrein)

Ubicazione	Come richiedere una connessione
AWS Bahrein DC53, Manama	Per completare la connessione, è possibile lavorare con uno dei nostri partner fornitori di rete nella posizione in cui stabilire la connettività. Fornirai quindi una lettera di autorizzazione (LOA) dal provider di rete AWS al AWS Support Center. AWS completa la connessione incrociata in questa posizione.
AWS Bahrain DC52, Manama	Per completare la connessione, è possibile lavorare con uno dei nostri partner fornitori di rete nella posizione in cui stabilire la connettività. Fornirai quindi una lettera di autorizzazione (LOA) dal provider di rete AWS al AWS Support Center. AWS completa la connessione incrociata in questa posizione.

Medio Oriente (Emirati Arabi Uniti)

Ubicazione	Come richiedere una connessione
Equinix DX1, Dubai, Emirati Arabi Uniti	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Etisalat SmartHub Data Center, Fujairah, Emirati Arabi Uniti	Contatta SmartHub Etisalat Data Center all'indirizzo -C& WS@etisalat.ae. IntlSales

Sud America (San Paolo)

Ubicazione	Come richiedere una connessione
Equinix RJ2, Rio de Janeiro	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Equinix SP4, San Paolo	Contatta Equinix all'indirizzo awsdealreg@equinix.com.
Tivit	Contatta Tivit all'indirizzo aws@tivit.com.br.

AWS GovCloud (Stati Uniti orientali)

Non puoi ordinare connessioni in questa regione.

AWS GovCloud (Stati Uniti occidentali)

Ubicazione	Come richiedere una connessione
Equinix SV5, San Jose	Contatta Equinix all'indirizzo awsdealreg@equinix.com.

AWS Direct Connect interfacce virtuali

È necessario creare una delle seguenti interfacce virtuali (VIF) per iniziare a utilizzare la connessione. AWS Direct Connect

- Interfaccia virtuale privata: un'interfaccia virtuale privata deve essere utilizzata per accedere a un VPC Amazon usando indirizzi IP privati.
- Interfaccia virtuale pubblica: un'interfaccia virtuale pubblica può accedere a tutti i servizi AWS pubblici utilizzando indirizzi IP pubblici.
- Interfaccia virtuale di transito: un'interfaccia virtuale di transito deve essere utilizzata per accedere a uno o più gateway di transito Amazon VPC associati ai gateway Direct Connect. È possibile utilizzare interfacce virtuali di transito con qualsiasi connessione AWS Direct Connect dedicata o ospitata a qualsiasi velocità. Per informazioni sulle configurazioni del gateway Direct Connect, consulta the section called “Gateway Direct Connect”.

Per connetterti ad altri AWS servizi utilizzando indirizzi IPv6, consulta la documentazione del servizio per verificare che l'indirizzamento IPv6 sia supportato.

Regole pubblicitarie per prefisso dell'interfaccia virtuale pubblica

Ti pubblicizziamo i prefissi Amazon appropriati in modo che tu possa raggiungere i tuoi VPC o altri servizi. AWS Puoi accedere a tutti i AWS prefissi tramite questa connessione, ad esempio Amazon EC2, Amazon S3 e Amazon.com. Non hai accesso ai prefissi non Amazon. Per un elenco aggiornato dei prefissi pubblicizzati da, consulta Intervalli di indirizzi IP in. AWSAWSRiferimenti generali di Amazon Web Services AWS non pubblicizza nuovamente i prefissi dei clienti ricevuti tramite le interfacce virtuali pubbliche AWS Direct Connect ad altri clienti. Per ulteriori informazioni sulle interfacce virtuali pubbliche e sulle policy di routing, consulta the section called “Policy di instradamento dell'interfaccia virtuale pubblica”.

> **Note**
>
> Ti consigliamo di utilizzare un filtro firewall (in base all'indirizzo di origine/destinazione dei pacchetti) per controllare il traffico da e verso alcuni prefissi. Se usi un filtro per il prefisso (mappa di instradamento), assicurati che questo accetti prefissi con corrispondenza esatta o

più lunghi. I prefissi pubblicizzati AWS Direct Connect possono essere aggregati e possono differire dai prefissi definiti nel filtro dei prefissi.

Interfacce virtuali ospitate

Per utilizzare la AWS Direct Connect connessione con un altro account, è possibile creare un'interfaccia virtuale ospitata per quell'account. Il proprietario dell'altro account deve accettare l'interfaccia virtuale in hosting per iniziare a utilizzarla. Un'interfaccia virtuale in hosting funziona esattamente come un'interfaccia virtuale standard e si può connettere a risorse pubbliche o a un VPC.

È possibile utilizzare interfacce virtuali di transito con connessioni Direct Connect dedicate o ospitate a qualsiasi velocità. Le connessioni ospitate supporta solo un'interfaccia virtuale.

Per creare un'interfaccia virtuale, è necessario disporre delle informazioni seguenti:

Risorsa	Informazioni obbligatorie
Connessione	La AWS Direct Connect connessione o il gruppo di aggregazione dei link (LAG) per cui si sta creando l'interfaccia virtuale.
Nome dell'interfaccia virtuale	Un nome per l'interfaccia virtuale.
Proprietario dell'interfaccia virtuale	Se stai creando l'interfaccia virtuale per un altro account, hai bisogno dell'ID dell'altro AWS account.
(Solo interfaccia virtuale privata) Connessione	Per connetterti a un VPC nella stessa AWS regione, è necessario il gateway privato virtuale per il tuo VPC. L'ASN per il lato Amazon della sessione BGP viene ereditato dal gateway virtuale privato. Quando crei un gateway privato virtuale, puoi specificare il tuo ASN privato. Altrimenti, Amazon fornisce un ASN predefinito. Per ulteriori informazioni, consulta l'articolo relativo alla Creare un gateway virtuale privato nella Guida dell'utente di Amazon VPC. Per la connessione a un VPC tramite un gateway Direct Connect, è necessari o il gateway Direct Connect. Per ulteriori informazioni, consulta Gateway Direct Connect.

Risorsa	Informazioni obbligatorie
VLAN	Un tag Rete dell'area locale virtuale (VLAN) univoco che non è già in uso sulla tua connessione. Il valore deve essere compreso tra 1 e 4094 e deve essere conforme allo standard Ethernet 802.1Q. Questo tag è necessario per tutto il traffico che attraversa la connessione AWS Direct Connect . Se disponi di una connessione ospitata, il tuo AWS Direct Connect partner offre questo valore. Non è possibile modificare il valore dopo aver creato l'interfaccia virtuale.

Risorsa	Informazioni obbligatorie

Indirizzi IP peer	Un'interfaccia virtuale può supportare una sessione di peering BGP per IPv4, IPv6 o una di ciascuna (dual-stack). Non utilizzare IP elastici (EIP) o Bring your own IP address (BYOIP) dal pool Amazon per creare un'interfaccia virtuale pubblica. Non puoi creare più sessioni BGP per la stessa famiglia di indirizzi IP sulla stessa interfaccia virtuale. Gli intervalli di indirizzi IP vengono assegnati a ciascuna estremità dell'interfaccia virtuale per la sessione di peering BGP.
	
	• IPv4:
	  • (Solo interfaccia virtuale pubblica) È necessario specificare indirizzi IPv4 pubblici univoci di cui si è proprietari. Il valore può essere uno dei seguenti:
	  • Un CIDR IPv4 di proprietà del cliente
	
	Questi possono essere qualsiasi IP pubblico (di proprietà del cliente o fornito da AWS), ma è necessario utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del router. AWS Ad esempio, se si assegna un `/31` intervallo, ad esempio, è possibile utilizzarlo per l'IP peer e `203.0.113.0` per l'IP peer. `203.0.113.0/31` `203.0.113.1` AWS Oppure, se allocate un `/24` intervallo, ad esempio, potreste utilizzarlo `198.51.100.10` per il vostro IP peer e `198.51.100.20` per l'IP peer. `198.51.100.0/24` AWS
	  • Un intervallo IP di proprietà del AWS Direct Connect partner o dell'ISP, insieme a un'autorizzazione LOA-CFA
	  • Un AWS CIDR /31 fornito. In caso contrario, contatta AWS Support per richiedere un CIDR IPv4 pubblico (e fornire un caso d'uso nella richiesta).
	
	Note
	Non possiamo garantire che saremo in grado di soddisfare tutte le richieste di indirizzi IPv4 pubblici AWS forniti.
	  • (Solo interfaccia virtuale privata) Amazon può generare indirizzi IPv4 privati per te. Se ne specifichi uno personalizzato, assicurati di specifica

Risorsa	Informazioni obbligatorie
	re i CIDR privati solo per l'interfaccia del router e l'interfaccia AWS Direct Connect. Ad esempio, non specificare altri indirizzi IP dalla rete locale. Analogamente a un'interfaccia virtuale pubblica, è necessari o utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del AWS router. Ad esempio, se si assegna un `/30` intervallo, ad esempio`192.168.0.0/30` , è possibile utilizzare `192.168.0.1` per l'IP peer e `192.168.0.2` per l'IP peer. AWS • IPv6: Amazon alloca automaticamente un CIDR IPv6 /125. Non puoi specificare indirizzi IPv6 peer personali.
Famiglia di indirizzi	Se la sessione di peering BGP sarà su IPv4 o IPv6.
Informazioni BGP	• Un numero di sistema autonomo (ASN) del Border Gateway Protocol (BGP) pubblico o privato per il lato della sessione BGP. Se utilizzi un ASN pubblico, devi esserne proprietario. Se utilizzi un ASN privato, puoi impostare un valore ASN personalizzato. Per un ASN a 16 bit, il valore deve Esser compreso nell'intervallo da 64512 a 65534. Per un ASN a 32 bit, il valore deve essere compreso nell'intervallo da 1 a 2147483647. La prependenza del sistema autonomo (AS) non funziona se utilizzi un ASN privato per un'interfaccia virtuale pubblica. • AWS abilita MD5 per impostazione predefinita. Tale opzione non è modificabile. • Una chiave di autenticazione MD5 BGP. Puoi fornire il tuo oppure lasciare che Amazon ne generi uno per te.

Risorsa	Informazioni obbligatorie

(Solo interfaccia virtuale pubblica) Prefissi che desideri pubblicizzare	Percorsi IPv4 pubblici o percorsi IPv6 per la pubblicità tramite BGP. Devi pubblicizzare almeno un prefisso utilizzando BGP, fino a un massimo di 1.000 prefissi.
	• IPv4: il CIDR IPv4 può sovrapporsi a un altro CIDR IPv4 pubblico annunciato utilizzando quando una delle seguenti condizioni è vera: AWS Direct Connect
	  • I CIDR AWS provengono da diverse regioni. Assicurati di applicare i tag della community BGP ai prefissi pubblici.
	  • Utilizzi AS_PATH quando disponi di un ASN pubblico in una configurazione attiva/passiva.
	  Per ulteriori informazioni, consulta la Policy di routing e community BGP.
	• IPv6: specificare una lunghezza di prefisso di /64 o inferiore.
	• È possibile aggiungere prefissi aggiuntivi a un file VIF pubblico esistente e pubblicizzarli contattando AWS support. Nel caso di supporto, fornisci un elenco di prefissi CIDR aggiuntivi che desideri aggiungere al file VIF pubblico e pubblicizzare.
	• Puoi specificare qualsiasi lunghezza del prefisso su un'interfaccia virtuale pubblica Direct Connect. IPv4 dovrebbe supportare qualsiasi cosa compresa tra /1 e /32 e IPv6 dovrebbe supportare qualsiasi cosa compresa tra /1 - /64.

Risorsa	Informazioni obbligatorie
(Solo interfaccia virtuale privata) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti in eccesso. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 9001 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettività di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I jumbo frame si applicano solo ai percorsi propagati da. AWS Direct Connect Se aggiungi route statiche a una tabella di routing che punta al gateway privato virtuale, il traffico instradato attraverso le route statiche viene inviato utilizzando 1500 MTU. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.
(Solo interfaccia virtuale Transit) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti superati. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 8500 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettiv ità di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I frame jumbo sono supportati fino a 8500 MTU per Direct Connect. Le route statiche e le rotte propagate configurate nella tabella di routing di Transit Gateway supporteranno i frame jumbo, incluse le istanze EC2 con voci della tabella di routing statica VPC al collegamento del gateway di transito alla VPN. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.

SiteLink

Se stai creando un'interfaccia virtuale privata o di transito, puoi usare. SiteLink

SiteLink è una funzionalità Direct Connect opzionale per interfacce private virtuali che consente la connettività tra due punti di presenza Direct Connect (PoPs) nella stessa AWS partizione utilizzando il percorso più breve disponibile sulla rete. AWS Ciò consente di connettere la rete on-premise tramite la rete globale AWS senza dover indirizzare il traffico attraverso una regione. Per ulteriori informazioni SiteLink , vedere Introduzione. AWS Direct Connect SiteLink

> **Note**
>
> SiteLink non è disponibile in nessuna AWS GovCloud (US) delle regioni della Cina.

È prevista una tariffa tariffaria separata per l'utilizzo SiteLink. Per ulteriori informazioni, consulta Prezzi di AWS Direct Connect.

SiteLink non supporta tutti i tipi di interfaccia virtuale. Nella seguente tabella viene indicato il tipo di interfaccia e se è supportata.

Tipo di interfaccia virtuale	Supportato/Non supportato
Interfaccia virtuale di transit	Supportato
Interfaccia virtuale privata associata a un gateway Direct Connect con un gateway virtuale.	Supportato
Interfaccia virtuale privata allegata a un gateway Direct Connect non associata un gateway virtuale o di transito.	Supportato
Interfaccia virtuale privata associata a un gateway virtuale.	Non supportato
Interfaccia virtuale pubblica	Non supportato

Il comportamento di routing del traffico da Regioni AWS (gateway virtuali o di transito) a posizioni locali tramite un'interfaccia virtuale SiteLink abilitata varia leggermente dal comportamento dell'interfaccia virtuale Direct Connect predefinita con preimpostazione del percorso. AWS Quando SiteLink è abilitata, le interfacce virtuali di An Regione AWS preferiscono un percorso BGP con una lunghezza del percorso AS inferiore da una posizione Direct Connect, indipendentemente dalla regione associata. Ad esempio, viene pubblicizzata una regione associata per ogni sede Direct Connect. Se SiteLink è disattivata, per impostazione predefinita il traffico proveniente da un gateway virtuale o di transito preferisce una posizione Direct Connect associata a tale posizione Regione AWS, anche se il router proveniente da sedi Direct Connect associate a diverse regioni pubblicizza un percorso con una lunghezza del percorso AS inferiore. Il gateway virtuale o di transito preferisce comunque il percorso dalle sedi Direct Connect locali alle Regione AWS associate.

SiteLink supporta una dimensione MTU massima del jumbo frame di 8500 o 9001, a seconda del tipo di interfaccia virtuale. Per ulteriori informazioni, consulta the section called “Impostazione di MTU di rete per interfacce virtuali private o di transito”.

Prerequisiti per le interfacce virtuali

Prima di creare un'interfaccia virtuale, esegui le operazioni descritte di seguito:

- Crea una connessione. Per ulteriori informazioni, consulta the section called “Creare una connessione utilizzando la procedura guidata di connessione”.
- Se hai più connessioni che vuoi trattare come fosse una sola, crea un Link Aggregation Group (LAG). Per informazioni, consulta Associazione di una connessione a un LAG..

Per creare un'interfaccia virtuale, è necessario disporre delle informazioni seguenti:

Risorsa	Informazioni obbligatorie
Connessione	La AWS Direct Connect connessione o il gruppo di aggregazione dei collegamenti (LAG) per cui si sta creando l'interfaccia virtuale.
Nome dell'interfaccia virtuale	Un nome per l'interfaccia virtuale.

Risorsa	Informazioni obbligatorie
Proprietario dell'interfaccia virtuale	Se stai creando l'interfaccia virtuale per un altro account, hai bisogno dell'ID dell'altro AWS account.
(Solo interfaccia virtuale privata) Connessione	Per connetterti a un VPC nella stessa AWS regione, è necessario il gateway privato virtuale per il tuo VPC. L'ASN per il lato Amazon della sessione BGP viene ereditato dal gateway virtuale privato. Quando crei un gateway privato virtuale, puoi specificare il tuo ASN privato. Altrimenti, Amazon fornisce un ASN predefinito. Per ulteriori informazioni, consulta l'articolo relativo alla Creare un gateway virtuale privato nella Guida dell'utente di Amazon VPC. Per la connessione a un VPC tramite un gateway Direct Connect, è necessari o il gateway Direct Connect. Per ulteriori informazioni, consulta Gateway Direct Connect.
VLAN	Un tag Rete dell'area locale virtuale (VLAN) univoco che non è già in uso sulla tua connessione. Il valore deve essere compreso tra 1 e 4094 e deve essere conforme allo standard Ethernet 802.1Q. Questo tag è necessario per tutto il traffico che attraversa la connessione AWS Direct Connect . Se disponi di una connessione ospitata, il tuo AWS Direct Connect partner offre questo valore. Non è possibile modificare il valore dopo aver creato l'interfaccia virtuale.

Risorsa	Informazioni obbligatorie

Indirizzi IP peer	Un'interfaccia virtuale può supportare una sessione di peering BGP per IPv4, IPv6 o una di ciascuna (dual-stack). Non utilizzare IP elastici (EIP) o Bring your own IP address (BYOIP) dal pool Amazon per creare un'interfaccia virtuale pubblica. Non puoi creare più sessioni BGP per la stessa famiglia di indirizzi IP sulla stessa interfaccia virtuale. Gli intervalli di indirizzi IP vengono assegnati a ciascuna estremità dell'interfaccia virtuale per la sessione di peering BGP.
	
	• IPv4:
	  • (Solo interfaccia virtuale pubblica) È necessario specificare indirizzi IPv4 pubblici univoci di cui si è proprietari. Il valore può essere uno dei seguenti:
	  • Un CIDR IPv4 di proprietà del cliente
	
	Questi possono essere qualsiasi IP pubblico (di proprietà del cliente o fornito da AWS), ma è necessario utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del router. AWS Ad esempio, se si assegna un `/31` intervallo, ad esempio, è possibile utilizzarlo per l'IP peer e `203.0.113.0` per l'IP peer. `203.0.113.0/31` `203.0.113.1` AWS Oppure, se allocate un `/24` intervallo, ad esempio, potreste utilizzarlo `198.51.100.10` per il vostro IP peer e `198.51.100.20` per l'IP peer. `198.51.100.0/24` AWS
	  • Un intervallo IP di proprietà del AWS Direct Connect partner o dell'ISP, insieme a un'autorizzazione LOA-CFA
	  • Un AWS CIDR /31 fornito. In caso contrario, contatta AWS Support per richiedere un CIDR IPv4 pubblico (e fornire un caso d'uso nella richiesta).
	
	Note
	Non possiamo garantire che saremo in grado di soddisfare tutte le richieste di indirizzi IPv4 pubblici AWS forniti.
	  • (Solo interfaccia virtuale privata) Amazon può generare indirizzi IPv4 privati per te. Se ne specifichi uno personalizzato, assicurati di specifica

Risorsa	Informazioni obbligatorie
	re i CIDR privati solo per l'interfaccia del router e l'interfaccia AWS Direct Connect. Ad esempio, non specificare altri indirizzi IP dalla rete locale. Analogamente a un'interfaccia virtuale pubblica, è necessari o utilizzare la stessa subnet mask sia per l'IP peer che per l'IP peer del AWS router. Ad esempio, se si assegna un `/30` intervallo, ad esempio`192.168.0.0/30` , è possibile utilizzare `192.168.0.1` per l'IP peer e `192.168.0.2` per l'IP peer. AWS • IPv6: Amazon alloca automaticamente un CIDR IPv6 /125. Non puoi specificare indirizzi IPv6 peer personali.
Famiglia di indirizzi	Se la sessione di peering BGP sarà su IPv4 o IPv6.
Informazioni BGP	• Un numero di sistema autonomo (ASN) del Border Gateway Protocol (BGP) pubblico o privato per il lato della sessione BGP. Se utilizzi un ASN pubblico, devi esserne proprietario. Se utilizzi un ASN privato, puoi impostare un valore ASN personalizzato. Per un ASN a 16 bit, il valore deve Esser compreso nell'intervallo da 64512 a 65534. Per un ASN a 32 bit, il valore deve essere compreso nell'intervallo da 1 a 2147483647. La prependenza del sistema autonomo (AS) non funziona se utilizzi un ASN privato per un'interfaccia virtuale pubblica. • AWS abilita MD5 per impostazione predefinita. Tale opzione non è modificabile. • Una chiave di autenticazione MD5 BGP. Puoi fornire il tuo oppure lasciare che Amazon ne generi uno per te.

Risorsa	Informazioni obbligatorie

(Solo interfaccia virtuale pubblica) Prefissi che desideri pubblicizzare	Percorsi IPv4 pubblici o percorsi IPv6 per la pubblicità tramite BGP. Devi pubblicizzare almeno un prefisso utilizzando BGP, fino a un massimo di 1.000 prefissi.
	• IPv4: il CIDR IPv4 può sovrapporsi a un altro CIDR IPv4 pubblico annunciato utilizzando quando una delle seguenti condizioni è vera: AWS Direct Connect
	  • I CIDR AWS provengono da diverse regioni. Assicurati di applicare i tag della community BGP ai prefissi pubblici.
	  • Utilizzi AS_PATH quando disponi di un ASN pubblico in una configurazione attiva/passiva.
	  Per ulteriori informazioni, consulta la Policy di routing e community BGP.
	• IPv6: specificare una lunghezza di prefisso di /64 o inferiore.
	• È possibile aggiungere prefissi aggiuntivi a un file VIF pubblico esistente e pubblicizzarli contattando AWS support. Nel caso di supporto, fornisci un elenco di prefissi CIDR aggiuntivi che desideri aggiungere al file VIF pubblico e pubblicizzare.
	• Puoi specificare qualsiasi lunghezza del prefisso su un'interfaccia virtuale pubblica Direct Connect. IPv4 dovrebbe supportare qualsiasi cosa compresa tra /1 e /32 e IPv6 dovrebbe supportare qualsiasi cosa compresa tra /1 - /64.

Risorsa	Informazioni obbligatorie
(Solo interfaccia virtuale privata) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti in eccesso. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 9001 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettività di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I jumbo frame si applicano solo ai percorsi propagati da. AWS Direct Connect Se aggiungi route statiche a una tabella di routing che punta al gateway privato virtuale, il traffico instradato attraverso le route statiche viene inviato utilizzando 1500 MTU. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.
(Solo interfaccia virtuale Transit) Frame jumbo	L'unità di trasmissione massima (MTU) dei pacchetti superati. AWS Direct Connect Il valore predefinito è 1500. L'impostazione della MTU di un'interf accia virtuale su 8500 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettiv ità di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. I frame jumbo sono supportati fino a 8500 MTU per Direct Connect. Le route statiche e le rotte propagate configurate nella tabella di routing di Transit Gateway supporteranno i frame jumbo, incluse le istanze EC2 con voci della tabella di routing statica VPC al collegamento del gateway di transito alla VPN. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella AWS Direct Connect console e trova la funzionalità Jumbo Frame compatibile nella pagina di configurazione generale dell'interfaccia virtuale.

Quando crei un'interfaccia virtuale puoi specificare l'account proprietario dell'interfaccia virtuale. Quando scegli un AWS account diverso dal tuo, si applicano le seguenti regole:

- Per le interfacce virtuali private e di transito, l'account si applica all'interfaccia virtuale e alla destinazione del gateway virtuale privato/Direct Connect.

- Per le interfacce virtuali pubbliche, l'account viene utilizzato per la fatturazione dell'interfaccia virtuale. L'utilizzo del Data Transfer Out (DTO) viene contabilizzato dal proprietario della risorsa alla velocità di trasferimento AWS Direct Connect dei dati.

> **Note**
>
> I prefissi a 31 bit sono supportati su tutti i tipi di interfaccia virtuale Direct Connect. Per ulteriori informazioni, consulta RFC 3021: Utilizzo dei prefissi a 31 bit sui collegamenti punto-punto IPv4.

Creazione di un'interfaccia virtuale.

Puoi creare un'interfaccia virtuale di transito per connetterti a un gateway di transito, un'interfaccia virtuale pubblica per connetterti a risorse pubbliche (servizi non VPC) o un'interfaccia virtuale privata per connetterti a un VPC.

Per creare un'interfaccia virtuale per account interni o AWS Organizations diversi dai tuoi AWS Organizations, crea un'interfaccia virtuale ospitata. Per ulteriori informazioni, consulta the section called "Crea un'interfaccia virtuale in hosting".

Prerequisiti

Prima di iniziare, assicurati di aver letto le informazioni riportate in Prerequisiti per le interfacce virtuali.

Creazione di un'interfaccia virtuale pubblica

Quando crei un'interfaccia virtuale pubblica, l'esame e l'approvazione della tua richiesta può richiedere fino a 72.

Per assegnare un'interfaccia virtuale pubblica

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).

4. In Virtual interface type (Tipo di interfaccia virtuale), per Type (Tipo) scegliere Public (Pubblico).
5. In Public virtual interface settings (Impostazioni interfaccia virtuale pubblica), procedere come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

   b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

   c. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

   d. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

      I valori validi sono 1-2147483647.
6. In Additional settings (Impostazioni aggiuntive), procedere come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

      [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

      - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
      - In Amazon router peer IP (IP peer del router Amazon), immettere l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

      [IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

   b. Per fornire la propria chiave BGP, immettere la chiave MD5 del BGP.

      Se non si inserisce un valore, procederemo a generare una chiave BGP. Se hai fornito la tua chiave, o se l'abbiamo generata noi, quel valore viene visualizzato nella colonna Chiave di autenticazione BGP nella pagina dei dettagli dell'interfaccia virtuale di Interfacce virtuali.

   c. Per pubblicizzare prefissi per Amazon, in Prefissi da pubblicizzare, immetti gli indirizzi CIDR IPv4 di destinazione (separati da virgole) a cui instradare il traffico tramite l'interfaccia virtuale.

> **Important**
>
> È possibile aggiungere prefissi aggiuntivi a un file VIF pubblico esistente e pubblicizzarli contattando AWS support. Nel caso di supporto, fornisci un elenco di prefissi CIDR aggiuntivi che desideri aggiungere al file VIF pubblico e pubblicizzare.

d. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).
8. Scarica la configurazione del router per il tuo dispositivo. Per ulteriori informazioni, consulta Download del file di configurazione del router.

Per creare un'interfaccia virtuale pubblica utilizzando l'API o la riga di comando

- create-public-virtual-interface (AWS CLI)
- CreatePublicVirtualInterface(AWS Direct Connect API)

Creare un'interfaccia virtuale privata.

È possibile fornire un'interfaccia virtuale privata a un gateway privato virtuale nella stessa regione della AWS Direct Connect connessione. Per ulteriori informazioni sulla fornitura di un'interfaccia virtuale privata a un AWS Direct Connect gateway, vedereUtilizzo dei gateway Direct Connect.

Se utilizzi la procedura guidata di VPC per creare un VPC, la propagazione dell'instradamento viene abilitata automaticamente. Con la propagazione dell'instradamento, gli instradamenti vengono popolati automaticamente nelle tabelle di routing nel tuo VPC. Se lo desideri, puoi disabilitare la propagazione dell'instradamento. Per ulteriori informazioni, consulta Abilitazione della propagazione del routing nella tabella di routing nella Guida per l'utente di Amazon VPC.

L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto maggiore consentito trasferibile attraverso la connessione. La MTU di un'interfaccia virtuale

privata può essere 1500 o 9001 (frame jumbo). La MTU di un'interfaccia virtuale di transito può essere 1500 o 8500 (frame jumbo). Puoi specificare la MTU quando crei l'interfaccia o la aggiorni dopo la creazione. L'impostazione della MTU di un'interfaccia virtuale su 8500 (frame jumbo) o 9001 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettività di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. Per controllare se una connessione o interfaccia virtuale supporta frame jumbo, selezionala nella console AWS Direct Connect e individua Jumbo Frame Capable (Predisposizione per frame jumbo) nella scheda Summary (Riepilogo).

Per effettuare il provisioning di un'interfaccia virtuale privata su un VPC

1. Aprire la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Tipo di interfaccia virtuale, scegli Privato.
5. In Impostazioni dell'interfaccia virtuale pubblica, procedi come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

   b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

   c. Per il proprietario dell'interfaccia virtuale, scegli Il mio AWS account se l'interfaccia virtuale è per il tuo AWS account.

   d. Per Direct Connect gateway (Gateway Direct Connect), selezionare il gateway Direct Connect.

   e. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

   f. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

      I valori validi sono compresi tra 1 e 2147483647.

6. In Impostazioni aggiuntive, procedi come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

      [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

- Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
- In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

> **Important**
>
> Se consenti l' AWS assegnazione automatica degli indirizzi IPv4, verrà allocato un CIDR /29 da 169.254.0.0/16 IPv4 Link-Local secondo RFC 3927 per la connettività. point-to-point AWS non consiglia questa opzione se si intende utilizzare l'indirizzo IP peer del router del cliente come origine e/o destinazione per il traffico VPC. È invece consigliabile utilizzare RFC 1918 o un altro indirizzo (diverso da RFC 1918) e specificare personalmente l'indirizzo.
>
> - Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.
> - Per ulteriori informazioni su RFC 3927, consulta Dynamic Configuration of IPv4 Link-Local Addresses.

[IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

b. Per modificare l'unità di trasmissione massima (MTU) da 1500 (predefinito) a 9001 (frame jumbo), seleziona Jumbo MTU (MTU size 9001) (MTU jumbo - dimensione della MTU 9001).

c. (Facoltativo) In Abilita SiteLink, scegli Abilitato per abilitare la connettività diretta tra i punti di presenza Direct Connect.

d. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).

8. Scarica la configurazione del router per il tuo dispositivo. Per ulteriori informazioni, consulta Download del file di configurazione del router.

Per creare un'interfaccia virtuale privata utilizzando l'API o la riga di comando

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface(AWS Direct Connect API)

Creazione di un'interfaccia virtuale di transito per un gateway Direct Connect

Per connettere la AWS Direct Connect connessione al gateway di transito, è necessario creare un'interfaccia di transito per la connessione. Specificare il gateway Direct Connect al quale connettersi.

L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto maggiore consentito trasferibile attraverso la connessione. La MTU di un'interfaccia virtuale privata può essere 1500 o 9001 (frame jumbo). La MTU di un'interfaccia virtuale di transito può essere 1500 o 8500 (frame jumbo). Puoi specificare la MTU quando crei l'interfaccia o la aggiorni dopo la creazione. L'impostazione della MTU di un'interfaccia virtuale su 8500 (frame jumbo) o 9001 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettività di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. Per controllare se una connessione o interfaccia virtuale supporta frame jumbo, selezionala nella console AWS Direct Connect e individua Jumbo Frame Capable (Predisposizione per frame jumbo) nella scheda Summary (Riepilogo).

> **Important**
>
> Se associ il tuo gateway di transito a uno o più gateway Direct Connect, il numero di sistema autonomo (ASN) utilizzato dal gateway di transito e dal gateway Direct Connect devono essere diversi. Ad esempio, se utilizzi l'ASN 64512 predefinito sia per il gateway di transito che per il gateway Direct Connect, la richiesta di associazione ha esito negativo.

Per effettuare il provisioning di un'interfaccia virtuale di transito in un gateway Direct Connect

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Virtual interface type (Tipo di interfaccia virtuale), per Type (Tipo) scegliere Transit (Transito).
5. In Transit virtual interface settings (Impostazioni interfaccia virtuale di transito), procedere come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

   b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

   c. Per il proprietario dell'interfaccia virtuale, scegli Il mio AWS account se l'interfaccia virtuale è per il tuo AWS account.

   d. Per Direct Connect gateway (Gateway Direct Connect), selezionare il gateway Direct Connect.

   e. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

   f. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

      I valori validi sono compresi tra 1 e 2147483647.

6. In Impostazioni aggiuntive, procedi come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

      [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

      - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
      - In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

      > **Important**
      >
      > Se consenti l' AWS assegnazione automatica degli indirizzi IPv4, verrà allocato un CIDR /29 da 169.254.0.0/16 IPv4 Link-Local secondo RFC 3927 per la connettività.

point-to-point AWS non consiglia questa opzione se si intende utilizzare l'indirizzo IP peer del router del cliente come origine e/o destinazione per il traffico VPC. È invece consigliabile utilizzare RFC 1918 o un altro indirizzo (diverso da RFC 1918) e specificare personalmente l'indirizzo.

- Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.
- Per ulteriori informazioni su RFC 3927, consulta Dynamic Configuration of IPv4 Link-Local Addresses.

[IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

b. Per modificare l'unità di trasmissione massima (MTU) da 1500 (predefinito) a 8500 (frame jumbo), selezionare Jumbo MTU (MTU size 8500) (MTU jumbo - dimensione della MTU 8500).

c. (Facoltativo) In Abilita SiteLink, scegli Abilitato per abilitare la connettività diretta tra i punti di presenza Direct Connect.

d. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).

Dopo aver creato l'interfaccia virtuale, è possibile scaricare la configurazione del router per il dispositivo. Per ulteriori informazioni, consulta Download del file di configurazione del router.

Per creare un'interfaccia virtuale di transito utilizzando l'API o la riga di comando

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS Direct Connect API)

Per visualizzare le interfacce virtuali collegate a un gateway Direct Connect utilizzando l'API o la riga di comando

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGatewayAllegati (AWS Direct Connect API)

Download del file di configurazione del router

Dopo aver creato l'interfaccia virtuale e quando lo stato dell'interfaccia è impostato, è possibile scaricare il file di configurazione del router per il router.

Se utilizzi uno dei seguenti router per interfacce virtuali con MACSec attivato, creiamo automaticamente il file di configurazione per il router:

- Switch Cisco Nexus serie 9K+ con software NX-OS 9.3 o versione successiva
- Router Juniper Networks serie M/MX con software JunOS 9.5 o versioni successive

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Selezionare l'interfaccia virtuale,quindi scegliere View details (Visualizza dettagli).
4. Scegliere Download router configuration (Scarica configurazione router).
5. In Download Router Configuration (Scarica configurazione router), procedere come segue:
   a. Per Vendor (Fornitore), selezionare il produttore del router.
   b. Per Platform (Piattaforma), selezionare il modello del router.
   c. Per Software, selezionare la versione software del router.
6. Scegliere Download (Scarica), quindi utilizzare la configurazione del router appropriata per assicurare la connettività ad AWS Direct Connect.

Considerazioni relative a MACsec

Se devi configurare manualmente il router per MACSec, utilizza la seguente tabella come linea guida.

Parametro	Descrizione
Lunghezza CKN	Si tratta di una stringa di 64 caratteri esadecimali (0 - 9, A - E). Utilizza l'intera lunghezza per massimizzare la compatibilità multipiattaforma.
Lunghezza CAK	Si tratta di una stringa di 64 caratteri esadecimali (0 - 9, A - E). Utilizza l'intera lunghezza per massimizzare la compatibilità multipiattaforma.
Algoritmo crittografico	AES_256_CMAC
Suite di cifratura SAK	• Per connessioni a 100 Gbps: GCM_AES_XPN_256 • Per connessioni a 10 Gbps: GCM_AES_XPN_256 o GCM_AES _256
Suite Key Cipher	16
Offset di riservatezza	0
Indicatore ICV	No
Tempo di emissione di chiave SAK	Rollover PN>

Visualizzazione dei dettagli dell'interfaccia virtuale

Puoi visualizzare lo stato attuale dell'interfaccia virtuale. I dettagli includono:

- Stato connessione
- Nome
- Ubicazione
- VLAN
- Dettagli BGP

- Indirizzi IP peer

Per visualizzare i dettagli relativi a un'interfaccia virtuale

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di sinistra, scegliere Virtual Interfaces (Interfacce virtuali).
3. Selezionare l'interfaccia virtuale,quindi scegliere View details (Visualizza dettagli).

Per descrivere le interfacce virtuali utilizzando l'API o la riga di comando

- describe-virtual-interfaces (AWS CLI)
- DescribeVirtualInterfacce (AWS Direct Connect API)

Aggiungere o eliminare un peer BGP

Aggiungi o elimina una sessione di peering BGP IPv4 o IPv6 all'interfaccia virtuale.

Un interfaccia virtuale può supportare un'unica sessione di peering BGP IPv4 e un'unica sessione di peering BGP IPv6.

Non è possibile specificare i propri indirizzi IPv6 peer per una sessione di peering BGP IPv6. Amazon alloca automaticamente un CIDR IPv6 /125.

Il BGP multiprotocollo non è supportato. IPv4 e IPv6 operano in modalità dual-stack per l'interfaccia virtuale.

AWS abilita MD5 per impostazione predefinita. Tale opzione non è modificabile.

Aggiunta di un peer BGP

Utilizza la procedura seguente per aggiungere un peer BGP.

Per aggiungere un peer BGP

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.

2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Selezionare l'interfaccia virtuale,quindi scegliere View details (Visualizza dettagli).
4. Scegliere Add peering (Aggiungi peering).
5. (Interfaccia virtuale privata) Per aggiungere peer BGP IPv4, procedi nel seguente modo:
   - Scegliere IPv4.
   - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico. In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.
6. (Interfaccia virtuale pubblica) Per aggiungere peer BGP IPv4, procedi nel seguente modo:
   - In Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui inviare il traffico.
   - In Amazon router peer IP (IP peer del router Amazon), immettere l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

   > **Important**
   >
   > Se consenti l' AWS assegnazione automatica degli indirizzi IP, verrà allocato un CIDR /29 da 169.254.0.0/16. AWS non consiglia questa opzione se si intende utilizzare l'indirizzo IP peer del router del cliente come origine e destinazione del traffico. Ti consigliamo invece di utilizzare RFC 1918 o un altro indirizzo e di specificare manualmente l'indirizzo. Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.
7. (Interfaccia virtuale privata o pubblica) Per aggiungere peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon; non è possibile specificare indirizzi IPv6 personalizzati.
8. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

   Per un'interfaccia virtuale pubblica, l'ASN deve essere privato o già autorizzato per l'interfaccia virtuale.

   I valori validi sono 1-2147483647.

   Se non si immette un valore, ne assegneremo automaticamente uno.

9. Per fornire la propria chiave BGP per BGP Authentication Key (Chiave autenticazione BGP), immettere la chiave MD5 del BGP.
10. Scegliere Add peering (Aggiungi peering).

Per creare un peer BGP utilizzando l'API o la riga di comando

- create-bgp-peer (AWS CLI)
- CreateBGPPeer (API)AWS Direct Connect

Per eliminare un peer BGP

Se la tua interfaccia virtuale dispone di una sessione di peering BGP sia IPv4 che IPv6, puoi eliminarne una (ma non entrambe).

Per eliminare un peer BGP

1. Apri la console all'indirizzo https://console.aws.amazon.com/directconnect/v2/home. AWS Direct Connect
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Selezionare l'interfaccia virtuale,quindi scegliere View details (Visualizza dettagli).
4. In Peerings (Peering), selezionare il peering da eliminare e scegliere Delete (Elimina).
5. Nella finestra di dialogo Remove peering from virtual interface (Rimuovi peering da interfaccia virtuale), scegliere Delete (Elimina).

Per eliminare un peer BGP utilizzando l'API o la riga di comando

- delete-bgp-peer (AWS CLI)
- DeleteBGPPeer (API)AWS Direct Connect

Impostazione di MTU di rete per interfacce virtuali private o di transito

AWS Direct Connect supporta una dimensione del frame Ethernet di 1522 o 9023 byte (intestazione Ethernet da 14 byte+tag VLAN da 4 byte+ byte per il datagramma IP + 4 byte FCS) a livello di collegamento.

L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto maggiore consentito trasferibile attraverso la connessione. La MTU di un'interfaccia virtuale privata può essere 1500 o 9001 (frame jumbo). La MTU di un'interfaccia virtuale di transito può essere 1500 o 8500 (frame jumbo). Puoi specificare la MTU quando crei l'interfaccia o la aggiorni dopo la creazione. L'impostazione della MTU di un'interfaccia virtuale su 8500 (frame jumbo) o 9001 (frame jumbo) può causare un aggiornamento della connessione fisica sottostante, se non è stata aggiornata per supportare i frame jumbo. L'aggiornamento della connessione interrompe la connettività di rete per tutte le interfacce virtuali associate alla connessione per un massimo di 30 secondi. Per verificare se una connessione o un'interfaccia virtuale supporta i jumbo frame, selezionala nella console e trova Jumbo Frame Capable nella scheda Riepilogo. AWS Direct Connect

Dopo aver abilitato i frame jumbo per l'interfaccia privata virtuale o l'interfaccia virtuale di transito, puoi associarla solamente a una connessione o LAG predisposta per frame jumbo. I frame jumbo sono supportati su interfacce private virtuali collegate a un gateway privato virtuale o a un gateway Direct Connect, o su un'interfaccia virtuale di transito collegata a un gateway Direct Connect. Se disponi di due interfacce virtuali private che pubblicizzano la stessa route ma utilizzano valori MTU diversi o se invece disponi di una VPN sito-sito che pubblicizza lo stesso percorso, viene utilizzato 1500 MTU.

> **Important**
>
> I jumbo frame si applicheranno solo ai percorsi propagati AWS Direct Connect e ai percorsi statici tramite i gateway di transito. I frame jumbo sui gateway di transito supportano solo 8500 byte.
> Se un'istanza EC2 non supporta frame jumbo, elimina i frame Jumbo da Direct Connect. Tutti i tipi di istanza EC2 supportano frame jumbo tranne C1, CC1, T1 e M1. Per ulteriori informazioni, consulta Network Maximum Transmission Unit (MTU) per la tua istanza EC2 nella Amazon EC2 User Guide.
> Per le connessioni ospitate, i frame Jumbo possono essere abilitati solo se originariamente abilitati sulla connessione principale ospitata da Direct Connect. Se i frame Jumbo non sono abilitati su quella connessione principale, non possono essere abilitati su nessuna connessione.

Per impostare la MTU di un'interfaccia virtuale privata

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.

2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Selezionare l'interfaccia virtuale e scegliere Edit (Modifica).
4. In Jumbo MTU (MTU size 9001) (MTU jumbo - dimensione della MTU 9001) o Jumbo MTU (MTU size 8500) (MTU jumbo - dimensione della MTU 8500), selezionare Enabled (Abilitato).
5. In Acknowledge (Accetta), selezionare I understand the selected connection(s) will go down for a brief period (Sono consapevole che le connessioni selezionate non saranno disponibili per un breve periodo. Lo stato dell'interfaccia virtuale è `pending` fino al termine dell'aggiornamento.

Per impostare la MTU di un'interfaccia virtuale privata utilizzando la riga di comando o l'API

- update-virtual-interface-attributes (AWS CLI)
- UpdateVirtualInterfaceAttributes(AWS Direct Connect API)

Per aggiungere o rimuovere un tag per interfacce virtuali

I tag forniscono un modo per identificare l'interfaccia virtuale. Puoi aggiungere o rimuovere un tag se sei il proprietario dell'account per l'interfaccia virtuale.

Per aggiungere o rimuovere un tag per interfacce virtuali

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Selezionare l'interfaccia virtuale e scegliere Edit (Modifica).
4. Aggiungi o rimuovi un tag.

   [Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.

   [Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).
5. Scegliere Edit virtual interface (Modifica interfaccia virtuale).

Per aggiungere e rimuovere i tag utilizzando la riga di comando

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Eliminazione di interfacce virtuali

Eliminare una o più interfacce virtuali. Per eliminare una connessione, è necessario eliminare la relativa interfaccia virtuale. L'eliminazione di un'interfaccia virtuale interrompe AWS Direct Connect i costi di trasferimento dei dati associati all'interfaccia virtuale.

Per eliminare un'interfaccia virtuale

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di sinistra, scegliere Virtual Interfaces (Interfacce virtuali).
3. Selezionare le interfacce virtuali e scegliere Delete (Elimina).
4. Nella finestra di dialogo di conferma Delete (Elimina), scegliere Delete (Elimina).

Per eliminare un'interfaccia virtuale utilizzando l'API o la riga di comando

- delete-virtual-interface (AWS CLI)
- DeleteVirtualInterfaccia (AWS Direct Connect API)

Crea un'interfaccia virtuale in hosting

Puoi creare un'interfaccia virtuale in hosting pubblica, di transito o privata. Prima di iniziare, assicurati di aver letto le informazioni riportate in Prerequisiti per le interfacce virtuali.

Per creare un'interfaccia virtuale in hosting privata

Per creare un'interfaccia virtuale in hosting privata

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).

3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Tipo di interfaccia virtuale, per Tipo scegli Pubblico.
5. In Impostazioni dell'interfaccia virtuale pubblica, procedi come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

   b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

   c. Per Proprietario dell'interfaccia virtuale, scegli Altro AWS account, quindi per Proprietario dell'interfaccia virtuale, inserisci l'ID dell'account proprietario dell'interfaccia virtuale.

   d. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

   e. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

      I valori validi sono 1-2147483647.

6. In Impostazioni aggiuntive, procedi come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

      [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

      - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
      - In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

      > **Important**
      >
      > Se consenti l' AWS assegnazione automatica degli indirizzi IP, verrà allocato un CIDR /29 da 169.254.0.0/16. AWS non consiglia questa opzione se si intende utilizzare l'indirizzo IP peer del router del cliente come origine e destinazione del traffico. È invece consigliabile utilizzare RFC 1918 o un altro indirizzo (diverso da RFC 1918) e specificare personalmente l'indirizzo. Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.

[IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

b. Per modificare l'unità di trasmissione massima (MTU) da 1500 (predefinito) a 9001 (frame jumbo), seleziona Jumbo MTU (MTU size 9001) (MTU jumbo - dimensione della MTU 9001).

c. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Dopo che il proprietario dell'altro account AWS avrà accettato l'interfaccia virtuale in hosting, potrai scaricare il file di configurazione del router.

Per creare un'interfaccia virtuale in hosting privata utilizzando l'API o la riga di comando

- allocate-private-virtual-interface (AWS CLI)
- AllocatePrivateVirtualInterface(API)AWS Direct Connect

Per creare un'interfaccia virtuale in hosting pubblica

Per creare un'interfaccia virtuale in hosting pubblica

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Virtual interface type (Tipo di interfaccia virtuale), per Type (Tipo) scegliere Public (Pubblico).
5. In Public Virtual Interface Settings (Impostazioni interfaccia virtuale pubblica), procedere come segue:

a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

c. Per Proprietario dell'interfaccia virtuale, scegli Altro AWS account, quindi per Proprietario dell'interfaccia virtuale, inserisci l'ID dell'account proprietario dell'interfaccia virtuale.

d. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

e. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

   I valori validi sono 1-2147483647.

6. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

   [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

   - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
   - In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

   > **Important**
   >
   > Se consenti l' AWS assegnazione automatica degli indirizzi IP, verrà allocato un CIDR /29 da 169.254.0.0/16. AWS non consiglia questa opzione se si intende utilizzare l'indirizzo IP peer del router del cliente come origine e destinazione del traffico. Ti consigliamo invece di utilizzare RFC 1918 o un altro indirizzo e di specificare manualmente l'indirizzo. Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.

   [IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

7. Per pubblicizzare prefissi per Amazon, in Prefissi da pubblicizzare, immetti gli indirizzi CIDR IPv4 di destinazione (separati da virgole) a cui instradare il traffico tramite l'interfaccia virtuale.

8. Per fornire una chiave personalizzata per l'autenticazione della sessione BGP, in Additional Settings (Impostazioni aggiuntive), per BGP authentication key (Chiave di autenticazione BGP) immettere la chiave.

   Se non si inserisce un valore, procederemo a generare una chiave BGP.

9. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

10. Scegliere Create virtual interface (Crea interfaccia virtuale).
11. Dopo che il proprietario dell'altro account AWS avrà accettato l'interfaccia virtuale in hosting, potrai scaricare il file di configurazione del router.

Per creare un'interfaccia virtuale in hosting pubblica utilizzando l'API o la riga di comando

- allocate-public-virtual-interface (AWS CLI)
- AllocatePublicVirtualInterface(AWS Direct Connect API)

Per creare un’interfaccia virtuale di transito in hosting

Per creare un’interfaccia virtuale di transito in hosting

> **Important**
>
> Se associ il tuo gateway di transito a uno o più gateway Direct Connect, il numero di sistema autonomo (ASN) utilizzato dal gateway di transito e dal gateway Direct Connect devono essere diversi. Ad esempio, se utilizzi l'ASN 64512 predefinito sia per il gateway di transito che per il gateway Direct Connect, la richiesta di associazione ha esito negativo.

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Virtual interface type (Tipo di interfaccia virtuale), per Type (Tipo) scegliere Transit (Transito).
5. In Transit virtual interface settings (Impostazioni interfaccia virtuale di transito), procedere come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

c. Per Proprietario dell'interfaccia virtuale, scegli Altro AWS account, quindi per Proprietario dell'interfaccia virtuale, inserisci l'ID dell'account proprietario dell'interfaccia virtuale.

d. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

e. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

   I valori validi sono 1-2147483647.

6. In Impostazioni aggiuntive, procedi come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

      [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

      - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
      - In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

      > **Important**
      >
      > Se consenti l' AWS assegnazione automatica degli indirizzi IP, verrà allocato un CIDR /29 da 169.254.0.0/16. AWS non consiglia questa opzione se si intende utilizzare l'indirizzo IP peer del router del cliente come origine e destinazione del traffico. Ti consigliamo invece di utilizzare RFC 1918 o un altro indirizzo e di specificare manualmente l'indirizzo. Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.

      [IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

   b. Per modificare l'unità di trasmissione massima (MTU) da 1500 (predefinito) a 8500 (frame jumbo), selezionare Jumbo MTU (MTU size 8500) (MTU jumbo - dimensione della MTU 8500).

   c. [Facoltativo] Aggiungere un tag. Esegui questa operazione:

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).
8. Dopo che il proprietario dell'altro account AWS avrà accettato l'interfaccia virtuale in hosting, potrai scaricare il file di configurazione del router.

Per creare un'interfaccia virtuale di transito in hosting utilizzando l'API o la riga di comando

- allocate-transit-virtual-interface (AWS CLI)
- AllocateTransitVirtualInterface(AWS Direct Connect API)

Accetta un'interfaccia virtuale in hosting.

Prima di iniziare a utilizzare un'interfaccia virtuale in hosting, devi accettare l'interfaccia virtuale. Per un'interfaccia virtuale privata, devi inoltre disporre di un gateway privato virtuale o di un gateway Direct Connect esistente. Per un'interfaccia virtuale di transito, devi disporre di un gateway di transito o di un gateway Direct Connect esistente.

Per accettare un'interfaccia virtuale in hosting

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Selezionare l'interfaccia virtuale,quindi scegliere View details (Visualizza dettagli).
4. Scegliere Accept (Accetta).
5. Questo vale per le interfacce virtuali private e le interfacce virtuali di transito.

   (Interfaccia virtuale di transito) Nella finestra di dialogo Accept virtual interface (Accetta interfaccia virtuale), selezionare un gateway Direct Connect, quindi scegliere Accept virtual interface (Accetta interfaccia virtuale).

(Interfaccia virtuale privata) Nella finestra di dialogo Accept virtual interface (Accetta interfaccia virtuale), selezionare un gateway virtuale privato o un gateway Direct Connect, quindi scegliere Accept virtual interface (Accetta interfaccia virtuale).

6. Dopo che aver accettato l'interfaccia virtuale in hosting, il proprietario della connessione AWS Direct Connect potrà scaricare il file di configurazione del router. L'opzione Download router configuration (Scarica configurazione router) non è disponibile per l'account che accetta l'interfaccia virtuale in hosting.

Per accettare un'interfaccia virtuale in hosting privata utilizzando l'API o la riga di comando

- confirm-private-virtual-interface (AWS CLI)
- ConfirmPrivateVirtualInterface(AWS Direct Connect API)

Per accettare un'interfaccia virtuale in hosting pubblica utilizzando l'API o la riga di comando

- confirm-public-virtual-interface (AWS CLI)
- ConfirmPublicVirtualInterface(AWS Direct Connect API)

Per accettare un'interfaccia virtuale di transito in hosting utilizzando l'API o la riga di comando

- confirm-transit-virtual-interface (AWS CLI)
- ConfirmTransitVirtualInterface(AWS Direct Connect API)

Per eseguire la migrazione di un'interfaccia virtuale

Utilizzare questa procedura per eseguire una delle seguenti operazioni di migrazione dell'interfaccia virtuale:

- Eseguire la migrazione di un'interfaccia virtuale esistente associata a una connessione a un altro LAG.
- Eseguire la migrazione di un'interfaccia virtuale esistente associata a un LAG esistente a un nuovo LAG.
- Eseguire la migrazione di un'interfaccia virtuale esistente associata a una connessione a un'altra connessione.

Note

- È possibile migrare un'interfaccia virtuale a una nuova connessione all'interno della stessa regione, ma non è possibile migrarla da una regione all'altra. Quando si esegue la migrazione o si associa un'interfaccia virtuale esistente a una nuova connessione, i parametri di configurazione associati alle interfacce virtuali sono gli stessi. Per risolvere il problema, è possibile pre-impostare la configurazione sulla connessione e quindi aggiornare la configurazione BGP.
- Non è possibile migrare un file VIF da una connessione ospitata a un'altra connessione ospitata. Gli ID VLAN sono unici; pertanto, un tale migrazione di un VIF comporterebbe una mancata corrispondenza tra le VLAN. È necessario eliminare la connessione o il file VIF e quindi ricrearlo utilizzando una VLAN uguale sia per la connessione che per il VIF.

Important

L'interfaccia virtuale sarà inattiva per un breve periodo. Si consiglia di eseguire questa procedura durante una finestra di manutenzione.

Per eseguire la migrazione di un'interfaccia virtuale

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Selezionare l'interfaccia virtuale e scegliere Edit (Modifica).
4. Per Connection (Connessione), selezionare il LAG o la connessione.
5. Scegliere Edit virtual interface (Modifica interfaccia virtuale).

Per eliminare un'interfaccia virtuale utilizzando l'API o la riga di comando

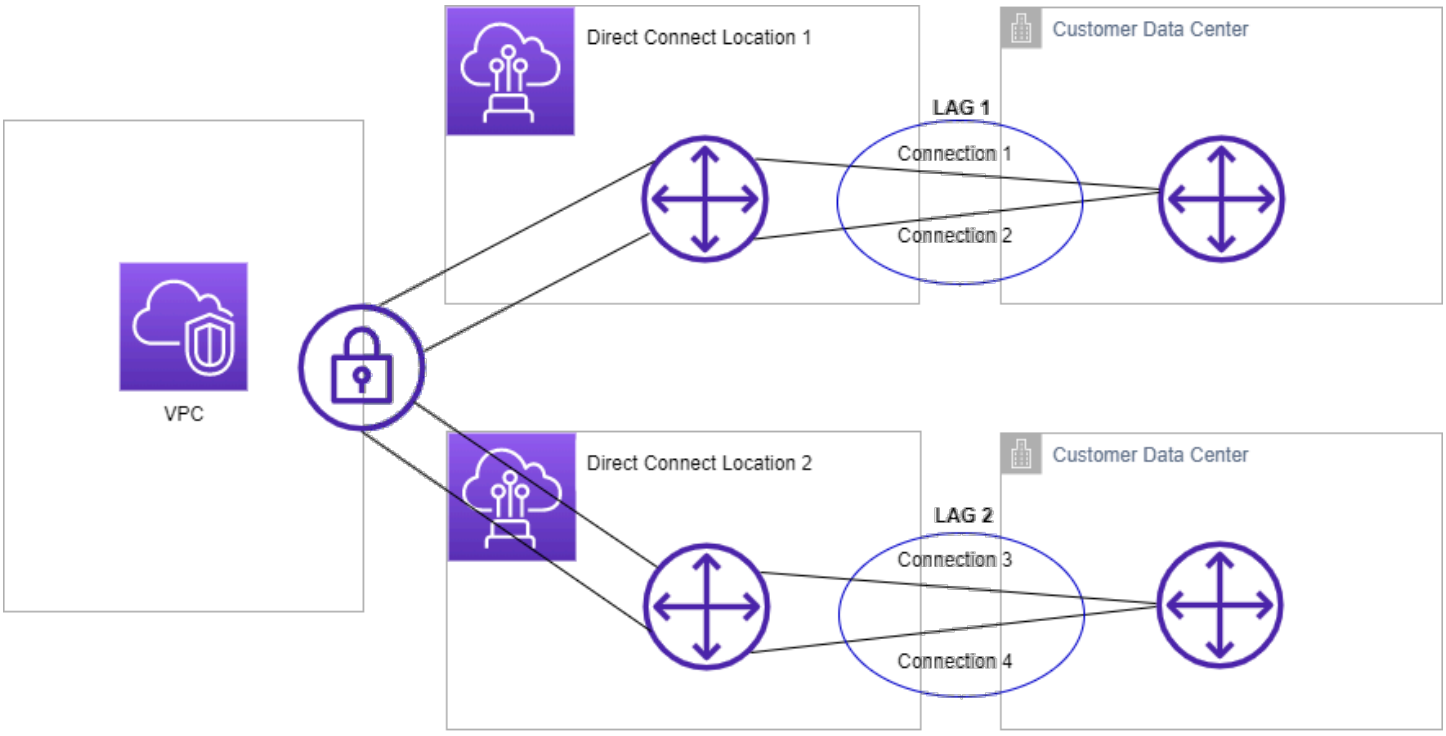
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterfaccia (AWS Direct Connect API)

Link aggregation groups

È possibile utilizzare più connessioni per aumentare la larghezza di banda disponibile. Un Link Aggregation Group (LAG) è un'interfaccia logica che utilizza il protocollo LACP (Link Aggregation Control Protocol) per raggruppare più connessioni in un singolo endpoint AWS Direct Connect, consentendoti di trattarle come una singola connessione gestita. I LAG semplificano la configurazione perché la configurazione LAG si applica a tutte le connessioni del gruppo.

> **Note**
>
> Il LAG multi-chassis (MLAG) non è supportato da AWS.

Nel seguente diagramma, disponi di quattro connessioni, con due connessioni a ciascuna posizione. È possibile creare un LAG per le connessioni che terminano sullo stesso AWS dispositivo e nella stessa posizione, quindi utilizzare i due LAG anziché le quattro connessioni per la configurazione e la gestione.



Puoi creare un LAG da connessioni esistenti oppure predisporne di nuove. Dopo averlo creato, puoi associare al LAG le connessioni esistenti, sia indipendenti che incluse in un altro LAG.

Si applicano le regole seguenti:

- Tutte le connessioni devono essere connessioni dedicate e avere una velocità di porta di 1 Gbps, 10 Gbps o 100 Gbps.
- La larghezza di banda deve essere la stessa per tutte le connessioni nel LAG.
- È possibile disporre in un LAG un massimo di due connessioni 100G o quattro connessioni con una velocità di porta inferiore a 100G. Ognuna di esse conta per il raggiungimento del limite di connessione generale per la regione.
- Tutte le connessioni nel LAG devono terminare nello stesso endpoint AWS Direct Connect.
- I LAG sono supportati per tutti i tipi di interfaccia virtuale: pubblica, privata e di transito.

Quando crei un LAG, puoi scaricare la Letter of Authorization and Connecting Facility Assignment (LOA-CFA) singolarmente per ogni nuova connessione fisica dalla console AWS Direct Connect. Per ulteriori informazioni, consulta Scaricare la LOA-CFA.

Tutti i LAG dispongono di un attributo che determina il numero minimo di connessioni che devono essere operative al suo interno perché il LAG stesso sia operativo. Di default, per i nuovi LAG questo attributo è impostato su 0. Puoi aggiornare i LAG specificando un altro valore: così facendo, tutto il LAG diventerà non operativo se il numero di connessioni operative scende al di sotto di tale soglia. Questo attributo può essere utilizzato per evitare l'utilizzo eccessivo delle connessioni restanti.

Tutte le connessioni di un LAG funzionano in modalità attivo/attivo.

> **Note**
>
> Quando crei un LAG o vi associ più connessioni, potremmo non essere in grado di garantire la disponibilità di un numero sufficiente di porte su un determinato endpoint AWS Direct Connect.

Considerazioni relative a MACsec

Quando desideri configurare MACsec su LAG, tieni in considerazione quanto segue:

- Quando crei un LAG da connessioni esistenti, dissociamo tutte le chiavi MACsec dalle connessioni. Quindi aggiungiamo le connessioni al LAG e associamo la chiave LAG MACsec alle connessioni.
- Quando si associa una connessione esistente a un LAG, le chiavi MACsec attualmente associate al LAG vengono associate alla connessione. Pertanto, dissociamo le chiavi MACsec dalla

connessione, aggiungiamo la connessione al LAG e quindi associamo la chiave MACsec LAG alla connessione.

Creazione di un LAG

Puoi creare un LAG raggruppando connessioni esistenti oppure predisponendone di nuove.

Non puoi creare un LAG con nuove connessioni se questo comporta il superamento del limite di connessioni per la regione.

Per creare un LAG da connessioni esistenti, queste devono essere sullo stesso dispositivo AWS (terminare nello stesso endpoint AWS Direct Connect). Devono anche usare la stessa larghezza di banda. Non ti sarà possibile trasferire una connessione da un LAG esistente se, con la rimozione della connessione, il numero minimo di connessioni operative nel LAG originale scende al di sotto della soglia impostata.

> **Important**
>
> Per le connessioni esistenti, la connettività ad AWS viene interrotta durante la creazione del LAG.

Create a LAG with new connections using the console

Per creare un LAG con nuove connessioni

1. Aprire la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione scegli LAGs (LAG).
3. Scegli Create LAG (Crea LAG).
4. In Lag creation type (Tipo creazione LAG), selezionare Request new connections (Richiedi nuove connessioni) e fornire le informazioni indicate di seguito:
   - LAG name (Nome LAG): un nome per il LAG.
   - Location (Sede): la sede per il LAG.
   - Port speed (Velocità porta): la velocità della porta per le connessioni.

- Number of new connections (Numero di nuove connessioni): il numero di nuove connessioni da creare. È possibile disporre di un massimo di quattro connessioni quando la velocità della porta è 1G o 10G o due quando la velocità della porta è 100G.
- (Facoltativo) Configura la sicurezza MAC (MACsec) per la connessione. In Impostazioni aggiuntive, seleziona Richiedi una porta compatibile con MACsec.

  MACsec è disponibile solo su connessioni dedicate.
- (Facoltativo) Aggiunta o rimozione di un tag.

  [Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:
  - In Chiave, immetti il nome della chiave.
  - In Valore, immetti il valore della chiave.

  [Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

5. Scegli Create LAG (Crea LAG).

Create a LAG with existing connections using the console

Per creare un LAG da connessioni esistenti

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione scegli LAGs (LAG).
3. Scegli Create LAG (Crea LAG).
4. In Lag creation type (Tipo creazione LAG), selezionare Use existing connections (Utilizza connessioni esistenti) e fornire le informazioni indicate di seguito:

   - LAG name (Nome LAG): un nome per il LAG.
   - Connessione: la connessione Direct Connect da utilizzare per il LAG.
   - (Facoltativo) Numero di nuove connessioni: il numero di nuove connessioni da creare. È possibile disporre di un massimo di quattro connessioni quando la velocità della porta è 1G o 10G o due quando la velocità della porta è 100G.
   - Minimum links (Collegamenti minimi): il numero minimo di connessioni che devono essere operative perché lo sia anche il LAG. Se non specifichi un valore, viene assegnato un valore di default pari a 0.
5. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

6. Scegli Create LAG (Crea LAG).

Command line

Per creare un LAG utilizzando l'API o la riga di comando

- create-lag (AWS CLI)
- CreateLag(AWS Direct ConnectAPI)

Per descrivere i LAG utilizzando l'API o la riga di comando

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

Per scaricare il documento LOA-CFA utilizzando l'API o la riga di comando

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct ConnectAPI)

Dopo aver creato un LAG, puoi associarvi connessioni o rimuovere l'associazione. Per ulteriori informazioni, consultare Associazione di una connessione a un LAG. e Annullamento dell'associazione di una connessione a un LAG..

Come visualizzare i dettagli del LAG

Dopo aver creato un LAG, puoi visualizzarne i dettagli.

Console

Per visualizzare le informazioni sul LAG

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione scegli LAGs (LAG).
3. Selezionare il LAG e scegliere View details (Visualizza dettagli).
4. Vengono visualizzate le informazioni sui LAG, tra cui il relativo ID e l'endpoint AWS Direct Connect su cui terminano le connessioni.

Command line

Per visualizzare le informazioni su un volume LAG tramite la riga di comando o l'API

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

Aggiornamento di un LAG

Puoi aggiornare i seguenti attributi del gruppo di aggregazione collegamenti (LAG):

- Il nome del LAG.
- Il numero minimo di connessioni che devono essere operative perché lo sia anche il LAG.
- La modalità di crittografia MACsec del LAG.

  MACsec è disponibile solo su connessioni dedicate.

  AWS assegna questo valore a ogni connessione che fa parte del LAG.

  I valori validi sono:

  - `should_encrypt`
  - `must_encrypt`

    Quando si imposta la modalità di crittografia su questo valore, le connessioni si interrompono quando la crittografia non è attiva.
  - `no_encrypt`

- I tag.

> **Note**
>
> Se modifichi il valore soglia per il numero minimo di connessioni operative, assicurati che il nuovo valore non ponga il LAG sotto la nuova soglia e che diventi non operativo.

Console

Per aggiornare un LAG

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione scegli LAGs (LAG).
3. Selezionare prima il LAG e quindi Modifica.
4. Modificare il LAG

   [Modificare il nome] Per LAG Name (Nome LAG), immettere un nuovo nome di LAG.

   [Regolare il numero minimo di connessioni] Per Collegamenti minimi, immettere il numero minimo di connessioni operative.

   [Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.

   [Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).
5. Selezionare Edit LAG (Modifica LAG).

Command line

Per aggiornare un LAG utilizzando l'API o la riga di comando

- update-lag (AWS CLI)
- UpdateLag(AWS Direct ConnectAPI)

Per aggiungere e rimuovere i tag utilizzando la riga di comando

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Associazione di una connessione a un LAG.

Puoi associare a un LAG una connessione esistente, sia indipendente che inclusa in un altro LAG. La connessione deve trovarsi sullo stesso dispositivo AWS e deve utilizzare la stessa larghezza di banda del LAG. Se la connessione è già associata a un altro LAG, non ti sarà possibile riassociarla se, con la rimozione della connessione, il numero minimo di connessioni operative nel LAG originale scende al di sotto della soglia impostata.

L'associazione di una connessione a un LAG comporta la riassociazione automatica delle interfacce virtuali a tale LAG.

> **Important**
>
> La connettività ad AWS sulla connessione viene interrotta durante l'associazione.

Console

Per associare una connessione a un LAG

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione scegli LAGs (LAG).
3. Seleziona il LAG e scegli Visualizza dettagli.
4. In Connections (Connessioni), scegliere Associate connection (Associa connessione).
5. In Connection (Connessione), scegliere la connessione Direct Connect da utilizzare per il LAG.
6. Scegliere Associate Connection (Associa connessione).

Command line

Per associare una connessione utilizzando l'API o la riga di comando

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag(AWS Direct ConnectAPI)

Annullamento dell'associazione di una connessione a un LAG.

Converti una connessione in modalità autonoma dissociandola da un LAG. Non puoi annullare l'associazione se, con questa operazione, il numero minimo di connessioni operative nel LAG originale scende al di sotto della soglia impostata.

L'annullamento dell'associazione di una connessione a un LAG non comporta automaticamente lo stesso risultato per le eventuali interfacce virtuali.

> **Important**
>
> La connessione ad AWS si è interrotta durante la rimozione dell'associazione.

Console

Per annullare l'associazione di una connessione a un LAG

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro a sinistra seleziona LAGs (LAG).
3. Seleziona il LAG e scegli Visualizza dettagli.
4. In Connections (Connessioni), selezionare la connessione dall'elenco delle connessioni disponibili e scegliere Disassociate (Annulla associazione).
5. Nella finestra di dialogo di conferma, scegliere Annulla associazione.

Command line

Per annullare l'associazione di una connessione utilizzando l'API o la riga di comando

- disassociate-connection-from-lag (AWS CLI)

- DisassociateConnectionFromLag(AWS Direct ConnectAPI)

Associa un MACsec CKN/CAK a un LAG

Dopo aver creato la connessione o il LAG che supporta MACsec, è necessario associare un CKN/CAK alla connessione.

> **Note**
>
> Non è possibile modificare una chiave segreta MACsec dopo averla associata a un LAG. Se è necessario modificare la chiave, dissocia la chiave dalla connessione e quindi associa una nuova chiave alla connessione. Per ulteriori informazioni sulla rimozione di un'associazione, consulta the section called “Rimozione dell'associazione tra una chiave segreta MACsec e un LAG”.

Console

Associare un MACsec CKN/CAK a un LAG

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione scegli LAGs (LAG).
3. Selezionare il LAG e scegliere View details (Visualizza dettagli).
4. Selezionare Associa chiave.
5. Immettere la chiave MACsec.

   [Usa la coppia CAK/CKN] Scegli Coppia di chiavi, quindi procedi come segue:

   - Per Connectivity Association Key (CAK), inserisci il CAK.
   - Per Connectivity Association Key Name (CKN), inserisci il CKN.

   [Usa il segreto] Scegli il segreto di Segreto di Segret Manager esistente, quindi per Segreto, seleziona la chiave segreta MACsec.
6. Selezionare Associa chiave.

Command line

Associare un MACsec CKN/CAK a un LAG

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(AWS Direct ConnectAPI)

Rimozione dell'associazione tra una chiave segreta MACsec e un LAG

Puoi rimuovere l'associazione tra una chiave segreta MACsec e un LAG

Console

Rimozione dell'associazione tra una chiave LAG e una chiave MACsec

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione scegli LAGs (LAG).
3. Selezionare il LAG e scegliere View details (Visualizza dettagli).
4. Seleziona il segreto MacSec da rimuovere, quindi scegli Annulla associazione chiave.
5. Nella finestra di dialogo di conferma immetti annulla associazione, quindi scegli Annulla associazione.

Command line

Rimozione dell'associazione tra una chiave LAG e una chiave MACsec

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct ConnectAPI)

Eliminazione dei LAG

Se non hai più bisogno di un LAG puoi eliminarlo, ma solo se non è associato a interfacce virtuali: in caso contrario devi prima eliminare le interfacce virtuali oppure associarle a un altro LAG o a un'altra

connessione. Con l'eliminazione di un LAG non si eliminano le relative connessioni, che dovranno essere rimosse manualmente. Per ulteriori informazioni, consulta Elimina connessioni.

Console

Per eliminare un LAG

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione scegli LAGs (LAG).
3. Seleziona i LAG e scegli Elimina.
4. Nella finestra di dialogo di conferma, seleziona Elimina.

Command line

Per eliminare un LAG utilizzando l'API o la riga di comando

- delete-lag (AWS CLI)
- DeleteLag(AWS Direct ConnectAPI)

Utilizzo dei gateway Direct Connect

Puoi lavorare con i AWS Direct Connect gateway utilizzando la console Amazon VPC o il. AWS CLI

Indice

Gateway Direct Connect

Usa il AWS Direct Connect gateway per connettere i tuoi VPC. È possibile associare un gateway AWS Direct Connect con uno dei seguenti gateway:

- Un gateway di transito quando si dispone di più VPC nella stessa regione
- Un gateway virtuale privato

Puoi anche utilizzare un gateway privato virtuale per estendere la tua zona locale. Questa configurazione consente al VPC associato alla zona locale di connettersi a un gateway Direct Connect. Il gateway Direct Connect si connette a una posizione Direct Connect in una regione. Il data center on-premise dispone di una connessione Direct Connect alla posizione Direct Connect. Per ulteriori informazioni, consulta Accedere alle zone locali usando un gateway Direct Connect nella Guida per l'utente di Amazon VPC.

Un gateway Direct Connect è una risorsa disponibile in tutto il mondo. Puoi connetterti a qualsiasi regione a livello globale utilizzando un gateway Direct Connect. Ciò include AWS GovCloud (US) ma non include le regioni della AWS Cina.

I clienti che utilizzano Direct Connect con VPC che attualmente bypassano una zona di disponibilità principale non saranno in grado di migrare le proprie connessioni Direct Connect o le interfacce virtuali.

Il gateway Direct Connect può essere utilizzato nei seguenti scenari.

Un gateway Direct Connect non consente alle associazioni gateway che si trovano nello stesso gateway Direct Connect di inviare traffico reciproco (ad esempio, da un gateway privato virtuale a

un altro gateway privato virtuale). Un'eccezione a questa regola, implementata a novembre 2021, è quando una supernet viene pubblicizzata su due o più VPC, i cui gateway privati virtuali (VGW) collegati sono associati allo stesso gateway Direct Connect e sulla stessa interfaccia virtuale. In questo caso, i VPC possono comunicare tra loro tramite l'endpoint Direct Connect. Ad esempio, se pubblicizzi una supernet (ad esempio 10.0.0.0/8 o 0.0.0.0/0) che si sovrappone ai VPC collegati a un gateway Direct Connect (ad esempio 10.0.0.0/24 e 10.0.1.0/24) e sulla stessa interfaccia virtuale, dalla rete on-premise i VPC possono comunicare tra loro.

Se desideri bloccare la comunicazione da VPC a VPC all'interno di un gateway Direct Connect, procedi nel seguente modo:

1. Configura gruppi di sicurezza sulle istanze e altre risorse nel VPC per bloccare il traffico tra i VPC, utilizzandoli anche come parte del gruppo di sicurezza predefinito nel VPC.
2. Evita di pubblicizzare una supernet dalla tua rete on-premise che si sovrappone ai VPC. Puoi invece pubblicizzare percorsi più specifici dalla tua rete on-premise che non si sovrappongano ai tuoi VPC.
3. Effettua il provisioning di un singolo gateway Direct Connect per ogni VPC che desideri connettere alla tua rete on-premise invece di utilizzare lo stesso gateway Direct Connect per più VPC. Ad esempio, anziché utilizzare un singolo gateway Direct Connect per i VPC di sviluppo e produzione, utilizza gateway Direct Connect separati per ciascuno di questi VPC.

Un gateway Direct Connect non impedisce di inviare del traffico da un'associazione gateway all'associazione gateway stessa (ad esempio quando disponi di una route supernet on-premise che contiene i prefissi dell'associazione gateway). Se disponi di una configurazione con più VPC collegati a gateway di transito associati allo stesso gateway Direct Connect, i VPC potrebbero comunicare. Per evitare che i VPC comunichino, associa una tabella di routing agli allegati VPC su cui è impostata l'opzione blackhole.

Il gateway Direct Connect può essere utilizzato nei seguenti scenari.

Scenari

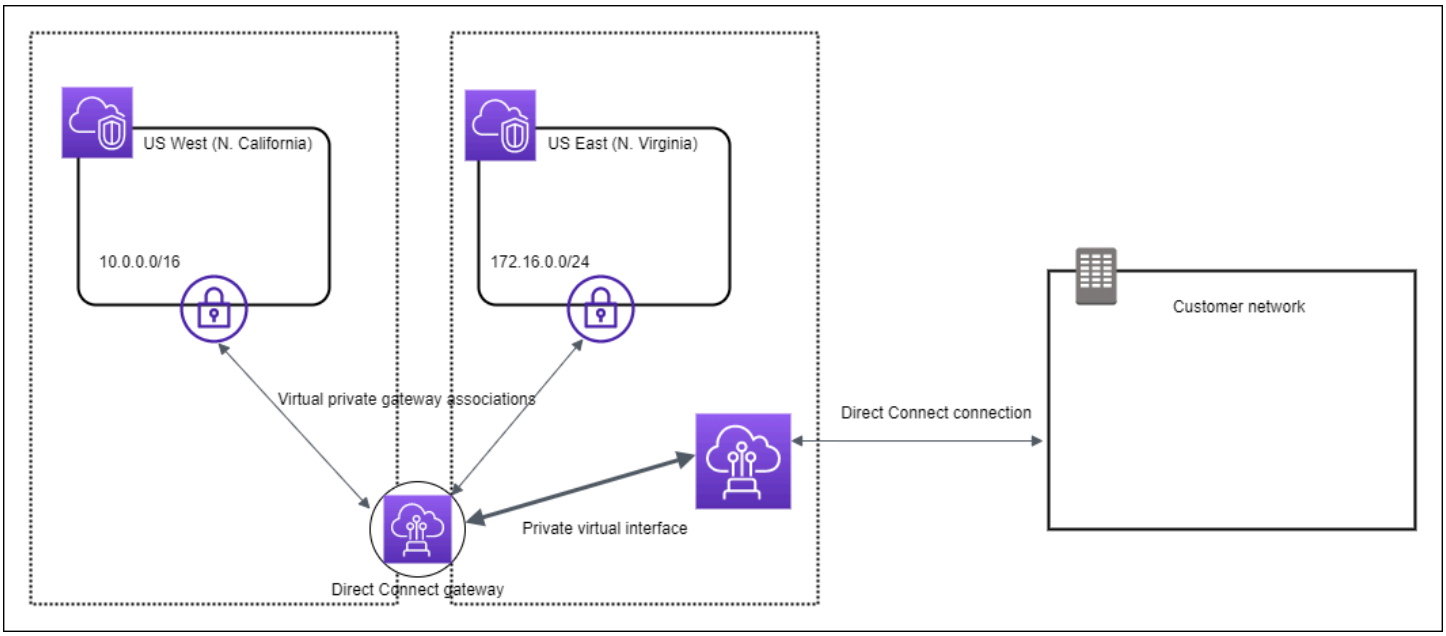
- Associazioni di gateway privati virtuali
- Associazioni di gateway privati virtuali tra account
- Associazioni di gateway di transito
- Associazioni di gateway di transito tra account
- Creazione di un gateway Direct Connect

- Eliminazione di gateway Direct Connect
- Migrazione da un gateway virtuale privato a un gateway Direct Connect

Associazioni di gateway privati virtuali

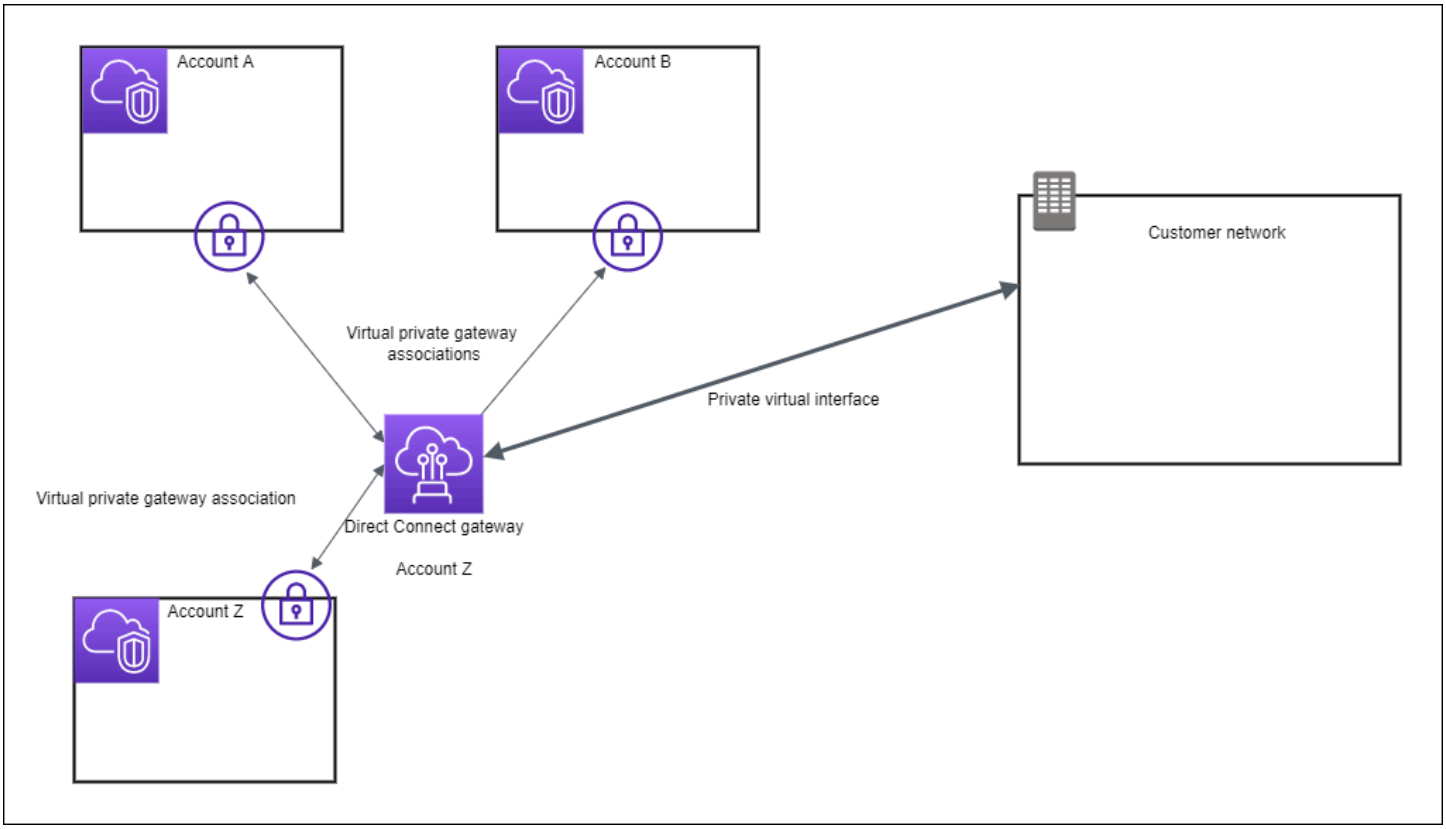
Nel diagramma seguente, il gateway Direct Connect consente di utilizzare la connessione AWS Direct Connect nella regione Stati Uniti orientali (Virginia settentrionale) per accedere ai VPC del proprio account nelle regioni Stati Uniti orientali (Virginia settentrionale) e Stati Uniti occidentali (California settentrionale).

Ogni VPC dispone di un gateway privato virtuale che si connette al gateway Direct Connect utilizzando un'associazione di gateway privati virtuali. Il gateway Direct Connect utilizza un'interfaccia virtuale privata per la connessione alla AWS Direct Connect posizione. È disponibile una connessione AWS Direct Connect dalla posizione al data center del cliente.



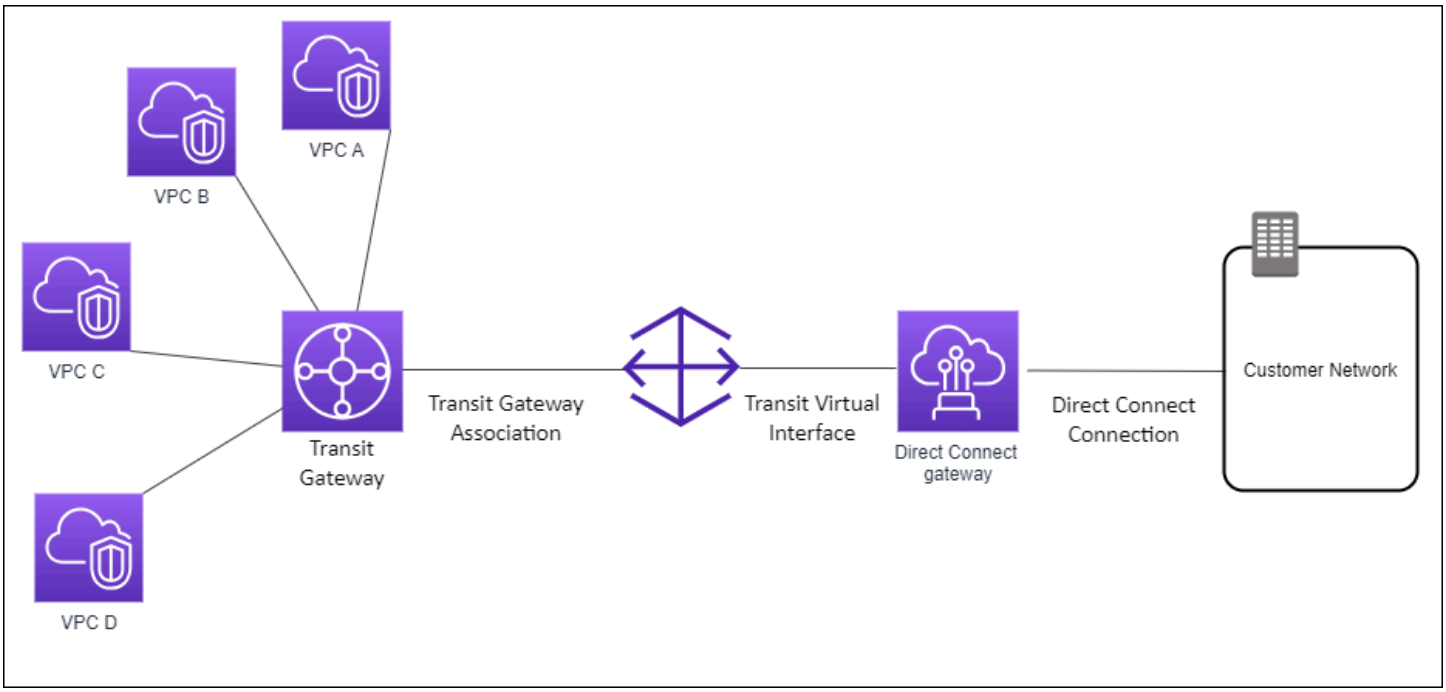
Associazioni di gateway privati virtuali tra account

Prendiamo ad esempio uno scenario in cui il proprietario del gateway Direct Connect è l'Account Z. L'Account A e l'Account B vogliono utilizzare il gateway Direct Connect, quindi ciascuno di essi invia una proposta di associazione all'Account Z. Quest'ultimo accetta le proposte di associazione e ha la possibilità di aggiornare i prefissi consentiti dal gateway privato virtuale dell'Account A o dell'Account B. Una volta che l'Account Z avrà accettato le proposte, l'Account A e l'Account B potranno instradare il traffico dal loro gateway privato virtuale al gateway Direct Connect. Poiché è il proprietario del gateway, l'Account Z è anche il titolare dell'instradamento ai clienti.



Associazioni di gateway di transito

Il seguente diagramma illustra il modo in cui il gateway Direct Connect consente di creare un'unica connessione alla connessione Direct Connect che può essere utilizzata da tutti i VPC.



La soluzione prevede i seguenti componenti:

- Un gateway di transito che dispone di allegati VPC.
- Un gateway Direct Connect.
- Un'associazione tra il gateway Direct Connect e il gateway di transito.
- Un'interfaccia virtuale di transito collegata al gateway Direct Connect.

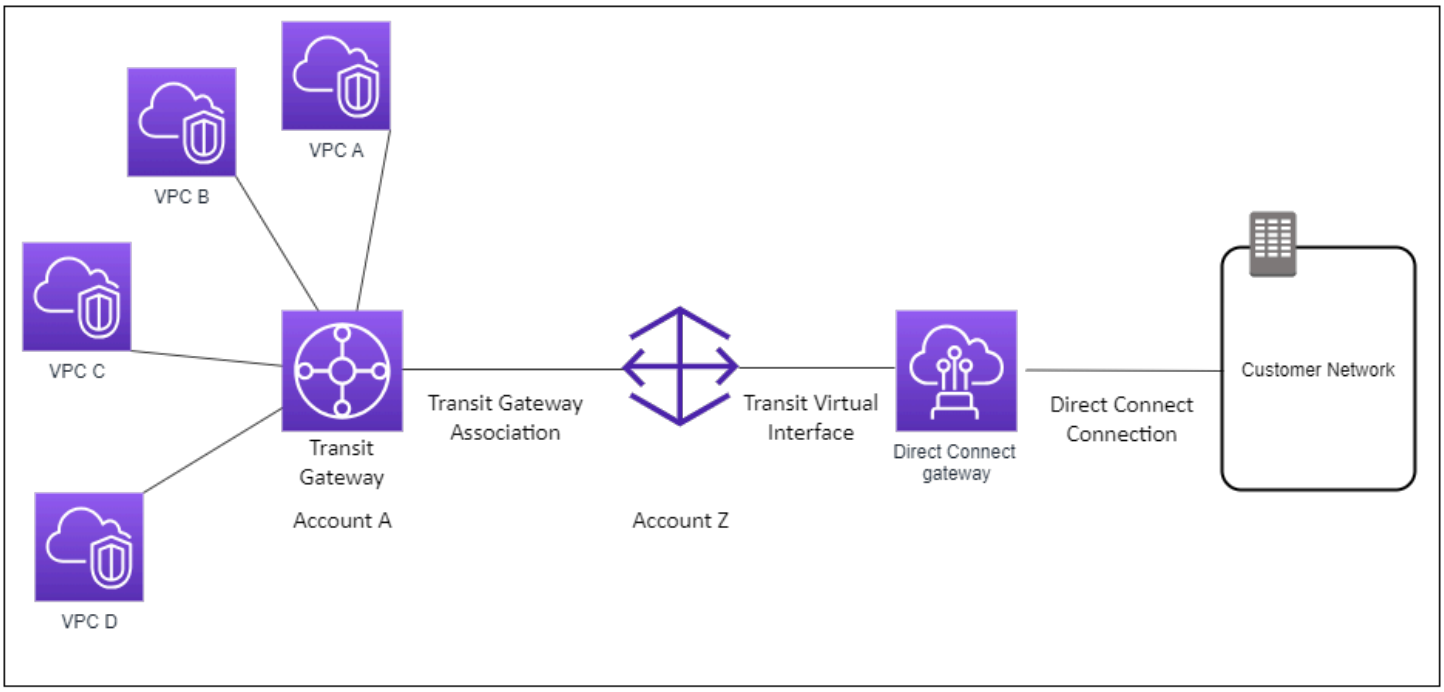
Questa configurazione offre i seguenti vantaggi. È possibile:

- Gestire un'unica connessione per più VPC o VPN che si trovano nella stessa regione.
- Pubblicizza i prefissi dall'ambiente locale a quello locale e viceversa. AWS AWS

Per ulteriori informazioni su come configurare i gateway di transito, consulta Lavorare con i gateway di transito nella Guida di gateway di transito per Amazon VPC.

Associazioni di gateway di transito tra account

Prendiamo ad esempio uno scenario in cui il proprietario del gateway Direct Connect è l'Account Z. L'Account A è proprietario del gateway di transito e desidera utilizzare il gateway Direct Connect. L'Account Z accetta le proposte di associazione e può facoltativamente aggiornare i prefissi che sono consentiti dal gateway di transito dell'Account A. Una volta che l'Account Z ha accettato le proposte, i VPC collegati al possono instradare il traffico dal gateway di transito al gateway Direct Connect. Poiché è il proprietario del gateway, l'Account Z è anche il titolare dell'instradamento ai clienti.



Indice

Creazione di un gateway Direct Connect

È possibile creare un gateway Direct Connect in qualsiasi Regione supportata.

Per creare un gateway Direct Connect

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegliere Direct Connect Gateways (Gateway Direct Connect).
3. Scegliere Create Direct Connect gateway (Crea gateway Direct Connect).
4. Specificare le informazioni riportate di seguito e scegliere Create Direct Connect gateway (Crea gateway Direct Connect).
   - Name (Nome): immettere un nome per semplificare l'identificazione del gateway Direct Connect.

- Amazon side ASN (ASN lato Amazon): specificare l'ASN per il lato Amazon della sessione BGP. L'ASN deve essere un valore incluso nell'intervallo tra 64.512 e 65.534 oppure tra 4.200.000.000 e 4.294.967.294.
- Virtual private gateway (Gateway privato virtuale): per poterlo associare, è necessario scegliere un gateway privato virtuale.

Per creare un gateway Direct Connect utilizzando l'API o la riga di comando

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway(AWS Direct Connect API)

Eliminazione di gateway Direct Connect

Se non è più necessario un gateway Direct Connect, è possibile eliminarlo. È necessario innanzitutto annullare l'associazione di tutti i gateway privati virtuali associati ed eliminare l'interfaccia virtuale privata collegata.

Per eliminare un gateway Direct Connect

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegliere Direct Connect Gateways (Gateway Direct Connect).
3. Selezionare i gateway, quindi scegliere Delete (Elimina).

Per eliminare un gateway Direct Connect utilizzando l'API o la riga di comando

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway(AWS Direct Connect API)

Migrazione da un gateway virtuale privato a un gateway Direct Connect

Se hai un gateway virtuale privato collegato a un'interfaccia virtuale e desideri eseguire la migrazione a un gateway Direct Connect, procedi nel seguente modo:

Per eseguire la migrazione a un gateway Direct Connect

1. Creare un gateway Direct Connect. Per ulteriori informazioni, consulta the section called “Creazione di un gateway Direct Connect”.
2. Creare un'interfaccia virtuale per il gateway Direct Connect. Per ulteriori informazioni, consulta the section called “Creazione di un'interfaccia virtuale.”.
3. Associare il gateway virtuale privato al gateway Direct Connect. Per ulteriori informazioni, consulta the section called “Associazione e annullamento dell'associazione di gateway virtuali privati”.
4. Eliminare l'interfaccia virtuale associata al gateway virtuale privato. Per ulteriori informazioni, consulta the section called “Eliminazione di interfacce virtuali”.

Associazioni di gateway privati virtuali

È possibile utilizzare un gateway AWS Direct Connect per collegare la connessione AWS Direct Connect tramite un'interfaccia virtuale privata a uno o più VPC in qualsiasi account che sia ubicato nella stessa regione o in regioni differenti. I gateway privati virtuali vengono associati a un gateway Direct Connect per il VPC. Quindi, crei un'interfaccia virtuale privata per la AWS Direct Connect connessione al gateway Direct Connect. Al gateway Direct Connect possono essere collegate più interfacce virtuali private.

Le seguenti regole si applicano alle associazioni di gateway privati virtuali:

- Non abilitate la propagazione delle rotte prima di aver associato un gateway virtuale a un gateway Direct Connect. Se abiliti la propagazione delle rotte prima di associare i gateway, le rotte potrebbero essere propagate in modo errato.
- Esistono dei limiti per la creazione e l'utilizzo di gateway Direct Connect. Per ulteriori informazioni, consulta Quote.
- Non è possibile collegare un gateway Direct Connect a un gateway virtuale privato quando il gateway Direct Connect è già associato a un gateway privato virtuale.
- I VPC a cui ci si connette tramite un gateway Direct Connect non possono avere blocchi CIDR sovrapposti. Se aggiungi un blocco CIDR IPv4 a un VPC associato a un gateway Direct Connect, accertati che il blocco CIDR non si sovrapponga a un blocco CIDR esistente per qualsiasi altro VPC associato. Per ulteriori informazioni, consulta l'articolo relativo all'aggiunta di blocchi CIDR IPv4 a un VPC nella Guida per l’utente di Amazon VPC.
- Non è possibile creare un'interfaccia virtuale pubblica in un gateway Direct Connect.

- I gateway Direct Connect supportano la comunicazione solo tra le interfacce virtuali private collegate e i gateway virtuali privati associati, e possono abilitare un gateway virtuale privato a un altro gateway privato. Non sono supportati i flussi di traffico seguenti:
  - Comunicazione diretta tra i VPC associati a un singolo gateway Direct Connect. È incluso il traffico da un VPC a un altro che utilizza un percorso di una rete on-premise tramite un singolo gateway Direct Connect.
  - Comunicazione diretta tra le interfacce virtuali collegate al gateway Direct Connect.
  - Comunicazione diretta tra le interfacce virtuali collegate a un singolo gateway Direct Connect e una connessione VPN su un gateway virtuale privato associato allo stesso gateway Direct Connect.
- Non è possibile associare un gateway virtuale privato a più di un gateway Direct Connect e non è possibile collegare un'interfaccia virtuale privata a più di un gateway Direct Connect.
- I gateway virtuali privati che si associano a un gateway Direct Connect devono essere collegati a un VPC.
- Una proposta di associazione di gateway virtuale privato scade 7 giorni dopo la creazione.
- Una proposta accettata di gateway virtuale privato o una proposta eliminata di gateway privato virtuale resta visibile per 3 giorni.
- Un gateway virtuale privato può essere associato a un gateway Direct Connect e anche collegato a un'interfaccia virtuale.
- Scollegare un gateway virtuale privato da un VPC dissocia anche il gateway virtuale privato da un gateway Direct Connect.

Per connettere la tua AWS Direct Connect connessione a un VPC solo nella stessa regione, puoi creare un gateway Direct Connect. In alternativa, è possibile creare un'interfaccia privata virtuale e collegarla al gateway privato virtuale per il VPC. Per ulteriori informazioni, consulta Creare un'interfaccia virtuale privata. and VPN CloudHub.

Per utilizzare la AWS Direct Connect connessione con un VPC in un altro account, puoi creare un'interfaccia virtuale privata ospitata per quell'account. Quando il proprietario dell'altro account accetta l'interfaccia virtuale in hosting, può scegliere di collegarla a un gateway privato virtuale o a un gateway Direct Connect nel proprio account. Per ulteriori informazioni, consulta AWS Direct Connect interfacce virtuali.

Indice

- Associazione e annullamento dell'associazione di gateway virtuali privati
- Creazione di un'interfaccia virtuale privata per un gateway Direct Connect
- Associazione di un gateway privato virtuale tra più account

Creazione di gateway virtuale privato

Il gateway virtuale privato deve essere collegato al VPC a cui si desidera connettersi.

> **Note**
>
> Se prevedi di utilizzare il gateway privato virtuale per un gateway Direct Connect e una connessione VPN dinamica, imposta l'ASN sul gateway privato virtuale sul valore necessario per la connessione VPN. In alternativa, l'ASN sul gateway virtuale privato può essere impostato su qualsiasi valore consentito. Il gateway Direct Connect pubblicizza tutti i VPC connessi sugli ASN a esso assegnati.

Dopo aver creato un gateway virtuale privato, devi collegarlo al VPC.

Per creare un gateway virtuale privato e collegarlo al VPC

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Gateway virtuale privato, quindi Crea gateway privato virtuale.
3. (Facoltativo) Immettere un nome per il gateway virtuale privato. In questo modo viene creato un tag con una chiave di `Name` e il valore specificato.
4. In ASN, lasciare la selezione predefinita per utilizzare l'Amazon ASN predefinito. In caso contrario, scegliere Custom ASN (ASN personalizzato) e immettere un valore. Per un ASN a 16 bit, il valore deve Esser compreso nell'intervallo da 64512 a 65534. Per un ASN a 32 bit, il valore deve Essere compreso nell'intervallo da 4200000000 a 4294967294.
5. Selezionare Create Virtual Private Gateway (Crea gateway virtuale privato).
6. Selezionare il gateway virtuale privato creato, quindi selezionare Actions (Operazioni), Attach to VPC (Collega a VPC).
7. Selezionare il VPC dall'elenco e scegliere Yes, Attach (Sì, collega).

Per creare un gateway virtuale privato utilizzando l'API o la riga di comando

- CreateVpnGateway(API di interrogazione Amazon EC2)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

Per collegare un gateway virtuale privato a un VPC utilizzando la riga di comando o l'API

- AttachVpnGateway(API di interrogazione Amazon EC2)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Associazione e annullamento dell'associazione di gateway virtuali privati

Puoi associare o disassociare un gateway virtuale privato e un gateway Direct Connect. Queste operazioni vengono eseguite dal proprietario dell'account del gateway virtuale privato.

Per associare un gateway virtuale privato

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Gateway Direct Connect, quindi seleziona il gateway Direct Connect.
3. Seleziona Visualizza dettagli.
4. Scegli Associazioni di gateway, quindi scegli Associa gateway.
5. In Gateways (Gateway), scegliere il gateway privato virtuale da associare, quindi Associate gateway (Associa gateway).

Per visualizzare tutti i gateway privati virtuali associati al gateway Direct Connect, scegliere Gateway associations (Associazioni di gateway).

Per annullare l'associazione di un gateway virtuale privato

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.

2. Nel riquadro di navigazione, scegliere Direct Connect gateways (Gateway Direct Connect), quindi selezionare il gateway Direct Connect.
3. Seleziona Visualizza dettagli.
4. Scegliere Gateway associations (Associazioni di gateway), quindi selezionare il gateway privato virtuale.
5. Scegli Dissocia.

Per associare un gateway virtuale privato utilizzando l'API o la riga di comando

- create-direct-connect-gateway-associazione ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

Per visualizzare il gateway virtuale privato associato a un gateway Direct Connect utilizzando l'API o la riga di comando

- describe-direct-connect-gateway-associazioni ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

Per annullare l'associazione di un gateway virtuale privato utilizzando l'API o la riga di comando

- delete-direct-connect-gateway-associazione ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

Creazione di un'interfaccia virtuale privata per un gateway Direct Connect

Per connettere la AWS Direct Connect connessione al VPC remoto, è necessario creare un'interfaccia virtuale privata per la connessione. Specificare il gateway Direct Connect al quale connettersi.

> **Note**
>
> Se si sta accettando un'interfaccia virtuale privata in hosting, è possibile associarla a un gateway Direct Connect nell'account. Per ulteriori informazioni, consulta Accetta un'interfaccia virtuale in hosting..

Per effettuare il provisioning di un'interfaccia virtuale privata in un gateway Direct Connect

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Tipo di interfaccia virtuale, scegli Privato.
5. In Impostazioni dell'interfaccia virtuale pubblica, procedi come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

   b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

   c. Per il proprietario dell'interfaccia virtuale, scegli Il mio AWS account se l'interfaccia virtuale è per il tuo AWS account.

   d. Per Direct Connect gateway (Gateway Direct Connect), selezionare il gateway Direct Connect.

   e. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

   f. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

      I valori validi sono compresi tra 1 e 2147483647.

6. In Impostazioni aggiuntive, procedi come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

      [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

      - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
      - In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

      > **Important**
      >
      > Se consenti l' AWS assegnazione automatica degli indirizzi IPv4, verrà allocato un CIDR /29 da 169.254.0.0/16 IPv4 Link-Local secondo RFC 3927 per la connettività. point-to-point AWS non consiglia questa opzione se si intende utilizzare l'indirizzo

IP peer del router del cliente come origine e/o destinazione per il traffico VPC. È invece consigliabile utilizzare RFC 1918 o un altro indirizzo (diverso da RFC 1918) e specificare personalmente l'indirizzo.

- Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.
- Per ulteriori informazioni su RFC 3927, consulta Dynamic Configuration of IPv4 Link-Local Addresses.

[IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

b. Per modificare l'unità di trasmissione massima (MTU) da 1500 (predefinito) a 9001 (frame jumbo), seleziona Jumbo MTU (MTU size 9001) (MTU jumbo - dimensione della MTU 9001).

c. (Facoltativo) In Abilita SiteLink, scegli Abilitato per abilitare la connettività diretta tra i punti di presenza Direct Connect.

d. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).

Dopo aver creato l'interfaccia virtuale, è possibile scaricare la configurazione del router per il dispositivo. Per ulteriori informazioni, consulta Download del file di configurazione del router.

Per creare un'interfaccia virtuale privata utilizzando l'API o la riga di comando

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface(AWS Direct Connect API)

Per visualizzare le interfacce virtuali collegate a un gateway Direct Connect utilizzando l'API o la riga di comando

- describe-direct-connect-gateway-allegati ()AWS CLI
- DescribeDirectConnectGatewayAttachments(API)AWS Direct Connect

Associazione di un gateway privato virtuale tra più account

È possibile associare un gateway Direct Connect a un gateway privato virtuale di proprietà di qualsiasi AWS account. Il gateway Direct Connect può essere un gateway esistente oppure è possibile creare un nuovo gateway. Il proprietario del gateway privato virtuale crea una proposta di associazione che il proprietario del gateway Direct Connect deve accettare.

Una proposta di associazione può contenere i prefissi che saranno consentiti dal gateway privato virtuale. Il proprietario del gateway Direct Connect ha la possibilità di sostituire qualsiasi prefisso richiesto nella proposta di associazione.

Prefissi consentiti

Quando si associa un gateway privato virtuale a un gateway Direct Connect, è necessario specificare un elenco di prefissi di Amazon VPC da pubblicizzare al gateway Direct Connect. L'elenco dei prefissi agisce come un filtro che consente di pubblicizzare CIDR uguali o più piccoli al gateway Direct Connect. È necessario impostare la voce Allowed prefixes (Prefissi consentiti) su un intervallo che sia uguale o più grande del CIDR del VPC, perché quest'ultimo viene assegnato per intero al gateway privato virtuale.

Prendiamo il caso di un CIDR del VPC pari a 10.0.0.0/16. È possibile impostare la voce Allowed prefixes (Prefissi consentiti) su 10.0.0.0/16 (il valore del CIDR del VPC) oppure su 10.0.0.0/15 (un valore maggiore del CIDR del VPC).

Qualsiasi interfaccia virtuale all'interno dei prefissi di rete pubblicizzati su Direct Connect viene propagata solo ai gateway di transito tra regioni, non all'interno della stessa regione. Per ulteriori informazioni su come i prefissi consentiti interagiscono con i gateway privati virtuali e i gateway di transito, consulta the section called “Interazioni dei prefissi consentiti”.

Attività

- Creazione di una proposta di associazione
- Accettazione o rifiuto di una proposta di associazione

- Aggiornamento dei prefissi consentiti per un'associazione
- Eliminazione di una proposta di associazione

Creazione di una proposta di associazione

Il proprietario del gateway privato virtuale deve creare una proposta di associazione. Il gateway privato virtuale deve essere collegato a un VPC del tuo AWS account. Il proprietario del gateway Direct Connect deve condividere l'ID del gateway Direct Connect e l'ID del relativo AWS account. Una volta creata la proposta, il proprietario del gateway Direct Connect deve accettarla per fornirti l'accesso alla rete locale su AWS Direct Connect.

Per creare una proposta di associazione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegliere Virtual private gateways (Gateway virtuali privati), quindi selezionare il gateway virtuale privato.
3. Seleziona Visualizza dettagli.
4. Scegliere prima Direct Connect gateway associations (Associazioni di gateway Direct Connect) e quindi Associate Direct Connect gateway (Associa gateway Direct Connect).
5. In Association account type (Tipo di account per associazione), in Account owner (Proprietario account) scegliere Another account (Altro account).
6. In Proprietario del gateway Direct Connect, immetti l'id dell'account AWS proprietario del gateway Direct Connect.
7. In Association settings (Impostazioni associazione), procedere come segue:
   a. In Direct Connect gateway ID (ID gateway Direct Connect), immettere l'ID del gateway Direct Connect.
   b. Per il proprietario del gateway Direct Connect, inserisci l'ID dell' AWS account proprietario del gateway Direct Connect per l'associazione.
   c. (facoltativo) Per specificare un elenco di prefissi da consentire per il gateway privato virtuale, aggiungerli agli Allowed prefixes (Prefissi consentiti), separandoli con virgole oppure inserendoli in righe separate.
8. Scegliere Associate Direct Connect gateway (Associa il gateway Direct Connect).

Per creare una proposta di associazione tramite API o riga di comando

- create-direct-connect-gateway-proposta di associazione ()AWS CLI
- CreateDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

Accettazione o rifiuto di una proposta di associazione

Per creare l'associazione, il proprietario del gateway Direct Connect deve accettare la proposta di associazione. In alternativa, è possibile rifiutarla.

Per accettare una proposta di associazione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegliere Direct Connect gateways (Gateway Direct Connect).
3. Selezionare il gateway Direct Connect proposte in attesa e scegliere View details (Visualizza dettagli).
4. Nella scheda Pending proposals (Proposte in attesa), selezionare la proposta e scegliere Accept proposal (Accetta proposta).
5. (facoltativo) Per specificare un elenco di prefissi da consentire per il gateway privato virtuale, aggiungerli agli Allowed prefixes (Prefissi consentiti), separandoli con virgole oppure inserendoli in righe separate.
6. Scegliere Accept proposal (Accetta proposta).

Per rifiutare una proposta di associazione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegliere Direct Connect gateways (Gateway Direct Connect).
3. Selezionare il gateway Direct Connect proposte in attesa e scegliere View details (Visualizza dettagli).
4. Nella scheda Pending proposals (Proposte in attesa), selezionare il gateway provato virtuale e scegliere Reject proposal (Rifiuta proposta).
5. Nella finestra di dialogo Reject proposal (Rifiuta proposta), immettere Delete (Elimina) e scegliere Reject proposal (Rifiuta proposta).

Per visualizzare le proposte di associazione tramite API o riga di comando

- describe-direct-connect-gateway-associazione-proposte ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposalsAWS Direct Connect (API)

Per accettare una proposta di associazione tramite API o riga di comando

- accept-direct-connect-gateway-proposta di associazione ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

Per rifiutare una proposta di associazione tramite API o riga di comando

- delete-direct-connect-gateway-proposta di associazione ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

Aggiornamento dei prefissi consentiti per un'associazione

È possibile aggiornare i prefissi consentiti dal gateway privato virtuale sul gateway Direct Connect.

Se sei il proprietario del gateway privato virtuale, crea una nuova proposta di associazione per gli stessi gateway Direct Connect e gateway privato virtuale, specificando i prefissi da consentire.

Se si è proprietari del gateway Direct Connect, aggiornare i prefissi consentiti quando si accetta la proposta di associazione oppure procedere come segue per aggiornarli per un'associazione esistente.

Per aggiornare i prefissi consentiti per un'associazione esistente tramite riga di comando o API

- update-direct-connect-gateway-associazione ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Eliminazione di una proposta di associazione

Il proprietario del gateway privato virtuale può eliminare la proposta di associazione con il gateway Direct Connect se questa è ancora in attesa di accettazione. Dopo che una proposta di accettazione è stata accettata non è possibile eliminarla, ma è possibile annullare l'associazione tra il gateway privato virtuale e il gateway Direct Connect. Per ulteriori informazioni, consulta the section called “Associazione e annullamento dell'associazione di gateway virtuali privati”.

Per eliminare una proposta di associazione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegliere Virtual private gateways (Gateway virtuali privati), quindi selezionare il gateway virtuale privato.
3. Seleziona Visualizza dettagli.
4. Scegliere Pending Direct Connect gateway associations (Associazioni gateway Direct Connect in attesa), selezionare l'associazione e scegliere Delete association (Elimina associazione).
5. Nella finestra di dialogo Delete association proposal (Elimina proposta di associazione), immettere Delete (Elimina) e scegliere Delete (Elimina).

Per eliminare una proposta di associazione in attesa tramite API o riga di comando

- delete-direct-connect-gateway-associazione-proposta ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

Associazioni di gateway di transito

Puoi utilizzare un gateway AWS Direct Connect per collegare la connessione AWS Direct Connect tramite un'interfaccia virtuale di transito ai VPC o alle VPN collegate al gateway di transito. È possibile associare un gateway Direct Connect al gateway di transito. Quindi, crea un'interfaccia virtuale di transito per la AWS Direct Connect connessione al gateway Direct Connect.

Le seguenti regole si applicano alle associazioni dei gateway di transito:

- Non è possibile collegare un gateway Direct Connect a un gateway di transito quando il gateway Direct Connect è già associato a un gateway privato virtuale o è collegato a un'interfaccia virtuale privata.
- Esistono dei limiti per la creazione e l'utilizzo di gateway Direct Connect. Per ulteriori informazioni, consulta Quote.
- Un gateway Direct Connect supporta la comunicazione tra le interfacce virtuali di transito collegate e i gateway di transito associati.
- Se ti connetti a più gateway di transito presenti in regioni diverse, utilizza ASN univoci per ciascun gateway di transito.

- Qualsiasi interfaccia virtuale all'interno dei prefissi di rete pubblicizzati su Direct Connect viene propagata solo ai gateway di transito tra le regioni, ma non all'interno della stessa regione

Associazione e annullamento dell'associazione di gateway di transito

Per associare un gateway di transito

1. Apri la console all'indirizzo https://console.aws.amazon.com/directconnect/v2/home. AWS Direct Connect
2. Nel riquadro di navigazione, scegliere Direct Connect gateways (Gateway Direct Connect), quindi selezionare il gateway Direct Connect.
3. Seleziona Visualizza dettagli.
4. Scegliere Gateway associations (Associazioni di gateway), quindi scegliere Associate gateway (Associa gateway).
5. Per Gateway, scegli il gateway di transito da associare.
6. In Prefissi consentiti, inserisci i prefissi (separati da una virgola o su una nuova riga) che il gateway Direct Connect pubblicizza al data center on-premise. Per ulteriori informazioni sui prefissi consentiti, consulta the section called “Interazioni dei prefissi consentiti”.
7. Scegli Associa gateway

Per visualizzare tutti i gateway associati al gateway Direct Connect, scegli Associazioni di gateway.

Come disassociare un gateway di transito

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegliere Direct Connect gateways (Gateway Direct Connect), quindi selezionare il gateway Direct Connect.
3. Seleziona Visualizza dettagli.
4. Scegliere Gateway associations (Associazioni di gateway), quindi selezionare il gateway di transito.
5. Scegli Dissocia.

Come aggiornare i prefissi consentiti per un gateway di transito

È possibile aggiungere o rimuovere prefissi consentiti al gateway di transito.

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Gateway Direct Connect, quindi il gateway Direct Connect per cui desideri aggiungere o rimuovere i prefissi consentiti.
3. Scegli la scheda Associazioni gateway.
4. Scegli il gateway che desideri modificare, quindi scegli Modifica.
5. In Prefissi consentiti, immetti i prefissi che il gateway Direct Connect pubblicizza al data center on-premise. Per più prefissi, separa ogni prefisso con una virgola o inserisci ogni prefisso su una nuova riga. I prefissi aggiunti devono corrispondere ai CIDR Amazon VPC per tutti i gateway privati virtuali. Per ulteriori informazioni sui prefissi consentiti, consulta the section called “Interazioni dei prefissi consentiti”.
6. Scegliere Edit association (Modifica associazione).

   Nella sezione associazione Gateway, lo Stato mostra Aggiornamento in corso. Al termine, lo Stato diventa Associato.
7. Seleziona Annulla associazione.
8. Scegli nuovamente Annulla associazione per confermare che desideri dissociare il gateway.

   Nella sezione Associazione gateway, viene visualizzato lo Stato annullamento dell'associazione. Al termine, viene visualizzato un messaggio di conferma e il gateway viene rimosso dalla sezione. Il completamento dell'operazione potrebbe richiedere qualche minuto.

Per associare unn gateway di transito utilizzando l'API o la riga di comando

- create-direct-connect-gateway-associazione ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

Per visualizzare i gateway di transito associati a un gateway Direct Connect utilizzando l'API o la riga di comando

- describe-direct-connect-gateway-associazioni ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

Per annullare l'associazione di un gateway di transito utilizzando l'API o la riga di comando

- delete-direct-connect-gateway-associazione ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

Per aggiornare i prefissi consentiti per un gateway di transito utilizzando l'API o la riga di comando

- update-direct-connect-gateway-associazione ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Creazione di un'interfaccia virtuale di transito per un gateway Direct Connect

Per connettere la AWS Direct Connect connessione al gateway di transito, è necessario creare un'interfaccia di transito per la connessione. Specificare il gateway Direct Connect al quale connettersi.

> **Important**
>
> Se associ il tuo gateway di transito a uno o più gateway Direct Connect, il numero di sistema autonomo (ASN) utilizzato dal gateway di transito e dal gateway Direct Connect devono essere diversi. Ad esempio, se utilizzi l'ASN 64512 predefinito sia per il gateway di transito che per il gateway Direct Connect, la richiesta di associazione ha esito negativo.

Per effettuare il provisioning di un'interfaccia virtuale di transito in un gateway Direct Connect

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Virtual Interfaces (Interfacce virtuali).
3. Scegliere Create virtual interface (Crea interfaccia virtuale).
4. In Virtual interface type (Tipo di interfaccia virtuale), per Type (Tipo) scegliere Transit (Transito).
5. In Transit virtual interface settings (Impostazioni interfaccia virtuale di transito), procedere come segue:

   a. In Nome interfaccia virtuale, immetti il nome dell'interfaccia virtuale.

b. In Connection (Connessione), scegliere la connessione Direct Connect che si intende utilizzare per questa interfaccia.

c. Per il proprietario dell'interfaccia virtuale, scegli Il mio AWS account se l'interfaccia virtuale è per il tuo AWS account.

d. Per Direct Connect gateway (Gateway Direct Connect), selezionare il gateway Direct Connect.

e. In VLAN, immettere il numero ID della rete LAN virtuale (VLAN).

f. Per BGP ASN, immetti il Numero di sistema autonomo del border gateway protocol del router peer on-premise per la nuova interfaccia virtuale.

   I valori validi sono compresi tra 1 e 2147483647.

6. In Impostazioni aggiuntive, procedi come segue:

   a. Per configurare un peer BGP IPv4 o IPv6, procedere come segue:

      [IPv4] Per configurare un peer BGP IPv4, scegliere IPv4, quindi eseguire una di queste azioni:

      - Per specificare in prima persona gli indirizzi IP, in Your router peer ip (Il tuo IP peer del router), immettere l'indirizzo CIDR IPv4 di destinazione a cui Amazon dovrà inviare il traffico.
      - In IP peer del router Amazon, immetti l'indirizzo CIDR IPv4 da utilizzare per inviare il traffico ad AWS.

      > **Important**
      >
      > Se consenti l' AWS assegnazione automatica degli indirizzi IPv4, verrà allocato un CIDR /29 da 169.254.0.0/16 IPv4 Link-Local secondo RFC 3927 per la connettività. point-to-point AWS non consiglia questa opzione se si intende utilizzare l'indirizzo IP peer del router del cliente come origine e/o destinazione per il traffico VPC. È invece consigliabile utilizzare RFC 1918 o un altro indirizzo (diverso da RFC 1918) e specificare personalmente l'indirizzo.
      >
      > - Per ulteriori informazioni su RFC 1918, consulta Address Allocation for Private Internets.
      > - Per ulteriori informazioni su RFC 3927, consulta Dynamic Configuration of IPv4 Link-Local Addresses.

[IPv6] Per configurare un peer BGP IPv6, scegliere IPv6. Gli indirizzi IPv6 peer vengono assegnati automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile specificare indirizzi IPv6 personalizzati.

b. Per modificare l'unità di trasmissione massima (MTU) da 1500 (predefinito) a 8500 (frame jumbo), selezionare Jumbo MTU (MTU size 8500) (MTU jumbo - dimensione della MTU 8500).

c. (Facoltativo) In Abilita SiteLink, scegli Abilitato per abilitare la connettività diretta tra i punti di presenza Direct Connect.

d. (Facoltativo) Aggiunta o rimozione di un tag.

[Aggiungere un tag] Scegliere Add tag (Aggiungi tag) e procedere come segue:

- In Chiave, immetti il nome della chiave.
- In Valore, immetti il valore della chiave.

[Rimuovere un tag] Accanto al tag, scegliere Remove tag (Rimuovi tag).

7. Scegliere Create virtual interface (Crea interfaccia virtuale).

Dopo aver creato l'interfaccia virtuale, è possibile scaricare la configurazione del router per il dispositivo. Per ulteriori informazioni, consulta Download del file di configurazione del router.

Per creare un'interfaccia virtuale di transito utilizzando l'API o la riga di comando

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS Direct Connect API)

Per visualizzare le interfacce virtuali collegate a un gateway Direct Connect utilizzando l'API o la riga di comando

- describe-direct-connect-gateway-allegati ()AWS CLI
- DescribeDirectConnectGatewayAttachments(API)AWS Direct Connect

Associazione di un gateway di transito tra più account

È possibile associare un gateway Direct Connect esistente o un nuovo gateway Direct Connect a un gateway di transito di proprietà di qualsiasi AWS account. Il proprietario del gateway di transito crea una proposta di associazione che il proprietario del gateway Direct Connect deve accettare.

Una proposta di associazione può contenere i prefissi che saranno consentiti dal gateway di transito. Il proprietario del gateway Direct Connect ha la possibilità di sostituire qualsiasi prefisso richiesto nella proposta di associazione.

Prefissi consentiti

Per un'associazione del gateway di transito, devi effettuare il provisioning dell'elenco dei prefissi consentiti sul gateway Direct Connect. L'elenco viene utilizzato per instradare il traffico dall'ambiente locale al AWS gateway di transito anche se i VPC collegati al gateway di transito non dispongono di CIDR assegnati. I prefissi nell'elenco dei prefissi consentiti del gateway Direct Connect hanno origine sul gateway Direct Connect e sono pubblicizzati alla rete locale. Per ulteriori informazioni su come i prefissi consentiti interagiscono con i gateway di transito e i gateway privati virtuali, consulta the section called “Interazioni dei prefissi consentiti”.

Attività

- Creazione di una proposta di associazione per gateway di transito
- Accettazione o rifiuto di una proposta di associazione per gateway di transito
- Aggiornamento dei prefissi consentiti per un'associazione di gateway di transito
- Eliminazione di una proposta di associazione per gateway di transito

Creazione di una proposta di associazione per gateway di transito

Se si è proprietari del gateway di transito, è necessario creare la proposta di associazione. Il gateway di transito deve essere collegato a un VPC o VPN nel tuo AWS account. Il proprietario del gateway Direct Connect deve condividere l'ID del gateway Direct Connect e l'ID del suo account AWS . Una volta creata la proposta, il proprietario del gateway Direct Connect deve accettarla per fornirti l'accesso alla rete locale su AWS Direct Connect.

Per creare una proposta di associazione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.

2. Nel riquadro di navigazione scegli Gateway di transito e seleziona il gateway di transito.
3. Seleziona Visualizza dettagli.
4. Scegliere Direct Connect gateway associations (Associazioni di gateway Direct Connect), quindi Associate Direct Connect gateway (Associa gateway Direct Connect).
5. In Association account type (Tipo di account per associazione), in Account owner (Proprietario account) scegliere Another account (Altro account).
6. In Proprietario del gateway Direct Connect, immetti l'ID dell'account proprietario del gateway Direct Connect.
7. In Association settings (Impostazioni associazione), procedere come segue:

   a. In Direct Connect gateway ID (ID gateway Direct Connect), immettere l'ID del gateway Direct Connect.

   b. In Proprietario dell'interfaccia virtuale, immetti l'ID dell'account proprietario dell'interfaccia virtuale per l'associazione.

   c. (facoltativo) Per specificare un elenco di prefissi consentiti dal gateway di transito, aggiungerli ai Prefissi consentiti, separandoli con virgole oppure inserendoli in righe separate.
8. Scegliere Associate Direct Connect gateway (Associa il gateway Direct Connect).

Per creare una proposta di associazione tramite API o riga di comando

- create-direct-connect-gateway-associazione-proposta ()AWS CLI
- CreateDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

Accettazione o rifiuto di una proposta di associazione per gateway di transito

Per creare l'associazione, il proprietario del gateway Direct Connect deve accettare la proposta di associazione. È inoltre possibile rifiutare la proposta di associazione.

Per accettare una proposta di associazione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegliere Direct Connect gateways (Gateway Direct Connect).
3. Selezionare il gateway Direct Connect con proposte in attesa, quindi scegliere View details (Visualizza dettagli).

4. Nella scheda Pending proposals (Proposte in attesa), selezionare la proposta, quindi scegliere Accept proposal (Accetta proposta).
5. (facoltativo) Per specificare un elenco di prefissi consentiti dal gateway di transito, aggiungerli ai Prefissi consentiti, separandoli con virgole oppure inserendoli in righe separate.
6. Scegliere Accept proposal (Accetta proposta).

Per rifiutare una proposta di associazione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegliere Direct Connect gateways (Gateway Direct Connect).
3. Selezionare il gateway Direct Connect con proposte in attesa, quindi scegliere View details (Visualizza dettagli).
4. Nella scheda Pending proposals (Proposte in attesa), selezionare il gateway di transito, quindi scegliere Reject proposal (Rifiuta proposta).
5. Nella finestra di dialogo Reject proposal (Rifiuta proposta), immettere Delete (Elimina), quindi scegliere Reject proposal (Rifiuta proposta).

Per visualizzare le proposte di associazione tramite API o riga di comando

- describe-direct-connect-gateway-associazione-proposte ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposalsAWS Direct Connect (API)

Per accettare una proposta di associazione tramite API o riga di comando

- accept-direct-connect-gateway-proposta di associazione ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

Per rifiutare una proposta di associazione tramite API o riga di comando

- delete-direct-connect-gateway-proposta di associazione ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

Aggiornamento dei prefissi consentiti per un'associazione di gateway di transito

È possibile aggiornare i prefissi che sono consentiti dal gateway di transito tramite il gateway Direct Connect.

Se sei il proprietario del gateway di transito, devi creare una nuova proposta di associazione per lo stesso gateway Direct Connect e gateway privato virtuale, specificando i prefissi da consentire.

Se si è proprietari del gateway Direct Connect, aggiornare i prefissi consentiti quando si accetta la proposta di associazione oppure procedere come segue per aggiornarli per un'associazione esistente.

Per aggiornare i prefissi consentiti per un'associazione esistente tramite riga di comando o API

- update-direct-connect-gateway-associazione ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Eliminazione di una proposta di associazione per gateway di transito

Il proprietario del gateway di transito può eliminare la proposta di associazione con il gateway Direct Connect se questa è ancora in attesa di accettazione. Dopo che una proposta di accettazione è stata accettata non è possibile eliminarla, ma è possibile annullare l'associazione tra il gateway di transito e il gateway Direct Connect. Per ulteriori informazioni, consulta the section called "Creazione di una proposta di associazione per gateway di transito".

Per eliminare una proposta di associazione

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione scegli Gateway di transito e seleziona il gateway di transito.
3. Seleziona Visualizza dettagli.
4. Scegliere Pending gateway associations (Associazioni gateway in attesa), selezionare l'associazione e scegliere Delete association (Elimina associazione).
5. Nella finestra di dialogo Delete association proposal (Elimina proposta di associazione), immettere Delete (Elimina) e scegliere Delete (Elimina).

Per eliminare una proposta di associazione in attesa tramite API o riga di comando

- delete-direct-connect-gateway-associazione-proposta ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

Interazioni dei prefissi consentiti

Scopri come i prefissi consentiti interagiscono con i gateway di transito e i gateway virtuali privati. Per ulteriori informazioni, consulta the section called “Policy di instradamento e comunità BGP”.

Associazioni di gateway privati virtuali

L'elenco dei prefissi (IPv4 e IPv6) agisce come un filtro che consente di pubblicizzare CIDR uguali o un intervallo più piccolo di CIDR al gateway Direct Connect. È necessario impostare i prefissi su un intervallo uguale o più ampio del blocco CIDR VPC.

> **Note**
>
> L'elenco consentito funziona solo come filtro e solo il CIDR VPC associato verrà pubblicizzato al gateway del cliente.

Considerare lo scenario in cui si dispone di un VPC con CIDR 10.0.0.0/16 collegato a un gateway virtuale privato.

- Quando l'elenco dei prefissi consentiti è impostato su 22.0.0.0/24, non si riceve nessuna route perché 22.0.0.0/24 non è uguale o più ampio di 10.0.0.0/16.
- Quando l'elenco dei prefissi consentiti è impostato su 10.0.0.0/24, non si riceve nessuna route perché 10.0.0.0/24 non è uguale a 10.0.0.0/16.
- Quando l'elenco dei prefissi consentiti è impostato su 10.0.0.0/15, si riceve 10.0.0.0/16 perché l'indirizzo IP è più ampio di 10.0.0.0/16.

Quando rimuovi o aggiungi un prefisso consentito, il traffico che non utilizza tale prefisso non viene influenzato. Durante gli aggiornamenti lo stato cambia da `associated` a `updating`. La modifica di un prefisso esistente può ritardare solo il traffico che utilizza quel prefisso.

Associazioni di gateway di transito

Per un'associazione del gateway di transito, devi effettuare il provisioning dell'elenco dei prefissi consentiti sul gateway Direct Connect. L'elenco instrada il traffico dall'ambiente on-premise da o verso il gateway Direct Connect nel gateway di transito, anche quando i VPC associati al gateway di transito non dispongono di CIDT assegnati. I prefissi consentiti funzionano in modo diverso, a seconda del tipo di gateway:

- Per le associazioni di gateway di transito, solo i prefissi consentiti inseriti verranno pubblicizzati on-premise. Questi verranno visualizzati come provenienti dall'ASN del gateway Direct Connect.
- Per i gateway privati virtuali, i prefissi consentiti inseriti fungono da filtro per consentire CIDR uguali o più piccoli.

Considerare lo scenario in cui si dispone di un VPC con CIDR 10.0.0.0/16 collegato a un gateway di transito.

- Quando l'elenco dei prefissi consentiti è impostato su 22.0.0.0/24, si riceve 22.0.0.0/24 tramite BGP sull'interfaccia virtuale di transito. Non si riceve 10.0.0.0/16 perché effettuiamo direttamente il provisioning dei prefissi che sono nell'elenco dei prefissi consentiti.
- Quando l'elenco dei prefissi consentiti è impostato su 10.0.0.0/24, si riceve 10.0.0.0/24 tramite BGP sull'interfaccia virtuale di transito. Non si riceve 10.0.0.0/16 perché effettuiamo direttamente il provisioning dei prefissi che sono nell'elenco dei prefissi consentiti.
- Quando l'elenco dei prefissi consentiti è impostato su 10.0.0.0/8, si riceve 10.0.0.0/8 tramite BGP sull'interfaccia virtuale di transito.

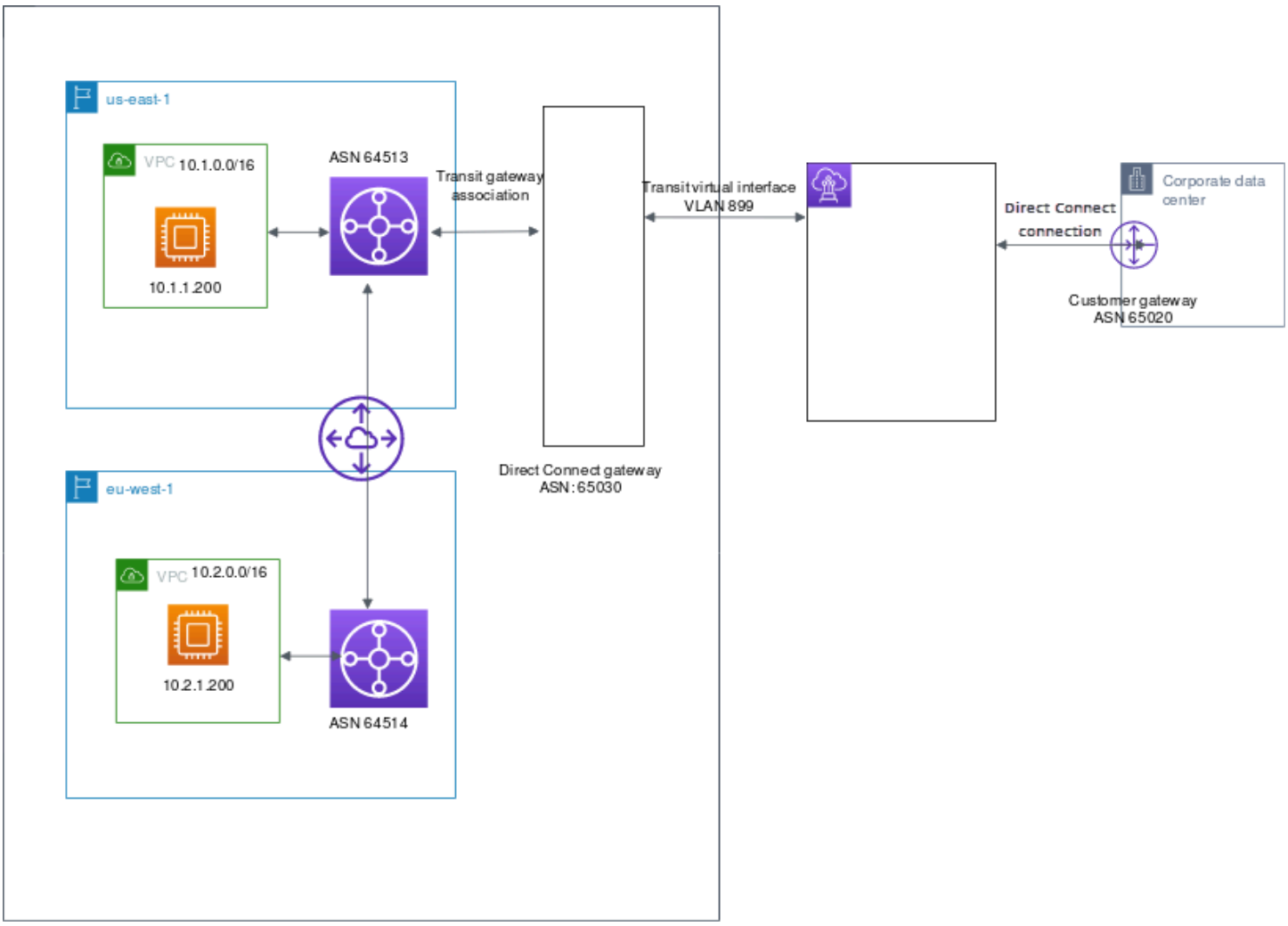
Le sovrapposizioni di prefissi consentite non sono consentite quando più gateway di transito sono associati a un gateway Direct Connect. Ad esempio, se si dispone di un gateway di transito con un elenco di prefissi consentiti che include 10.1.0.0/16 e un secondo gateway di transito con un elenco di prefissi consentiti che include 10.2.0.0/16 e 0.0.0.0/0, non è possibile impostare le associazioni dal secondo gateway di transito su 0.0.0.0/0. Poiché 0.0.0.0/0 include tutte le reti IPv4, non è possibile configurare 0.0.0.0/0 se più gateway di transito sono associati a un gateway Direct Connect. Viene restituito un errore che indica che le rotte consentite si sovrappongono a una o più rotte consentite esistenti sul gateway Direct Connect.

Quando rimuovi o aggiungi un prefisso consentito, il traffico che non utilizza tale prefisso non viene influenzato. Durante gli aggiornamenti lo stato cambia da `associated` a `updating`. La modifica di un prefisso esistente può ritardare solo il traffico che utilizza quel prefisso.

Esempio: prefissi consentiti in una configurazione di gateway di transito

Prendi in considerazione la configurazione in cui sono presenti istanze in due diverse regioni AWS che devono accedere al data center aziendale. È possibile configurare le seguenti risorse per questa configurazione:

- Un gateway di transito in ogni regione.
- Connessioni di peering del gateway di transito.
- Un gateway Direct Connect.
- Un'associazione di gateway di transito tra uno dei gateway di transito (quello in us-east-1) e il gateway Direct Connect.
- Un'interfaccia virtuale di transito tra la sede on-premise e la posizione AWS Direct Connect.



Configura le opzioni seguenti per le risorse.

- Gateway Direct Connect: imposta l'ASN su 65030. Per ulteriori informazioni, consulta the section called “Creazione di un gateway Direct Connect”.
- Interfaccia virtuale di transito: imposta la VLAN su 899 e l'ASN su 65020. Per ulteriori informazioni, consulta the section called “Creazione di un'interfaccia virtuale di transito per un gateway Direct Connect”.
- Associazione del gateway Direct Connect al gateway di transito: imposta i prefissi consentiti su 10.0.0.0/8.

  Questo blocco CIDR copre entrambi i blocchi CIDR VPC. Per ulteriori informazioni, consulta the section called “Associazione e annullamento dell'associazione di gateway di transito”.
- Percorso VPC: per indirizzare il traffico dal VPC 10.2.0.0, crea un percorso nella tabella di routing VPC con una destinazione di 0.0.0.0/0 e l'ID del gateway di transito come destinazione. Per

maggiori informazioni sul routing verso un gateway di transito, consulta Routing per un gateway di transito nella Guida per l'utente di Amazon VPC.

Tagging delle risorse AWS Direct Connect

Un tag è un'etichetta che il propritario di una risorsa assegna alle proprie risorse AWS Direct Connect. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili. I tag consentono al proprietario della risorsa di categorizzare le risorse AWS Direct Connect in modi diversi, ad esempio, per scopo o ambiente. Questa funzionalità è molto utile quando hai tante risorse dello stesso tipo: puoi rapidamente individuare una risorsa specifica in base ai tag assegnati.

Ad esempio, disponi di due connessioni AWS Direct Connect in una regione, ciascuna in diverse sedi. La connessione `dxcon-11aa22bb` è una connessione dedicata al traffico di produzione ed è associata all'interfaccia virtuale `dxvif-33cc44dd`. La connessione `dxcon-abcabcab` è una connessione ridondante (di backup) ed è associata all'interfaccia virtuale `dxvif-12312312`. Puoi scegliere di contrassegnare con dei tag le connessioni e le interfacce virtuali come segue, per distinguerle meglio:

ID risorsa	Chiave tag	Valore tag
`dxcon-11aa22bb`	Scopo	Produzione
	Ubicazione	Amsterdam
`dxvif-33cc44dd`	Scopo	Produzione
`dxcon-abcabcab`	Scopo	Backup
	Ubicazione	Francoforte
`dxvif-12312312`	Scopo	Backup

Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti di ciascun tipo di risorsa. Tramite un set di chiavi di tag coerente la gestione delle risorse risulta notevolmente semplificata. I tag non hanno alcun significato semantico per AWS Direct Connect e vengono interpretati rigorosamente come una stringa di caratteri. Inoltre, i tag non vengono assegnati automaticamente alle risorse. Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore

sovrascrive quello precedente. Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa.

È possibile assegnare i tag alle seguenti risorse AWS Direct Connect utilizzando la console AWS Direct Connect, l'API AWS Direct Connect, l'AWS CLI, il AWS Tools for Windows PowerShell o un SDK AWS. Quando utilizzi questi strumenti per gestire i tag, devi specificare l'Amazon Resource Name (ARN) della risorsa. Per ulteriori informazioni sull'utilizzo degli ARN, consulta Amazon Resource Name (ARN) nella Riferimenti generali di Amazon Web Services.

Risorsa	Supporta tag	Supporto dei tag in fase di creazione	Supporto dei tag che controllano l'accesso e l'allocazione delle risorse	Supporto dell'allocazione dei costi
Connessioni	Sì	Sì	Sì	Sì
Interfacce virtuali	Sì	Sì	Sì	No
Link aggregation groups (LAG)	Sì	Sì	Sì	Sì
Interconnessioni	Sì	Sì	Sì	Sì
Gateway Direct Connect	No	No	No	No

Limitazioni applicate ai tag

Ai tag si applicano le seguenti regole e limitazioni:

- numero massimo di tag per risorsa: 50
- lunghezza massima della chiave: 128 caratteri Unicode;
- lunghezza massima del valore: 265 caratteri Unicode;
- Per chiavi e valori di tag viene fatta la distinzione tra maiuscole e minuscole.

- Il prefisso `aws:` è riservato per l'uso di AWS. Non puoi modificare o eliminare la chiave o il valore di un tag quando il tag ha una chiave tag con il prefisso `aws:`. I tag con il prefisso `aws:` non vengono conteggiati per il limite del numero di tag per risorsa.
- I caratteri consentiti sono lettere, spazi e numeri rappresentabili in formato UTF-8, più i caratteri speciali: + - = . _ : / @
- Soltanto il proprietario della risorsa può aggiungere o rimuovere tag. Ad esempio, se c'è una connessione in hosting, il partner non è in grado di aggiungere, eliminare o visualizzare i tag.
- I tag di allocazione dei costi sono supportati solo per le connessioni, le interconnessioni e i LAG. Per informazioni su come usare i tag con la gestione dei costi, consulta Utilizzo dei tag per l'allocazione dei costi nellaGuida per utente di AWS Billing and Cost Management.

Utilizzo di tag tramite la CLI o l'API

Utilizza le seguenti informazioni per aggiungere, aggiornare, elencare ed eliminare i tag per le risorse.

Attività	API	CLI
Aggiungere sovrascrivere uno o più tag.	TagResource	tag-resource
Eliminare uno o più tag.	UntagResource	untag-resource
Descrivere uno o più tag.	DescribeTags	describe-tags

Esempi

Utilizza il comando tag-resource per applicare il tag alla connessione `dxcon-11aa22bb`.

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

Utilizza il comando describe-tags per descrivere i tag della connessione `dxcon-11aa22bb`.

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb
```

Utilizza il comando untag-resource per rimuovere un tag dalla connessione `dxcon-11aa22bb`.

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

Sicurezza in AWS Direct Connect

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformità AWS. Per ulteriori informazioni sui programmi di conformità che si applicano a AWS Direct Connect, consulta Servizi coperti dal programma di conformitàAWS.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione facilitaconsenteladicomprensionecomprenderedell'applicazionecomedelapplicare il modello di responsabilità condivisa quando utilizzisi usaAWS Direct Connect. I seguenti argomenti illustrano come configurare AWS Direct Connect per soddisfare gli obiettivi di sicurezza e conformità. Scoprirai anche come utilizzare altri servizi di AWS per monitorare e proteggere le risorse AWS Direct Connect.

Argomenti

Protezione dei dati in AWS Direct Connect

Il modello di responsabilità condivisa di AWSsi applica alla protezione dei dati in AWS Direct Connect. Come descritto in questo modello, AWSè responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWSattraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Questo vale quando si lavora con l'AWS Direct Connect e altri Servizi AWS utilizzando la console, l'API, la AWS CLI o gli SDK di AWS. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Per ulteriori informazioni sulla protezione dei dati, consulta il post del blog AWS Modello di responsabilità condivisa e GDPR su AWS Security Blog.

Argomenti

- Riservatezza del traffico Internet in AWS Direct Connect
- Crittografia in transito AWS Direct Connect

Riservatezza del traffico Internet in AWS Direct Connect

Traffico tra servizio e applicazioni e client locali

Sono disponibili due opzioni di connettività tra la rete privata e AWS:

- Un'associazione a un AWS Site-to-Site VPN. Per ulteriori informazioni, consulta the section called “Sicurezza dell'infrastruttura”.
- Un'associazione ai VPC. Per ulteriori informazioni, consulta the section called “Associazioni di gateway privati virtuali” e the section called “Associazioni di gateway di transito”.

Traffico tra risorse AWS nella stessa Regione

Sono disponibili due opzioni di connettività:

- Un'associazione a un AWS Site-to-Site VPN. Per ulteriori informazioni, consulta the section called “Sicurezza dell'infrastruttura”.
- Un'associazione ai VPC. Per ulteriori informazioni, consulta the section called “Associazioni di gateway privati virtuali” e the section called “Associazioni di gateway di transito”.

Crittografia in transito AWS Direct Connect

AWS Direct Connect per impostazione predefinita, non crittografa il traffico in transito. Per crittografare i dati in transito che li attraversano AWS Direct Connect, è necessario utilizzare le opzioni di crittografia del transito per quel servizio. Per ulteriori informazioni sulla crittografia del traffico delle istanze EC2, consulta Encryption in Transit nella Amazon EC2 User Guide.

Con AWS Direct Connect e AWS Site-to-Site VPN, puoi combinare una o più connessioni di rete AWS Direct Connect dedicate con Amazon VPC VPN. Questa combinazione fornisce una

connessione privata crittografata con IPSec che riduce anche i costi di rete, aumenta la velocità di trasmissione effettiva della larghezza di banda e offre un'esperienza di rete più coerente rispetto alle connessioni VPN basate su Internet. Per ulteriori informazioni, consulta Opzioni di connettività da Amazon VPC ad Amazon VPC.

MAC Security (MACsec) è uno standard IEEE che garantisce la riservatezza dei dati, l'integrità dei dati e l'autenticità dell'origine dei dati. Puoi utilizzare AWS Direct Connect connessioni che supportano MacSec per crittografare i dati dal data center aziendale alla sede. AWS Direct Connect Per ulteriori informazioni, consulta MAC Security.

Identity and Access Management per Direct Connect

AWS Identity and Access Management (IAM) è un Servizio AWSche consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (chi può effettuare l'accesso) e autorizzato (chi dispone delle autorizzazioni) a utilizzare risorse Direct Connect. IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Funzionamento di Direct Connect con IAM
- Esempi di policy basate su identità per Direct Connect
- Ruoli collegati ai servizi per AWS Direct Connect
- Policy gestite da AWS per AWS Direct Connect
- Risoluzione dei problemi relativi all'identità e all'accesso di Direct Connect

Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni che vengono eseguite in Direct Connect.

Utente del servizio: se utilizzi il servizio Direct Connect per eseguire il tuo lavoro, l'amministratore ti fornirà le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità Direct Connect utilizzate per svolgere il tuo lavoro, potrebbero essere necessarie ulteriori autorizzazioni.

La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Direct Connect, consulta Risoluzione dei problemi relativi all'identità e all'accesso di Direct Connect.

Amministratore del servizio: se sei il responsabile delle risorse Direct Connect presso la tua azienda, probabilmente disponi dell'accesso completo a Direct Connect. Il compito dell'utente è determinare le caratteristiche e le risorse Direct Connect a cui gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Direct Connect, consulta Funzionamento di Direct Connect con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dettagli su come scrivere policy per gestire l'accesso a Direct Connect. Per visualizzare policy basate su identità Direct Connect di esempio che puoi utilizzare in IAM, consulta Esempi di policy basate su identità per Direct Connect.

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWScon le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWScome identità federata utilizzando le credenziali fornite attraverso un'origine di identità. AWS IAM Identity Center Gli esempi di identità federate comprendono gli utenti del centro identità IAM, l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWStramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Consoleo al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione Come accedere al tuo Account AWSnella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta Firma delle richieste AWS nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWSe le risorse nell'account. Tale identità è detta utente root Account AWSed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conservare le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come best practice, richiedere agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWSutilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, AWS Directory Service, la directory Identity Center o qualsiasi utente che accede a Servizi AWS utilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono a Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli Account AWS. Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center.

Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWSche dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con

utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità all'interno di Account AWSche dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Consolemediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'operazione AWS CLIo API AWSoppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.

- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso multi-servizio: alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Inoltro delle sessioni di accesso (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, tale utente o ruolo viene considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWSe sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWSa un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le

credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWSche, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWSvaluta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWSJSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLIo l'API AWS.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le

policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWSe le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy gestite da AWSda IAM in una policy basata su risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAFe Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi

di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.

- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

Funzionamento di Direct Connect con IAM

Prima di utilizzare IAM per gestire l'accesso a Direct Connect, scopri quali funzionalità di IAM sono disponibili per l'uso con Direct Connect.

Funzionalità di IAM che puoi utilizzare con Direct Connect

Funzionalità IAM	Supporto Direct Connect
Policy basate su identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì

Funzionalità IAM	Supporto Direct Connect
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	No

Per ottenere un quadro generale del funzionamento di Direct Connect e altri servizi AWS con la maggior parte delle caratteristiche di IAM, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Policy basate su identità per Direct Connect

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate su identità per Direct Connect

Per visualizzare esempi di policy basate su identità di Direct Connect, consulta Esempi di policy basate su identità per Direct Connect.

Policy basate su risorse all'interno di Direct Connect

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni di policy per Direct Connect

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy JSON AWSper specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le operazioni di policy hanno spesso lo stesso nome

dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni Direct Connect, vedere Azioni definite da Direct Connect nel riferimento di autorizzazione del servizio.

Le operazioni delle policy in Direct Connect utilizzano il seguente prefisso prima dell'operazione:

```
Direct Connect
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "Direct Connect:action1",
      "Direct Connect:action2"
         ]
```

Risorse di policy per Direct Connect

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy JSON AWSper specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse e relativi ARN, consulta Tipi di risorse definiti da Direct Connect nella Guida di riferimento per le API AWS Direct Connect. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta Operazioni definite da Direct Connect.

Per visualizzare esempi di policy basate su identità di Direct Connect, consulta Esempi di policy basate su identità per Direct Connect.

Per visualizzare esempi di policy basate su risorse di Direct Connect, consulta Esempi di policy basate su identità Direct Connect con condizioni basate su tag.

Chiavi di condizione per Direct Connect

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy JSON AWSper specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Per visualizzare un elenco delle chiavi di condizione di Direct Connect, consulta Chiavi di condizione per Direct Connect nella Guida di riferimento per le API AWS Direct Connect. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, vedere Azioni, risorse e chiavi di condizione per Direct Connect nel riferimento di autorizzazione del servizio.

Per visualizzare esempi di policy basate su identità di Direct Connect, consulta Esempi di policy basate su identità per Direct Connect.

ACL in Direct Connect

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Direct Connect

Supporta ABAC (tag nelle policy)	Parziale

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Direct Connect

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWSnon funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWS che funzionano con le credenziali temporanee, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Consoleutilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi ad AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLIo l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWSconsiglia di generare le credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni del principale tra servizi per Direct Connect

Supporta sessioni di accesso diretto (FAS)	Sì

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per Direct Connect

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità di Direct Connect. Modificare i ruoli di servizio solo quando Direct Connect fornisce le indicazioni per farlo.

Ruoli collegati ai servizi per Direct Connect

Supporta i ruoli collegati ai servizi	No

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWSe sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate su identità per Direct Connect

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Direct Connect. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, l'AWS Command Line Interface (AWS CLI) o l'API AWS. Per concedere agli

utenti l'autorizzazione per eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle operazioni e sui tipi di risorse definiti da Direct Connect, incluso il formato degli ARN per ogni tipo di risorse, consulta Operazioni, risorse e chiavi di condizione per Direct Connect nella Guida di riferimento per l'autorizzazione del servizio.

Argomenti

Best practice per le policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminare le risorse Direct Connect nell'account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWSspecifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come

autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.

- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Operazioni, risorse e chiavi di condizione per Direct Connect

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Direct Connect supporta operazioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le operazioni di policy hanno spesso lo stesso nome

dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le operazioni delle policy in Direct Connect utilizzano il seguente prefisso prima dell'operazione: `directconnect:`. Ad esempio, per concedere a qualcuno l'autorizzazione per eseguire un'istanza Amazon EC2 con l'operazione API `DescribeVpnGateways` Amazon EC2, è necessario includere l'operazione `ec2:DescribeVpnGateways` nella policy. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Direct Connect definisce un proprio insieme di operazioni che descrivono le attività che puoi eseguire con quel servizio.

La seguente policy esemplificativa consente l'accesso in lettura a AWS Direct Connect.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

La seguente policy esemplificativa consente l'accesso completo a AWS Direct Connect.

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

```
    ]
}
```

Per visualizzare un elenco di azioni Direct Connect, consulta Azioni definite da Direct Connect nella Guida per l'utente IAM.

Risorse

Gli amministratori possono utilizzare le policy JSON AWSper specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Direct Connect utilizza i seguenti ARN:

ARN delle risorse Direct Connect

Tipo di risorsa	ARN
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`

Tipo di risorsa	ARN
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`

Per ulteriori informazioni sul formato degli ARN, consulta Nome della risorsa Amazon (ARN) e spazi dei nomi del servizio AWS.

Ad esempio, per specificare l'interfaccia `dxcon-11aa22bb` nell'istruzione, utilizza il seguente ARN:

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

Per specificare tutte le istanze virtuali che appartengono a un account specifico, utilizza il carattere jolly (*):

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

Alcune operazioni Direct Connect, ad esempio quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse e relativi ARN, consulta Tipi di risorse Direct Connect definite da AWS Direct Connect nella Guida per l'utente IAM. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta SERVICE-ACTIONS-URL.

Chiavi di condizione

Gli amministratori possono utilizzare le policy JSON AWS per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se specifichi

più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione OR logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Direct Connect definisce il proprio set di chiavi di condizione e, inoltre, supporta l'uso di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente IAM.

Puoi utilizzare le chiavi di condizione con la risorsa tag. Per ulteriori informazioni, consultare Esempio: limitazione dell'accesso a una regione specifica.

Per visualizzare un elenco delle chiavi di condizione di Direct Connect, consulta Chiavi di condizione per Direct Connect nella Guida per l'utente IAM. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta SERVICE-ACTIONS-URL.

Utilizzo della console Direct Connect

Per accedere alla console Direct Connect, è necessario disporre di un set di autorizzazioni minimo. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli relativi alle risorse Direct Connect nell'account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (o ruoli) associate a tale policy.

Per garantire che tali entità possano ancora utilizzare la console Direct Connect, collega anche la seguente policy gestita di AWS alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM:

```
directconnect
```

Non sono necessarie le autorizzazioni minime della console per gli utenti che effettuano chiamate solo alla AWS CLIo all'API AWS. Al contrario, puoi accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLIo l'API AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Accesso in sola lettura a AWS Direct Connect

La seguente policy esemplificativa consente l'accesso in lettura a AWS Direct Connect.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Accesso completo a AWS Direct Connect

La seguente policy esemplificativa consente l'accesso completo a AWS Direct Connect.

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

Esempi di policy basate su identità Direct Connect con condizioni basate su tag

Puoi controllare l'accesso alle risorse e alle richieste utilizzando le condizioni delle chiavi di tag. Puoi utilizzare una condizione nella policy IAM per controllare se specifiche chiavi di tag possono essere utilizzate su una risorsa o in una richiesta.

Per informazioni su come utilizzare i tag con le policy IAM, consulta Controllo dell'accesso tramite tag nella Guida per l'utente IAM.

Associazione di interfacce virtuali Direct Connect in base ai tag

L'esempio seguente mostra come è possibile creare una policy che consente di associare un'interfaccia virtuale solo se il tag contiene la chiave di ambiente e i valori di preproduzione o di produzione.

```
    {
   "Version": "2012-10-17",
   "Statement": [
     {
       "Effect": "Allow",
       "Action": [
         "directconnect:AssociateVirtualInterface"
       ],
       "Resource": "arn:aws:directconnect:*:*:dxvif/*",
       "Condition": {
         "StringEquals": {
           "aws:ResourceTag/environment": [
             "preprod",
             "production"
           ]
         }
       }
     },
     {
       "Effect": "Allow",
       "Action": "directconnect:DescribeVirtualInterfaces",
       "Resource": "*"
     }
   ]
}
```

Controllo dell'accesso alle richieste in base ai tag

Puoi utilizzare le condizioni nelle policy IAM per controllare quali coppie chiave-valore di tag possono essere trasferite in una richiesta che applica tag a una risorsa AWS. L'esempio seguente mostra come è possibile creare una politica che consenta di utilizzare l'AWS Direct Connect TagResource azione per allegare tag a un'interfaccia virtuale solo se il tag contiene la chiave di ambiente e i valori di preproduzione o di produzione. Come best practice, utilizza il modificatore `ForAllValues` con la chiave di condizione `aws:TagKeys` per indicare che nella richiesta è ammesso solo l'ambiente della chiave.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "directconnect:TagResource",
        "Resource": "arn:aws:directconnect:*:*:dxvif/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/environment": [
                    "preprod",
                    "production"
                ]
            },
            "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
        }
    }
}
```

Controllo delle chiavi di tag

Puoi utilizzare una condizione nelle policy IAM per controllare se specifiche chiavi di tag possono essere utilizzate su una risorsa o in una richiesta.

L'esempio seguente mostra come è possibile creare una policy che consente di applicare i tag alle risorse, ma solo con l'ambiente della chiave del tag

```
 {
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "directconnect:TagResource",
```

```
        "Resource": "*",
        "Condition": {
          "ForAllValues:StringEquals": {
            "aws:TagKeys": [
              "environment"
            ]
          }
        }
      }
    }
```

Ruoli collegati ai servizi per AWS Direct Connect

AWS Direct Connect utilizza ruoli collegati al servizio AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a AWS Direct Connect. I ruoli collegati ai servizi sono definiti automaticamente da AWS Direct Connect e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di AWS Direct Connect perché non dovrai più aggiungere manualmente le autorizzazioni necessarie. AWS Direct Connect definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, AWS Direct Connect potrà assumere solo i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di AWS Direct Connect perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consultare Servizi AWS che funzionano con IAM e cercare i servizi che riportano Sì nella colonna Ruolo collegato ai servizi. Scegli Yes (Sì) in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per AWS Direct Connect

AWS Direct Connect usa il ruolo collegato ai servizi denominato `AWSServiceRoleForDirectConnect`. Ciò consente a AWS Direct Connect di recuperare per tuo conto i segreti MACsec archiviati in AWS Secrets Manager.

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForDirectConnect` considera attendibili i seguenti servizi:

- `directconnect.amazonaws.com`

Il ruolo collegato ai servizi `AWSServiceRoleForDirectConnect` utilizza la policy gestita `AWSDirectConnectServiceRolePolicy`.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per consentire la corretta creazione del ruolo collegato ai servizi `AWSServiceRoleForDirectConnect`, l'identità IAM con la quale utilizzi AWS Direct Connect deve disporre delle autorizzazioni richieste. Per concedere le autorizzazioni richieste, collega la seguente policy all'identità IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "directconnect.amazonaws.com"
                }
            },
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:GetRole",
            "Effect": "Allow",
            "Resource": "*"
       }
    ]
}
```

Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per AWS Direct Connect

Non hai bisogno di creare manualmente un ruolo collegato al servizio. AWS Direct Connect crea il ruolo collegato al servizio appropriato per te. Quando esegui il comando `associate-mac-sec-key`, AWS crea un ruolo collegato al servizio che consente a AWS Direct Connect di recuperare i segreti

MACsec archiviati per tuo conto nell'AWS Secrets Manager nella AWS Management Console, nella AWS CLI o nell'API AWS.

> **Important**
>
> Questo ruolo collegato ai servizi può apparire nell'account se è stata completata un'operazione in un altro servizio che utilizza le funzionalità supportate dal ruolo. Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato ai servizi e devi poi ricrearlo nuovamente, puoi utilizzare lo stesso processo per ricreare il ruolo nel tuo account. AWS Direct Connect crea nuovamente per tuo conto il ruolo collegato al servizio.

Puoi utilizzare la console IAM anche per creare un ruolo collegato ai servizi con il caso d'uso AWS Direct Connect. In AWS CLI o in AWS API, crea un ruolo collegato ai servizi con il nome di servizio `directconnect.amazonaws.com`. Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per AWS Direct Connect

AWS Direct Connect non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForDirectConnect`. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS Direct Connect

Non è necessario eliminare manualmente il ruolo `AWSServiceRoleForDirectConnect`. Quando si elimina il ruolo collegato al servizio, è necessario eliminare tutte le risorse associate archiviate nel servizio Web AWS Secrets Manager. La AWS Management Console, la AWS CLI, o l'API di AWS, AWS Direct Connect pulisce le risorse ed elimina il ruolo collegato ai servizi per tuo conto.

Puoi utilizzare la console IAM per eliminare un ruolo collegato ai servizi. Per farlo, dovrai prima pulire manualmente le risorse associate al ruolo collegato ai servizi e poi eliminarlo manualmente.

> **Note**
>
> Se il servizio AWS Direct Connect utilizza tale ruolo quando tenti di eliminare le risorse, è possibile che l'eliminazione non abbia esito positivo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse di AWS Direct Connect utilizzate da **`AWSServiceRoleForDirectConnect`**

1. Rimuovi l'associazione tra tutte le chiavi e le connessioni MACsec. Per ulteriori informazioni, consulta the section called “Rimozione dell'associazione tra una chiave segreta MACsec e una connessione”
2. Rimuovi l'associazione tra tutte le chiavi MACsec e i LAG. Per ulteriori informazioni, consulta the section called “Rimozione dell'associazione tra una chiave segreta MACsec e un LAG”

Per eliminare manualmente il ruolo collegato ai servizi utilizzando IAM

Utilizza la console IAM, la AWS CLI o l'API AWS per eliminare il ruolo collegato ai servizi `AWSServiceRoleForDirectConnect`. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi AWS Direct Connect

AWS Direct Connect supporta l'utilizzo di ruoli collegati ai servizi in tutte le Regioni AWS in cui è disponibile la funzionalità MAC Security. Per maggiori informazioni, consulta Sedi AWS Direct Connect.

Policy gestite da AWS per AWS Direct Connect

Una policy gestita da AWSè una policy autonoma creata e amministrata da AWS. Le policy gestite da AWSsono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Ricorda che le policy gestite da AWSpotrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWSaggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWSaggiorni una policy gestita da AWSquando viene lanciato un nuovo Servizio AWSo nuove operazioni API diventano disponibili per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWSpolitica gestita: AWSDirectConnectFullAccess

È possibile allegare la policy `AWSDirectConnectFullAccess`alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso completo ad AWS Direct Connect.

Per visualizzare le autorizzazioni per questa policy, consulta AWSDirectConnectFullAccess nella AWS Management Console.

AWSpolitica gestita: AWSDirectConnectReadOnlyAccess

È possibile allegare la policy `AWSDirectConnectReadOnlyAccess`alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso in sola lettura ad AWS Direct Connect.

Per visualizzare le autorizzazioni per questa policy, consulta AWSDirectConnectReadOnlyAccess nella AWS Management Console.

AWSpolitica gestita: AWSDirectConnectServiceRolePolicy

Questa policy è allegata al ruolo collegato al servizio denominato AWSServiceRoleForDirectConnectper consentire di AWS Direct Connect recuperare i segreti di sicurezza MAC per tuo conto. Per ulteriori informazioni, consulta the section called “Ruoli collegati ai servizi”.

Per visualizzare le autorizzazioni per questa policy, consulta AWSDirectConnectServiceRolePolicy nella AWS Management Console.

Aggiornamenti di AWS Direct Connectalle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWSper AWS Direct Connectda quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti di AWS Direct Connect.

Modifica	Descrizione	Data
AWSDirectConnectServiceRolePolicy: nuova policy	Per supportare MAC Security, è stato aggiunto il ruolo collegato al AWSServiceRoleForDirectConnectservizio.	31 marzo 2021
AWS Direct Connect ha iniziato il rilevamento delle modifiche	AWS Direct Connect ha iniziato a monitorare le modifiche per le sue policy gestite da AWS.	31 marzo 2021

Risoluzione dei problemi relativi all'identità e all'accesso di Direct Connect

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Direct Connect e IAM.

Argomenti

- Non sono autorizzato a eseguire un'operazione in Direct Connect
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire alle persone esterne al mio account Account AWS di accedere alle mie risorse Direct Connect

Non sono autorizzato a eseguire un'operazione in Direct Connect

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `directconnect:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 directconnect:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `directconnect:`*`GetWidget`*.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se si riceve un errore che indica che non si dispone dell'autorizzazione a eseguire l'operazione `iam:PassRole`, per passare un ruolo a Direct Connect è necessario aggiornare le policy.

Alcuni Servizi AWSconsentono di trasmettere un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` prova a utilizzare la console per eseguire un'operazione in Direct Connect. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire alle persone esterne al mio account Account AWS di accedere alle mie risorse Direct Connect

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se Direct Connect supporta queste funzionalità, consulta Funzionamento di Direct Connect con IAM.

- Per informazioni su come garantire l'accesso alle risorse negli Account AWSche possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta Fornire l'accesso agli Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Registrazione e monitoraggio in AWS Direct Connect

Per controllare AWS Direct Connect e segnalare l'eventuale presenza di problemi, puoi usare gli strumenti di monitoraggio automatici seguenti:

- Allarmi di Amazon CloudWatch: osserva un singolo parametro per il periodo di tempo specificato. Gli allarmi eseguono una o più operazioni basate sul valore del parametro relativo a una soglia prestabilita per un certo numero di periodi. L'operazione corrisponde all'invio di una notifica a un argomento Amazon SNS. Gli allarmi CloudWatch non richiamano operazioni semplicemente perché sono in un determinato stato. È necessario che lo stato sia cambiato e che sia rimasto invariato per una serie specificata di periodi. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.
- Monitoraggio dei log di AWS CloudTrail: puoi condividere file di log tra gli account e monitorare i file di log CloudTrail in tempo reale inviandoli a CloudWatch Logs. Inoltre, puoi scrivere applicazioni per l'elaborazione di log in Java e verificare che i file di log non siano cambiati dopo la consegna effettuata da CloudTrail. Per ulteriori informazioni, consulta Registrazione di chiamate API AWS Direct Connect con AWS CloudTrail e anche Utilizzo dei file di log di CloudTrail nella Guida per l'utente di AWS CloudTrail.

Per ulteriori informazioni, consulta Monitoraggio.

Convalida della conformità per AWS Direct Connect

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.

- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in AWS Direct Connect

L'infrastruttura globale di AWS è basata su Regioni e zone di disponibilità AWS. AWS Le Regioni forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le zone di disponibilità, è possibile progettare e gestire le applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle Regioni AWS e sulle zone di disponibilit, consulta Infrastruttura globale di AWS.

Oltre all'infrastruttura globale di AWS, AWS Direct Connect offre numerose funzionalità per supportare la resilienza dei dati e le esigenze di backup.

Per informazioni su come utilizzare VPN con AWS Direct Connect, consulta AWS VPN Direct Connect Plus.

Failover

L'AWS Direct Connect Resiliency Toolkit fornisce una procedura guidata di connessione con più modelli di resilienza che consente di ordinare le connessioni dedicate per ottenere l'obiettivo dello SLA. Puoi selezionare un modello di resilienza, quindi l'AWS Direct Connect Resiliency Toolkit ti guiderà attraverso il processo di ordinamento della connessione dedicata. I modelli di resilienza sono progettati per garantire il numero appropriato di connessioni dedicate in più posizioni.

- Resilienza massima: è possibile ottenere la massima resilienza per carichi di lavoro critici utilizzando connessioni separate che terminano su dispositivi separati in più di una posizione. Questo modello fornisce resilienza contro i guasti del dispositivo, della connettività e della posizione completa.
- Elevata resilienza: è possibile ottenere un'elevata resilienza per carichi di lavoro critici utilizzando due connessioni singole a più posizioni. Questo modello fornisce resilienza agli errori di connettività causati da un taglio di fibra o da un guasto del dispositivo. Inoltre, aiuta a prevenire un errore di percorso completo.
- Sviluppo e test: è possibile ottenere la resilienza di sviluppo e test per carichi di lavoro non critici utilizzando connessioni separate che terminano su dispositivi separati in un'unica posizione. Questo modello fornisce resilienza ai guasti del dispositivo, ma non fornisce resilienza ai guasti della posizione.

Per ulteriori informazioni, consulta Utilizzo del AWS Direct Connect Resiliency Toolkit per iniziare.

Sicurezza dell'infrastruttura in AWS Direct Connect

Come servizio gestito, AWS Direct Connect è protetto dalle procedure di sicurezza della rete globale AWS. Utilizza le chiamate API pubblicate di AWS per accedere a AWS Direct Connect tramite la rete. I client devono supportare Transport Layer Security (TLS) 1.2 o versioni successive. È consigliabile TLS 1.3. I client devono, inoltre, supportare le suite di cifratura con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Puoi chiamare queste operazioni API da qualsiasi posizione di rete, ma AWS Direct Connect supporta le policy di accesso basate sulle risorse, che possono includere limitazioni in base all'indirizzo IP di origine. È inoltre possibile utilizzare le policy di AWS Direct Connect per controllare l'accesso da endpoint Amazon Virtual Private Cloud (Amazon VPC) o VPC specifici. Di fatto, questo isola l'accesso di rete a una risorsa AWS Direct Connect specificata solo dal VPC specifico all'interno della rete AWS. Per un esempio, consulta the section called “Esempi di policy basate su identità”.

Sicurezza Border Gateway Protocol (BGP)

Internet si affida in gran parte al BGP per il routing delle informazioni tra i sistemi di rete. Il routing BGP a volte può essere suscettibile ad attacchi malevoli o al dirottamento del protocollo BGP. Per capire come AWS lavora per proteggere in modo più sicuro la rete dagli attacchi BGP, consulta Come AWS contribuisce a proteggere il routing su Internet.

Utilizzo di AWS CLI

Puoi utilizzare AWS CLI per creare e utilizzare risorse AWS Direct Connect.

Nell'esempio seguente vengono utilizzati i comandi della AWS CLI per creare una connessione AWS Direct Connect. È anche possibile scaricare la Letter of Authorization and Connecting Facility Assignment (LOA-CFA) o effettuare il provisioning di un'interfaccia virtuale privata o pubblica.

Prima di iniziare, assicurati di avere installato e configurato la AWS CLI. Per ulteriori informazioni, consulta la Guida per l'utente di AWS Command Line Interface.

Indice

Fase 1: creazione di una connessione

Il primo passo è quello di inviare una richiesta di connessione. Assicurati di conoscere la velocità della porta richiesta e la località AWS Direct Connect. Per ulteriori informazioni, consulta AWS Direct Connect connessioni.

Per creare una richiesta di connessione

1. Descrivere le sedi AWS Direct Connect per la regione corrente. Prendere nota del codice della località in cui si desidera stabilire la connessione, riportato nell'output restituito.

```
aws directconnect describe-locations
```

```
{
    "locations": [
        {
            "locationName": "City 1, United States",
            "locationCode": "Example Location 1"
        },
        {
            "locationName": "City 2, United States",
            "locationCode": "Example location"
```

```
        }
    ]
}
```

2. Creare la connessione e specificare un nome, la velocità della porta e il codice della località. Prendere nota dell'ID di connessione riportato nell'output restituito; sarà necessario per ottenere la LOA-CFA nella fase successiva.

```
aws directconnect create-connection --location Example location --bandwidth 1Gbps
 --connection-name "Connection to AWS"
```

```
{
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-EXAMPLE",
    "connectionState": "requested",
    "bandwidth": "1Gbps",
    "location": "Example location",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

Fase 2: download della LOA-CFA

Dopo avere richiesto una connessione, è possibile ottenere la LOA-CFA utilizzando il comando `describe-loa`. L'output è con codifica base64. Bisogna estrarre i contenuti LOA rilevanti, decodificarli e creare un file PDF.

Per ottenere la LOA-CFA utilizzando Linux o macOS

In questo esempio, la parte finale del comando decodifica i contenuti utilizzando l'utility base64 e invia l'output in un file PDF.

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

Per ottenere la LOA-CFA utilizzando Windows

In questo esempio, l'output viene estratto in un file denominato myLoaCfa.base64. Il secondo comando utilizza l'utility `certutil` per decodificare il file e inviare l'output in un file PDF.

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

Dopo avere scaricato la LOA-CFA, inviarla al provider di rete o di co-location.

Fase 3: creazione di un'interfaccia virtuale e acquisizione della configurazione del router

Dopo aver effettuato un ordine per una connessione AWS Direct Connect, è necessario creare un'interfaccia virtuale per iniziare a usarla. È possibile creare un'interfaccia virtuale privata per connettersi al tuo VPC. In alternativa, puoi creare un'interfaccia virtuale pubblica per connetterti ai servizi AWS che non sono in un VPC. Si può creare un'interfaccia virtuale che supporti il traffico IPv4 o IPv6.

Prima di iniziare, è necessario leggere i prerequisiti in Prerequisiti per le interfacce virtuali.

Quando si crea un'interfaccia virtuale utilizzando la AWS CLI, l'output include le informazioni di configurazione generali del router. Per creare una configurazione del router specifica per il dispositivo, utilizza la console AWS Direct Connect. Per ulteriori informazioni, consulta Download del file di configurazione del router.

Per creare un'interfaccia virtuale privata

1. Scaricare l'ID del gateway virtuale privato (vgw-xxxxxxxx) collegato al VPC. L'ID sarà necessario per creare l'interfaccia virtuale nella fase successiva.

   ```
   aws ec2 describe-vpn-gateways
   ```

   ```
   {
       "VpnGateways": [
           {
               "State": "available",
               "Tags": [
                   {
                       "Value": "DX_VGW",
                       "Key": "Name"
   ```

```
                }
            ],
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-ebaa27db",
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-24f33d4d"
                }
            ]
        }
    ]
}
```

2. Creare un'interfaccia virtuale privata. È necessario specificare un nome, un ID VLAN e un Autonomous System Number (ASN) BGP.

   Per il traffico IPv4, bisogna disporre di un indirizzo IPv4 privato per ogni termine della sessione di peering BGP. È possibile specificare i propri indirizzi IPv4 oppure lasciare che vengano generati da Amazon. Nell'esempio seguente, gli indirizzi IPv4 vengono generati da Amazon.

```
aws directconnect create-private-virtual-interface --
connection-id dxcon-fg31dyv6 --new-private-virtual-interface
 virtualInterfaceName=PrivateVirtualInterface,vlan=101,asn=65000,virtualGatewayId=vgw-
ebaa27db,addressFamily=ipv4
```

```
{
    "virtualInterfaceState": "pending",
    "asn": 65000,
    "vlan": 101,
    "customerAddress": "192.168.1.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "vgw-ebaa27db",
    "virtualInterfaceId": "dxvif-ffhhk74f",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
```

```
            "customerAddress": "192.168.1.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "pending",
            "amazonAddress": "192.168.1.1/30",
            "asn": 65000
        }
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-ffhhk74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>private</connection_type>\n</
logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "PrivateVirtualInterface"
}
```

Per creare un'interfaccia virtuale privata che supporti il traffico IPv6, bisogna utilizzare lo stesso comando riportato sopra e specificare `ipv6` per il parametro `addressFamily`. Non è possibile specificare i propri indirizzi IPv6 per la sessione di peering BGP, in quanto vengono assegnati da Amazon.

3. Per visualizzare le informazioni di configurazione del router in formato XML, descrivere l'interfaccia virtuale creata. Utilizzare il parametro `--query` per estrarre le informazioni `customerRouterConfig` e il parametro `--output` per organizzare il testo in righe delimitate da tabulazione.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-ffhhk74f
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhhk74f">
  <vlan>101</vlan>
  <customer_address>192.168.1.2/30</customer_address>
  <amazon_address>192.168.1.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>private</connection_type>
```

```
</logical_connection>
```

Per creare un'interfaccia virtuale pubblica

1. Per creare un'interfaccia virtuale pubblica, è necessario specificare un nome, un ID VLAN e un Autonomous System Number (ASN) BGP.

   Per il traffico IPv4, bisogna specificare anche un indirizzo IPv4 pubblico per ogni termine della sessione di peering BGP e gli instradamenti IPv4 pubblici che saranno pubblicizzati tramite BGP. Nell'esempio seguente viene creata un'interfaccia virtuale pubblica per il traffico IPv4.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/
{cidr=203.0.113.4/30}]
```

```
{
    "virtualInterfaceState": "verifying",
    "asn": 65000,
    "vlan": 2000,
    "customerAddress": "203.0.113.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "",
    "virtualInterfaceId": "dxvif-fgh0hcrk",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [
        {
            "cidr": "203.0.113.0/30"
        },
        {
            "cidr": "203.0.113.4/30"
        }
    ],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "203.0.113.2/30",
            "addressFamily": "ipv4",
```

```
            "authKey": "asdf34example",
            "bgpPeerState": "verifying",
            "amazonAddress": "203.0.113.1/30",
            "asn": 65000
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>public</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

Per creare un'interfaccia virtuale pubblica che supporti il traffico IPv6, è possibile specificare gli instradamenti IPv6 che saranno pubblicizzati tramite BGP. Non è possibile specificare gli indirizzi IPv6 per la sessione di peering, in quanto vengono assegnati da Amazon. Nell'esempio seguente viene creata un'interfaccia virtuale pubblica per il traffico IPv6.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,addressFamily=ipv6,routeFi
{cidr=2001:db8:64ce:ba01::/64}]
```

2. Per visualizzare le informazioni di configurazione del router in formato XML, descrivere l'interfaccia virtuale creata. Utilizzare il parametro `--query` per estrarre le informazioni `customerRouterConfig` e il parametro `--output` per organizzare il testo in righe delimitate da tabulazione.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-fgh0hcrk
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-fgh0hcrk">
  <vlan>2000</vlan>
  <customer_address>203.0.113.2/30</customer_address>
```

```
  <amazon_address>203.0.113.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>public</connection_type>
</logical_connection>
```

Registrazione di chiamate API AWS Direct Connect con AWS CloudTrail

AWS Direct Connect è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un servizio AWS in AWS Direct Connect. CloudTrail acquisisce tutte le chiamate API AWS Direct Connect come eventi. Le chiamate acquisite includono le chiamate dalla console di AWS Direct Connect e le chiamate di codice alle operazioni delle API AWS Direct Connect. Se si crea un trail, è possibile abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per AWS Direct Connect. Se non si configura un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata ad AWS Direct Connect, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni, consulta la Guida per l'utente di AWS CloudTrail.

Informazioni su AWS Direct Connect in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività in AWS Direct Connect, tale attività viene registrata in un evento CloudTrail insieme ad altri eventi di servizio AWS nella Cronologia eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi nella cronologia degli eventi di CloudTrail.

Per una registrazione continua degli eventi nell'account AWS che includa gli eventi per AWS Direct Connect, creare un trail. Un percorso abilita la distribuzione da parte di CloudTrail dei file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più regioni e Ricezione di file di log CloudTrail da più account

Tutte le operazioni AWS Direct Connect vengono registrate da CloudTrail e sono documentate nella documentazione di riferimento delle API di AWS Direct Connect. Ad esempio, le chiamate alle operazioni `CreateConnection` e `CreatePrivateVirtualInterface` generano voci nei file di log di CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (utente IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta l'elemento CloudTrail `userIdentity`.

Comprensione delle voci dei file di log di AWS Direct Connect

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, sulla data e sull'ora dell'operazione, sui parametri richiesti e così via. I file di log CloudTrail non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

Di seguito sono elencati alcuni esempi di record di log CloudTrail per AWS Direct Connect.

Example Esempio: CreateConnection

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
```

```
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:28:16Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "location": "EqSE2",
            "connectionName": "MyExampleConnection",
            "bandwidth": "1Gbps"
        },
        "responseElements": {
            "location": "EqSE2",
            "region": "us-west-2",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-fhajolyy",
            "connectionName": "MyExampleConnection"
        }
    },
    ...
  ]
}
```

Example Esempio: CreatePrivateVirtualInterface

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
```

```
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
                "customerAddress": "[PROTECTED]",
                "authKey": "[PROTECTED]",
                "asn": -1,
                "virtualGatewayId": "vgw-bb09d4a5",
                "amazonAddress": "[PROTECTED]",
                "vlan": 123
            }
        },
        "responseElements": {
            "virtualInterfaceId": "dxvif-fgq61m6w",
            "authKey": "[PROTECTED]",
            "virtualGatewayId": "vgw-bb09d4a5",
            "customerRouterConfig": "[PROTECTED]",
            "virtualInterfaceType": "private",
            "asn": -1,
            "routeFilterPrefixes": [],
            "virtualInterfaceName": "MyVirtualInterface",
            "virtualInterfaceState": "pending",
            "customerAddress": "[PROTECTED]",
            "vlan": 123,
            "ownerAccount": "123456789012",
            "amazonAddress": "[PROTECTED]",
            "connectionId": "dxcon-fhajolyy",
            "location": "EqSE2"
```

```
        }
    },
    ...
  ]
}
```

Example Esempio: DescribeConnections

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:27:28Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeConnections",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": null,
        "responseElements": null
    },
    ...
  ]
}
```

Example Esempio: DescribeVirtualInterfaces

```
{
    "Records": [
```

```
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:37:53Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeVirtualInterfaces",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy"
        },
        "responseElements": null
    },
    ...
  ]
}
```

Monitoraggio AWS Direct Connect delle risorse

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle risorse Direct Connect. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica uno. Prima di iniziare a monitorare Direct Connect, tuttavia, è necessario creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Quali risorse devono essere monitorate?
- Con quale frequenza devi eseguire il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio puoi utilizzare?
- Chi esegue le attività di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

Il passaggio successivo consiste nello stabilire una linea di base per le normali prestazioni di Direct Connect nell'ambiente in uso, misurando le prestazioni in diversi momenti e in diverse condizioni di carico. Durante il monitoraggio di Direct Connect, memorizza i dati di monitoraggio storici. In questo modo, puoi confrontare i dati con i dati sulle prestazioni correnti, identificare i normali modelli di prestazioni e le anomalie e ideare metodi per risolvere i problemi.

Per stabilire una linea di base, è necessario monitorare l'utilizzo, lo stato e lo stato delle connessioni fisiche Direct Connect.

Indice

Strumenti di monitoraggio

AWS fornisce vari strumenti che è possibile utilizzare per monitorare una AWS Direct Connect connessione. Alcuni di questi strumenti possono essere configurati in modo che eseguano automaticamente il monitoraggio, mentre altri richiedono l'intervento manuale. Si consiglia di automatizzare il più possibile i processi di monitoraggio.

Strumenti di monitoraggio automatici

Puoi utilizzare i seguenti strumenti di monitoraggio automatizzato per guardare Direct Connect e segnalare quando qualcosa non va:

- Amazon CloudWatch Alarms: monitora una singola metrica in un periodo di tempo specificato. Gli allarmi eseguono una o più operazioni basate sul valore del parametro relativo a una soglia prestabilita per un certo numero di periodi. L'azione è una notifica inviata a un argomento di Amazon SNS. CloudWatch gli allarmi non richiamano azioni semplicemente perché si trovano in uno stato particolare; lo stato deve essere cambiato e mantenuto per un determinato numero di periodi. Per informazioni sui parametri e sulle dimensioni disponibili, consulta Monitoraggio con Amazon CloudWatch.
- AWS CloudTrail Monitoraggio dei registri: condividi i file di registro tra account e monitora i file di CloudTrail registro in tempo reale inviandoli a CloudWatch Logs. È anche possibile scrivere applicazioni per l'elaborazione di log in Java e verificare che i file di log non siano cambiati dopo la consegna effettuata da CloudTrail. Per ulteriori informazioni, consulta Registrazione di chiamate API AWS Direct Connect con AWS CloudTrail la sezione Lavorare con i file di CloudTrail registro nella Guida per l'AWS CloudTrail utente.

Strumenti di monitoraggio manuali

Un'altra parte importante del monitoraggio di una AWS Direct Connect connessione consiste nel monitorare manualmente gli elementi che gli CloudWatch allarmi non coprono. I dashboard di Direct Connect e della CloudWatch console forniscono una at-a-glance visione dello stato dell' AWS ambiente.

- La AWS Direct Connect console mostra:
  - Stato connessione (vedi la colonna State (Stato))
  - Stato dell'interfaccia virtuale (vedi la colonna State (Stato))
- La CloudWatch home page mostra:
  - Stato e allarmi attuali
  - Grafici degli allarmi e delle risorse
  - Stato di integrità dei servizi

  Inoltre, è possibile utilizzare CloudWatch per effettuare le seguenti operazioni:
  - Creare pannelli di controllo personalizzati per monitorare i servizi di interesse.

- Creare grafici dei dati dei parametri per la risoluzione di problemi e il rilevamento di tendenze.
- Cerca e sfoglia tutte le metriche AWS delle tue risorse.
- Crea e modifica gli allarmi per ricevere le notifiche dei problemi.

Monitoraggio con Amazon CloudWatch

Puoi monitorare AWS Direct Connect le connessioni fisiche e le interfacce virtuali utilizzando CloudWatch. CloudWatch raccoglie dati grezzi da Direct Connect e li elabora in metriche leggibili. Per impostazione predefinita, CloudWatch fornisce i dati metrici Direct Connect a intervalli di 5 minuti.

Per informazioni dettagliate su CloudWatch, consulta la Amazon CloudWatch User Guide. Puoi anche monitorare i tuoi servizi CloudWatch per vedere quali risorse stanno utilizzando. Per ulteriori informazioni, consulta AWS Servizi che pubblicano CloudWatch metriche.

Indice

AWS Direct Connect metriche e dimensioni

Le metriche sono disponibili per le connessioni AWS Direct Connect fisiche e le interfacce virtuali.

AWS Direct Connect Metriche di connessione

Le seguenti metriche sono disponibili nelle connessioni dedicate Direct Connect.

Parametro	Descrizione
`ConnectionState`	Lo stato della connessione.1 indica up e 0 indica down. Questo parametro è disponibile per connessioni dedicate e ospitate.

Parametro	Descrizione
	Note Questa metrica è disponibile anche negli account dei proprietari delle interfacce virtuali ospitate oltre agli account dei proprietari della connessione. Unità: booleane
`ConnectionBpsEgress`	Il bitrate per i dati in uscita dal AWS lato della connessione. Il numero indicato è il valore aggregato (media) su un periodo di tempo specificato (il valore predefinito è 5 minuti e il valore minimo è 1 minuto). Puoi modificare l'aggregazione predefinita. Questo parametro potrebbe non essere disponibile per una nuova connessione o al riavvio di un dispositivo. Il parametro inizia quando la connessione viene utilizzata per inviare o ricevere traffico. Unità: bit al secondo
`ConnectionBpsIngress`	Il bitrate per i dati in entrata AWS sul lato della connessione. Questo parametro potrebbe non essere disponibile per una nuova connessione o al riavvio di un dispositivo. Il parametro inizia quando la connessione viene utilizzata per inviare o ricevere traffico. Unità: bit al secondo

Parametro	Descrizione
`ConnectionPpsEgress`	La velocità dei pacchetti per i dati in uscita dal AWS lato della connessione. Il numero indicato è il valore aggregato (media) su un periodo di tempo specificato (il valore predefinito è 5 minuti e il valore minimo è 1 minuto). Puoi modificare l'aggregazione predefinita. Questo parametro potrebbe non essere disponibile per una nuova connessione o al riavvio di un dispositivo. Il parametro inizia quando la connessione viene utilizzata per inviare o ricevere traffico. Unità: pacchetti al secondo
`ConnectionPpsIngress`	La velocità dei pacchetti per i dati in ingresso AWS sul lato della connessione. Il numero indicato è il valore aggregato (media) su un periodo di tempo specificato (il valore predefinito è 5 minuti e il valore minimo è 1 minuto). Puoi modificare l'aggregazione predefinita. Questo parametro potrebbe non essere disponibile per una nuova connessione o al riavvio di un dispositivo. Il parametro inizia quando la connessione viene utilizzata per inviare o ricevere traffico. Unità: pacchetti al secondo
`ConnectionCRCErrorCount`	Questo conteggio non è più in uso. Usare invece `ConnectionErrorCount` .

Parametro	Descrizione
`ConnectionErrorCount`	Il numero totale di errori per tutti i tipi di errori a livello MAC sul dispositivo AWS . Il totale include errori CRC (Cyclic Ridondancy Check). Questa metrica rappresenta il conteggio degli errori verificatisi dall'ultimo datapoint segnalato. In caso di errori sull'interfaccia, la metrica riporta valori diversi da zero. Per ottenere il conteggio totale di tutti gli errori per l'intervallo selezionato in CloudWatch, ad esempio, 5 minuti, applica la statistica «sum». Per ulteriori informazioni su come ottenere la statistica della somma, consulta Getting Statistics for a Metric nella Amazon CloudWatch User Guide. Il valore della metrica viene impostato su 0 quando gli errori sull'interfaccia si interrompono. **Note** Questa metrica sostituisce `ConnectionCRCErrorCount` , che non è più in uso. Unità: numero
`ConnectionLightLevelTx`	Indica lo stato della connessione in fibra per il traffico in uscita (in uscita) dal AWS lato della connessione. Ci sono due dimensioni per questo parametro. Per ulteriori informazioni, consulta the section called “AWS Direct Connect dimensioni disponibili”. Unità: dBm

Parametro	Descrizione
`ConnectionLightLevelRx`	Indica lo stato della connessione in fibra per il traffico in entrata (in ingresso) verso il AWS lato della connessione. Ci sono due dimensioni per questo parametro. Per ulteriori informazioni, consulta the section called “AWS Direct Connect dimensioni disponibili”. Unità: dBm
`ConnectionEncryptionState`	Indica lo stato di crittografia della connessione. 1 indica che la crittografia della connessione è up, mentre 0 indica che la crittografia della connessio ne è down. Quando questa metrica viene applicata a un LAG, 1 indica che tutte le connessioni nel LAG presentano una crittografia up. 0 indica che almeno una connessione LAG presenta una crittografia down.

AWS Direct Connect metriche dell'interfaccia virtuale

Le seguenti metriche sono disponibili nelle interfacce AWS Direct Connect virtuali.

Parametro	Descrizione
`VirtualInterfaceBpsEgress`	Il bitrate per i dati in uscita dal AWS lato dell'inte rfaccia virtuale. Il numero indicato è il valore aggregato su un periodo di tempo specificato (il valore predefinito è 5 minuti). Unità: bit al secondo
`VirtualInterfaceBpsIngress`	Il bitrate per i dati in entrata AWS sul lato dell'inte rfaccia virtuale.

Parametro	Descrizione
	Il numero indicato è il valore aggregato su un periodo di tempo specificato (il valore predefinito è 5 minuti). Unità: bit al secondo
`VirtualInterfacePpsEgress`	La velocità dei pacchetti per i dati in uscita dal AWS lato dell'interfaccia virtuale. Il numero indicato è il valore aggregato su un periodo di tempo specificato (il valore predefinito è 5 minuti). Unità: pacchetti al secondo
`VirtualInterfacePpsIngress`	La velocità dei pacchetti per i dati in ingresso AWS sul lato dell'interfaccia virtuale. Il numero indicato è il valore aggregato su un periodo di tempo specificato (il valore predefinito è 5 minuti). Unità: pacchetti al secondo

AWS Direct Connect dimensioni disponibili

È possibile filtrare i AWS Direct Connect dati utilizzando le seguenti dimensioni.

Dimensione	Descrizione
`ConnectionId`	Questa dimensione è disponibile nelle metriche per la connessione Direct Connect e l'interfaccia virtuale. Questa dimensione filtra i dati per connessione.
`OpticalLaneNumber`	Questa dimensione filtra i `ConnectionLightLevelTx` dati e i `ConnectionLightLevelRx` dati e filtra i dati in base al numero della corsia ottica della connessione Direct Connect.

Dimensione	Descrizione
`VirtualInterfaceId`	Questa dimensione è disponibile nelle metriche per l'interfaccia virtuale Direct Connect e filtra i dati in base all'interfaccia virtuale.

Visualizzazione delle metriche AWS Direct Connect CloudWatch

AWS Direct Connect invia le seguenti metriche sulle connessioni Direct Connect. Amazon aggrega CloudWatch quindi questi punti dati a intervalli di 1 minuto o 5 minuti. Per impostazione predefinita, i dati metrici di Direct Connect vengono scritti a CloudWatch intervalli di 5 minuti.

> **Note**
>
> Se imposti un intervallo di 1 minuto, Direct Connect farà del suo meglio per scrivere le metriche per CloudWatch utilizzare questo intervallo, ma non sempre è possibile garantirlo.

È possibile utilizzare le seguenti procedure per visualizzare le metriche per le connessioni Direct Connect.

Per visualizzare le metriche utilizzando la console CloudWatch

I parametri vengono raggruppati prima in base allo spazio dei nomi del servizio e successivamente in base alle diverse combinazioni di dimensioni all'interno di ogni spazio dei nomi. Per ulteriori informazioni sull'utilizzo Amazon CloudWatch per visualizzare i parametri di Direct Connect, inclusa l'aggiunta di funzioni matematiche o query predefinite, consulta Using Amazon CloudWatch metrics in the Amazon User Guide. CloudWatch

1. Apri la console all'indirizzo https://console.aws.amazon.com/cloudwatch/. CloudWatch
2. Nel pannello di navigazione, scegli Parametri quindi scegli Tutti i parametri.
3. Nella sezione Metriche, scegli DX.
4. Scegliete un nome ConnectionIdo una metrica, quindi scegliete una delle seguenti opzioni per definire ulteriormente la metrica:
   - Aggiungi alla ricerca: aggiunge questa metrica ai risultati della ricerca.
   - Cerca solo questo: cerca solo questa metrica.

- Rimuovi dal grafico: rimuove questa metrica dal grafico.
- Includi nel grafico solo questo parametro: rappresenta graficamente solo questo parametro.
- Includi nel grafico tutti i risultati di ricerca: rappresenta graficamente tutti i parametri.
- Grafico con query SQL: apre Informazioni dettagliate sulle metriche - Query Builder, che consente di scegliere ciò che si desidera rappresentare graficamente creando una query SQL. Per ulteriori informazioni sull'utilizzo di Metric Insights, consulta Interroga i tuoi parametri con CloudWatch Metrics Insights nella Amazon CloudWatch User Guide.

Per visualizzare le metriche utilizzando la console AWS Direct Connect

1. Apri la AWS Direct Connectconsole all'indirizzo https://console.aws.amazon.com/directconnect/v2/home.
2. Nel riquadro di navigazione, scegli Connections (Connessioni).
3. Seleziona la connessione.
4. La scheda Monitoraggio visualizza i parametri per la connessione.

Per visualizzare le metriche utilizzando il AWS CLI

Al prompt dei comandi utilizza il comando seguente.

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```

Creazione di CloudWatch allarmi per monitorare le connessioni AWS Direct Connect

Puoi creare un CloudWatch allarme che invia un messaggio Amazon SNS quando l'allarme cambia stato. Un allarme monitora un singolo parametro per un periodo di tempo specificato. Invia una notifica a un argomento Amazon SNS in funzione del valore del parametro rispetto a una soglia prestabilita per un certo numero di periodi.

Ad esempio, puoi creare un allarme per monitorare lo stato della connessione AWS Direct Connect . Si invia una notifica quando lo stato della connessione è down per cinque periodi consecutivi di 1 minuto. Per dettagli su cosa sapere per creare un allarme e per ulteriori informazioni sulla creazione di un allarme, consulta Using Amazon CloudWatch Alarms nella Amazon CloudWatch User Guide.

Per creare un CloudWatch allarme.

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, scegli Alarms (Allarmi), quindi Create alarm (Tutti gli allarmi).
3. Scegli Crea allarme.
4. Scegli Seleziona parametro e quindi DX.
5. Scegli la metrica Parametri connessione.
6. Seleziona la AWS Direct Connect connessione, quindi scegli la metrica Seleziona la metrica.
7. Nella pagina Specifica metriche e condizioni, configura i parametri per l'allarme. Per ulteriori informazioni su metriche e condizioni, consulta Using Amazon CloudWatch Alarms nella Amazon CloudWatch User Guide.
8. Seleziona Avanti.
9. Configura le operazioni di allarme nella pagina Configura azioni. Per ulteriori informazioni sulla configurazione delle azioni di allarme, consulta le azioni di allarme nella Amazon CloudWatch User Guide.
10. Seleziona Avanti.
11. Nella pagina Aggiungi nome e descrizione, inserisci Nome dell'allarme e Descrizione dell'allarme per descrivere l'allarme (facoltativo) e scegli Successivo.
12. Verifica l'allarme proposto nella pagina di Anteprima e creazione.
13. Se necessario, scegli Modifica per modificare qualsiasi informazione, quindi scegli Crea allarme.

    La pagina Allarmi mostra una nuova riga con informazioni sul nuovo avviso. Lo stato Operazioni mostra Operazioni abilitate, a indicare che l'allarme è attivo.

AWS Direct Connect quote

La tabella seguente elenca le quote relative a AWS Direct Connect.

Componente	Quota	Commenti
Interfacce virtuali private o pubbliche per AWS Direct Connect connessione dedicata	50	Questo limite non può essere aumentato.
Interfacce virtuali di transito per AWS Direct Connect connessione dedicata	4	Questo limite non può essere aumentato.
Interfacce virtuali private o pubbliche per connessione AWS Direct Connect dedicata e interfacce virtuali di transito per connessione dedicata AWS Direct Connect	51	Quando è stato lanciato il AWS Direct Connect supporto per Amazon VPC Transit Gateways, è stata aggiunta una quota di una (1) interfaccia virtuale di transito alla quota di 50 interfacce virtuali private o pubbliche per connessione dedicata. Il numero di interfacce virtuali di transito consentite è ora quattro (4) e viene conteggiato per un massimo di 51 interfacce virtuali per connessione dedicata. Questo limite non può essere aumentato.
Interfacce virtuali private, pubbliche o di transito per connessione ospitata AWS Direct Connect	1	Questo limite non può essere aumentato.
AWS Direct Connect Connessioni attive per località Direct Connect per regione per account	10	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Numero di interfacce virtuali per Link Aggregation Group (LAG)	51	Quando è stato lanciato il AWS Direct Connect supporto per Amazon VPC Transit Gateways, è stata aggiunta una quota di una (1) interfaccia virtuale di

Componente	Quota	Commenti
		transito alla quota di 50 interfacce virtuali private o pubbliche per LAG. Il numero di interfacce virtuali di transito consentite è ora quattro (4) e viene conteggiato per un massimo di 51 interfacce virtuali per LAG. Questo limite non può essere aumentato.
Sessione Routes per Border Gateway Protocol (BGP) su un'interfaccia virtuale privata o interfaccia virtuale di transito da locale a. AWS Se si pubblicizzano più di 100 instradamenti per IPv4 E ipV6 durante la sessione BGP, la sessione BGP diventa inattiva con lo stato di inattività DOWN.	100 ciascuno per IPv4 e IPv6	Questo limite non può essere aumentato.
Instradamenti per sessione BGP (Border Gateway Protocol) su un'interfaccia virtuale pubblica	1.000	Questo limite non può essere aumentato.

Componente	Quota	Commenti
Connessioni dedicate per Link Aggregation Group (LAG)	4 quando la velocità della porta è inferiore a 100G 2 quando la velocità della porta è 100G	
Link Aggregation Group (LAG) per regione	10	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
AWS Direct Connect gateway per account	200	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Gateway privati virtuali per gateway AWS Direct Connect	20	Questo limite non può essere aumentato.
Gateway di transito per gateway AWS Direct Connect	6	Questo limite non può essere aumentato.
Interfacce virtuali (private o di transito) per gateway AWS Direct Connect	30	Questo limite non può essere aumentato.

Componente	Quota	Commenti
Numero di prefissi AWS Transit Gateway da AWS a locale su un'interfaccia virtuale di transito	200 in totale per IPv4 e IPv6	Questo limite non può essere aumentato.
Numero di interfacce virtuali per gateway privato virtuale	Nessun limite.	
Numero di gateway Direct Connect associati al gateway di transito.	20	Questo limite non può essere aumentato.
SiteLink limite di prefisso	100	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.

AWS Direct Connect supporta le seguenti velocità di porta su fibra monomodale: 1 Gbps: 1000BASE-LX (1310 nm), 10 Gbps: 10GBASE-LR (1310 nm) e 100 Gbps: 100GBASE-LR4.

Quote BGP

Di seguito sono riportate le quote BGP. I timer BGP negoziano fino al valore più basso tra i router. Gli intervalli BFD sono definiti dal dispositivo più lento.

- Timer di attesa predefinito: 90 secondi
- Timer di attesa minimo: 3 secondi

  Un valore di mantenimento pari a 0 non è supportato.
- Timer keepalive predefinito: 30 secondi
- Timer minimo keepAlive: 1 secondo
- Timer di riavvio regolare: 120 secondi

  Consigliamo di non configurare il riavvio regolare e BFD contemporaneamente.
- Intervallo minimo di rilevamento della vivacità BFD: 300 ms
- Moltiplicatore minimo BFD: 3

Considerazioni sul bilanciamento del carico

Se desideri utilizzare il bilanciamento del carico con più interfacce virtuali pubbliche, tutte le interfacce virtuali devono trovarsi nella stessa regione.

Risoluzione dei problemi AWS Direct Connect

Le informazioni seguenti possono essere utili per risolvere i problemi di connessione ad AWS Direct Connect .

Indice

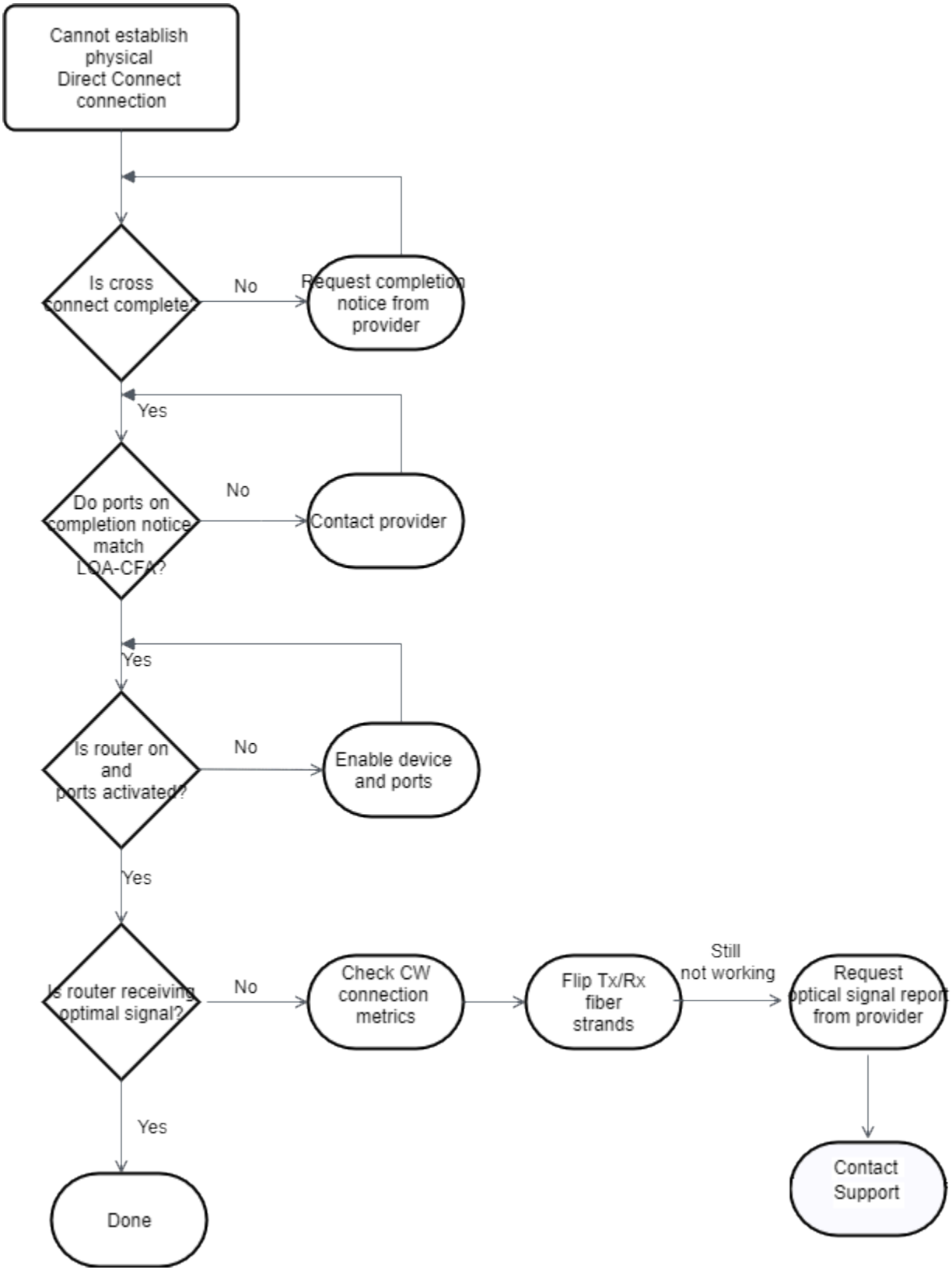
Risoluzione dei problemi di livello 1 (fisico)

Se tu o il tuo provider di rete avete difficoltà a stabilire la connettività fisica a un AWS Direct Connect dispositivo, utilizzate i seguenti passaggi per risolvere il problema.

1. Verifica con il provider di co-location che l'interconnessione sia completa, chiedendo a questi o al provider di rete di fornirti una notifica di completamento dell'interconnessione, quindi confronta le porte con quelle riportate nel tuo documento LOA-CFA.
2. Verifica che il router di proprietà tua o del provider sia acceso e che tutte le porte siano attive.
3. Assicurati che i router utilizzino il ricetrasmettitore ottico corretto. La negoziazione automatica per una porta deve essere disabilitata per una connessione con una velocità di porta superiore a 1 Gbps. Tuttavia, a seconda dell'endpoint AWS Direct Connect che serve la connessione, potrebbe essere necessario abilitare o disabilitare la negoziazione automatica per le connessioni da 1 Gbps. Se è necessario disabilitare la negoziazione automatica per le connessioni, la velocità delle porte e la modalità full duplex devono essere configurate manualmente. Se l'interfaccia virtuale rimane inattiva, consulta Risoluzione dei problemi di livello 2 (collegamento dati).
4. Verifica che il segnale ottico ricevuto dal router tramite l'interconnessione sia accettabile.
5. Prova a capovolgere (girare) i filamenti di fibra di trasmissione/ricezione.
6. Controlla i CloudWatch parametri di Amazon per AWS Direct Connect. Puoi verificare le letture ottiche Tx/Rx del AWS Direct Connect dispositivo (sia a 1 Gbps che a 10 Gbps), il conteggio degli errori fisici e lo stato operativo del dispositivo. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.

7. Contatta il provider di co-location e richiedi un report scritto relativo al segnale ottico in trasmissione/ricezione per l'interconnessione.
8. Se i problemi fisici di connettività permangono anche dopo aver seguito questa procedura, contatta AWS Support fornendo la notifica di completamento dell'interconnessione e il report sul segnale ottico ricevuti dal provider di co-locazione.

Nel seguente diagramma di flusso è riportata la procedura per la diagnosi dei problemi con la connessione fisica.

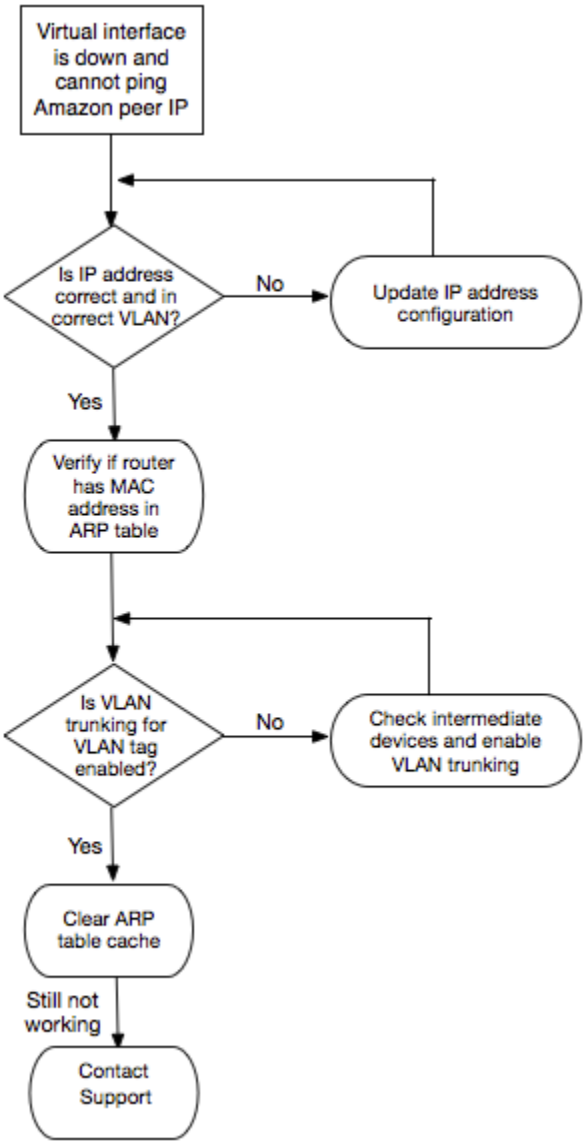

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

Risoluzione dei problemi di livello 2 (collegamento dati)

Se la connessione AWS Direct Connect fisica è attiva ma l'interfaccia virtuale non è attiva, utilizza i seguenti passaggi per risolvere il problema.

1. Se non riesci a effettuare il ping dell'indirizzo IP peer di Amazon, verifica che il tuo indirizzo IP peer sia stato impostato correttamente e nella VLAN appropriata. Assicurati che l'indirizzo IP sia configurato nella sottointerfaccia VLAN e non nell'interfaccia fisica (ad esempio, GigabitEthernet 0/0.123 anziché 0/0). GigabitEthernet
2. Verifica se il router ha un indirizzo MAC dall' AWS endpoint nella tabella ARP (Address Resolution Protocol).
3. Verifica che per tutti i dispositivi intermedi tra gli endpoint sia abilitato il trunking VLAN per il tag VLAN 802.1Q. L'ARP non può essere stabilito AWS lateralmente finché non AWS riceve traffico contrassegnato.
4. Cancella la cache della tabella ARP tua o del tuo provider.
5. Se i passaggi precedenti non stabiliscono l'ARP o non riesci ancora a eseguire il ping dell'IP peer di Amazon, contatta il supporto AWS.

Nel seguente diagramma di flusso è riportata la procedura per la diagnosi dei problemi con il collegamento dati.



Se la sessione BGP non viene comunque stabilita dopo aver seguito questa procedura, consulta Risoluzione dei problemi di livello 3/4 (rete/trasporto). Se la sessione BGP viene stabilita ma si verificano problemi di instradamento, consulta Risoluzione dei problemi di instradamento.

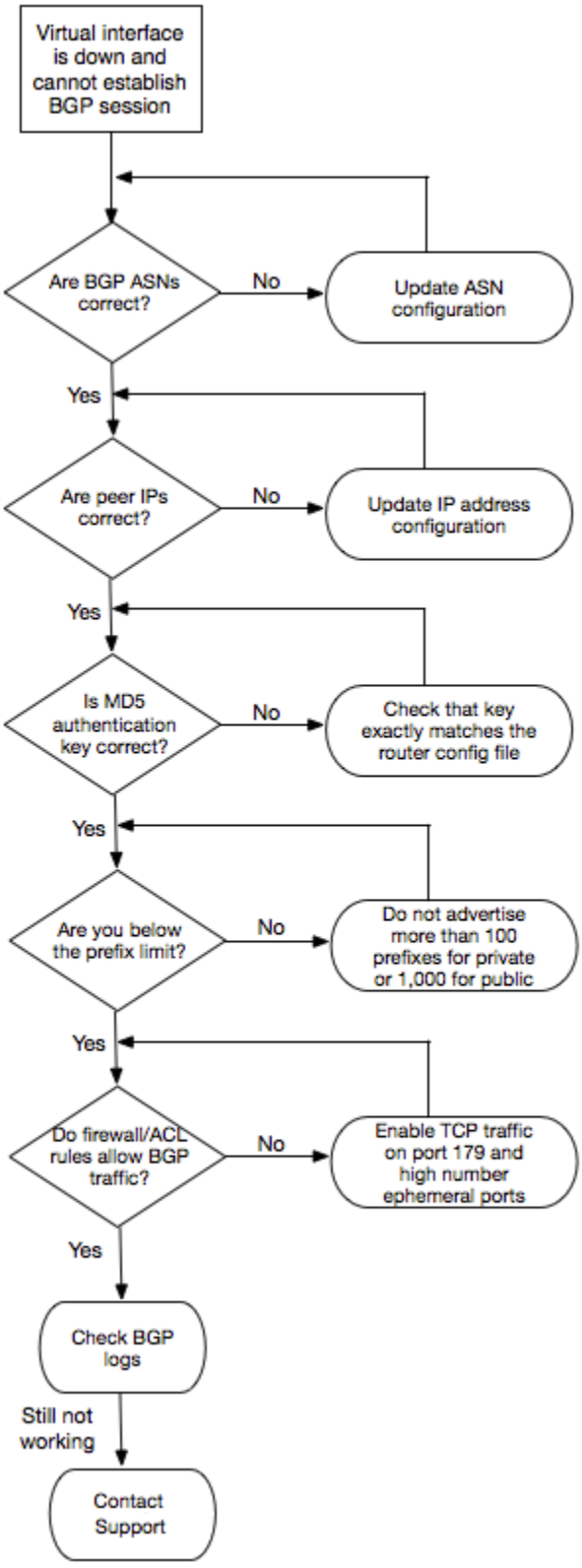
Risoluzione dei problemi di livello 3/4 (rete/trasporto)

Prendi in considerazione una situazione in cui la tua connessione AWS Direct Connect fisica è attiva e puoi eseguire il ping dell'indirizzo IP peer di Amazon. Se l'interfaccia virtuale è inattiva e la sessione di peering BGP non può essere stabilita, utilizza la procedura seguente per risolvere il problema:

1. Assicurati che l'Autonomous System Number (ASN) BGP locale e l'ASN di Amazon siano configurati correttamente.

2. Assicurati che gli indirizzi IP peer su entrambi i lati della sessione di peering BGP siano configurati correttamente.
3. Verifica che la chiave di autenticazione MD5 sia configurata e corrisponda esattamente alla chiave presente nel file di configurazione scaricato per il router. Verifica che non ci siano spazi o caratteri aggiuntivi.
4. Verifica che tu o il tuo provider non stiate pubblicizzando oltre 100 prefissi per le interfacce virtuali private o 1.000 prefissi per le interfacce virtuali pubbliche, perché si tratta di limiti rigidi che non possono essere superati.
5. Verifica che non ci siano regole firewall o ACL che comportino il blocco della porta TCP 179 o di altre porte TCP effimere con numerazione alta, perché sono necessarie per consentire a BGP di stabilire una connessione TCP tra peer.
6. Controlla se nei log BGP sono presenti errori o messaggi di avviso.
7. Se i passaggi precedenti non consentono di stabilire la sessione di peering BGP, contatta l'assistenza. AWS

Nel seguente diagramma di flusso è riportata la procedura per la diagnosi dei problemi con la sessione di peering BGP.



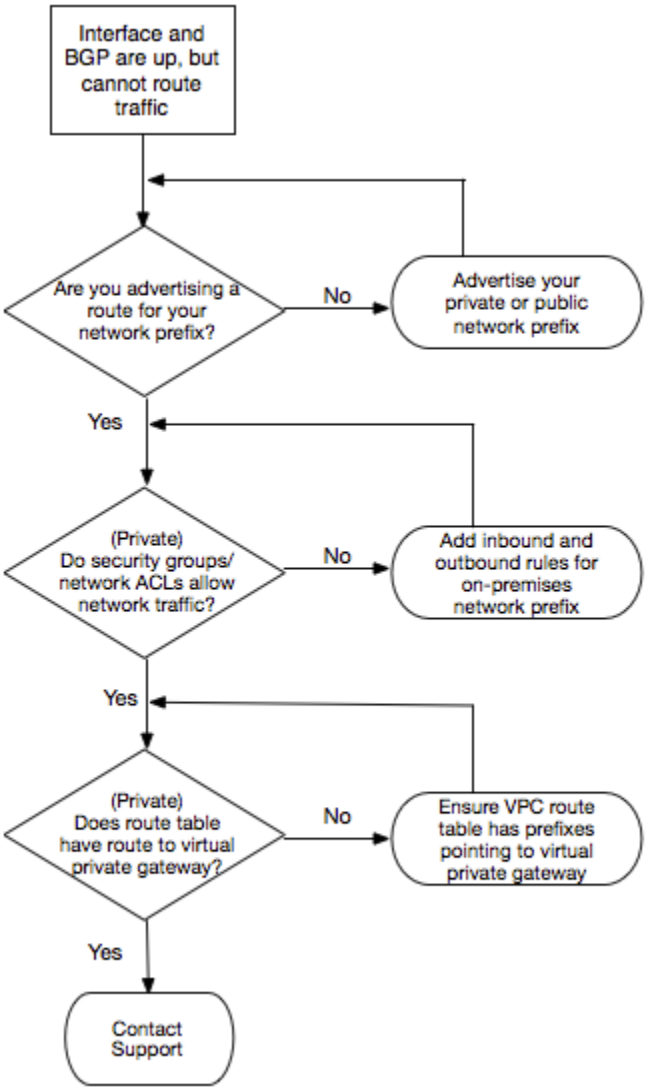
Se la sessione di peering BGP viene stabilita ma si verificano problemi di instradamento, consulta Risoluzione dei problemi di instradamento.

Risoluzione dei problemi di instradamento

Considera una situazione in cui l'interfaccia virtuale è attiva e tu hai stabilito una sessione di peering BGP. Se non puoi instradare il traffico tramite l'interfaccia virtuale, utilizza la procedura seguente per risolvere il problema:

1. Assicurati di pubblicizzare un instradamento per il prefisso di rete locale tramite la sessione BGP. Per un'interfaccia virtuale privata, può trattarsi di un prefisso di rete privato o pubblico. Per un'interfaccia virtuale pubblica, deve essere il prefisso di rete instradabile pubblicamente.
2. Per un'interfaccia virtuale privata, assicurati che i gruppi di sicurezza VPC e le liste di controllo degli accessi di rete consentano il traffico in entrata e in uscita per il prefisso di rete locale. Per ulteriori informazioni, consulta le sezioni relative ai gruppi di sicurezza e alle ACL di rete nella Guida per l'utente di Amazon VPC.
3. Per un'interfaccia virtuale privata, assicurati che i prefissi nelle tabelle di routing VPC rimandino al gateway virtuale privato al quale è connessa l'interfaccia virtuale privata. Ad esempio, se desideri che tutto il traffico venga instradato per impostazione predefinita attraverso la rete locale, puoi aggiungere il percorso predefinito (0.0.0.0/0 o ::/0) con il gateway privato virtuale come destinazione nelle tabelle di instradamento VPC.
   - In alternativa, puoi abilitare la propagazione dell'instradamento per aggiornare automaticamente gli instradamenti nelle tabelle di routing in base all'annuncio di routing BGP dinamico. Ogni tabella di routing può contenere fino a 100 instradamenti propagati. Questo limite non può essere aumentato. Per ulteriori informazioni consulta la sezione Abilitazione e disabilitazione della propagazione del routing nella Guida per l'utente di Amazon VPC.
4. Se i passaggi precedenti non risolvono i problemi di routing, contatta l' AWS assistenza.

Nel seguente diagramma di flusso è riportata la procedura per la diagnosi dei problemi di instradamento.


Interface and BGP are up, but cannot route traffic
Are you advertising a route for your network prefix?
No
Advertise your private or public network prefix
Yes
(Private) Do security groups/ network ACLs allow network traffic?
No
Add inbound and outbound rules for on-premises network prefix
Yes
(Private) Does route table have route to virtual private gateway?
No
Ensure VPC route table has prefixes pointing to virtual private gateway
Yes
Contact Support

Cronologia dei documenti

La tabella seguente descrive le versioni dei AWS Direct Connect.

Funzionalità	Descrizione	Data
Support per SiteLink	È possibile creare un'interfaccia privata virtuale che abiliti la connettività tra due punti di presenza Direct Connect (PoPs) nella stessa AWS regione. Per ulteriori informazioni, consulta Interfacce virtuali ospitate.	01/12/2021
Support MAC Security	È possibile utilizzare connessioni AWS Direct Connect che supportano MACsec per crittografare i dati dal data center aziendale alla sede AWS Direct Connect. Per ulteriori informazi oni, consulta MAC Security.	2021-03-31
Supporto per 100G	Argomenti aggiornati per includere il supporto per le connessioni dedicate 100G.	2021-02-12
Nuova sede in Italia	Argomento aggiornato per includere l'aggiunta della nuova sede di Italia. Per ulteriori informazioni, consulta the section called “Europa (Milano)”.	2021-01-22
Nuova sede in Israele	Argomento aggiornato per includere l'aggiunta della nuova sede di Israele. Per ulteriori informazioni, consulta the section called “Israele (Tel Aviv)”.	2020-07-07
Toolkit di resilienza - Supporto al test di failover	Utilizzare la funzionalità Test di failover del Toolkit di resilienz a per verificare la resilienza delle connessioni. Per ulteriori informazioni, consulta the section called “Test di failover AWS Direct Connect”.	2020-06-03
CloudWatc h Supporto metrico VIF	È possibile monitorare AWS Direct Connect le connessioni fisiche e le interfacce virtuali utilizzando. CloudWatch Per ulteriori informazioni, consulta the section called “Monitoraggio con Amazon CloudWatch”.	2020-05-11

Funzionalità	Descrizione	Data
AWS Direct Connect Resiliency Toolkit	L'AWS Direct Connect Resiliency Toolkit fornisce una procedura guidata di connessione con più modelli di resilienza che consente di ordinare le connessioni dedicate per ottenere l'obiettivo dello SLA. Per ulteriori informazioni, consulta Utilizzo del AWS Direct Connect Resiliency Toolkit per iniziare.	07-10-2019
Supporto regionale aggiuntivo per il supporto di AWS Transit Gateway tra account	Per informazioni, consulta the section called “Associazioni di gateway di transito”.	30-09-2019
Supporto di AWS Direct Connect per AWS Transit Gateway	È possibile utilizzare un gateway AWS Direct Connect per collegare la connessione AWS Direct Connect tramite un'interfaccia virtuale di transito ai VPC o alle VPN collegate al gateway di transito. Associare un gateway Direct Connect al gateway di transito, quindi creare un'interfaccia virtuale di transito per la connessione AWS Direct Connect al gateway Direct Connect. Per informazioni, consultare the section called “Associazioni di gateway di transito”.	27-03-2019
Supporto frame Jumbo	Puoi inviare frame jumbo (9001 MTU) su AWS Direct Connect. Per ulteriori informazioni, consulta Impostazione di MTU di rete per interfacce virtuali private o di transito.	11-10-2018
Comunità BGP di preferenza locale	Puoi usare i tag per le comunità BGP di preferenza locale per raggiungere il bilanciamento del carico e instradare la preferenza per il traffico in entrata verso la rete. Per ulteriori informazioni, consulta Comunità BGP di preferenza locale.	06-02-2018

Funzionalità	Descrizione	Data
AWS Direct ConnectGateway	Puoi utilizzare un gateway Direct Connect per collegare la connessione AWS Direct Connect a VPC nelle regioni remote. Per ulteriori informazioni, consulta Utilizzo dei gateway Direct Connect.	01-11-2017
CloudWatch Metriche Amazon	Puoi visualizzare le CloudWatch metriche per le tue AWS Direct Connect connessioni. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.	29-06-2017
Link aggregation group	Puoi creare un link aggregation group (LAG) per aggregare più connessioni AWS Direct Connect. Per ulteriori informazioni, consulta Link aggregation groups.	13-02-2017
Supporto IPv6	L'interfaccia virtuale può supportare una sessione di peering BGP IPv6. Per ulteriori informazioni, consulta Aggiungere o eliminare un peer BGP.	01-12-2016
Supporto del tagging	Puoi contrassegnare con dei tag le risorse di AWS Direct Connect. Per ulteriori informazioni, consulta Tagging delle risorse AWS Direct Connect.	04-11-2016
LOA-CFA self-service	Puoi scaricare la Letter of Authorization and Connecting Facility Assignment (LOA-CFA) utilizzando la console o l'API AWS Direct Connect.	22-06-2016
Nuovo sito nella Silicon Valley	Argomento aggiornato in modo da includere l'aggiunta del nuovo sito nella Silicon Valley nella regione Stati Uniti occidentali (California settentrionale).	03-06-2016
Nuovo sito ad Amsterdam	Argomento aggiornato in modo da includere l'aggiunta del nuovo sito ad Amsterdam nella regione Europa (Francoforte).	19-05-2016
Nuovi siti a Portland, Oregon e Singapore	Argomento aggiornato per includere l'aggiunta dei nuovi siti Portland, Oregon e Singapore nelle regioni Stati uniti occidentali (Oregon) e Asia Pacifico (Singapore).	27-04-2016

Funzionalità	Descrizione	Data
Nuovo sito a San Paolo, Brasile	Argomento aggiornato in modo da includere l'aggiunta del nuovo sito a San Paolo nella regione Sud America (San Paolo).	09-12-2015
Nuovi siti a Dallas, a Londra, nella Silicon Valley e a Mumbai	Argomenti aggiornati che includono l'aggiunta di nuove sedi a Dallas (regione Stati Uniti orientali (Virginia settentrionale)), Londra (Europa (Irlanda)), Silicon Valley AWS GovCloud (regione Stati Uniti occidentali) e Mumbai (regione Asia Pacifico (Singapore)).	27-11-2015
Nuova sede nella regione Cina (Pechino)	Argomenti aggiornati in modo da includere l'aggiunta del nuovo sito a Pechino nella regione Cina (Pechino).	14-04-2015
Nuovo sito a Las Vegas nella regione Stati Uniti occidentali (Oregon)	Argomenti aggiornati in modo da includere l'aggiunta del nuovo sito AWS Direct Connect a Las Vegas nella regione Stati Uniti occidentali (Oregon).	10-11-2014
Nuova regione UE (Francoforte)	Argomenti aggiornati in modo da includere l'aggiunta dei nuovi siti AWS Direct Connect che servono la regione UE (Francoforte).	23-10-2014
Nuovi siti nella regione Asia Pacifico (Sydney)	Argomenti aggiornati in modo da includere l'aggiunta dei nuovi siti AWS Direct Connect che servono la regione Asia Pacifico (Sydney).	14-07-2014
Supporto per AWS CloudTrail	È stato aggiunto un nuovo argomento per spiegare come utilizzare CloudTrail per registrare le attività. AWS Direct Connect Per ulteriori informazioni, consulta Registrazione di chiamate API AWS Direct Connect con AWS CloudTrail.	04-04-2014

Funzionalità	Descrizione	Data
Supporto per accedere alle regioni AWS remote	Aggiunto un nuovo argomento per spiegare in che modo puoi accedere a risorse pubbliche in una regione remota. Per ulteriori informazioni, consulta Accesso a una regione AWS remota.	19-12-2013
Supporto per le connessioni in hosting	Argomenti aggiornati per includere il supporto per le connessioni in hosting.	22-10-2013
Nuovo sito nella regione UE (Irlanda)	Argomenti aggiornati in modo da includere l'aggiunta del nuovo sito AWS Direct Connect che serve la regione UE (Irlanda).	24-06-2013
Nuovo sito a Seattle nella regione Stati Uniti occidentali (Oregon)	Argomenti aggiornati in modo da includere l'aggiunta del nuovo sito AWS Direct Connect a Seattle che serve la regione Stati Uniti occidentali (Oregon).	08-05-2013
Supporto per l'uso di IAM con AWS Direct Connect	Aggiunto un argomento sull'utilizzo di AWS Identity and Access Management con AWS Direct Connect. Per ulteriori informazioni, consulta the section called “Identity and Access Management”.	21-12-2012
Nuova regione Asia Pacifico (Sydney)	Argomenti aggiornati in modo da includere l'aggiunta del nuovo sito AWS Direct Connect che serve la regione Asia Pacifico (Sydney).	14-12-2012

Funzionalità	Descrizione	Data
Nuova console AWS Direct Connect e regioni Stati Uniti orientali (Virginia settentrionale) e Sud America (San Paolo)	La Guida alle operazioni di base di AWS Direct Connect è stata sostituita con la Guida per l'utente di AWS Direct Connect. Aggiunti nuovi argomenti per coprire la nuova console AWS Direct Connect, aggiunto un argomento di fatturazione, aggiunte le informazioni sulla configurazione del router e aggiornati gli argomenti per includere l'aggiunta di due nuove località AWS Direct Connect che servono le regioni Stati Uniti orientali (Virginia settentrionale) e Sud America (San Paolo).	13-08-2012
Supporto per le regioni UE (Irlanda), Asia Pacifico (Singapore) e Asia Pacifico (Tokyo)	Aggiunta una nuova sezione di risoluzione dei problemi e aggiornati gli argomenti per includere l'aggiunta di quattro nuovi siti AWS Direct Connect che servono le regioni Stati Uniti occidentali (California settentrionale), UE (Irlanda), Asia Pacifico (Singapore) e Asia Pacifico (Tokyo).	10-01-2012
Supporto per la regione Stati Uniti occidentali (California settentrionale)	Aggiornati argomenti per includere l'aggiunta della regione Stati Uniti occidentali (California settentrionale).	08-09-2011
Versione pubblica	Il primo rilascio di AWS Direct Connect.	03-08-2011

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.