aws

Guida per l'utente

# Amazon Virtual Private Cloud

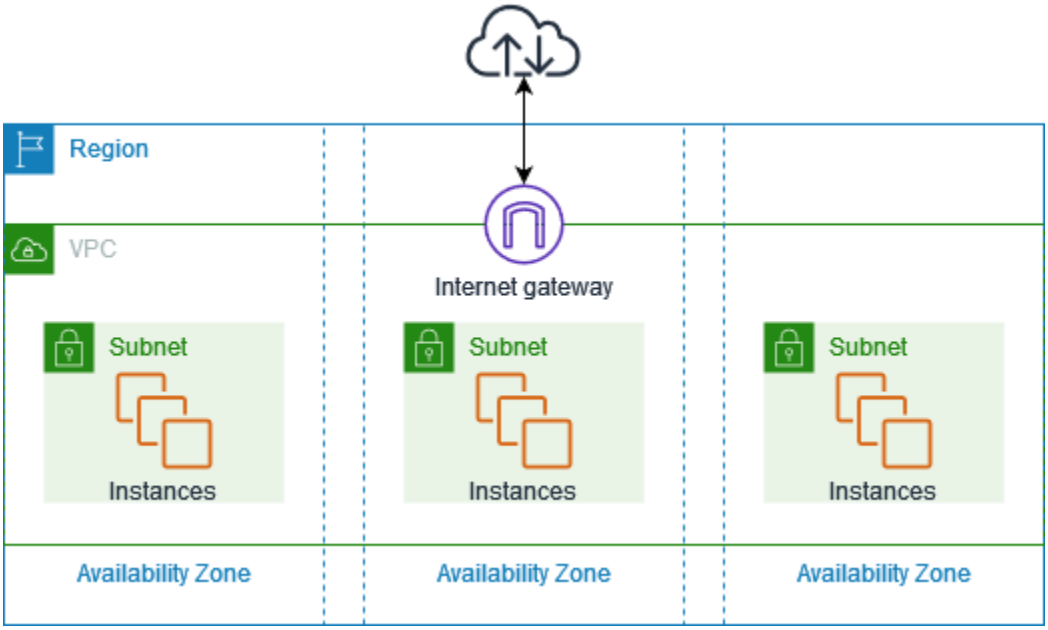
# Amazon Virtual Private Cloud: Guida per l'utente

# Table of Contents

# Cos'è Amazon VPC?

Con Amazon Virtual Private Cloud (Amazon VPC), puoi avviare AWS risorse in una rete virtuale logicamente isolata che hai definito. Questa rete virtuale è simile a una comune rete da gestire all'interno del proprio data center, ma con i vantaggi dell'infrastruttura scalabile di AWS.

Il seguente diagramma mostra un esempio di VPC. Il VPC ha una sottorete in ogni zona di disponibilità nella regione, le istanze EC2 in ogni sottorete, mentre il gateway Internet consente la comunicazione tra le risorse nel VPC e Internet.




Per ulteriori informazioni, consulta Amazon Virtual Private Cloud (Amazon VPC).

## Funzionalità

Le seguenti funzionalità consentono di configurare un VPC per fornire la connettività necessaria alle applicazioni:

Cloud privati virtuali (VPC)

Un VPC è una rete virtuale simile a una rete tradizionale che potresti utilizzare nel tuo data center. Dopo aver creato un VPC, puoi aggiungere sottoreti.

Sottoreti

una sottorete è un intervallo di indirizzi IP nel VPC; Una sottorete deve risiedere in una singola zona di disponibilità. Dopo aver aggiunto le sottoreti, puoi distribuire AWS risorse nel tuo VPC.

Assegnazione di indirizzi IP

Puoi assegnare indirizzi IP, sia IPv4 sia IPv6, ai VPC e alle sottoreti Puoi anche trasferire i tuoi indirizzi IPv4 pubblici e gli indirizzi GUA IPv6 AWS e allocarli alle risorse del tuo VPC, come istanze EC2, gateway NAT e Network Load Balancer.

Routing

Usa le tabelle di instradamento per determinare la destinazione del traffico di rete proveniente dalla sottorete o dal gateway.

Gateway ed endpoint

Un gateway connette il tuo VPC a un'altra rete. Ad esempio, utilizza un gateway Internet per connettere il VPC a Internet. Usa un endpoint VPC per connetterti Servizi AWS privatamente, senza l'uso di un gateway Internet o di un dispositivo NAT.

Connessioni peering

Usa una connessione peering VPC per instradare il traffico tra le risorse in due VPC.

Mirroring del traffico

Copia il traffico di rete dalle interfacce di rete e invialo alle apparecchiature di sicurezza e monitoraggio per l'ispezione approfondita dei pacchetti.

Gateway di transito

Utilizza un gateway di transito, che funge da hub centrale, per instradare il traffico tra i tuoi VPC, le connessioni VPN e le connessioni. AWS Direct Connect

Log di flusso VPC

Il log di flusso acquisisce informazioni sul traffico IP verso e dalle interfacce di rete nel VPC.

Connessioni VPN

Connetti i VPC alle reti on-premise usando AWS Virtual Private Network (AWS VPN).

# Nozioni di base su Amazon VPC

In ognuno di essi è Account AWS incluso un VPC predefinito. Regione AWS I VPC predefiniti sono configurati in modo da poter iniziare immediatamente l'avvio e la connessione alle istanze EC2. Per ulteriori informazioni, consulta Inizia a usare.

Puoi scegliere di creare VPC aggiuntivi con le sottoreti, gli indirizzi IP, i gateway e il routing di cui hai bisogno. Per ulteriori informazioni, consulta the section called “Crea un VPC”.

# Uso di Amazon VPC

È possibile creare e gestire i VPC utilizzando una qualsiasi delle seguenti interfacce:

- AWS Management Console — Fornisce un'interfaccia web da utilizzare per l'accesso ai VPC.
- AWS Command Line Interface (AWS CLI) — Fornisce comandi per un'ampia gamma di AWS servizi, tra cui Amazon VPC, ed è supportato su Windows, Mac e Linux. Per ulteriori informazioni, consulta AWS Command Line Interface.
- AWS SDK: fornisce API specifiche per la lingua e si occupa di molti dettagli di connessione, come il calcolo delle firme, la gestione dei tentativi di richiesta e la gestione degli errori. Per ulteriori informazioni, consulta SDK di AWS.
- API di query: forniscono operazioni API di basso livello accessibili tramite richieste HTTPS. L'API di query è il modo più diretto per accedere ad Amazon VPC, ma richiede che la propria applicazione gestisca dettagli di basso livello, come la generazione di un hash per la firma della richiesta e la gestione degli errori. Per ulteriori informazioni, consulta Operazioni di Amazon VPC nella Documentazione di riferimento delle API di Amazon EC2.

# Prezzi per Amazon VPC

Non ci sono costi aggiuntivi per l'utilizzo di un VPC. Tuttavia, sono previsti costi per alcuni componenti VPC, come gateway NAT, IP Address Manager, traffic mirroring, Reachability Analyzer e Network Access Analyzer. Per ulteriori informazioni, consulta la pagina dei Prezzi di Amazon VPC.

Quasi tutte le risorse che lanci nel tuo cloud privato virtuale (VPC) ti forniscono un indirizzo IP per la connettività. La stragrande maggioranza delle risorse del tuo VPC utilizza indirizzi IPv4 privati. Le risorse che richiedono l'accesso diretto a Internet tramite IPv4, tuttavia, utilizzano indirizzi IPv4 pubblici.

Prezzi degli indirizzi IPv4 pubblici

Un indirizzo IPv4 pubblico è un indirizzo IPv4 instradabile da Internet. Un indirizzo IPv4 pubblico è necessario affinché una risorsa sia direttamente raggiungibile da Internet tramite IPv4.

Se sei un cliente del piano AWS gratuito esistente o nuovo, ricevi 750 ore di utilizzo degli indirizzi IPv4 pubblici gratuitamente. Se non utilizzi il piano AWS gratuito, verranno addebitati gli indirizzi

IPv4 pubblici. Per informazioni specifiche sui prezzi, consulta la scheda Indirizzo IPv4 pubblico nella pagina Prezzi di Amazon VPC.

Gli Indirizzi IPv4 privati (RFC 1918) non sono a pagamento. Per ulteriori informazioni su come vengono addebitati gli indirizzi IPv4 pubblici per i VPC condivisi, vedi Fatturazione e misurazione per il proprietario e i partecipanti.

Gli indirizzi IPv4 pubblici hanno i seguenti tipi:

- Indirizzi IP elastici (EIP): indirizzi IPv4 statici e pubblici forniti da Amazon che puoi associare a un'istanza, un'interfaccia di rete elastica o una risorsa EC2. AWS
- Indirizzi IPv4 pubblici per EC2: indirizzi IPv4 pubblici assegnati a un'istanza EC2 da Amazon (se l'istanza EC2 viene avviata in una sottorete predefinita o in una sottorete configurata per assegnare automaticamente un indirizzo IPv4 pubblico).
- Indirizzi BYOIPv4: indirizzi IPv4 pubblici nell'intervallo di indirizzi IPv4 che hai introdotto utilizzando Bring your own IP address (BYOIP). AWS
- Indirizzi IPv4 gestiti dal servizio: indirizzi IPv4 pubblici assegnati automaticamente alle risorse e gestiti da un servizio. AWS AWS Ad esempio, indirizzi IPv4 pubblici su Amazon ECS, Amazon RDS o Amazon. WorkSpaces

L'elenco seguente mostra i AWS servizi più comuni che possono utilizzare indirizzi IPv4 pubblici.

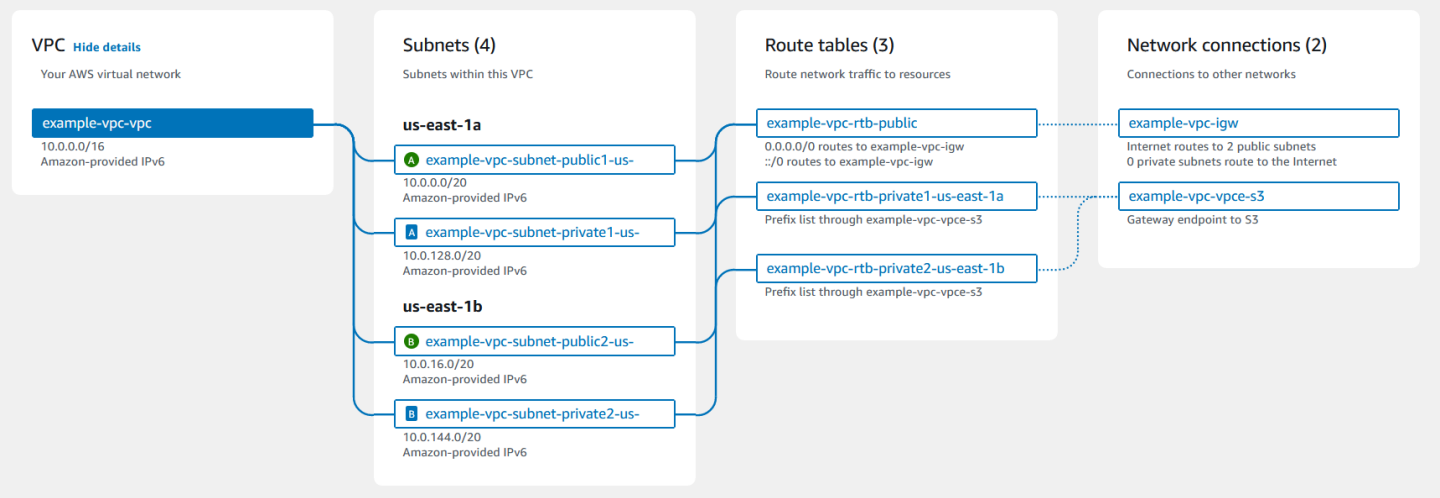
- Amazon AppStream 2.0
- AWS Client VPN
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR
- Amazon GameLift
- AWS Global Accelerator
- AWS Mainframe Modernization
- Amazon Managed Streaming per Apache Kafka
- Amazon MQ
- Amazon RDS

- Amazon Redshift
- AWS Site-to-Site VPN
- Gateway NAT di Amazon VPC
- Amazon WorkSpaces
- Sistema di bilanciamento del carico elastico

# Come funziona Amazon VPC

Con Amazon Virtual Private Cloud (Amazon VPC), puoi avviare AWS risorse in una rete virtuale logicamente isolata che hai definito. Questa rete virtuale è simile a una comune rete da gestire all'interno del proprio data center, ma con i vantaggi dell'infrastruttura scalabile di AWS.

Di seguito è riportata una rappresentazione visiva di un VPC e delle relative risorse mostrate nel riquadro di Anteprima quando crei un VPC tramite AWS Management Console. Per un VPC esistente, puoi accedere a questa visualizzazione nella scheda Mappa delle risorse. Questo esempio mostra le risorse inizialmente selezionate nella pagina Crea VPC quando scegli di creare il VPC e altre risorse di rete. Questo VPC è configurato con un CIDR IPv4 e un CIDR IPv6 fornito da Amazon in due zone di disponibilità, tre tabelle di instradamento, un gateway Internet e un endpoint del gateway. Poiché è stato selezionato il gateway Internet, la visualizzazione mostra che il traffico proveniente dalle sottoreti pubbliche viene indirizzato verso Internet perché la tabella di instradamento corrispondente invia il traffico verso il gateway Internet.




Concetti

- VPC e sottoreti
- VPC predefiniti e non predefiniti
- Tabelle di routing
- Accesso a Internet
- Accesso a una rete domestica o aziendale
- Connessione di VPC e reti
- AWS rete globale privata

# VPC e sottoreti

Un cloud privato virtuale (VPC) è una rete virtuale dedicata al tuo account AWS . È logicamente isolato dalle altre reti virtuali nel cloud. AWS Puoi specificare un intervallo di indirizzi IP per il VPC, aggiungere sottoreti e associare gruppi di sicurezza.

una sottorete è un intervallo di indirizzi IP nel VPC; Le risorse AWS , ad esempio le istanze Amazon EC2, vengono avviate nelle sottoreti. È possibile connettere una sottorete a Internet, ad altri VPC e ai propri data center e instradare il traffico da e verso le sottoreti utilizzando le tabelle di instradamento.

Ulteriori informazioni

- Assegnazione di indirizzi IP
- Cloud privati virtuali
- Sottoreti

# VPC predefiniti e non predefiniti

Se è stato creato dopo il 4 dicembre 2013, il tuo account dispone di un VPC predefinito in ogni Regione. Un VPC predefinito è già configurato e pronto all'uso. Ad esempio, ha una sottorete predefinita in ciascuna Zona di disponibilità della Regione, un gateway Internet allegato, un instradamento nella tabella di instradamento principale che invia tutto il traffico al Gateway Internet e impostazioni DNS che forniscono alle istanze indirizzi IP pubblici e nomi host DNS e consentono la risoluzione DNS tramite il server DNS fornito da Amazon (consulta Attributi DNS nel VPC). Pertanto, un'istanza EC2 avviata in una sottorete predefinita ha automaticamente accesso a Internet. Se disponi di un VPC predefinito in una Regione e non specifichi una sottorete all'avvio dell'istanza EC2 in quella Regione, sceglieremo una delle sottoreti predefinite e avvieremo l'istanza in quella sottorete.

Puoi inoltre creare il tuo VPC e configurarlo in base alle esigenze. Questo è il cosiddetto VPC non predefinito. Le sottoreti create nel VPC non predefinito e le altre sottoreti create nel VPC predefinito vengono chiamate sottoreti non predefinite.

Ulteriori informazioni

- the section called “VPC di default”
- the section called “Crea un VPC”

# Tabelle di routing

Una tabella di instradamento contiene un insieme di regole, denominate route, che consentono di determinare la direzione del traffico di rete proveniente dal VPC. Puoi associare esplicitamente una sottorete a una particolare tabella di instradamento. In caso contrario, la sottorete è implicitamente associata alla tabella di instradamento principale.

Ogni route in una tabella di instradamento specifica l'intervallo di indirizzi IP in cui si desidera instradare il traffico (la destinazione) e il gateway, l'interfaccia di rete o la connessione attraverso cui inviare il traffico (il target).

Ulteriori informazioni

- Configurare le tabelle di routing

# Accesso a Internet

Puoi controllare il modo in cui le istanze che avvii in un VPC accedono alle risorse Esterne al VPC.

Un VPC predefinito include un Internet gateway e ogni sottorete predefinita è una sottorete pubblica. Ciascuna istanza avviata in una sottorete predefinita ha un indirizzo IPv4 privato e uno pubblico. Queste istanze possono comunicare con Internet tramite l'Internet gateway. Un Internet gateway permette alle istanze di connettersi a Internet tramite l'edge della rete Amazon EC2.

Per impostazione predefinita, tutte le istanze avviate in una sottorete non predefinita hanno un indirizzo IPv4 privato ma non hanno indirizzi IPv4 pubblici, a meno che tu non gliene assegni uno in fase di avvio o non modifichi l'attributo dell'indirizzo IP pubblico. Queste istanze possono comunicare tra di loro, ma non possono accedere a Internet.

Puoi abilitare l'accesso Internet di un'istanza avviata in una sottorete non predefinita collegando un Internet gateway al VPC (se il VPC non è predefinito) e associando all'istanza un indirizzo IP elastico.

In alternativa, per consentire a un'istanza nel VPC di avviare connessioni in uscita a Internet ma impedire connessioni in entrata indesiderate da Internet, puoi utilizzare un dispositivo di network address translation (NAT). NAT associa più indirizzi IPv4 privati a un solo indirizzo IPv4 pubblico. Puoi configurare il dispositivo NAT con un indirizzo IP elastico e connetterlo a Internet tramite un gateway Internet. Ciò consente a un'istanza di una sottorete privata di connettersi a Internet tramite il dispositivo NAT, che instrada il traffico dall'istanza al gateway Internet e le risposte all'istanza.

Se associ un blocco CIDR IPv6 al VPC e assegni indirizzi IPv6 alle istanze, le istanze possono connettersi a Internet su IPv6 tramite un gateway Internet. In alternativa, le istanze possono avviare connessioni in uscita a Internet su IPv6 tramite un Internet gateway egress-only. Il traffico IPv6 è distinto dal traffico IPv4; le tue tabelle di routing devono includere percorsi separati per il traffico IPv6.

Ulteriori informazioni

- Eseguire la connessione a Internet utilizzando un gateway Internet
- Abilitazione del traffico in uscita IPv6 utilizzando un gateway Internet egress-only
- Eseguire la connessione a Internet o ad altri VPC utilizzando dispositivi NAT

## Accesso a una rete domestica o aziendale

Opzionalmente, puoi connettere il tuo VPC al tuo data center aziendale utilizzando una connessione AWS Site-to-Site VPN IPSec, rendendo AWS il Cloud un'estensione del tuo data center.

Una connessione VPN da sito a sito è costituita da due tunnel VPN tra un gateway privato virtuale o un gateway di transito laterale e un dispositivo gateway AWS del cliente situato nel data center. Un dispositivo gateway del cliente è un dispositivo fisico o un'appliance software che puoi configurare sul tuo lato della connessione Site-to-Site VPN.

Ulteriori informazioni

- AWS Site-to-Site VPN Guida per l'utente
- Amazon VPC Transit Gateway

## Connessione di VPC e reti

Puoi creare una connessione peering VPC tra due VPC che consente di instradare il traffico tra gli stessi in modo privato. Le istanze in uno qualsiasi dei VPC possono comunicare tra loro come se fossero nella stessa rete.

Puoi inoltre creare un gateway di transito e utilizzarlo per interconnettere i VPC e le reti on-premise. Il gateway di transito funge da router virtuale regionale per il traffico che scorre tra i suoi allegati, che può includere VPC, connessioni VPN, gateway e connessioni peering con AWS Direct Connect gateway di transito.

Ulteriori informazioni

- Amazon VPC Peering Guide
- Amazon VPC Transit Gateway

# AWS rete globale privata

AWS fornisce una rete globale privata ad alte prestazioni e bassa latenza che offre un ambiente di cloud computing sicuro per supportare le esigenze di rete. AWS Le regioni sono collegate a più provider di servizi Internet (ISP) e a una dorsale di rete globale privata che fornisce prestazioni di rete migliorate per il traffico interregionale inviato dai clienti.

Tieni presente le seguenti considerazioni:

- Il traffico che si trova in una zona di disponibilità o tra zone di disponibilità in tutte le regioni viene AWS indirizzato sulla rete globale privata.
- Il traffico tra le regioni viene sempre AWS indirizzato sulla rete globale privata, ad eccezione delle regioni cinesi.

La perdita di pacchetti di rete può essere causata da una serie di fattori, tra cui conflitti di flusso di rete, errori di livello inferiore (livello 2) e altri errori di rete. Progettiamo e gestiamo le nostre reti per ridurre al minimo la perdita di pacchetti. Misuriamo il tasso di perdita di pacchetti (PLR) sulla dorsale globale che collega le regioni. AWS Gestiamo la nostra rete backbone per raggiungere un p99 del PLR orario inferiore allo 0,0001%.

# Nozioni di base su Amazon VPC

Completa le seguenti attività per iniziare a creare e connettere i tuoi VPC. Al termine dell'operazione, sari pronto a implementare l'applicazione su AWS.

Attività

- Iscriviti per un Account AWS
- Verificare le autorizzazioni
- Determina gli intervalli di indirizzi IP
- Seleziona le tue zone di disponibilità
- Pianifica la tua connettività Internet
- Creazione di un VPC
- Distribuzione dell'applicazione

## Iscriviti 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.

# Verificare le autorizzazioni

Prima di poter utilizzare Amazon VPC, devi disporre delle autorizzazioni richieste. Per ulteriori informazioni, consulta Identity and Access Management per Amazon VPC e Esempi delle policy di Amazon VPC.

# Determina gli intervalli di indirizzi IP

Le risorse nel VPC comunicano tra loro e con le risorse su Internet tramite indirizzi IP. Quando crei VPC e sottoreti, puoi selezionare i relativi intervalli di indirizzi IP. Quando sono distribuite risorse in una sottorete, ad esempio istanze EC2, tali risorse ricevono indirizzi IP dall'intervallo di indirizzi IP della sottorete. Per ulteriori informazioni, consulta Assegnazione di indirizzi IP.

Quando scegli una dimensione per il VPC, valuta di quanti indirizzi IP avrai bisogno per gli Account AWS e i VPC. Assicurati che gli intervalli di indirizzi IP per i tuoi VPC non si sovrappongano agli intervalli di indirizzi IP della tua rete. Se hai bisogno di connettività tra più VPC, devi accertarti che non abbiano indirizzi IP sovrapposti.

IP Address Manager (IPAM) semplifica la pianificazione, il tracciamento e il monitoraggio degli indirizzi IP per la tua applicazione. Per ulteriori informazioni, consulta Guida a IP Address Manager.

# Seleziona le tue zone di disponibilità

Una AWS regione è un luogo fisico in cui raggruppiamo i data center, noti come zone di disponibilità. Ogni zona di disponibilità dispone di alimentazione, raffreddamento e sicurezza fisica indipendenti, con alimentazione, rete e connettività ridondanti. Le zone di disponibilità di una regione sono separate fisicamente da una distanza significativa e interconnesse tramite rete ad alta larghezza di banda e bassa latenza. Puoi progettare la tua applicazione in modo che venga eseguita in più zone di disponibilità per ottenere una tolleranza agli errori ancora maggiore.

Ambiente di produzione

Per un ambiente di produzione, consigliamo di selezionare almeno due zone di disponibilità e di distribuire le AWS risorse in modo uniforme in ciascuna zona di disponibilità attiva.

Ambienti di sviluppo o test

Per un ambiente di sviluppo o test, puoi risparmiare denaro implementando le tue risorse in una sola zona di disponibilità.

# Pianifica la tua connettività Internet

Pianifica di dividere ogni VPC in sottoreti in base ai tuoi requisiti di connettività. Per esempio:

- Se hai server web che riceveranno traffico dai client su Internet, crea una sottorete per questi server in ogni zona di disponibilità.
- Se hai anche server che riceveranno traffico solo dai altri server nel VPC, per questi server crea una sottorete distinta in ogni zona di disponibilità.
- Se hai server che riceveranno traffico solo tramite una connessione VPN alla tua rete, per questi server crea una sottorete distinta in ogni zona di disponibilità.

Se l'applicazione riceverà traffico da Internet, il VPC deve disporre di un gateway Internet. Il collegamento di un gateway Internet a VPC virtuale non rende automaticamente accessibili le istanze da Internet. Oltre a collegare il gateway Internet, è necessario aggiornare la tabella di routing della sottorete con un routing al gateway Internet. Inoltre, è necessario assicurarsi che le istanze dispongano di indirizzi IP pubblici e di un gruppo di sicurezza associato che consenta il traffico da Internet su porte e protocolli specifici richiesti dall'applicazione.

In alternativa, registra le istanze con un sistema di bilanciamento del carico connesso a Internet. Il sistema di bilanciamento del carico riceve traffico dai client e lo distribuisce tra le istanze registrate in una o più zone di disponibilità. Per ulteriori informazioni, consulta Elastic Load Balancing. Per consentire alle istanze di una sottorete privata di accedere a Internet (ad esempio, per scaricare gli aggiornamenti) senza consentire connessioni in entrata non desiderate da Internet, aggiungi un gateway NAT pubblico in ogni zona di disponibilità attiva e aggiorna la tabella di instradamento per inviare traffico Internet al gateway NAT. Per ulteriori informazioni, consulta the section called “Accesso a Internet da una sottorete privata”.

# Creazione di un VPC

Dopo aver stabilito il numero di VPC e sottoreti di cui hai bisogno, i blocchi CIDR da assegnare a VPC e sottoreti e la modalità di connessione del VPC a Internet, sei pronto a creare il tuo VPC. Se crei il tuo VPC utilizzando AWS Management Console e includi sottoreti pubbliche nella tua configurazione, creiamo una tabella di routing per la sottorete e aggiungiamo le rotte necessarie per l'accesso diretto a Internet. Per ulteriori informazioni, consulta the section called “Crea un VPC”.

# Distribuzione dell'applicazione

Dopo aver creato il VPC, puoi implementare l'applicazione.

Ambiente di produzione

Per un ambiente di produzione, è possibile utilizzare uno dei seguenti servizi per implementare server in più zone di disponibilità, configurare la scalabilità in modo da mantenere il numero minimo di server richiesto dall'applicazione e registrare i server con un sistema di bilanciamento del carico per distribuire il traffico in modo uniforme tra i server.

- Dimensionamento automatico Amazon EC2
- Parco istanze EC2
- Amazon Elastic Container Service (Amazon ECS)

Ambiente di sviluppo o test

Per un ambiente di sviluppo o test, puoi scegliere di avviare una singola istanza EC2. Per ulteriori informazioni, consulta Nozioni di base su Amazon VPC nella Guida per l'utente di Amazon EC2.

# Indirizzi IP per i tuoi VPC e sottoreti

Gli indirizzi IP permettono alle risorse nel VPC di comunicare tra loro e con le risorse su Internet.

La notazione routing interdominio senza classi (CIDR) è un modo per rappresentare un indirizzo IP e la relativa maschera di rete. Il formato di questi indirizzi è il seguente:

- Un singolo indirizzo IPv4 è a 32 bit, con 4 gruppi composti da un massimo di 3 cifre decimali. Ad esempio, 10.0.1.0.
- Un blocco CIDR IPv4 ha quattro gruppi con un massimo di tre cifre decimali, 0-255, separati da punti, seguiti da una barra e un numero compreso tra 0 e 32. Ad esempio, 10.0.0.0/16.
- Un singolo indirizzo IPv6 è a 128 bit, con 8 gruppi composti da un massimo di 4 cifre esadecimali. Ad esempio, 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
- Un blocco CIDR IPv6 ha quattro gruppi con un massimo di quattro cifre decimali, separati da due punti, seguiti da una barra e un numero compreso tra 1 e 128. Ad esempio, 2001:db8:1234:1a00::/56.

Per ulteriori informazioni, consulta Che cos'è CIDR?

Indice

# Confronto tra IPv4 e IPv6

La seguente tabella riepiloga le differenze tra IPv4 e IPv6 in Amazon EC2 e in Amazon VPC. Per un elenco di AWS servizi che supportano la configurazione dual-stack (IPv4 e IPv6) e configurazioni solo IPv6, vedere. Servizi che supportano IPv6

| Caratteristica | IPv4 | IPv6 |
| --- | --- | --- |
| Dimensione VPC | Un massimo di 5 CIDR da /16 a /28. Questa quota è modificabile. | Fino a 5 CIDR da /44 a /60 con incrementi di /4. Questa quota è modificabile. |
| Dimensione sottorete | Da /16 a /28. | Da /44 a /64 con incrementi di /4. |
| Selezione indirizzo | È possibile scegliere il blocco CIDR IPv4 per il VPC oppure allocare un blocco CIDR da Amazon VPC IP Address Manager (IPAM). Per ulteriori informazioni, consulta Cos'è IPAM? nella Guida per l'utente IPAM di Amazon VPC. | Puoi importare il tuo blocco CIDR IPv6 per AWS il tuo VPC, scegliere un blocco CIDR IPv6 fornito da Amazon oppure allocare un blocco CIDR da Amazon VPC IP Address Manager (IPAM). Per ulteriori informazioni, consulta Cos'è IPAM? nella Guida per l'utente IPAM di Amazon VPC. |
| Accesso a Internet | Richiede un gateway Internet. | Richiede un gateway Internet. Supporta la comunicazione solo in uscita utilizzando un gateway Internet egress-only. |
| Indirizzi IP elastici | Supportato. Assegna a un'istanza EC2 un indirizzo IPv4 pubblico statico permanente. | Non supportato. Gli EIP consentono di mantenere statico l'indirizzo IPv4 pubblico di un'istanza anche dopo il riavvio dell'istanza stessa. Gli indirizzi IPv6 sono statici per impostazione predefinita. |

| Caratteristica | IPv4 | IPv6 |
| --- | --- | --- |
| Gateway NAT | Supportato. Le istanze nelle sottoreti private possono connettersi a Internet tramite un gateway NAT pubblico o a risorse in altri VPC tramite un gateway NAT privato. | Supportato. Utilizzando un gateway NAT con NAT64, è possibile consentire alle istanze all'interno di una sottorete solo IPv6 di comunicar e con risorse solo IPv4 all'interno della stessa VPC, tra VPC, nelle reti on-premise o su Internet. |
| Nomi DNS | Le istanze ricevono i nomi DNS basati su IPBN o RBN forniti da Amazon. Il nome DNS viene risolto nei registri DNS selezionati per l'istanza. | Un'istanza riceve nomi DNS basati su IPBN o RBN forniti da Amazon. Il nome DNS viene risolto nei registri DNS selezionati per l'istanza. |

# Indirizzi IPv4 privati

Gli indirizzi IPv4 privati (in questo argomento chiamati anche indirizzi IP privati) non sono raggiungibili tramite Internet e si possono utilizzare per la comunicazione tra le istanze presenti nel VPC. Quando avvii un'istanza in un VPC, all'interfaccia di rete predefinita (eth0) dell'istanza viene assegnato un indirizzo IP privato primario dall'intervallo di indirizzi IPv4 della sottorete. Ciascuna istanza riceve anche un nome host DNS privato (interno) che si risolve nell'indirizzo IP privato dell'istanza. Il nome host può essere di due tipi: basato su risorse o basato su IP. Per ulteriori informazioni, consulta Denominazione delle istanze Amazon EC2. Se non specifichi un indirizzo IP privato primario, saremo noi a selezionare per tuo conto un indirizzo IP disponibile nell'intervallo della sottorete. Per ulteriori informazioni sulle interfacce di rete, consulta Elastic Network Interfaces nella Amazon EC2 User Guide.

Puoi assegnare ulteriori indirizzi IP privati, i cosiddetti indirizzi IP privati secondari, alle istanze in esecuzione in un VPC. A differenza di quello primario, un indirizzo IP privato secondario può essere riassegnato da un'interfaccia di rete a un'altra. Un indirizzo IP privato rimane associato all'interfaccia di rete quando l'istanza viene arrestata e riavviata; è rilasciato quando l'istanza viene terminata. Per ulteriori informazioni sugli indirizzi IP primari e secondari, consulta Multiple IP Addresses nella Amazon EC2 User Guide.

Ci riferiamo agli indirizzi IP privati come agli indirizzi IP compressi nell'intervallo CIDR IPv4 del VPC. La maggior parte degli intervalli di indirizzi IP del VPC rientra negli intervalli di indirizzi IP privati (non instradabili pubblicamente) specificati in RFC 1918; puoi comunque utilizzare blocchi CIDR instradabili pubblicamente nel tuo VPC. Indipendentemente dall'intervallo di indirizzi IP del VPC, non supportiamo l'accesso diretto a Internet dal blocco CIDR del VPC e neppure da un blocco CIDR instradabile pubblicamente. È necessario configurare l'accesso a Internet tramite un gateway, ad esempio un gateway Internet, un gateway privato virtuale, una AWS Site-to-Site VPN connessione o AWS Direct Connect.

Non rendiamo mai pubblico su Internet l'intervallo di indirizzi IPv4 di una sottorete.

## Indirizzi IPv4 pubblici

Tutte le sottoreti hanno un attributo che determina se un'interfaccia di rete creata nella sottorete riceve automaticamente un indirizzo IPv4 pubblico (in questo argomento denominato indirizzo IP pubblico). Di conseguenza, quando avvii un'istanza in una sottorete dotata di questo attributo, all'interfaccia di rete primaria (eth0) creata per l'istanza viene assegnato un indirizzo IP pubblico. Un indirizzo IP pubblico è associato all'indirizzo IP privato primario tramite conversione degli indirizzi di rete (network address translation, NAT).

> **Note**
>
> AWS costi per tutti gli indirizzi IPv4 pubblici, inclusi gli indirizzi IPv4 pubblici associati alle istanze in esecuzione e gli indirizzi IP elastici. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla pagina dei prezzi di Amazon VPC.

Puoi controllare se la tua istanza riceve un indirizzo IP pubblico eseguendo le seguenti operazioni:

- Modificando l'attributo di indirizzamento IP pubblico della sottorete. Per ulteriori informazioni, consulta Modifica dell'attributo di assegnazione degli indirizzi IPv4 pubblici per la sottorete.
- Abilitando o disabilitando la funzione di indirizzamento IP pubblico durante l'avvio dell'istanza, funzione che sostituisce l'attributo di indirizzamento IP pubblico della sottorete.
- Puoi annullare l'assegnazione di un indirizzo IP pubblico all'istanza dopo l'avvio gestendo gli indirizzi IP associati a un'interfaccia di rete. Per ulteriori informazioni, consulta Manage IP address nella Amazon EC2 User Guide.

L'indirizzo IP pubblico viene assegnato alla tua istanza dal pool di indirizzi IP pubblici di Amazon; non è associato al tuo account. Quando un indirizzo IP pubblico viene disassociato dalla tua istanza, viene reinserito nel pool di indirizzi e non potrai più utilizzarlo. In alcuni casi, rilasciamo l'indirizzo IP pubblico dalla tua istanza o gliene assegniamo uno nuovo. Per ulteriori informazioni, consulta Indirizzi IP pubblici nella Guida per l'utente di Amazon EC2.

Se ti occorre un indirizzo IP pubblico persistente allocato sul tuo account che puoi assegnare o rimuovere dalle istanza in base alle tue Esigenze, è preferibile utilizzare un indirizzo IP elastico. Per ulteriori informazioni, consulta Associare gli indirizzi IP elastici alle risorse nel VPC.

Se il tuo VPC può supportare i nomi host DNS, ogni istanza che riceve un indirizzo IP pubblico o un indirizzo IP elastico riceve anche un nome host DNS pubblico. Verrà risolto un nome host DNS pubblico nell'indirizzo IP pubblico dell'istanza al di fuori della rete dell'istanza e nell'indirizzo IP privato dell'istanza all'interno della sua rete. Per ulteriori informazioni, consulta Attributi DNS per il VPC.

## Indirizzi IPv6

È possibile scegliere di associare un blocco CIDR IPv6 al tuo VPC e di associare blocchi CIDR IPv6 alle proprie sottoreti. Per ulteriori informazioni, consulta i seguenti argomenti:

- Come aggiungere un blocco CIDR IPv6 al VPC.
- Come aggiungere un blocco CIDR IPv6 alla sottorete

Gli indirizzi IPv6 sono univoci a livello globale, e possono essere configurati per rimanere privati o essere raggiungibili via Internet. L'istanza riceve un indirizzo IPv6 se al VPC e alla sottorete è associato un blocco CIDR IPv6 e se una delle seguenti condizioni è vera:

- La tua sottorete è configurata per assegnare automaticamente un indirizzo IPv6 a un'istanza durante l'avvio. Per ulteriori informazioni, consulta Modifica dell'attributo di assegnazione di indirizzi IPv6 pubblici per la sottorete.
- Assegni un indirizzo IPv6 alla tua istanza durante l'avvio.
- Assegni un indirizzo IPv6 all'interfaccia di rete primaria dell'istanza dopo l'avvio.
- Assegni un indirizzo IPv6 a un'interfaccia di rete nella stessa sottorete e colleghi l'interfaccia di rete all'istanza dopo l'avvio.

Quando l'istanza riceve un indirizzo IPv6 durante l'avvio, l'indirizzo viene associato all'interfaccia di rete primaria (eth0) dell'istanza. Puoi gestire gli indirizzi IPv6 per l'interfaccia di rete primaria (eth0) delle istanze nei seguenti modi:

- Assegna o annulla l'assegnazione di indirizzi IPv6 dall'interfaccia di rete. Il numero di indirizzi IPv6 che puoi assegnare a un'interfaccia di rete e il numero di interfacce di rete collegabili a un'istanza variano a seconda del tipo di istanza. Per ulteriori informazioni, consulta Indirizzi IP per interfaccia di rete per tipo di istanza nella Guida per l'utente di Amazon EC2.
- Abilita un indirizzo IPv6 primario. Un indirizzo IPv6 primario ti consente di evitare l'interruzione del traffico verso istanze o ENI. Per ulteriori informazioni, consulta Creare un'interfaccia di rete e Gestire gli indirizzi IP nella Guida per l'utente di Amazon EC2.

Un indirizzo IPv6 persiste quando arresti e avvii o iberni e avvii un'istanza e viene rilasciato quando la termini. Non è possibile riassegnare un indirizzo IPv6 mentre è già assegnato a un'altra interfaccia di rete: devi prima annullare l'assegnazione.

Puoi verificare se le istanze sono raggiungibili tramite i loro indirizzi IPv6 controllando il routing della sottorete o tramite le regole del gruppo di sicurezza e della lista di controllo accessi di rete. Per ulteriori informazioni, consulta Riservatezza del traffico Internet in Amazon VPC.

Per ulteriori informazioni sugli intervalli di indirizzi IPv6 riservati, consulta Registro degli indirizzi a scopi speciali IPv6 IANA e RFC4291.

## Utilizzo dei propri indirizzi IP

Puoi aggiungere parte o tutto il tuo intervallo di indirizzi IPv4 o IPv6 pubblico al tuo account. AWS Continuerai a essere il titolare dell'intervallo di indirizzi, ma AWS lo pubblicizza su Internet per impostazione predefinita. Dopo aver portato l'intervallo di indirizzi a AWS, questo viene visualizzato nel tuo account come pool di indirizzi. È possibile creare un indirizzo IP elastico dal pool di indirizzi IPv4 e associare un blocco CIDR IPv6 dal pool di indirizzi IPv6 a un VPC.

Per ulteriori informazioni, consulta Bring your own IP address (BYOIP) nella Amazon EC2 User Guide.

# Utilizzo di Gestione indirizzi IP di Amazon VPC

Amazon VPC IP Address Manager (IPAM) è una funzionalità VPC che semplifica la pianificazione, il monitoraggio e il monitoraggio degli indirizzi IP per i carichi di lavoro. AWS È possibile utilizzare IPAM per allocare i CIDR degli indirizzi IP ai VPC utilizzando regole aziendali specifiche.

Per ulteriori informazioni, consulta Cos'è IPAM? nella Guida per l'utente IPAM di Amazon VPC.

# Blocchi CIDR del VPC

Gli indirizzi IP del cloud privato virtuale (VPC) sono rappresentati utilizzando la notazione routing interdominio senza classi (CIDR). Un VPC deve avere un blocco CIDR IPv4 associato. Facoltativamente, puoi associare blocchi CIDR IPv4 aggiuntivi e uno o più blocchi CIDR IPv6. Per ulteriori informazioni, consulta Indirizzi IP per i tuoi VPC e sottoreti.

Indice



## Blocchi CIDR del VPC IPv4

Quando crei un VPC, devi specificare un blocco CIDR IPv4 per il VPC. Le dimensioni del blocco consentite sono comprese tra una netmask `/16` (65.536 indirizzi IP) e una netmask `/28` (16 indirizzi IP). Dopo aver creato il VPC, potrai associare blocchi CIDR IPv4 aggiuntivi al VPC. Per ulteriori informazioni, consulta Come aggiungere un blocco CIDR IPv4 al VPC..

Quando crei un VPC, ti consigliamo di specificare un blocco CIDR dagli intervalli di indirizzi IPv4 privati, come specificato in RFC 1918.

| Intervallo RFC 1918 | Esempio di blocco CIDR |
| --- | --- |
| 10.0.0.0 - 10.255.255.255 (prefisso 10/8) | 10.0.0.0/16 |
| 172.16.0.0 - 172.31.255.255 (prefisso 172.16/12) | 172.31.0.0/16 |

| Intervallo RFC 1918 | Esempio di blocco CIDR |
| --- | --- |
| 192.168.0.0 - 192.168.255.255 (prefisso 192.168/16) | 192,168,0/20 |

> **Important**
>
> Alcuni servizi utilizzano AWS la gamma CIDR. `172.17.0.0/16` Per evitare conflitti futuri, non utilizzare questo intervallo quando crei il tuo VPC. Ad esempio, servizi come AWS Cloud9 Amazon SageMaker possono riscontrare conflitti di indirizzi IP se l'intervallo di indirizzi `172.17.0.0/16` IP è già in uso in qualsiasi punto della rete. Per ulteriori informazioni, consulta Impossibile connettersi all'ambiente EC2 perché gli indirizzi IP di VPC sono utilizzati da Docker nella Guida per l'utente di AWS Cloud9 .

Puoi creare un VPC dotato di un blocco CIDR instradabile pubblicamente che non rientra negli intervalli di indirizzi IPv4 privati specificati in RFC 1918. Tuttavia, per gli scopi di questa documentazione, per indirizzi IP privati intendiamo indirizzi IPv4 compresi nell'intervallo CIDR del tuo VPC.

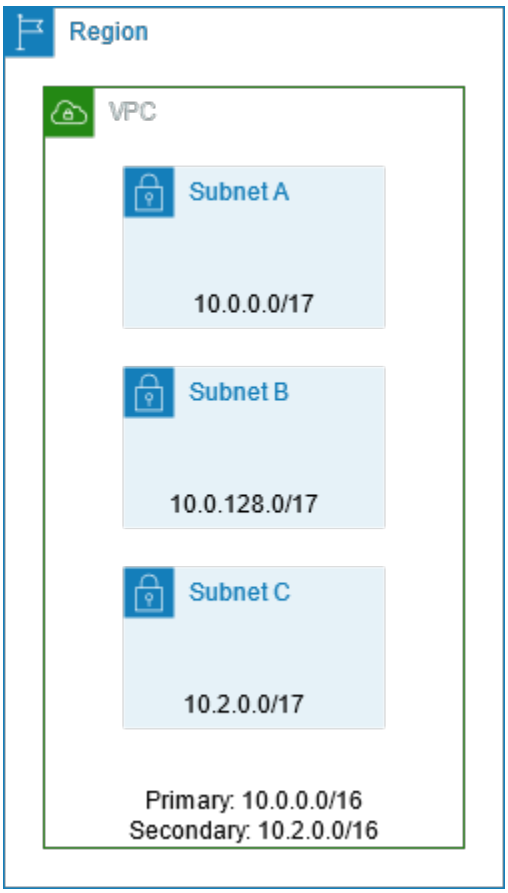
Quando crei un VPC da utilizzare con un AWS servizio, consulta la documentazione del servizio per verificare se esistono requisiti specifici per la sua configurazione.

Se si crea un VPC mediante uno strumento a riga di comando o con l'API Amazon EC2, il blocco CIDR viene modificato automaticamente nel suo formato canonico. Ad esempio, se si specifica 100.68.0.18/18 per il blocco CIDR, viene creato un blocco CIDR di 100.68.0.0/18.

## Gestione dei blocchi CIDR IPv4 per un VPC

Puoi associare blocchi CIDR IPv4 secondari al VPC. Quando associ un blocco CIDR al VPC, una route viene aggiunta automaticamente alle tabelle di routing VPC per abilitare il routing all'interno del VPC (la destinazione è il blocco CIDR e il target è `local`).

Nell'esempio seguente, il VPC dispone sia di un blocco CIDR primario che secondario. I blocchi CIDR per la sottorete A e la sottorete B provengono dal blocco CIDR VPC primario. Il blocco CIDR per la sottorete C proviene dal blocco CIDR VPC secondario.




La tabella di instradamento seguente mostra i route per il VPC.

| Destinazione | Target |
|---|---|
| 10.0.0.0/16 | Locale |
| 10.2.0.0/16 | Locale |

Per aggiungere un blocco CIDR al VPC, si applicano le seguenti regole:

- Le dimensioni di blocco consentite devono essere comprese tra una netmask `/28` e una netmask `/16`.
- Il blocco CIDR non deve sovrapporsi a qualsiasi blocco CIDR esistente associato al VPC.
- Esistono limitazioni agli intervalli di indirizzi IPv4 che puoi utilizzare. Per ulteriori informazioni, consulta Limitazioni dell'associazione blocco CIDR IPv4.
- Non puoi incrementare o decrementare la dimensione di un blocco CIDR esistente.

- Esiste una quota per il numero di blocchi CIDR che puoi associare a un VPC e al numero di route che puoi aggiungere a una tabella di instradamento. Non puoi associare un blocco CIDR se comporta il superamento delle quote. Per ulteriori informazioni, consulta Quote Amazon VPC.
- Il blocco CIDR non deve essere identico o più grande dell'intervallo CIDR di un routing in una qualsiasi delle tabelle di routing VPC. Ad esempio, in un VPC in cui si trova il blocco CIDR primario `10.2.0.0/16`, si dispone di un routing esistente in una tabella di instradamento con una destinazione di `10.0.0.0/24` a un gateway virtuale privato. Si desidera associare un blocco CIDR secondario nell'intervallo `10.0.0.0/16`. A causa del routing esistente, non è possibile associare un blocco CIDR di `10.0.0.0/24` o di dimensioni maggiori. Tuttavia, puoi associare un blocco CIDR secondario di `10.0.0.0/25` o più piccolo.
- Le seguenti regole si applicano quando aggiungi blocchi CIDR IPv4 a un VPC che fa parte di una connessione peering VPC:
  - Se la connessione peering VPC è `active`, puoi aggiungere blocchi CIDR a un VPC a condizione che non si sovrappongano a un blocco CIDR del VPC in peering.
  - Se la connessione peering VPC è `pending-acceptance`, il proprietario del VPC richiedente non può aggiungere Eventuali blocchi CIDR al VPC, a prescindere che si sovrappongano al blocco CIDR del VPC accettante. Il proprietario del VPC accettante deve accettare la connessione peering o il proprietario del VPC richiedente deve Eliminare la richiesta di connessione peering VPC, aggiungere il blocco CIDR, quindi richiedere una nuova connessione peering VPC.
  - Se la connessione peering VPC è `pending-acceptance`, il proprietario del VPC accettante può aggiungere blocchi CIDR al VPC. Se il bocco CIDR secondario si sovrappone a un blocco CIDR del VPC richiedente, la richiesta di connessione peering VPC non va a buon fine E non può essere accettata.
- Se utilizzi la connessione AWS Direct Connect a più VPC tramite un gateway Direct Connect, i VPC associati al gateway Direct Connect non devono avere blocchi CIDR sovrapposti. Se aggiungi un blocco CIDR a uno dei VPC associati al gateway Direct Connect, accertati che il nuovo blocco CIDR non si sovrapponga a un blocco CIDR esistente di qualsiasi altro VPC associato. Per ulteriori informazioni, consulta Gateway Direct Connect nella Guida per l'utente di AWS Direct Connect .
- Quando aggiungi o rimuovi un blocco CIDR, può passare attraverso vari stati: `associating` | `associated` | `disassociating` | `disassociated` | `failing` | `failed`. Il blocco CIDR è pronto per l'uso quando è nello stato `associated`.

Puoi disassociare un blocco CIDR associato al VPC; tuttavia, non puoi disassociare il blocco CIDR con cui il VPC è stato originariamente creato (il blocco CIDR principale). Per visualizzare il CIDR

principale per il VPC nella console Amazon VPC, seleziona Your VPCs (I tuoi VPC), scegli la casella di controllo relativa al VPC e scegli la scheda CIDRs (CIDR). Per visualizzare il CIDR primario utilizzando il AWS CLI, usa il comando describe-vpcs come segue. Il CIDR primario viene restituito nell'`CidrBlock element` di livello superiore.

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d --query Vpcs[*].CidrBlock --output text
```

Di seguito è riportato un output di esempio.

```
10.0.0.0/16
```

## Limitazioni dell'associazione blocco CIDR IPv4

La tabella seguente fornisce una panoramica delle associazioni di blocchi CIDR VPC consentite e limitate. Il motivo delle restrizioni è che alcuni AWS servizi utilizzano funzionalità cross-VPC e cross-account che richiedono blocchi CIDR non in conflitto sul lato del servizio. AWS

| Intervallo di indirizzo IP | Associazioni limitate | Associazioni consentite |
| --- | --- | --- |
| 10.0.0.0/8 | Blocchi CIDR da altri intervalli RFC 1918* (172.16.0.0/12 e 192.168.0 .0/16).<br><br>Se uno qualsiasi dei blocchi CIDR associati al VPC è compreso nell'inte rvallo 10.0.0.0/15 (da 10.0.0.0 a 10.1.255.255), non potrai aggiunger e un blocco CIDR dall'intervallo 10.0.0.0/16 (da 10.0.0.0 a 10.0.255. 255).<br><br>Blocchi CIDR dall'intervallo 198.19.0. 0/16. | Qualsiasi altro blocco CIDR compreso nell'intervallo 10.0.0.0/ 8 compreso tra una maschera di rete /16 e una maschera di rete /28 che non sia soggetto a restrizioni.<br><br>Qualsiasi blocco CIDR IPv4 instradab ile pubblicamente (non RFC 1918) tra una maschera di rete /16 e una maschera di rete /28 o un blocco CIDR tra una maschera di rete /16 e una maschera di rete /28 dell'inte rvallo 100.64.0.0/10. |
| 169.254.0.0/16 | I blocchi CIDR del blocco "link local" sono riservati come descritto nella | |

| Intervallo di indirizzo IP | Associazioni limitate | Associazioni consentite |
| --- | --- | --- |
| | RFC 5735 e non possono essere assegnati ai VPC. | |
| 172.16.0.0/12 | Blocchi CIDR da altri intervalli RFC 1918* (10.0.0.0/8 e 192.168.0.0/16).<br><br>Blocchi CIDR dall'intervallo 172.31.0.0/16.<br><br>Blocchi CIDR dall'intervallo 198.19.0.0/16. | Qualsiasi altro blocco CIDR dell'intervallo 172.16.0.0/12 compreso tra una netmask /16 e una netmask /28 che non sia limitato.<br><br>Qualsiasi blocco CIDR IPv4 instradabile pubblicamente (non RFC 1918) compreso tra una maschera di rete /16 e una maschera di rete /28 o un blocco CIDR tra una maschera di rete /16 e una maschera di rete /28 dell'intervallo 100.64.0.0/10. |
| 192.168.0.0/16 | Blocchi CIDR da altri intervalli RFC 1918* (10.0.0.0/8 e 172.16.0.0/12).<br><br>Blocchi CIDR dall'intervallo 198.19.0.0/16. | Qualsiasi altro blocco CIDR compreso nell'intervallo 192.168.0.0/16 compreso tra una netmask /16 e una netmask /28.<br><br>Qualsiasi blocco CIDR IPv4 instradabile pubblicamente (non RFC 1918) tra una netmask /16 e una netmask /28 o un blocco CIDR compreso nell'intervallo 100.64.0.0/10 tra una netmask /16 e una netmask /28. |
| 198.19.0.0/16 | Blocchi CIDR dagli intervalli RFC 1918*. | Qualsiasi blocco CIDR IPv4 instradabile pubblicamente (non RFC 1918) tra una netmask /16 e una netmask /28 o un blocco CIDR compreso nell'intervallo 100.64.0.0/10 tra una netmask /16 e una netmask /28. |

| Intervallo di indirizzo IP | Associazioni limitate | Associazioni consentite |
| --- | --- | --- |
| Blocco CIDR indirizzabile pubblicamente (non RFC 1918) o un blocco CIDR dall'inte rvallo 100.64.0. 0/10 | Blocchi CIDR dagli intervalli RFC 1918*.<br><br>Blocchi CIDR dall'intervallo 198.19.0. 0/16. | Qualsiasi altro blocco CIDR IPv4 instradabile pubblicamente (non RFC 1918) tra una netmask /16 e una netmask /28 o un blocco CIDR tra una netmask /16 e una netmask /28 dell'intervallo 100.64.0.0/10. |

* Intervalli RFC 1918 sono gli intervalli di indirizzi IPv4 privati specificati in RFC 1918.

## Blocchi CIDR del VPC IPv6

Puoi associare un singolo blocco CIDR IPv6 quando crei un nuovo VPC oppure puoi associare fino a cinque blocchi CIDR IPv6 da `/44` a `/60` con incrementi di `/4`. Puoi richiedere un blocco CIDR IPv6 dal pool di indirizzi IPv6 di Amazon. Per ulteriori informazioni, consulta Come aggiungere un blocco CIDR IPv6 al VPC..

Se hai associato un blocco CIDR IPv6 al VPC, potrai associare un blocco CIDR IPv6 a una sottorete esistente nel VPC o alla creazione di una nuova sottorete. Per ulteriori informazioni, consulta the section called “Dimensionamento delle sottoreti in IPv6”.

Ad esempio, crea un VPC e specifica che desideri associare al VPC un blocco CIDR IPv6 fornito da Amazon. Amazon assegna il seguente blocco CIDR IPv6 al VPC: `2001:db8:1234:1a00::/56`. Non puoi scegliere autonomamente l'intervallo di indirizzi IP. Puoi creare una sottorete E associare un blocco CIDR IPv6 da questo intervallo; ad esempio, `2001:db8:1234:1a00::/64`.

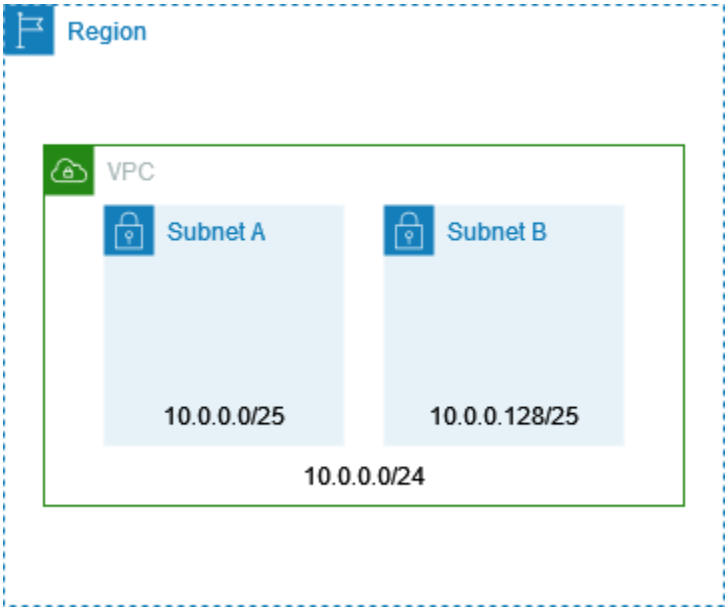
Puoi disassociare un blocco CIDR IPv6 da un VPC. Dopo aver annullato l'associazione di un blocco CIDR IPv6 a un VPC, non puoi aspettarti di ricevere lo stesso CIDR se associ nuovamente un blocco CIDR IPv6 al VPC in seguito.

# Blocchi CIDR di sottorete

Gli indirizzi IP per le sottoreti sono rappresentati utilizzando la notazione routing interdominio senza classi (CIDR). Il blocco CIDR di una sottorete può essere identico al blocco CIDR per il VPC (per una

sottorete singola nel VPC) o una sottorete del blocco CIDR per il VPC (per creare più sottoreti nel VPC). Se crei più di una sottorete in un VPC, i blocchi CIDR delle sottoreti non possono sovrapporsi.

Ad esempio, se crei un VPC con blocco CIDR `10.0.0.0/24`, supporta 256 indirizzi IP. Puoi suddividere questo blocco CIDR in due sottoreti, ciascuna delle quali supporta 128 indirizzi IP. Una sottorete utilizza il blocco CIDR `10.0.0.0/25` (per indirizzi `10.0.0.0` - `10.0.0.127`) e l'altra utilizza il blocco CIDR `10.0.0.128/25` (per indirizzi `10.0.0.128` - `10.0.0.255`).




Su Internet sono disponibili alcuni strumenti che facilitano il calcolo e la creazione di blocchi CIDR di sottoreti IPv4 e IPv6. Puoi trovare strumenti che soddisfano le tue esigenze cercando termini come "calcolatore di sottoreti" o "calcolatore CIDR". Anche il gruppo di progettazione della rete può facilitare la determinazione dei blocchi CIDR IPv4 e IPv6 da specificare per le sottoreti.

## Dimensionamento delle sottoreti per IPv4

Le dimensioni di blocco CIDR IPv4 consentite per una sottorete sono comprese tra una maschera di rete `/28` e una maschera di rete `/16`. I primi quattro indirizzi IP e l'ultimo indirizzo IP in ogni blocco CIDR della sottorete non sono disponibili per l'utilizzo e non possono essere assegnati a una risorsa, ad esempio a un'istanza EC2. Ad esempio, in una sottorete con blocco CIDR `10.0.0.0/24`, i cinque indirizzi IP seguenti sono riservati:

- 10.0.0.0: indirizzo di rete.
- 10.0.0.1: Riservato da AWS per il router VPC.
- 10.0.0.2: Riservato da. AWS L'indirizzo IP del server DNS è la base dell'intervallo di rete VPC più due. Per VPC con più blocchi CIDR, l'indirizzo IP del server DNS si trova nel CIDR principale. Ci

riserviamo anche la base di ogni intervallo di sottorete più due per tutti i blocchi CIDR nel VPC. Per ulteriori informazioni, consulta Server DNS Amazon.

- 10.0.0.3: Riservato da per AWS utilizzi futuri.
- 10.0.0.255: indirizzo di trasmissione di rete. Non supportiamo la trasmissione in un VPC, pertanto riserviamo questo indirizzo.

Se si crea una sottorete mediante uno strumento a riga di comando o con l'API Amazon EC2, il blocco CIDR viene modificato automaticamente nel suo formato canonico. Ad esempio, se si specifica 100.68.0.18/18 per il blocco CIDR, viene creato un blocco CIDR di 100.68.0.0/18.

Se si AWS utilizza BYOIP per un intervallo di indirizzi IPv4, è possibile utilizzare tutti gli indirizzi IP dell'intervallo, incluso il primo indirizzo (l'indirizzo di rete) e l'ultimo indirizzo (l'indirizzo di trasmissione).

## Dimensionamento delle sottoreti in IPv6

Se hai associato un blocco CIDR IPv6 al VPC, puoi associare un blocco CIDR IPv6 a una sottorete Esistente nel VPC o quando crei una nuova sottorete. Le lunghezze possibili delle netmask IPv6 sono comprese tra `/44` e `/64` con incrementi di `/4`.

Ci sono strumenti disponibili su Internet per aiutarti a calcolare e creare blocchi CIDR di sottoreti IPv6. È possibile trovare strumenti che soddisfano le proprie esigenze cercando termini come "calcolatore di sottorete IPv6" o "Calcolatore CIDR IPv6". Inoltre, il gruppo di progettazione della rete può aiutare a determinare i blocchi CIDR IPv6 da specificare per le sottoreti.

I primi quattro indirizzi IPv6 e l'ultimo indirizzo IPv6 in ogni blocco CIDR della sottorete non sono disponibili per l'utilizzo e non possono essere assegnati a un'istanza EC2. Ad esempio, in una sottorete con blocco CIDR `2001:db8:1234:1a00/64`, i cinque indirizzi IP seguenti sono riservati:

- `2001:db8:1234:1a00::`
- `2001:db8:1234:1a00::1`: Riservato da AWS per il router VPC.
- `2001:db8:1234:1a00::2`
- `2001:db8:1234:1a00::3`
- `2001:db8:1234:1a00:ffff:ffff:ffff:ffff`

Oltre all'indirizzo IP riservato da AWS per il router VPC nell'esempio precedente, i seguenti indirizzi IPv6 sono riservati al router VPC predefinito:

- Un indirizzo IPv6 locale del collegamento nell'intervallo FE80::/10 generato utilizzando EUI-64. Per ulteriori informazioni sugli indirizzi locali del collegamento, consulta Indirizzo locale del collegamento.
- L'indirizzo IPv6 locale del collegamento `FE80:ec2::1`.

Se è necessario comunicare con il router VPC tramite IPv6, è possibile configurare le applicazioni in modo che comunichino con l'indirizzo più adatto alle proprie esigenze.

# Raggruppamento di blocchi CIDR utilizzando elenchi di prefissi gestiti

Un elenco di prefissi gestiti è un set di uno o più blocchi CIDR. Puoi utilizzare gli elenchi di prefissi per semplificare la configurazione e la gestione dei gruppi di sicurezza e delle tabelle di routing. Puoi creare un elenco di prefissi dagli indirizzi IP utilizzati di frequente e fare riferimento ad essi come set nelle regole e nelle route dei gruppi di sicurezza anziché fare riferimento a tali indirizzi singolarmente. Ad esempio, puoi consolidare le regole dei gruppi di sicurezza con blocchi CIDR diversi ma la stessa porta e protocollo in un'unica regola che utilizza un elenco di prefissi. Se ridimensioni la rete e hai bisogno di consentire il traffico da un altro blocco CIDR, puoi aggiornare l'elenco di prefissi pertinente e tutti i gruppi di sicurezza che utilizzano quell'elenco dei prefissi saranno aggiornati. È inoltre possibile utilizzare elenchi di prefissi gestiti con altri AWS account utilizzando Resource Access Manager (RAM).

Esistono due tipi di elenchi di prefissi:

- Elenchi di prefissi gestiti dal cliente: i set di intervalli di indirizzi IP definiti e gestiti dall'utente. È possibile condividere l'elenco dei prefissi con altri AWS account, consentendo a tali account di fare riferimento all'elenco dei prefissi nelle proprie risorse.
- AWS-elenchi di prefissi gestiti: set di intervalli di indirizzi IP per i servizi. AWS Non è possibile creare, modificare, condividere o eliminare un elenco di prefissi gestiti da AWS.

Indice

- Utilizzo di elenchi di prefissi condivisi
- Riferimento a elenchi di prefissi nelle risorse AWS

## Concetti e regole degli elenchi di prefissi

Un elenco di prefissi è costituito da voci. Ogni voce è costituita da un blocco CIDR e, facoltativamente, da una descrizione del blocco CIDR.

Elenchi di prefissi gestiti dal cliente

Le regole seguenti si applicano agli elenchi di prefissi gestiti dal cliente:

- Un elenco di prefissi supporta solo un singolo tipo di indirizzamento IP (IPv4 o IPv6). Non è possibile combinare blocchi CIDR IPv4 e IPv6 in un unico elenco di prefissi.
- Un elenco di prefissi si applica solo alla regione in cui è stato creato.
- Quando si crea un elenco di prefissi, è necessario specificare il numero massimo di voci supportate dall'elenco di prefissi.
- Quando fai riferimento a un elenco di prefissi in una risorsa, il numero massimo di voci per gli elenchi di prefissi viene conteggiato rispetto alla quota del numero di voci per la risorsa. Ad esempio, se crei un elenco di prefissi con 20 voci e fai riferimento a tale elenco in una regola di gruppo di sicurezza, questo valore viene conteggiato come 20 regole per il gruppo di sicurezza.
- Quando si fa riferimento a un elenco di prefissi in una tabella di instradamento, vengono applicate le regole di priorità della route. Per ulteriori informazioni, consulta Elenco di priorità di route e prefisso.
- È possibile modificare un elenco di prefissi. Quando si aggiungono o si rimuovono voci, viene creata una nuova versione dell'elenco di prefissi. Le risorse che fanno riferimento al prefisso utilizzano sempre la versione corrente (più recente). È possibile ripristinare le voci da una versione precedente dell'elenco di prefissi, creando così una nuova versione.
- Esistono quote relative agli elenchi di prefissi. Per ulteriori informazioni, consulta Elenchi di prefissi gestiti dal cliente.
- Gli elenchi di prefissi gestiti dal cliente sono disponibili in tutte le AWS regioni commerciali (incluse le regioni GovCloud (Stati Uniti) e Cina).

AWS Elenchi di prefissi gestiti da

Le seguenti regole si applicano agli elenchi di prefissi AWS-managed:

- Non è possibile creare, modificare, condividere o eliminare un elenco di prefissi AWS-managed.
- I diversi elenchi di prefissi AWS-managed hanno un peso diverso quando vengono utilizzati. Per ulteriori informazioni, consulta Peso dell'elenco dei prefissi gestiti da AWS.
- Non è possibile visualizzare il numero di versione di un elenco di prefissi AWS-managed.

## Identity and access management per gli elenchi di prefissi

Per impostazione predefinita, gli utenti non dispongono delle autorizzazioni per creare, visualizzare, modificare o eliminare elenchi di prefissi. È possibile creare una policy IAM e collegarla a un ruolo che consenta agli utenti di utilizzare gli elenchi di prefissi.

Per visualizzare un elenco delle azioni Amazon VPC e le chiavi delle risorse e delle condizioni che puoi utilizzare in una policy IAM, consulta Azioni, Risorse e Chiavi condizione per Amazon EC2 nella Guida dell'utente IAM.

La policy di esempio seguente consente agli utenti di visualizzare e utilizzare solo l'elenco di prefissi `pl-123456abcde123456`. Gli utenti non possono creare o eliminare elenchi di prefissi.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:ModifyManagedPrefixList",
        "ec2:RestoreManagedPrefixListVersion"
      ],
      "Resource": "arn:aws:ec2:region:account:prefix-list/pl-123456abcde123456"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeManagedPrefixLists",
      "Resource": "*"
    }
   ]
}
```

Per ulteriori informazioni sull'utilizzo di IAM in Amazon VPC, consulta Identity and Access Management per Amazon VPC.

# Utilizzo degli elenchi di prefissi gestiti dal cliente

È possibile creare e gestire gli elenchi di prefissi gestiti dal cliente. È possibile visualizzare gli elenchi di prefissi AWS-managed.

Attività

- Creazione di un elenco di prefissi
- Visualizzazione di elenchi di prefissi
- Visualizzazione delle voci per un elenco di prefissi
- Visualizzazione delle associazioni (riferimenti) per l'elenco di prefissi
- Modifica di un elenco di prefissi
- Ridimensionamento di un elenco di prefissi
- Ripristino di una versione precedente di un elenco di prefissi
- Eliminazione di un elenco di prefissi

## Creazione di un elenco di prefissi

Quando si crea un elenco di prefissi, è necessario specificare il numero massimo di voci supportate dall'elenco di prefissi.

Limitazione

Non è possibile aggiungere un elenco di prefissi a una regola del gruppo di sicurezza se il numero di regole più le voci massime per l'elenco dei prefissi supera la quota per le regole per gruppo di sicurezza per l'account.

Per creare un elenco di prefissi utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elenchi di prefissi gestiti.
3. Scegliere Crea un elenco di prefissi.
4. In Nome dell'elenco di prefissi, immettere un nome per l'elenco di prefissi.
5. Per Numero massimo di voci, immettere il numero massimo di voci per l'elenco di prefissi.
6. Per Famiglia di indirizzi, scegliere se l'elenco di prefissi supporta le voci IPv4 o IPv6.

7. Per Voci dell'elenco di prefissi, scegliere Aggiungi nuova voce e immettere il blocco CIDR e una descrizione per la voce. Ripetere questa fase per ogni voce.
8. (Facoltativo) Per Tag, aggiungere tag all'elenco di prefissi per consentirne l'identificazione in un secondo momento.
9. Scegliere Crea un elenco di prefissi.

Per creare un elenco di prefissi utilizzando AWS CLI

Utilizza il comando create-managed-prefix-list.

## Visualizzazione di elenchi di prefissi

È possibile visualizzare gli elenchi di prefissi, gli elenchi di prefissi condivisi e gli elenchi di prefissi gestiti da AWS.

Per visualizzare gli elenchi di prefissi utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elenchi di prefissi gestiti.
3. La colonna Owner ID mostra l'ID dell' AWS account del proprietario dell'elenco di prefissi. Per gli elenchi di prefissi AWS-managed, l'ID proprietario è. AWS

Per visualizzare gli elenchi di prefissi utilizzando il AWS CLI

Utilizza il comando describe-managed-prefix-lists.

## Visualizzazione delle voci per un elenco di prefissi

È possibile visualizzare le voci degli elenchi di prefissi, degli elenchi di prefissi condivisi con l'utente e degli elenchi di prefissi AWS-managed.

Per visualizzare le voci di un elenco di prefissi utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elenchi di prefissi gestiti.
3. Selezionare la casella di controllo relativa all'elenco di prefissi.
4. Nel riquadro inferiore scegliere Voci per visualizzare le voci dell'elenco di prefissi.

Per visualizzare le voci di un elenco di prefissi, utilizzare AWS CLI

Utilizzate il comando get-managed-prefix-list-entries.

## Visualizzazione delle associazioni (riferimenti) per l'elenco di prefissi

È possibile visualizzare gli ID e i proprietari delle risorse associate all'elenco di prefissi. Le risorse associate sono risorse che fanno riferimento all'elenco di prefissi nelle relative voci o regole.

Limitazione

Non è possibile visualizzare le risorse associate per un elenco di prefissi AWS-managed.

Per visualizzare le associazioni degli elenchi di prefissi utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elenchi di prefissi gestiti.
3. Selezionare la casella di controllo relativa all'elenco di prefissi.
4. Nel riquadro inferiore scegliere Associazioni per visualizzare le risorse che fanno riferimento all'elenco di prefissi.

Per visualizzare le associazioni degli elenchi di prefissi, utilizzare AWS CLI

Utilizzare il comando get-managed-prefix-list-associations.

## Modifica di un elenco di prefissi

È possibile modificare il nome dell'elenco di prefissi e aggiungere o rimuovere voci. Per modificare il numero massimo di voci, consulta Ridimensionamento di un elenco di prefissi.

L'aggiornamento delle voci di un elenco di prefissi crea una nuova versione dell'elenco di prefissi. L'aggiornamento del nome o del numero massimo di voci di un elenco di prefissi non crea una nuova versione dell'elenco di prefissi.

Considerazioni

- Non è possibile modificare un elenco di prefissi AWS-managed.
- Quando si aumenta il numero massimo di voci in un elenco di prefissi, la dimensione massima aumentata viene applicata alla quota di voci per le risorse che fanno riferimento all'elenco di

prefissi. Se una di queste risorse non è in grado di supportare la dimensione massima aumentata, l'operazione di modifica ha esito negativo e viene ripristinata la dimensione massima precedente.

Per modificare un elenco di prefissi utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elenchi di prefissi gestiti.
3. Selezionare la casella di controllo dell'elenco di prefissi e scegliere Operazioni, Modifica elenco di prefissi.
4. In Nome dell'elenco di prefissi, immettere un nuovo nome per l'elenco di prefissi.
5. Per Voci dell'elenco di prefissi, scegliere Rimuovi per rimuovere una voce esistente. Per aggiungere una nuova voce, scegliere Aggiungi nuova voce e immettere il blocco CIDR e una descrizione per la voce.
6. Scegliere Salva l'elenco di prefissi.

Per modificare un elenco di prefissi utilizzando il AWS CLI

Utilizza il comando modify-managed-prefix-list.

## Ridimensionamento di un elenco di prefissi

È possibile ridimensionare un elenco di prefissi e modificare il numero massimo di voci per l'elenco di prefissi fino a 1.000. Per ulteriori informazioni sulle quote degli elenchi di prefissi gestite dal cliente, consulta Elenchi di prefissi gestiti dal cliente.

Ridimensionamento di un elenco di prefissi utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elenchi di prefissi gestiti.
3. Seleziona la casella di controllo dell'elenco di prefissi e scegli Actions (Operazioni), Resize prefix list (Ridimensiona elenco di prefissi).
4. Per New max entries (Massimo nuove voci), inserisci un valore.
5. Scegliere Ridimensiona.

Per ridimensionare un elenco di prefissi utilizzando il AWS CLI

Utilizza il comando modify-managed-prefix-list.

## Ripristino di una versione precedente di un elenco di prefissi

È possibile ripristinare le voci da una versione precedente dell'elenco di prefissi. In questo modo viene creata una nuova versione dell'elenco di prefissi.

Se le dimensioni dell'elenco di prefissi vengono ridotte, è necessario assicurarsi che l'elenco di prefissi sia sufficientemente grande da contenere le voci della versione precedente.

Per ripristinare una versione precedente di un elenco di prefissi utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elenchi di prefissi gestiti.
3. Selezionare la casella di controllo per l'elenco di prefissi e scegliere Operazioni, Ripristina elenco di prefissi.
4. Per Seleziona versione dell'elenco di prefissi selezionare una versione precedente. Le voci per la versione selezionata vengono visualizzate in Voci dell'elenco di prefissi.
5. Scegliere Ripristina l'elenco di prefissi.

Per ripristinare una versione precedente di un elenco di prefissi utilizzando AWS CLI

Utilizzate il comando restore-managed-prefix-list-version.

## Eliminazione di un elenco di prefissi

Per eliminare un elenco di prefissi, è necessario innanzitutto rimuovere tutti i riferimenti ad esso contenuti nelle risorse (ad esempio nelle tabelle di routing). Se l'elenco di prefissi è stato condiviso utilizzando AWS RAM, tutti i riferimenti nelle risorse di proprietà del consumatore devono prima essere rimossi.

Limitazione

Non è possibile eliminare un elenco di prefissi AWS-managed.

Per eliminare un elenco di prefissi utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elenchi di prefissi gestiti.

3. Selezionare l'elenco di prefissi e scegliere Operazioni, Elimina l'elenco di prefissi.
4. Nella finestra di dialogo di conferma immettere `delete` e quindi scegliere Elimina.

Per eliminare un elenco di prefissi utilizzando il AWS CLI

Utilizza il comando delete-managed-prefix-list.

# Lavora con gli elenchi di AWS prefissi -managed

AWS-managed prefix list sono insiemi di intervalli di indirizzi IP per i servizi. AWS

Indice



## Usa un elenco di prefissi AWS-managed

AWS Gli elenchi di prefissi -managed vengono creati e gestiti da AWS e possono essere utilizzati da chiunque disponga di un account. AWS Non è possibile creare, modificare, condividere o eliminare un elenco di prefissi AWS-managed.

Analogamente agli elenchi di prefissi gestiti dal cliente, è possibile utilizzare gli elenchi di prefissi AWS-managed con AWS risorse come gruppi di sicurezza e tabelle di routing. Per ulteriori informazioni, consulta Riferimento a elenchi di prefissi nelle risorse AWS.

## Peso dell'elenco dei prefissi gestiti da AWS

Il peso di un elenco di prefissi AWS-managed si riferisce al numero di voci che occupa in una risorsa.

Ad esempio, il peso di un elenco di prefissi CloudFront gestiti da Amazon è 55. Ecco come questo influisce sulle quote Amazon VPC:

- Gruppi di sicurezza: la quota predefinita è di 60 regole, lasciando spazio a solo 5 regole aggiuntive in un gruppo di sicurezza. È possibile richiedere un aumento di questa quota.
- Tabelle di instradamento: la quota predefinita è di 50 instradamenti, quindi prima di poter aggiungere l'elenco dei prefissi a una tabella di instradamento è necessario richiedere un aumento di quota.

## Elenchi di AWS prefissi gestiti disponibili

I seguenti servizi forniscono elenchi di prefissi AWS gestiti.

| Servizio AWS | Nome elenco dei prefissi | Weight |
|---|---|---|
| Amazon CloudFront | com.amazonaws.global.cloudfront.origin-facing | 55 |
| Amazon DynamoDB | com.amazonaws.*region*dynamodb | 1 |
| AWS Ground Station | com.amazonaws.global.groundstation | 5 |
| Amazon Route 53 | com.amazonaws.*region*.ipv6.route53-healthchecks | 25 |
| | com.amazonaws.*region*.route53-healthchecks | 25 |
| Amazon S3 | com.amazonaws.*region*.s3 | 1 |
| Amazon S3 Express One Zone | com.amazonaws.*region*.s3express | 6 |
| Amazon VPC Lattice | com.amazonaws.*regione*.vpc-lattice | 10 |
| | com.amazonaws.*region*.ipv6.vpc-lattice | 10 |

Per visualizzare gli elenchi AWS di prefissi gestiti utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elenchi di prefissi gestiti.
3. Nel campo di ricerca aggiungi il filtro Owner ID: AWS.

Per visualizzare gli elenchi dei AWS prefissi -managed utilizzando il AWS CLI

Utilizza il comando describe-managed-prefix-lists come riportato di seguito.

```
aws ec2 describe-managed-prefix-lists --filters Name=owner-id,Values=AWS
```

# Utilizzo di elenchi di prefissi condivisi

Con AWS Resource Access Manager (AWS RAM), il proprietario di un elenco di prefissi può condividere un elenco di prefissi con quanto segue:

- AWS Account specifici all'interno o all'esterno della sua organizzazione in AWS Organizations
- Un'unità organizzativa all'interno della propria organizzazione in AWS Organizations
- Un'intera organizzazione in AWS Organizations

I consumatori con cui è stato condiviso un elenco di prefissi possono visualizzare l'elenco dei prefissi e le relative voci e possono fare riferimento all'elenco dei prefissi nelle proprie risorse. AWS

Per ulteriori informazioni in merito AWS RAM, consulta la Guida per l'AWS RAM utente.

Indice



## Prerequisiti per la condivisione degli elenchi di prefissi

- Per condividere un elenco di prefissi, è necessario possederlo. Non è possibile condividere un elenco di prefissi che è stato condiviso con te. Non è possibile condividere un elenco di prefissi AWS-managed.
- Per condividere un elenco di prefissi con la tua organizzazione o un'unità organizzativa in AWS Organizations, devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilitare la condivisione con AWS Organizations nella Guida per l'utente di AWS RAM .

## Condivisione di un elenco di prefissi

Per condividere un elenco di prefissi, è necessario aggiungerlo a una condivisione di risorse. Se non si dispone di una condivisione di risorse, è innanzitutto necessario crearne una utilizzando la console AWS RAM.

Se fai parte di un'organizzazione e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso all'elenco di prefissi condivisi. AWS Organizations In caso contrario, i consumatori ricevono l'invito a partecipare alla condivisione di risorse e, dopo averlo accettato, ottengono l'accesso all'elenco di prefissi condiviso.

È possibile creare una condivisione di risorse e condividere un elenco di prefissi di cui si è proprietari utilizzando la console AWS RAM o l' AWS CLI.

Per creare una condivisione di risorse e condividere un elenco di prefissi utilizzando la console AWS RAM

Segui la procedura descritta in Creazione di una condivisione di risorse nella Guida per l'utente di AWS RAM . In Seleziona il tipo di risorsa, scegliere Elenchi di prefissi, quindi selezionare la casella di controllo relativa all'elenco di prefissi.

Per aggiungere un elenco di prefissi a una condivisione di risorse esistente utilizzando la console AWS RAM

Per aggiungere un prefisso gestito di proprietà a una condivisione di risorse esistente, attenersi alla procedura descritta in Aggiornamento di una condivisione di risorse nella Guida per l'utente di AWS RAM . In Seleziona il tipo di risorsa, scegliere Elenchi di prefissi, quindi selezionare la casella di controllo relativa all'elenco di prefissi.

Per condividere un elenco di prefissi di tua proprietà, utilizza il AWS CLI

Utilizzare i seguenti comandi per creare e aggiornare una condivisione di risorse:

- create-resource-share
- associate-resource-share
- update-resource-share

## Identificazione di un elenco di prefissi condiviso

Proprietari e consumatori possono identificare gli elenchi di prefissi condivisi mediante la console Amazon VPC e AWS CLI.

Per identificare un elenco di prefissi condiviso utilizzando la console Amazon VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elenchi di prefissi gestiti.
3. Nella pagina vengono visualizzati gli elenchi di prefissi di cui si è proprietari e gli elenchi di prefissi condivisi con l'utente. La colonna ID proprietario mostra l'ID dell'account AWS del proprietario dell'elenco di prefissi.
4. Per visualizzare le informazioni sulla condivisione delle risorse per un elenco di prefissi, selezionarlo e scegliere Condivisione nel riquadro inferiore.

Per identificare un elenco di prefissi condiviso utilizzando AWS CLI

Utilizza il comando describe-managed-prefix-lists. Il comando restituisce gli elenchi di prefissi di cui sei proprietario e gli elenchi di prefissi condivisi con te. `OwnerId`mostra l'ID dell' AWS account del proprietario dell'elenco di prefissi.

## Identificazione dei riferimenti a un elenco di prefissi condiviso

I proprietari possono identificare le risorse di proprietà del consumer che fanno riferimento a un elenco di prefissi condiviso.

Per identificare i riferimenti a un elenco di prefissi condiviso utilizzando la console Amazon VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elenchi di prefissi gestiti.
3. Selezionare l'elenco dei prefissi e scegliere Associazioni nel riquadro inferiore.
4. Gli ID delle risorse che fanno riferimento all'elenco di prefissi sono elencati nella colonna ID risorsa. I proprietari delle risorse sono elencati nella colonna Proprietario della risorsa.

Per identificare i riferimenti a un elenco di prefissi condiviso utilizzando AWS CLI

Utilizzare il comando get-managed-prefix-list-associations.

## Annullamento della condivisione di un elenco di prefissi condiviso

Quando si annulla la condivisione di un elenco di prefissi, i consumatori non possono più visualizzare l'elenco di prefissi o le relative voci nel proprio account e non possono fare riferimento all'elenco di prefissi nelle proprie risorse. Se nelle risorse del consumatore esistono già riferimenti all'elenco di prefissi condiviso, tali riferimenti continuano a funzionare normalmente ed è possibile continuare a visualizzarli. Se si aggiorna l'elenco di prefissi a una nuova versione, i riferimenti utilizzano la versione più recente.

Per annullare la condivisione di un elenco di prefissi condiviso di cui sei proprietario, devi rimuoverlo dalla condivisione di risorse utilizzando. AWS RAM

Per annullare la condivisione di un elenco di prefissi condiviso di cui sei proprietario utilizzando la console AWS RAM

ConsultaAggiornamento di una condivisione di risorse nella Guida per l'utente di AWS RAM .

Per annullare la condivisione di un elenco di prefissi condiviso di cui sei proprietario, utilizza AWS CLI

Utilizza il comando disassociate-resource-share.

## Autorizzazioni dell'elenco di prefissi condivisi

### Autorizzazioni per i proprietari

I proprietari sono responsabili della gestione di un elenco di prefissi condiviso e delle relative voci. I proprietari possono visualizzare gli ID delle AWS risorse che fanno riferimento all'elenco dei prefissi. Tuttavia, non possono aggiungere o rimuovere riferimenti a un elenco di prefissi nelle AWS risorse di proprietà dei consumatori.

I proprietari non possono eliminare un elenco di prefissi se in una risorsa di proprietà di un consumatore esiste un riferimento a tale elenco.

### Autorizzazioni per gli utenti

I consumatori possono visualizzare le voci in un elenco di prefissi condiviso e possono fare riferimento a un elenco di prefissi condiviso nelle proprie risorse. AWS Tuttavia, i consumatori non possono modificare, ripristinare o eliminare un elenco di prefissi condiviso.

## Fatturazione e misurazione

Non sono previsti costi aggiuntivi per la condivisione di elenchi di prefissi condivisi.

### Quote per AWS RAM

Per ulteriori informazioni, consultare Service quotas.

## Riferimento a elenchi di prefissi nelle risorse AWS

È possibile fare riferimento a un elenco di prefissi nelle seguenti AWS risorse.

Risorse

- Gruppi di sicurezza VPC
- Tabelle di routing di sottoreti
- Tabelle di routing del gateway di transito
- AWS Network Firewall gruppi di regole
- Controllo degli accessi di rete di Grafana gestito da Amazon
- AWS Outposts traccia i gateway locali

### Gruppi di sicurezza VPC

È possibile specificare un elenco di prefissi come origine per una regola in ingresso o come destinazione per una regola in uscita. Per ulteriori informazioni, consulta Gruppi di sicurezza.

Per fare riferimento a un elenco di prefissi in una regola di gruppo di sicurezza utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
3. Selezionare il gruppo di sicurezza da aggiornare.
4. Scegliere Actions (Operazioni), Edit inbound rules (Modifica regole in entrata) o Actions (Operazioni), Edit outbound rules (Modifica regole in uscita).
5. Scegliere Add rule (Aggiungi regola). Per Tipo, selezionare il tipo di traffico. Per Origine (regole in entrata) o Destinazione (regole in uscita), scegliere l'ID dell'elenco di prefissi.
6. Scegliere Save rules (Salva regole).

Per fare riferimento a un elenco di prefissi in una regola del gruppo di sicurezza utilizzando il AWS CLI

Utilizzare i authorize-security-group-egresscomandi authorize-security-group-ingressand. Per il parametro `--ip-permissions`, specificare l'ID dell'elenco di prefissi utilizzando `PrefixListIds`.

### Tabelle di routing di sottoreti

È possibile specificare un elenco di prefissi come destinazione per la voce della tabella di instradamento. Non è possibile fare riferimento a un elenco di prefissi in una tabella di instradamento del gateway. Per ulteriori informazioni sulle tabelle di routing, consulta Configurare le tabelle di routing.

Per fare riferimento a un elenco di prefissi in una tabella di routing utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione selezionare Route Tables (Tabelle di routing), quindi scegliere la tabella di routing.
3. Selezionare Actions (Operazioni), Edit routes (Modifica route).
4. Per aggiungere una route scegliere Add route (Aggiungi route).
5. Per Destinazione immettere l'ID di un elenco di prefissi.
6. In Target scegliere un target.
7. Seleziona Salva modifiche.

Per fare riferimento a un elenco di prefissi in una tabella di routing utilizzando AWS CLI

Utilizzare il comando create-route (AWS CLI). Utilizzare il parametro `--destination-prefix-list-id` per specificare l'ID di un elenco di prefissi.

### Tabelle di routing del gateway di transito

È possibile specificare un elenco di prefissi come destinazione per un percorso. Per maggiori informazioni, consulta Riferimenti all'elenco dei prefissi in Gateway Amazon VPC Transit.

### AWS Network Firewall gruppi di regole

Un gruppo di AWS Network Firewall regole è un insieme riutilizzabile di criteri per l'ispezione e la gestione del traffico di rete. Se si creano gruppi di regole stateful compatibili con Suricata in, è possibile fare riferimento a un elenco di AWS Network Firewall prefissi del gruppo di regole. Per ulteriori informazioni, consulta Riferimento agli elenchi di prefissi Amazon VPC e Creazione di un gruppo di regole stateful nella Guida per gli sviluppatori AWS Network Firewall .

### Controllo degli accessi di rete di Grafana gestito da Amazon

Puoi specificare uno o più elenchi di prefissi come regola in entrata per le richieste destinate alle aree di lavoro di Grafana gestito da Amazon. Per ulteriori informazioni sul controllo degli accessi di rete delle aree di lavoro di Grafana, inclusa la modalità di riferimento a elenchi di prefissi, consulta Gestione dell'accesso di rete nella Guida per l'utente di Grafana gestito da Amazon.

### AWS Outposts traccia i gateway locali

Ogni AWS Outposts rack fornisce un gateway locale che consente di connettere le risorse Outpost alle reti locali. È possibile raggruppare i CIDR utilizzati di frequente in un elenco di prefissi e fare riferimento a questo elenco come destinazione di percorso nella tabella di routing del gateway locale. Per ulteriori informazioni, consulta Manage Local Gateway Route Table Route nella Guida per l'AWS Outposts utente dei rack.

## AWS Intervalli di indirizzi IP

AWS pubblica gli intervalli di indirizzi IP correnti in formato JSON. Con queste informazioni, è possibile identificare il traffico proveniente da. AWSÈ inoltre possibile utilizzare queste informazioni per consentire o negare il traffico da o verso alcuni AWS servizi.

> **Note**
>
> - Solo alcuni intervalli di indirizzi IP dei AWS servizi sono pubblicati in ip-ranges.json; pubblichiamo gli intervalli di indirizzi IP per i servizi su cui i clienti generalmente desiderano eseguire il filtro in uscita.
> - I servizi possono utilizzare gli intervalli di indirizzi IP per comunicare con altri servizi oppure i servizi possono utilizzare gli intervalli IP per comunicare con una rete di clienti.

Per vedere gli intervalli correnti, scarica il file `.json`. Per mantenere la cronologia, salva le versioni successive del file `.json` nel sistema. Per stabilire se ci sono state modifiche dall'ultima volta che hai salvato il file, verifica l'ora di pubblicazione del file corrente e confrontala con quella dell'ultimo file che hai salvato.

Gli intervalli di indirizzi IP a cui accedi AWS tramite Bring your own IP address (BYOIP) non sono inclusi nel `.json` file.

In alternativa, alcuni servizi pubblicano i propri intervalli di indirizzi utilizzando elenchi di prefissi AWS-managed. Per ulteriori informazioni, consulta the section called “Elenchi di AWS prefissi gestiti disponibili”.

Indice



## Scarica

Scarica ip-ranges.json.

Se accedi a questo file in modo programmatico, è tua responsabilità assicurare che l'applicazione scarichi il file solo dopo aver completato la verifica del certificato TLS presentato dal server.

## Sintassi

La sintassi di `ip-ranges.json` è la seguente.

```
{
  "syncToken": "0123456789",
  "createDate": "yyyy-mm-dd-hh-mm-ss",
  "prefixes": [
    {
      "ip_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ],
  "ipv6_prefixes": [
    {
```

```
      "ipv6_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ]
}
```

syncToken

L'ora di pubblicazione nel formato epoch Unix.

- Tipo: stringa

Esempio: `"syncToken": "1416435608"`

createDate

Data e ora di pubblicazione, in formato UTC YY-MM-DD-. hh-mm-ss

- Tipo: stringa

Esempio: `"createDate": "2014-11-19-23-29-02"`

prefissi

I prefissi IP per gli intervalli di indirizzi IPv4.

Tipo: Array

ipv6_prefixes

I prefissi IP per gli intervalli di indirizzi IPv6.

Tipo: Array

ip_prefix

L'intervallo di indirizzi IPv4 pubblici nella notazione CIDR. Nota che AWS potrebbe pubblicizzare un prefisso in intervalli più specifici. Ad esempio, il prefisso 96.127.0.0/17 nel file potrebbe essere visualizzato come 96.127.0.0/21, 96.127.8.0/21, 96.127.32.0/19 e 96.127.64.0/18.

- Tipo: stringa

Esempio: `"ip_prefix": "198.51.100.2/24"`

ipv6_prefix

L'intervallo di indirizzi IPv6 pubblici nella notazione CIDR. Nota che AWS potrebbe pubblicizzare un prefisso in intervalli più specifici.

- Tipo: stringa

Esempio: `"ipv6_prefix": "2001:db8:1234::/64"`

network_border_group

Il nome del gruppo di confine di rete, che è un insieme univoco di Availability Zones o Local Zones da cui AWS pubblicizza gli indirizzi IP, oppure`GLOBAL`. Il traffico per `GLOBAL` i servizi può essere attratto o provenire da più (fino a tutte) Zone di disponibilità o Local Zones da cui AWS pubblicizza gli indirizzi IP.

- Tipo: stringa

Esempio: `"network_border_group": "us-west-2-lax-1"`

Regione

La AWS regione o. `GLOBAL` Il traffico destinato `GLOBAL` ai servizi può essere attratto o provenire da più AWS regioni (fino a tutte).

- Tipo: stringa

Valori validi: `af-south-1` | `ap-east-1` | `ap-northeast-1` | `ap-northeast-2` | `ap-northeast-3` | `ap-south-1` | `ap-south-2` | `ap-southeast-1` | `ap-southeast-2` | `ap-southeast-3` | `ap-southeast-4` | `ca-central-1` | `cn-north-1` | `cn-northwest-1` | `eu-central-1` | `eu-central-2` | `eu-north-1` | `eu-south-1` | `eu-south-2` | `eu-west-1` | `eu-west-2` | `eu-west-3` | `me-central-1` | `me-south-1` | `sa-east-1` | `us-east-1` | `us-east-2` | `us-gov-east-1` | `us-gov-west-1` | `us-west-1` | `us-west-2` | `GLOBAL`

Esempio: `"region": "us-east-1"`

service

Il sottoinsieme di intervalli di indirizzi IP. Gli indirizzi indicati per `API_GATEWAY` sono solo in uscita. Specificare `AMAZON` per ottenere tutti gli intervalli di indirizzi IP (il che significa che ogni sottoinsieme è anche nel sottoinsieme `AMAZON`). Tuttavia, alcuni intervalli di indirizzi IP sono solo nel sottoinsieme `AMAZON` (il che significa che non sono disponibili anche in un altro sottoinsieme).

- Tipo: stringa

Valori validi: AMAZON AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | IVS_REALTIME | KINESIS_VIDEO_STREAMS | MEDIA_PACKAGE_V2 | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS

Esempio: `"service": "AMAZON"`

## Sovrapposizione di intervalli

Gli intervalli di indirizzi IP restituiti da qualsiasi codice di servizio vengono restituiti anche dal codice di servizio AMAZON. Ad esempio, tutti gli intervalli di indirizzi IP restituiti dal codice di servizio S3 vengono restituiti anche da quello AMAZON.

Quando il servizio A utilizza delle risorse provenienti dal servizio B, gli intervalli di indirizzi IP restituiti dai codici di servizio appartengono sia al servizio A che al servizio B. Tuttavia, questi intervalli di indirizzi IP vengono utilizzati esclusivamente dal servizio A, non dal servizio B. Ad esempio, Amazon S3 utilizza le risorse provenienti da Amazon EC2, per cui sono presenti intervalli di indirizzi IP che vengono restituiti sia dal codice di servizio S3 che da quello EC2. Tuttavia, questi intervalli di indirizzi IP vengono utilizzati esclusivamente da Amazon S3. Pertanto, il codice di servizio S3 restituisce tutti gli intervalli di indirizzi IP utilizzati esclusivamente da Amazon S3. Per identificare gli intervalli di indirizzi IP utilizzati esclusivamente da Amazon EC2, individua gli intervalli di indirizzi IP restituiti dal codice di servizio EC2 ma non da quello S3.

## Filtraggio del file JSON

È possibile scaricare uno strumento a riga di comando che consenta di filtrare solo le informazioni desiderate.

### Windows

AWS Tools for Windows PowerShell include un cmdlet, `Get-AWSPublicIpAddressRange`, per analizzare questo file JSON. I seguenti esempi ne illustrato l'utilizzo. Per ulteriori informazioni, vedere Interrogazione degli intervalli di indirizzi IP pubblici per AWS e Get- AWSPublicIpAddressRange.

Example 1. Come ottenere la data di creazione

```
PS C:\> Get-AWSPublicIpAddressRange -OutputPublicationDate
```

```
Wednesday, August 22, 2018 9:22:35 PM
```

Example 2. Come ottenere le informazioni su una regione specifica

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1

IpPrefix        Region      NetworkBorderGroup         Service
--------        ------       -------                   -------
23.20.0.0/14    us-east-1    us-east-1                 AMAZON
50.16.0.0/15    us-east-1    us-east-1                 AMAZON
50.19.0.0/16    us-east-1    us-east-1                 AMAZON
...
```

Example 3. Come ottenere tutti gli indirizzi IP

```
PS C:\> (Get-AWSPublicIpAddressRange).IpPrefix
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
2406:da00:ff00::/64
2600:1fff:6000::/40
2a01:578:3::/64
2600:9000::/28
```

Example 4. Come ottenere tutti gli indirizzi IPv4

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv4"} | select
 IpPrefix

IpPrefix
--------
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

Example 5. Come ottenere tutti gli indirizzi IPv6

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv6"} | select
 IpPrefix
```

```
IpPrefix
--------
2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

Example 6. Come ottenere tutti gli indirizzi IP per un servizio specifico

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey CODEBUILD | select IpPrefix

IpPrefix
--------
52.47.73.72/29
13.55.255.216/29
52.15.247.208/29
...
```

## Linux

I comandi di esempio seguenti utilizzano lo strumento jq per analizzare una copia locale del file JSON.

Example 1. Come ottenere la data di creazione

```
$ jq .createDate < ip-ranges.json

"2016-02-18-17-22-15"
```

Example 2. Come ottenere le informazioni su una regione specifica

```
$ jq '.prefixes[] | select(.region=="us-east-1")' < ip-ranges.json

{
  "ip_prefix": "23.20.0.0/14",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
```

```
  "ip_prefix": "50.16.0.0/15",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.19.0.0/16",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
...
```

Example 3. Come ottenere tutti gli indirizzi IPv4

```
$ jq -r '.prefixes | .[].ip_prefix' < ip-ranges.json

23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

Example 4. Come ottenere tutti gli indirizzi IPv6

```
$ jq -r '.ipv6_prefixes | .[].ipv6_prefix' < ip-ranges.json

2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

Example 5. Come ottenere tutti gli indirizzi IPv4 per un servizio specifico

```
$ jq -r '.prefixes[] | select(.service=="CODEBUILD") | .ip_prefix' < ip-ranges.json

52.47.73.72/29
13.55.255.216/29
52.15.247.208/29
...
```

Example 6. Come ottenere tutti gli indirizzi IPv4 per un servizio specifico in una regione specifica

```
$ jq -r '.prefixes[] | select(.region=="us-east-1") | select(.service=="CODEBUILD")
 | .ip_prefix' < ip-ranges.json

34.228.4.208/28
```

Example 7. Ottenere informazioni per un determinato gruppo di confine di rete

```
$ jq -r '.prefixes[] | select(.region=="us-west-2") |
 select(.network_border_group=="us-west-2-lax-1") | .ip_prefix' < ip-ranges.json
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

## Implementazione del controllo in uscita

Per consentire alle risorse create con un AWS servizio di accedere solo ad altri AWS servizi, puoi utilizzare le informazioni sull'intervallo di indirizzi IP nel file ip-ranges.json per eseguire il filtraggio in uscita. Assicurati che le regole del gruppo di sicurezza consentano il traffico in uscita verso i blocchi CIDR nell'elenco AMAZON. Sono previste quote per i gruppi di sicurezza. A seconda del numero di intervalli di indirizzi IP in ciascuna regione, potrebbero essere necessari più gruppi di sicurezza per regione.

> **Note**
>
> Alcuni AWS servizi sono basati su EC2 e utilizzano lo spazio degli indirizzi IP EC2. Se blocchi il traffico verso lo spazio dell'indirizzo IP EC2, blocchi anche il traffico verso questi servizi non EC2.

## AWS Intervalli di indirizzi IP, notifiche.

Ogni volta che viene apportata una modifica agli intervalli di indirizzi AWS IP, inviamo notifiche agli abbonati all'`AmazonIpSpaceChange`argomento. Il payload contiene informazioni nel formato seguente:

```
{
  "create-time":"yyyy-mm-ddThh:mm:ss+00:00",
```

```
  "synctoken":"0123456789",
  "md5":"6a45316e8bc9463c9e926d5d37836d33",
  "url":"https://ip-ranges.amazonaws.com/ip-ranges.json"
}
```

create-time

Data e ora di creazione.

Le notifiche potrebbero essere recapitate senza seguire un ordine. Consigliamo pertanto di verificare i time stamp per garantire l'ordine corretto.

synctoken

L'ora di pubblicazione nel formato epoch Unix.

md5

Il valore hash di crittografia del file `ip-ranges.json`. Puoi utilizzare questo valore per controllare se il file scaricato è danneggiato.

url

La posizione del file `ip-ranges.json`.

Se desideri ricevere una notifica ogni volta che viene apportata una modifica agli intervalli di indirizzi AWS IP, puoi abbonarti come segue per ricevere notifiche tramite Amazon SNS.

Per iscriverti alle notifiche relative all'intervallo di indirizzi AWS IP

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. Devi selezionare questa regione perché le notifiche SNS per le quali hai effettuato l'iscrizione sono state create in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Scegli Crea sottoscrizione.
5. Nella finestra di dialogo Crea sottoscrizione segui questi passaggi:
   a. In Topic ARN (ARN argomento) copia il seguente Amazon Resource Name (ARN):

```
arn:aws:sns:us-east-1:806199016981:AmazonIpSpaceChanged
```

b. In Protocol (Protocollo) scegli il protocollo da utilizzare (ad esempio `Email`).

c. In Endpoint digita l'endpoint per la ricezione della notifica (ad esempio il tuo indirizzo e-mail).

d. Scegli Crea sottoscrizione.

6. Verrai contattato sull'endpoint specificato e ti verrà chiesto di confermare la sottoscrizione. Ad esempio, se hai specificato un indirizzo e-mail, riceverai un messaggio e-mail con l'oggetto `AWS Notification - Subscription Confirmation`. Segui le istruzioni per confermare la tu sottoscrizione.

Le notifiche sono soggette alla disponibilità dell'endpoint. Pertanto, è opportuno controllare periodicamente i file JSON per essere sicuri di aver ricevuto gli intervalli più recenti. Per ulteriori informazioni sull'affidabilità di Amazon SNS, consultare https://aws.amazon.com/sns/faqs/#Reliability.

Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

Per annullare l'iscrizione alle notifiche relative agli intervalli di indirizzi AWS IP

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
3. Seleziona la casella di controllo per la sottoscrizione.
4. Scegli Actions (Operazioni), Delete subscriptions (Cancella sottoscrizioni).
5. Quando viene richiesta la conferma, seleziona Delete (Elimina).

Per ulteriori informazioni su Amazon SNS, consultare la Guida per gli sviluppatori di Amazon Simple Notification Service.

## Note di rilascio

Nella tabella seguente vengono descritti gli aggiornamenti alla sintassi di `ip-ranges.json`. Aggiungiamo anche nuovi codici regione con ogni avvio della regione.

| Descrizione | Data di rilascio |
| --- | --- |
| Aggiunto il codice `IVS_REALTIME` di servizio. | 11 giugno 2024 |

| Descrizione | Data di rilascio |
| --- | --- |
| Aggiunto il codice `MEDIA_PACKAGE_V2` di servizio. | 9 maggio 2023 |
| Aggiunto il codice `CLOUDFRONT_ORIGIN_FACING` di servizio. | 12 ottobre 2021 |
| Aggiunto il codice `ROUTE53_RESOLVER` di servizio. | 24 giugno 2021 |
| Aggiunto il codice `EBS` di servizio. | 12 maggio 2021 |
| Aggiunto il codice `KINESIS_VIDEO_STREAMS` di servizio. | 19 novembre 2020 |
| Aggiunti i codici di servizio `CHIME_MEETINGS` e `CHIME_VOICECONNECTOR` . | 19 giugno 2020 |
| Aggiunto il codice `AMAZON_APPFLOW` di servizio. | 9 giugno 2020 |
| Aggiungere il supporto per il gruppo di confine di rete. | 7 aprile 2020 |
| Aggiunto il codice `WORKSPACES_GATEWAYS` di servizio. | 30 marzo 2020 |
| Aggiunto il codice `ROUTE53_HEALTHCHECK_PUBLISHING` di servizio. | 30 gennaio 2020 |
| Aggiunto il codice `API_GATEWAY` di servizio. | 26 settembre 2019 |
| Aggiunto il codice `EC2_INSTANCE_CONNECT` di servizio. | 26 giugno 2019 |
| Aggiunto il codice `DYNAMODB` di servizio. | 25 aprile 2019 |
| Aggiunto il codice `GLOBALACCELERATOR` di servizio. | 20 dicembre 2018 |

| Descrizione | Data di rilascio |
| --- | --- |
| Aggiunto il codice `AMAZON_CONNECT` di servizio. | 20 giugno 2018 |
| Aggiunto il codice `CLOUD9` di servizio. | 20 giugno 2018 |
| Aggiunto il codice `CODEBUILD` di servizio. | 19 aprile 2018 |
| Aggiunto il codice `S3` di servizio. | 28 febbraio 2017 |
| Aggiunto il supporto per gli intervalli di indirizzi IPv6. | 22 agosto 2016 |
| Rilascio iniziale | 19 Novembre 2014 |

## Ulteriori informazioni

- `AMAZON_APPFLOW`: Intervalli di indirizzi IP
- `AMAZON_CONNECT`: Configurazione della rete
- `CHIME_MEETINGS`: Configurazione per servizi multimediali e segnalazione
- `CLOUDFRONT`— Posizioni e intervalli di indirizzi IP dei server CloudFront periferici
- `DYNAMODB`: Intervalli di indirizzi IP
- `EC2`: Indirizzi IPV4 pubblici
- `EC2_INSTANCE_CONNECT`: Prerequisiti di EC2 Instance Connect
- `GLOBALACCELERATOR`: Posizioni e intervalli di indirizzi IP dei server edge Global Accelerator
- `ROUTE53`: Intervalli di indirizzi IP di server Amazon Route 53
- `ROUTE53_HEALTHCHECKS`: Intervalli di indirizzi IP di server Amazon Route 53
- `ROUTE53_HEALTHCHECKS_PUBLISHING`: Intervalli di indirizzi IP di server Amazon Route 53
- `WORKSPACES_GATEWAYS`: Server gateway PCoIP

# Aggiungi il supporto IPv6 al tuo VPC

Se disponi di un VPC esistente che supporta solo IPv4 e risorse nella sottorete configurate per utilizzare solo IPv4, puoi aggiungere il supporto IPv6 per il tuo VPC e le tue risorse. Il VPC può

operare in modalità dual-stack: le risorse possono comunicare via IPv4, IPv6 o entrambi. Le comunicazioni IPv4 e IPv6 sono indipendenti tra loro.

Non puoi disabilitare il supporto IPv4 per il VPC e le sottoreti in quanto si tratta del sistema di indirizzamento IP predefinito per Amazon VPC e Amazon EC2.

Considerazioni

- Non esiste un percorso di migrazione da sottoreti solo IPv4 a sottoreti solo IPv6.
- Questo esempio presume che esista un VPC con sottoreti pubbliche e private. Per informazioni sulla creazione di un nuovo VPC da utilizzare con IPv6, consulta la pagina the section called “Crea un VPC”.
- Prima di iniziare a utilizzare IPv6, assicurati di aver letto le funzionalità di indirizzamento IPv6 per Amazon VPC:. Confronto tra IPv4 e IPv6

Processo

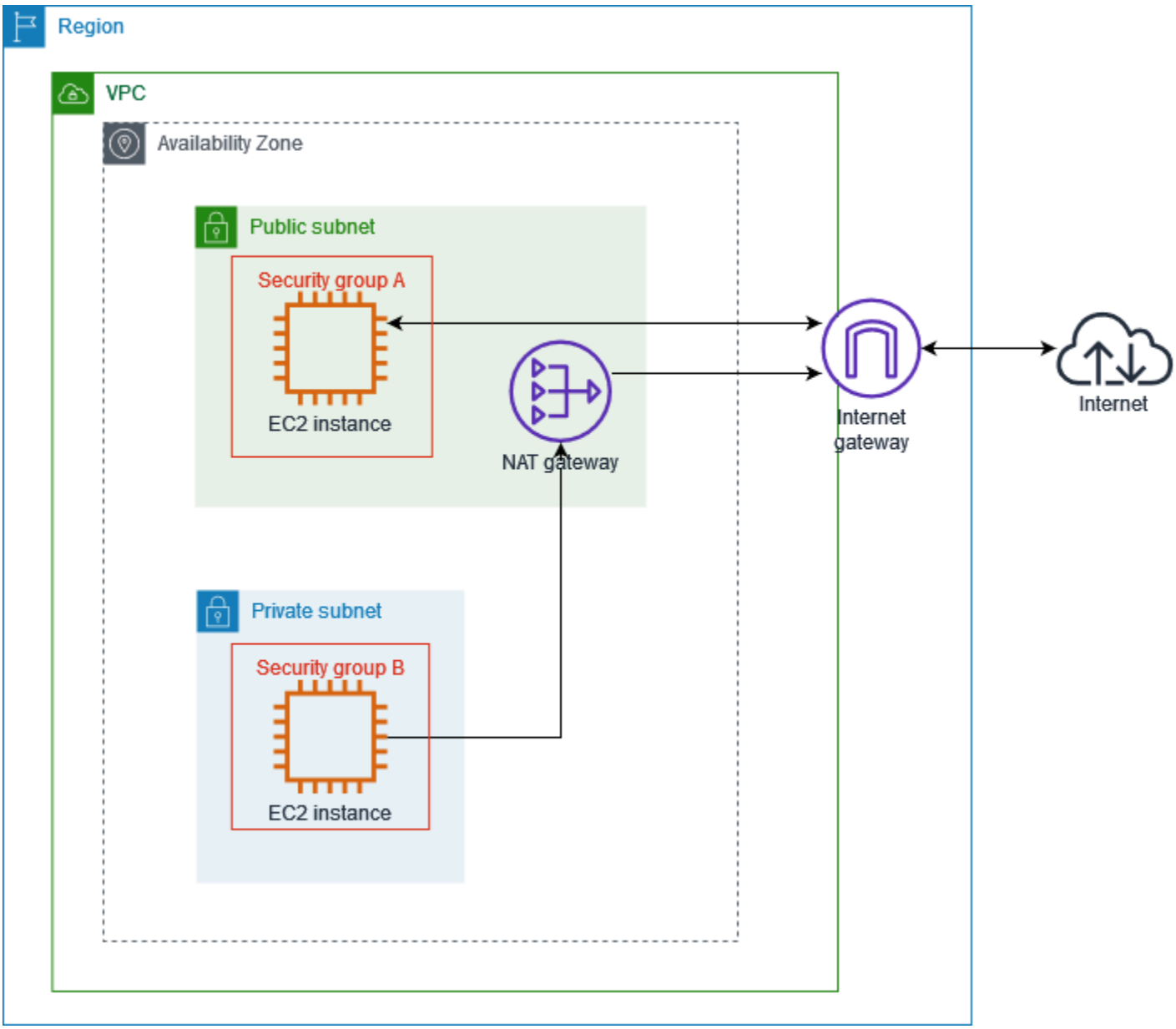
La tabella seguente fornisce una panoramica del processo per abilitare IPv6 sul VPC.

| Fase | Note |
| --- | --- |
| Fase 1: associazione di un blocco CIDR IPv6 al VPC e alle sottoreti | Associa un blocco CIDR BYOIP IPv6 o fornito da Amazon al VPC e alle sottoreti. |
| Fase 2: aggiornamento delle tabelle di routing | Aggiorna le tabelle di routing per instradare il traffico IPv6. Per una sottorete pubblica, crea una route che instrada tutto il traffico IPv6 dalla sottorete all'Internet Gateway. Per una sottorete privata, crea una route che instrada tutto il traffico IPv6 destinato a Internet dalla sottorete a un Internet Gateway egress-only. |
| Fase 3: aggiornamento delle regole di gruppo di sicurezza | Aggiorna le regole di gruppo di sicurezza per includere regole relative agli indirizzi IPv6. In questo modo, si abilita il flusso di traffico IPv6 verso e dalle istanze. Se hai creato regole di lista di controllo accessi di rete personalizzate per controllare il flusso di traffico verso e dalla |

| Fase | Note |
| --- | --- |
| | sottorete, devi includere regole per il traffico IPv6. |
| Fase 4: assegnazione di indirizzi IPv6 alle istanze | Assegna degli indirizzi IPv6 alle istanze dall'intervallo di indirizzi IPv6 della sottorete. |

## Esempio: abilitazione di IPv6 in un VPC con una sottorete pubblica e una privata

In questo esempio, il VPC ha un una sottorete pubblica e privata. Nella sottorete privata è presente un'istanza di database che ha comunicazioni in uscita con Internet via un gateway NAT nel VPC. Disponi inoltre di un server Web pubblico nella sottorete pubblica che ha accesso a Internet tramite l'Internet Gateway. Il diagramma seguente rappresenta l'architettura del tuo VPC.




Il gruppo di sicurezza per il server Web (ad esempio, con l'ID del gruppo di sicurezza `sg-11aa22bb11aa22bb1`) ha le seguenti regole in entrata:

| Type | Protocollo | Intervallo porte | Origine | Commento |
|---|---|---|---|---|
| Tutto il traffico | Tutti | Tutti | sg-33cc44 dd33cc44dd3 | Consente l'accesso in entrata per tutto il traffico dalle istanze associate |

| Type | Protocollo | Intervallo porte | Origine | Commento |
|---|---|---|---|---|
| | | | | a sg-33cc44 dd33cc44dd3 (l'istanza di database). |
| HTTP | TCP | 80 | 0.0.0.0/0 | Consente il traffico in entrata da Internet via HTTP. |
| HTTPS | TCP | 443 | 0.0.0.0/0 | Consente il traffico in entrata da Internet via HTTPS. |
| SSH | TCP | 22 | 203.0.113 .123/32 | Consente l'accesso SSH in entrata dal computer locale; ad esempio, quando devi connetterti all'istanza per eseguire attività amministrative. |

Il gruppo di sicurezza per l'istanza di database (ad esempio, con l'ID del gruppo di sicurezza `sg-33cc44dd33cc44dd3`) ha la seguente regola in entrata:

| Type | Protocollo | Intervallo porte | Origine | Commento |
|---|---|---|---|---|
| MySQL | TCP | 3306 | sg-11aa22 bb11aa22bb1 | Consente l'accesso in entrata per il traffico MySQL |

| Type | Protocollo | Intervallo porte | Origine | Commento |
| --- | --- | --- | --- | --- |
| | | | | dalle istanze associate a sg-11aa22 bb11aa22b b1 (l'istanza di server Web). |

Entrambi i gruppi di sicurezza hanno la regola in uscita predefinita che consente tutto il traffico IPv4 in uscita e nessun'altra regola in uscita.

Il server Web è il tipo di istanza `t2.medium`. Il server di database è un `m3.large`.

Vuoi che il VPC e le risorse siano abilitati per IPv6 e funzionino in modalità dual-stack; in altre parole, intendi utilizzare gli indirizzamenti IPv6 e IPv4 tra le risorse nel VPC e le risorse su Internet.

## Fase 1: associazione di un blocco CIDR IPv6 al VPC e alle sottoreti

Puoi associare un blocco CIDR IPv6 al tuo VPC e quindi un blocco CIDR `/64` di quell'intervallo a ogni sottorete.

Per associare un blocco CIDR IPv6 a un VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegliere Your VPCs (I tuoi VPC).
3. Seleziona il tuo VPC.
4. Seleziona Azioni, Modifica CIDR, quindi Aggiungi nuovo CIDR IPv6.
5. Seleziona una delle seguenti opzioni, quindi Seleziona CIDR:

   - Blocco CIDR IPv6 fornito da Amazon: richiede un blocco CIDR IPv6 dal pool di indirizzi IPv6 di Amazon. Per Network Border Group, scegli il gruppo da cui pubblicizza gli indirizzi IP. AWS
   - Blocco CIDR IPv6 allocato da IPAM: usa un blocco CIDR IPv6 da un pool IPAM. Seleziona il pool IPAM e il blocco CIDR IPv6.
   - CIDR IPv6 di mia proprietà: usa un blocco CIDR IPv6 dal pool di indirizzi IPv6 (BYOIP). Seleziona il pool di indirizzi IPv6 e il blocco CIDR IPv6.
6. Scegli Chiudi.

Per associare un blocco CIDR IPv6 a una sottorete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
3. Seleziona una sottorete.
4. Seleziona Azioni, Modifica CIDR IPv6 quindi Aggiungi CIDR IPv6.
5. Modifica il blocco CIDR in base alle esigenze (ad esempio, sostituisci il `00`).
6. Selezionare Salva.
7. Ripeti questa procedura per tutte le altre sottoreti nel VPC.

Per ulteriori informazioni, consulta Blocchi CIDR del VPC IPv6.

## Fase 2: aggiornamento delle tabelle di routing

Quando un blocco CIDR IPv6 viene associato al VPC, automaticamente viene aggiunta una route locale a ciascuna tabella di routing per consentire il traffico IPv6 all'interno del VPC.

È necessario aggiornare le tabelle di routing per le sottoreti pubbliche, per consentire alle istanze (come i server Web) di utilizzare l'Internet Gateway per il traffico IPv6. È necessario aggiornare le tabelle di routing per le sottoreti private, consentire alle istanze (come le istanze di database) di utilizzare un Internet Gateway egress-only per il traffico IPv6, poiché i gateway NAT non supportano IPv6.

Aggiornare la tabella di routing per una sottorete pubblica

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti). Seleziona la sottorete pubblica. Nella scheda Tabella di routing, seleziona l'ID della tabella di routing per aprire la pagina dei dettagli.
3. Seleziona la tabella di instradamento del . Nella scheda Route, scegli Modifica route.
4. Scegli Aggiungi route. Seleziona `::/0` per Destinazione. Scegli l'ID del gateway Internet per Target.
5. Seleziona Salvataggio delle modifiche.

Aggiornare la tabella di routing per una sottorete privata

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel riquadro di navigazione, seleziona Gateway Internet solo in uscita. Seleziona Crea gateway Internet solo in uscita. Seleziona il VPC da VPC, quindi Crea gateway Internet solo in uscita.

   Per ulteriori informazioni, consulta Abilitazione del traffico in uscita IPv6 utilizzando un gateway Internet egress-only.
3. Nel pannello di navigazione, scegli Subnets (Sottoreti). Seleziona la sottorete privata. Nella scheda Tabella di routing, seleziona l'ID della tabella di routing per aprire la pagina dei dettagli.
4. Seleziona la tabella di instradamento del . Nella scheda Route, scegli Modifica route.
5. Scegli Aggiungi route. Seleziona `::/0` per Destinazione. Scegli l'ID del gateway Internet solo in uscita per Target.
6. Seleziona Salvataggio delle modifiche.

Per ulteriori informazioni, consulta Opzioni di routing di esempio.

## Fase 3: aggiornamento delle regole di gruppo di sicurezza

Per consentire alle istanze di inviare E ricevere traffico via IPv6, devi aggiornare le regole di gruppo di sicurezza affinché includano le regole per gli indirizzi IPv6. Ad esempio, nell'esempio precedente, puoi aggiornare il gruppo di sicurezza del server Web (`sg-11aa22bb11aa22bb1`) per aggiungere regole che consentono l'accesso HTTP, HTTPS e SSH in entrata dagli indirizzi IPv6. Non è necessario apportare alcuna modifica alle regole in entrata per il gruppo di sicurezza di database. La regola che consente tutte le comunicazioni da `sg-11aa22bb11aa22bb1` include le comunicazioni IPv6.

Aggiornare le regole di gruppo di sicurezza in entrata

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona (Gruppi di sicurezza e seleziona il gruppo di sicurezza del server Web.
3. Nella scheda Regole in entrata, seleziona Modifica regole in entrata.
4. Per ogni regola che consente il traffico IPv4, seleziona Aggiungi regola e configurala per consentire il traffico IPv6 corrispondente. Ad esempio, per aggiungere una regola che consente tutto il traffico HTTP su IPv6, seleziona HTTP per Tipo e `::/0` per Origine.
5. Una volta completata l'aggiunta delle regole, seleziona Salva.

Per aggiornare le regole in uscita del gruppo di sicurezza

Quando un blocco CIDR IPv6 viene associato al VPC, una regola in uscite viene automaticamente aggiunta ai gruppi di sicurezza del VPC perché consenta tutto il traffico IPv6. Tuttavia, se hai modificato le regole in uscita originali per il gruppo di sicurezza, questa regola non viene automaticamente aggiunta e devi aggiungere regole in uscita equivalenti per il traffico IPv6.

Aggiornamento delle regole di lista di controllo accessi di rete

Quando un blocco CIDR IPv6 viene associato al VPC, automaticamente vengono aggiunte regole alla lista di controllo accessi (ACL) della rete predefinita per consentire il traffico IPv6. Tuttavia, se hai modificato la lista di controllo accessi della rete predefinita o ne hai creata una personalizzata, devi aggiungere manualmente delle regole per il traffico IPv6. Per ulteriori informazioni, consulta Utilizzo di ACL di rete.

## Fase 4: assegnazione di indirizzi IPv6 alle istanze

Tutti i tipi di istanza della generazione corrente supportano IPv6. Se il tuo tipo di istanza non supporta IPv6, devi ridimensionare l'istanza a un tipo di istanza supportato prima di poter assegnare un indirizzo IPv6. Il processo che utilizzerai dipende dalla compatibilità del nuovo tipo di istanza scelto con il tipo di istanza corrente. Per ulteriori informazioni, consulta Modifica del tipo di istanza nella Guida per l'utente di Amazon EC2. Se devi avviare un'istanza da una nuova AMI per supportare IPv6, puoi assegnare un indirizzo IPv6 all'istanza durante l'avvio.

Dopo aver verificato che tipo di istanza supporta IPv6, puoi assegnare un indirizzo IPv6 all'istanza tramite la console Amazon EC2. L'indirizzo IPv6 viene assegnato all'interfaccia di rete primaria (eth0) dell'istanza. Per ulteriori informazioni, consulta Assegnare un indirizzo IPv6 a un'istanza nella Amazon EC2 User Guide.

È possibile connettersi a un'istanza utilizzando il relativo indirizzo IPv6. Per ulteriori informazioni, consulta Connettiti alla tua istanza Linux usando un client SSH nella Amazon EC2 User Guide o Connect a un'istanza Windows usando il suo indirizzo IPv6 nella Amazon EC2 User Guide.

Se hai avviato l'istanza utilizzando un'AMI per una versione corrente del tuo sistema operativo, l'istanza è configurata per IPv6. Se non riesci a eseguire il ping di un indirizzo IPv6 dalla tua istanza, consulta la documentazione del tuo sistema operativo per configurare IPv6.

# AWS servizi che supportano IPv6

I computer e i dispositivi intelligenti utilizzano gli indirizzi IP per comunicare tra loro su Internet e su altre reti. Man mano che Internet continua a crescere, aumenta anche la necessità di indirizzi IP. Il

formato più comune per gli indirizzi IP è IPv4. Il nuovo formato per gli indirizzi IP è IPv6, che fornisce uno spazio di indirizzi più ampio rispetto a IPv4.

Servizi AWS il supporto per IPv6 include il supporto per la configurazione dual stack (IPv4 e IPv6) o solo per le configurazioni IPv6. Ad esempio, un cloud privato virtuale (VPC) è una sezione logicamente isolata Cloud AWS in cui è possibile avviare le risorse. AWS All'interno di un VPC, è possibile creare sottoreti solo IPv4, dual stack o solo IPv6.

Servizi AWS supporta l'accesso tramite endpoint pubblici. Alcuni supportano Servizi AWS anche l'accesso tramite endpoint privati forniti da. AWS PrivateLink Servizi AWS possono supportare IPv6 tramite i propri endpoint privati anche se non supportano IPv6 tramite i propri endpoint pubblici. Gli endpoint che supportano IPv6 possono rispondere alle query DNS con record AAAA.

## Servizi che supportano IPv6

La tabella seguente elenca quelli Servizi AWS che forniscono il supporto dual stack, il supporto solo per IPv6 e gli endpoint che supportano IPv6. Aggiorneremo questa tabella non appena verrà rilasciato supporto aggiuntivo per IPv6. Per informazioni specifiche su come un servizio supporta IPv6, consulta la documentazione per il servizio.

| Nome servizio | Supporto dual stack | Supporto solo IPv6 | Gli endpoint pubblici supportano IPv6 | Gli endpoint privati supportano IPv6 [1] |
|---|---|---|---|---|
| AWS App Mesh | Sì | Sì | Sì | No |
| Amazon AppStream 2.0 | Sì | No | No | No |

| Nome servizio | Supporto dual stack | Supporto solo IPv6 | Gli endpoint pubblici supportano IPv6 | Gli endpoint privati supportano IPv6 [1] |
|---|---|---|---|---|
| Amazon Athena | Sì | No | Sì | Sì |
| Amazon Aurora | Sì | No | Sì | No |
| AWS Cloud9 | Sì | No | Sì | |
| Amazon CloudFront | Sì | No | No | |
| CloudWatch Registri Amazon | S | No | Sì | No |
| AWS Cloud Map | Sì | Sì | Sì | Sì |

| Nome servizio | Supporto dual stack | Supporto solo IPv6 | Gli endpoint pubblici supportano IPv6 | Gli endpoint privati supportano IPv6 [1] |
|---|---|---|---|---|
| AWS WAN nel cloud |  Sì |  No |  Sì |  No |
| Amazon Cognito |  Sì |  No |  Sì | |
| AWS Database Migration Service |  Sì |  No |  No |  No |
| AWS Direct Connect |  Sì |  Sì |  No | |
| Amazon EC2 |  Sì |  Sì |  Sì |  No |
| Amazon ECS |  Sì |  No |  No |  No |

| Nome servizio | Supporto dual stack | Supporto solo IPv6 | Gli endpoint pubblici supportano IPv6 | Gli endpoint privati supportano IPv6 [1] |
|---|---|---|---|---|
| Amazon EKS | Nodi: sì/Pods: no | Pod: Sì/Nodi: no | No | No |
| Sistema di bilanciamento del carico elastico | Sistemi di bilanciamento del carico: Sì Gruppi di destinazione: No | Sistemi di bilanciamento del carico: No Gruppi di destinazione: Sì | No | No |
| Amazon ElastiCache | Sì | Sì | No | No |
| AWS Fargate | Sì | No | No | No |
| AWS Global Accelerator | Sì | No | No | |
| AWS Glue | No | No | No | Sì |

| Nome servizio | Supporto dual stack | Supporto solo IPv6 | Gli endpoint pubblici supportano IPv6 | Gli endpoint privati supportano IPv6 [1] |
|---|---|---|---|---|
| AWS IoT |  Sì |  No |  Sì |  No |
| AWS Lake Formation |  No |  No |  No |  Sì |
| AWS Lambda |  Sì |  No |  Sì |  No |
| Amazon Lightsail |  Sì |  Sì |  No | |
| AWS Network Firewall |  Sì |  Sì |  No | |
| OpenSearch Servizio Amazon |  Sì |  No |  Sì |  No |

| Nome servizio | Supporto dual stack | Supporto solo IPv6 | Gli endpoint pubblici supportano IPv6 | Gli endpoint privati supportano IPv6 [1] |
|---|---|---|---|---|
| AWS PrivateLink |  Sì |  Sì |  Sì | |
| Amazon RDS |  Sì |  No |  Sì |  No |
| Amazon Route 53 |  Sì |  Sì |  No | |
| Amazon S3 |  Sì |  No |  Sì |  No |
| AWS Secrets Manager |  Sì |  No |  Sì |  No |
| AWS Shield |  Sì |  Sì |  No | |

| Nome servizio | Supporto dual stack | Supporto solo IPv6 | Gli endpoint pubblici supportano IPv6 | Gli endpoint privati supportano IPv6 [1] |
|---|---|---|---|---|
| AWS Site-to-Site VPN | Sì | No | Sì | No |
| AWS Transit Gateway | Sì | No | Sì | No |
| Amazon VPC | Sì | Sì | Sì | No |
| AWS WAF | Sì | Sì | No | |
| Amazon WorkSpaces | Sì | No | No | No |

[1] Una cella vuota indica che il servizio non si integra con AWS PrivateLink.

## Supporto IPv6 aggiuntivo

### Calcolo

- Amazon EC2 supporta l'avvio di istanze basate su NitroSystem in sottoreti solo IPv6.

- Amazon EC2 fornisce endpoint IPv6 per Instance Metadata Service (Instance Metadata Service) e il servizio di sincronizzazione oraria di Amazon.

Reti e distribuzione di contenuti

- Amazon VPC supporta la creazione di sottoreti solo IPv6.
- Amazon VPC aiuta le risorse IPv6 a comunicare con AWS le risorse IPv4 supportando DNS64 sulle sottoreti e NAT64 sui gateway NAT.

Sicurezza, identità e conformità

- AWS Identity and Access Management (IAM) supporta gli indirizzi IPv6 nelle politiche IAM.
- Amazon Macie supporta gli indirizzi IPv6 nelle Informazioni personali di identificazione (PII).

Gestione e governance

- AWS CloudTrail i record includono informazioni IPv6 di origine.
- AWS CLI v2 supporta il download tramite connessioni IPv6 per client solo IPv6.

## Ulteriori informazioni

- IPv6 su AWS
- Architetture di riferimento Amazon VPC dual-stack e solo IPv6 (PDF)

# Cloud privati virtuali (VPC)

Un cloud privato virtuale (VPC) è una rete virtuale dedicata nel tuo account Account AWS. Il VPC è isolato a livello logico dalle altre reti virtuali del cloud AWS. Puoi avviare le risorse AWS, ad esempio le istanze Amazon EC2, nel VPC.

Il tuo account contiene un VPC predefinito per ogni regione AWS. Puoi anche creare ulteriori VPC.

Indice



## Nozioni di base sui VPC

Un VPC interessa tutte le zone di disponibilità di una regione. Dopo aver creato un VPC, puoi aggiungere una o più sottoreti in ciascuna zona di disponibilità. Per ulteriori informazioni, consulta Sottoreti.

Indice



### Intervallo di indirizzi IP VPC

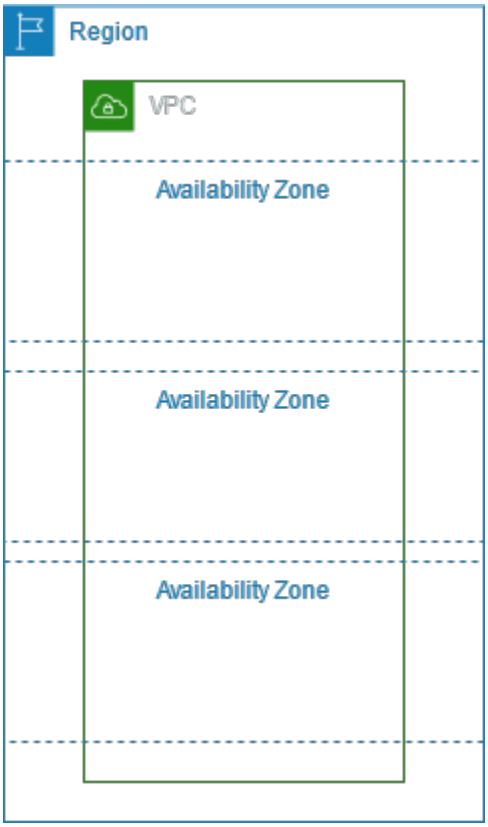
Quando crei un VPC, devi specificare i relativi indirizzi IP come segue:

- Solo IPv4: il VPC ha un blocco CIDR IPv4 ma non un blocco CIDR IPv6.
- Dual-stack: il VPC ha sia un blocco CIDR IPv4 che un blocco CIDR IPv6.

Per ulteriori informazioni, consulta Indirizzi IP per i tuoi VPC e sottoreti.

## Diagramma di un VPC

Il seguente diagramma mostra un VPC senza risorse VPC aggiuntive. Per degli esempi di configurazione del VPC, consulta la pagina Esempi.




## Risorse VPC

Ogni VPC viene fornito automaticamente con le seguenti risorse:

- Set di opzioni DHCP predefinito
- Lista di controllo accessi di rete predefinita
- Gruppo di sicurezza predefinito
- Tabella di routing principale

Per il tuo VPC puoi creare le seguenti risorse:

- liste di controllo accessi di rete
- Tabelle di routing personalizzate
- Gruppi di sicurezza
- Internet Gateway
- Gateway NAT

# VPC di default

Quando inizi a utilizzare Amazon VPC, disponi già di un VPC predefinito in ogni regione AWS. Un VPC di default include una sottorete pubblica in ogni zona di disponibilità, un gateway Internet e impostazioni per abilitare la risoluzione DNS. È possibile quindi iniziare immediatamente ad avviare istanze Amazon EC2 in un VPC di default. Puoi anche utilizzare servizi come Elastic Load Balancing, Amazon RDS e Amazon EMR nel tuo VPC predefinito.

Un VPC predefinito è idoneo per iniziare rapidamente ad avviare e utilizzare le istanze pubbliche come un blog o un semplice sito Web. Puoi modificare i componenti del VPC predefinito in base alle Esigenze.

Puoi inoltre aggiungere sottoreti al VPC di default. Per ulteriori informazioni, consulta the section called “Creazione di una sottorete”.

Indice



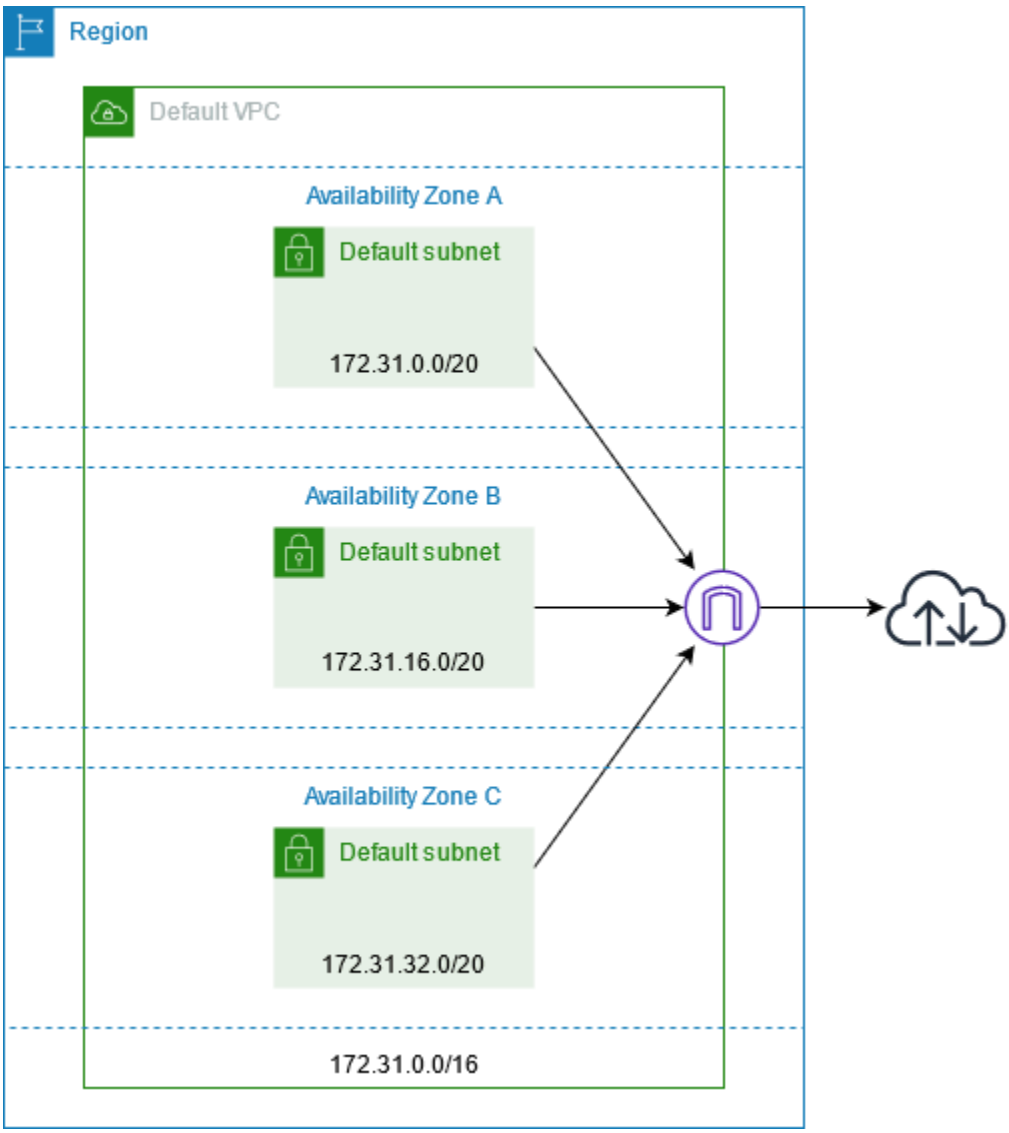
## Componenti VPC predefiniti

Durante la creazione di un VPC predefinito, eseguiamo le seguenti operazioni per configuralo per conto dell'utente:

- Creiamo un VPC con un blocco CIDR IPv4 di dimensione `/16` (`172.31.0.0/16`). Ciò fornisce fino a 65.536 indirizzi IPv4 privati.
- Creiamo una sottorete predefinita di dimensione `/20` in ogni zona di disponibilità. Ciò fornisce fino a 4096 indirizzi per sottorete, alcuni dei quali sono riservati per il nostro utilizzo.
- Creiamo un Internet Gateway e lo colleghiamo VPC predefinito.
- Aggiungi una route alla tabella di instradamento principale che indirizza tutto il traffico (`0.0.0.0/0`) al gateway Internet.
- Creiamo un gruppo di sicurezza predefinito e lo associamo al VPC predefinito.
- Creiamo una lista di controllo accessi di rete predefinita e la associamo al VPC predefinito.
- Associamo le opzioni DHCP predefinite impostate per l'account AWS al VPC predefinito.

> **Note**
>
> Amazon crea le risorse di cui sopra per tuo conto. Le policy IAM non si applicano a queste operazioni perché non esegui tali operazioni. Ad esempio, se hai una policy IAM che impedisce di chiamare CreateInternetGateway, e quindi chiami CreateDefaultVpc, viene comunque creato il gateway Internet nel VPC predefinito.

Nella figura seguente sono illustrati i componenti chiave impostati per un VPC predefinito.




La tabella seguente mostra le route nella tabella di instradamento principale per il VPC predefinito.

| Destinazione | Target |
| --- | --- |
| 172.31.0.0/16 | locale |
| 0.0.0.0/0 | *internet_gateway_id* |

Puoi utilizzare un VPC predefinito come qualsiasi altro VPC per eseguire le operazioni sottostanti:

- Aggiungere altre sottoreti non predefinite.
- Modificare la tabella di instradamento principale.

- Aggiungere altre tabelle di routing.
- Associare altri gruppi di sicurezza.
- Aggiornare le regole del gruppo di sicurezza predefinito.
- Aggiungere connessioni AWS Site-to-Site VPN.
- Aggiungere altri blocchi CIDR IPv4.
- Accedere ai VPC in un'area remota utilizzando un gateway Direct Connect. Per informazioni sulle opzioni del gateway Direct Connect, vedere Gateway Direct Connect nel Manuale dell'utente di AWS Direct Connect.

Puoi utilizzare una sottorete predefinita come qualsiasi altra sottorete; aggiungere tabelle di routing personalizzate E impostare liste di controllo accessi di rete. Puoi anche specificare una sottorete predefinita specifica quando avvii un'istanza EC2.

Facoltativamente, puoi associare un blocco CIDR IPv6 al VPC predefinito.

## Sottoreti predefinite

Per impostazione predefinita, una sottorete predefinita è pubblica perché la tabella di instradamento principale invia il traffico della sottorete destinato a Internet all'Internet Gateway. Puoi rendere una sottorete predefinita privata rimuovendo la route dalla destinazione 0.0.0.0/0 all'Internet Gateway. Tuttavia, in questo caso, nessuna istanza EC2 in esecuzione in tale sottorete può accedere a Internet.

Le istanze avviate in una sottorete predefinita ricevono entrambe un indirizzo IPv4 pubblico e un indirizzo IPv4 privato e nomi host DNS pubblici e privati. Le istanze avviate in una sottorete non predefinita in un VPC predefinito non ricevono un indirizzo IPv4 pubblico o un nome host DNS. Puoi modificare il comportamento di indirizzamento IP pubblico predefinito della sottorete. Per ulteriori informazioni, consulta Modifica dell'attributo di assegnazione degli indirizzi IPv4 pubblici per la sottorete.

Occasionalmente, AWS può aggiungere una nuova zona di disponibilità a una regione. Nella maggior parte dei casi, una nuova sottorete predefinita in questa zona di disponibilità viene creata automaticamente per il VPC predefinito entro pochi giorni. Tuttavia, se si apportano modifiche al VPC predefinito, non viene aggiunta una nuova sottorete predefinita. Se si desidera una sottorete predefinita per la nuova zona di disponibilità, crearla personalmente. Per ulteriori informazioni, consulta Creazione di una sottorete predefinita.

## Visualizzazione del VPC predefinito e delle sottoreti predefinite

Puoi visualizzare il VPC predefinito e le sottoreti tramite la console Amazon VPC o la riga di comando.

Per visualizzare il VPC predefinito e le sottoreti tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
3. Nella colonna Default VPC (VPC predefinito), cercare il valore Yes (Sì). Prendere nota dell'ID del VPC predefinito.
4. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
5. Nella barra di ricerca, digitare l'ID del VPC predefinito. Le sottoreti restituite sono quelle nel VPC predefinito.
6. Per verificare quali sottoreti sono predefinite, cercare un valore Yes (Sì) nella colonna Default Subnet (Sottorete predefinita).

Per descrivere il VPC predefinito tramite la riga di comando

- Utilizzare describe-vpcs (AWS CLI)
- Utilizzare Get-EC2Vpc (AWS Tools for Windows PowerShell)

Utilizzare i comandi con il filtro `isDefault` e impostare il valore del filtro su `true`.

Per descrivere le sottoreti predefinite utilizzando la riga di comando

- Utilizzare describe-subnets (AWS CLI)
- Utilizzare Get-EC2Subnet (AWS Tools for Windows PowerShell)

Utilizzare i comandi con il filtro `vpc-id` e impostare il valore del filtro sull'ID del VPC predefinito. Nell'output, il campo `DefaultForAz` è impostato su `true` per sottoreti predefinite.

## Creazione di un VPC predefinito

Se Elimini il VPC predefinito, puoi crearne uno nuovo. Non puoi ripristinare un VPC predefinito precedente che hai eliminato e non puoi contrassegnare un VPC non predefinito esistente come un VPC predefinito.

Un VPC predefinito viene creato originariamente con i componenti standard dello stesso, inclusa una sottorete predefinita in ogni zona di disponibilità. Non puoi specificare tuoi componenti. I blocchi CIDR della sottorete del nuovo VPC predefinito potrebbero non essere mappati alle stesse zone di disponibilità del VPC predefinito precedente. Ad esempio, se la sottorete con blocco CIDR `172.31.0.0/20` è stata creata in `us-east-2a` nel VPC predefinito precedente, può essere creata in `us-east-2b` nel nuovo VPC predefinito.

Se disponi già di un VPC predefinito nella regione, non puoi crearne un altro.

Per creare un VPC predefinito tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
3. Selezionare Actions (Operazioni), Create Default VPC (Crea VPC predefinito).
4. Seleziona Crea. Chiudi la schermata di conferma.

Per creare un VPC predefinito tramite la riga di comando

Puoi utilizzare il comando create-default-vpc di AWS CLI. Questo comando non dispone di parametri di input.

```
aws ec2 create-default-vpc
```

Di seguito è riportato un output di esempio.

```
{
    "Vpc": {
        "VpcId": "vpc-3f139646",
        "InstanceTenancy": "default",
        "Tags": [],
        "Ipv6CidrBlockAssociationSet": [],
        "State": "pending",
        "DhcpOptionsId": "dopt-61079b07",
        "CidrBlock": "172.31.0.0/16",
        "IsDefault": true
    }
}
```

In alternativa, è possibile utilizzare il comando New-EC2DefaultVpc Tools for Windows PowerShell o l'azione CreateDefaultVpc Amazon EC2 API.

## Creazione di una sottorete predefinita

Puoi creare una sottorete predefinita in una zona di disponibilità senza sottoreti. Ad esempio, puoi creare una sottorete predefinita se una è stata eliminata o se AWS ha aggiunto una nuova zona di disponibilità e non ha creato automaticamente una sottorete predefinita per tale zona nel VPC predefinito.

Una sottorete predefinita viene creata con un blocco CIDR IPv4 di dimensione `/20` nel successivo spazio contiguo disponibile nel VPC predefinito. Si applicano le regole seguenti:

- Non è possibile specificare personalmente il blocco CIDR.
- Non è possibile rispristinare una sottorete predefinita precedente che è stata eliminata.
- È consentita una sola sottorete predefinita per zona di disponibilità.
- Non puoi creare una sottorete predefinita in un VPC non predefinito.

Se lo spazio indirizzi nel VPC predefinito non è sufficiente per creare un blocco CIDR di dimensione `/20`, la richiesta non va a buon fine. Se occorre più spazio indirizzi, puoi aggiungere un blocco CIDR IPv4 al VPC.

Se hai associato un blocco CIDR IPv6 al VPC predefinito, la nuova sottorete non riceve automaticamente un blocco CIDR IPv6. Invece, puoi associare un blocco CIDR IPv6 alla sottorete predefinita dopo che è stata creata. Per ulteriori informazioni, consulta Come aggiungere un blocco CIDR IPv6 alla sottorete.

Non è possibile creare una sottorete predefinita utilizzando la AWS Management Console.

Per creare una sottorete predefinita utilizzando l'opzione AWS CLI

Utilizza il comando create-default-subnet di AWS CLI e specifica la zona di disponibilità in cui creare la sottorete.

```
aws ec2 create-default-subnet --availability-zone us-east-2a
```

Di seguito è riportato un output di esempio.

```
{
    "Subnet": {
        "AvailabilityZone": "us-east-2a",
        "Tags": [],
        "AvailableIpAddressCount": 4091,
        "DefaultForAz": true,
        "Ipv6CidrBlockAssociationSet": [],
        "VpcId": "vpc-1a2b3c4d",
        "State": "available",
        "MapPublicIpOnLaunch": true,
        "SubnetId": "subnet-1122aabb",
        "CidrBlock": "172.31.32.0/20",
        "AssignIpv6AddressOnCreation": false
    }
}
```

Per ulteriori informazioni sulla configurazione della AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.

In alternativa, è possibile utilizzare il comando New-EC2DefaultSubnet Tools for Windows PowerShell o l'azione CreateDefaultSubnet Amazon EC2 API.

## Eliminazione delle sottoreti predefinite e del VPC predefinito

Puoi eliminare una sottorete predefinita o un VPC predefinito proprio come qualsiasi altra sottorete o VPC. Tuttavia, se elimini le sottoreti predefinite o il VPC predefinito, devi specificare in maniera esplicita una sottorete in uno dei VPC all'avvio di istanze. Se non disponi di un altro VPC, devi creare un VPC con una sottorete in almeno una zona di disponibilità. Per ulteriori informazioni, consulta Crea un VPC.

Se Elimini il VPC predefinito, puoi crearne uno nuovo. Per ulteriori informazioni, consulta Creazione di un VPC predefinito.

Se Elimini una sottorete predefinita, puoi crearne una nuova. Per ulteriori informazioni, consulta Creazione di una sottorete predefinita. Per essere certo che la nuova sottorete predefinita si comporti come previsto, modifica l'attributo sottorete per assegnare indirizzi IP pubblici a istanze che sono avviate in tale sottorete. Per ulteriori informazioni, consulta Modifica dell'attributo di assegnazione degli indirizzi IPv4 pubblici per la sottorete. È possibile avere una sola sottorete predefinita per zona di disponibilità. Non puoi creare una sottorete predefinita in un VPC non predefinito.

# Crea un VPC

Usa le procedure seguenti per creare un cloud privato virtuale (VPC). Un VPC deve disporre di risorse aggiuntive, ad esempio sottoreti, tabelle di instradamento e gateway, per poter creare risorse AWS nel VPC.

Indice



Per informazioni sulla visualizzazione o la modifica di un VPC, consulta la pagina the section called “Configura il VPC”.

## Opzioni di configurazione del VPC

Puoi specificare le opzioni di configurazione seguenti durante la creazione di un VPC.

Zone di disponibilità

Data center separati con alimentazione, rete e connettività ridondanti in una regione AWS . Puoi utilizzare diverse zone di disponibilità per gestire applicazioni e database di produzione con maggiore disponibilità, tolleranza agli errori e scalabilità rispetto a un singolo data center. Il partizionamento delle applicazioni in esecuzione nelle sottoreti tra le zone di disponibilità comporterà un maggior grado di isolamento e protezione da problemi come interruzioni di corrente, fulmini, tornado, terremoti e altro ancora.

Blocchi CIDR

Devi specificare gli intervalli di indirizzi IP del VPC e delle sottoreti. Per ulteriori informazioni, consulta Indirizzi IP per i tuoi VPC e sottoreti.

Opzioni DNS

Se hai bisogno di nomi host DNS IPv4 pubblici per le istanze EC2 avviate nelle tue sottoreti, devi abilitare entrambe le opzioni DNS. Per ulteriori informazioni, consulta Attributi DNS per il VPC.

- Abilita nomi host DNS: le istanze EC2 avviate nel VPC ricevono i nomi host DNS pubblici che corrispondono ai relativi indirizzi IPv4 pubblici.

- Abilita risoluzione DNS: il server Amazon DNS, noto come Route 53 Resolver, fornisce una risoluzione DNS per i nomi host DNS privati del VPC.

Internet Gateway

Connette il VPC a Internet. Le istanze in una sottorete pubblica possono accedere a Internet poiché la tabella di instradamento della sottorete contiene un percorso che invia traffico destinato a Internet attraverso il gateway Internet. Se non è necessario che un server sia raggiungibile direttamente da Internet, non è necessario distribuirlo in una sottorete pubblica. Per ulteriori informazioni, consulta Gateway Internet

Nome

I nomi specificati per il VPC e le altre risorse VPC vengono utilizzati per creare tag dei nomi. Se nella console utilizzi la funzione di generazione automatica dei tag dei nomi, i valori dei tag hanno il formato *nome-risorsa*.

Gateway NAT

Consente alle istanze di una sottorete privata di inviare il traffico in uscita su Internet, tuttavia impedisce alle risorse su Internet di connettersi alle istanze. In produzione, è raccomandata l'implementazione di un gateway NAT in ogni zona di disponibilità attiva. Per ulteriori informazioni, consulta Gateway NAT.

Tabelle di instradamento

Contiene un insieme di regole, denominate instradamenti, che consentono di determinare la direzione del traffico di rete dalla sottorete o dal gateway. Per ulteriori informazioni, consulta Tabelle di instradamento

Sottoreti

Un intervallo di indirizzi IP nel VPC. Puoi avviare AWS risorse, come le istanze EC2, nelle tue sottoreti. Ogni sottorete risiede totalmente all'interno di una zona di disponibilità. Avviando le istanze in almeno due zone di disponibilità, puoi proteggere le applicazioni dagli errori di una singola zona di disponibilità.

Una sottorete pubblica ha un instradamento diretto a un gateway Internet. Le risorse di una sottorete pubblica possono accedere alla rete Internet pubblica. Una sottorete privata non ha un instradamento diretto a un gateway Internet. Le risorse in una sottorete privata richiedono un altro componente, ad esempio un dispositivo NAT, per accedere alla rete Internet pubblica.

Per ulteriori informazioni, consulta Sottoreti.

Tenancy

Questa opzione definisce se le istanze EC2 avviate nel VPC verranno eseguite su hardware condiviso con altri Account AWS o su hardware dedicato esclusivamente all'uso personale. Se scegli la tenancy del VPC, le istanze EC2 *`Default`* avviate in questo VPC utilizzeranno l'attributo di tenancy specificato all'avvio dell'istanza. Per ulteriori informazioni, consulta Launch an instance using defined parameters nella Amazon EC2 User Guide. Se scegli che la tenancy del VPC sia `Dedicated`, le istanze verranno sempre eseguite come Istanze dedicate su un hardware dedicato per il tuo utilizzo. Se utilizzi AWS Outposts, Outpost richiede una connettività privata; devi usare la locazione. `Default`

## Creazione di un VPC e di altre risorse VPC

Usa la procedura seguente per creare un VPC con risorse VPC aggiuntive necessarie all'esecuzione di un'applicazione, ad eesmpio sottoreti, tabelle di instradamento, gateway Internet e gateway NAT. Per degli esempi di configurazione del VPC, consulta la pagina Esempi.

Come creare un VPC, sottoreti e altre risorse VPC tramite la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nella scheda VPC, scegli Create VPC (Crea modulo VPC).
3. Per Risorse da creare, scegli VPC e altro.
4. Mantieni selezionata la generazione automatica dei tag Nome per creare i tag Nome per le risorse VPC o deselezionala per fornire i tuoi tag Nome per le risorse VPC.
5. Per il blocco CIDR IPv4 inserisci un intervallo di indirizzi IPv4 del VPC. Un VPC deve disporre di un intervallo di indirizzi IPv4.
6. (Facoltativo) Per il Blocco CIDR IPv6, scegli Blocco CIDR IPv6 fornito da Amazon.
7. Scegli un'opzione di tenancy. Questa opzione definisce se le istanze EC2 avviate nel VPC verranno eseguite su hardware condiviso con altri Account AWS o su hardware dedicato esclusivamente all'uso personale. Se scegli la tenancy del VPC, le istanze EC2 `Default` avviate in questo VPC utilizzeranno l'attributo di tenancy specificato all'avvio dell'istanza. Per ulteriori informazioni, consulta Launch an instance using defined parameters nella Amazon EC2 User Guide. Se scegli che la tenancy del VPC sia `Dedicated`, le istanze verranno sempre eseguite come Istanze dedicate su un hardware dedicato per il tuo utilizzo. Se utilizzi AWS Outposts, Outpost richiede una connettività privata; devi usare la locazione. `Default`

8. Per quanto riguarda il Numero di zone di disponibilità (AZ), è preferibile eseguire il provisioning delle sottoreti in almeno due zone di disponibilità per un ambiente di produzione. Per scegliere le zone di disponibilità delle sottoreti, espandi Personalizza le zone di disponibilità. Altrimenti, lascia che li AWS scelga per te.
9. Per configurare le sottoreti, scegli i valori per Numero di sottoreti pubbliche e Numero di sottoreti private. Per scegliere gli intervalli di indirizzi IP delle sottoreti, espandi Personalizza i blocchi CIDR delle sottoreti. Altrimenti, lasciate che li AWS scelga per voi.
10. (Opszionale) Se le risorse di una sottorete privata richiedono l'accesso alla rete Internet pubblica, per Gateway NAT scegli il numero di zone di disponibilità in cui creare i gateway NAT. In fase di produzione, è preferibile implementare un gateway NAT in ogni zona di disponibilità con risorse che richiedono l'accesso alla rete Internet pubblica. Tieni presente che esiste un costo associato ai gateway NAT. Per ulteriori informazioni, consulta Prezzi.
11. (Facoltativo) Se le risorse di una sottorete privata devono accedere alla rete Internet pubblica tramite IPv6, per Gateway Internet solo in uscita scegli Sì.
12. (Facoltativo) Se devi accedere ad Amazon S3 direttamente dal tuo VPC, scegli Endpoint VPC e Gateway S3. Questa operazione crea un endpoint VPC del gateway per Amazon S3. Per ulteriori informazioni, consulta la sezione Endpoint VPC del gateway nella Guida di AWS PrivateLink .
13. (Facoltativo) Per quanto riguarda le Opzioni DNS, entrambe le opzioni per la risoluzione dei nomi di dominio sono abilitate per impostazione predefinita. Se l'impostazione predefinita non soddisfa le tue esigenze, puoi disabilitare queste opzioni.
14. (Facoltativo) Per aggiungere un tag al VPC, espandi Altri tag, scegli Aggiungi nuovo tag e immetti una chiave e un valore di tag.
15. Nel riquadro Anteprima puoi visualizzare le relazioni tra le risorse configurate nel VPC. Le linee continue rappresentano le relazioni tra le risorse. Le linee tratteggiate rappresentano il traffico di rete diretto ai gateway NAT, ai gateway Internet e agli endpoint dei gateway. Dopo la creazione del VPC, puoi visualizzare in qualunque momento le risorse del tuo VPC in questo formato tramite la scheda Mappa delle risorse. Per ulteriori informazioni, consulta Come visualizzare le risorse nel VPC.
16. Al termine della configurazione del VPC, scegli Crea VPC

## Creare solo un VPC

Utilizza la procedura seguente per creare un VPC senza risorse VPC aggiuntive tramite la console Amazon VPC.

Come creare un VPC senza risorse VPC aggiuntive tramite la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nella scheda VPC, scegli Create VPC (Crea modulo VPC).
3. Per Risorse da creare scegli Solo VPC.
4. (Facoltativo) Per Tag dei nomi immetti un nome per il VPC. In questo modo viene creato un tag con una chiave di `Name` e il valore specificato.
5. Per IPv4 CIDR block (Blocco CIDR IPv4), effettua una delle seguenti operazioni:
   - Scegli Input manuale CIDR IPv4 e immetti un intervallo di indirizzi IPv4 per il VPC.
   - Scegli Blocco CIDR IPv4 allocato da IPAM, seleziona il pool di indirizzi IPv4 di Amazon VPC IP Address Manager (IPAM) e una maschera di rete. La dimensione del blocco CIDR è limitata dalle regole di allocazione sul pool IPAM. IPAM è una funzionalità VPC che semplifica la pianificazione, il monitoraggio e il monitoraggio degli indirizzi IP per AWS i carichi di lavoro. Per ulteriori informazioni, consulta la Amazon VPC IPAM User Guide.

     Se utilizzi IPAM per gestire gli indirizzi IP, è preferibile scegliere questa opzione. In caso contrario, il blocco CIDR specificato per il VPC potrebbe sovrapporsi a un'allocazione CIDR IPAM.
6. (Facoltativo) Per creare un cloud privato virtuale a dual-stack, specifica un intervallo di indirizzi IPv6 per il VPC. Per IPv6 CIDR block (Blocco CIDR IPv6), effettua una delle seguenti operazioni:
   - Scegli IPAM-allocated IPv6 CIDR block (Blocco CIDR IPv5 allocato tramite IPAM) se utilizzi Gestione indirizzi IP di Amazon VPC e se desideri eseguire il provisioning di un CIDR IPv6 da un pool IPAM. Sono disponibili due opzioni per eseguire il provisioning di un intervallo di indirizzi IP al VPC in CIDR block (Blocco CIDR):
     - Netmask length (Lunghezza maschera di rete): scegli questa opzione per selezionare una lunghezza della maschera di rete per il CIDR. Esegui una di queste operazioni:
       - Se è selezionata una lunghezza della maschera di rete predefinita per il pool IPAM, puoi scegliere Default to IPAM netmask length (Lunghezza predefinita della maschera di rete IPAM) per utilizzare la lunghezza della maschera di rete predefinita impostata per il pool IPAM dall'amministratore IPAM. Per ulteriori informazioni sulla regola di allocazione della lunghezza della maschera di rete predefinita opzionale, consulta Creare un pool IPv6 regionale nella Guida per l'utente IPAM di Amazon VPC.
       - Se non è selezionata alcuna lunghezza della maschera di rete predefinita per il pool IPAM, scegli una lunghezza della maschera di rete più specifica della lunghezza della

maschera di rete del CIDR del pool IPAM. Ad esempio, se il CIDR del pool IPAM è /50, puoi scegliere una lunghezza della maschera di rete compresa tra /52 e /60 per il VPC. Le lunghezze possibili delle maschere di rete sono comprese tra /44 e /60 con incrementi di /4.

- Select a CIDR (Seleziona un CIDR): scegli questa opzione per inserire manualmente un indirizzo IPv6. Puoi scegliere solo una lunghezza della maschera di rete più specifica della lunghezza della maschera di rete del CIDR del pool IPAM. Ad esempio, se il CIDR del pool IPAM è /50, puoi scegliere una lunghezza della maschera di rete compresa tra /52 e /60 per il VPC. Le lunghezze possibili delle maschere di rete IPv6 sono comprese tra /44 e /60 con incrementi di /4.

- Scegli Blocco CIDR IPv6 fornito da Amazon per richiedere un blocco CIDR IPv6 dal pool di indirizzi IPv6 di Amazon. Per Network Border Group, seleziona il gruppo da cui AWS pubblicizza gli indirizzi IP. Amazon fornisce una dimensione fissa del blocco CIDR IPv6 /56.
- Scegli IPv6 CIDR owned by me (CIDR IPv6 di mia proprietà) per eseguire il provisioning di un CIDR IPv6 già portato in AWS. Per ulteriori informazioni su come trasferire i propri intervalli di indirizzi IP a AWS, consulta Bring your own IP address (BYOIP) nella Amazon EC2 User Guide. È possibile fornire un intervallo di indirizzi IP per il VPC utilizzando le seguenti opzioni per il blocco CIDR:
  - No preference (Nessuna preferenza): scegli questa opzione per utilizzare la lunghezza della maschera di rete /56.
  - Select a CIDR (Seleziona un CIDR): scegli questa opzione per inserire manualmente un indirizzo IPv6, quindi scegli una lunghezza della maschera di rete più specifica della dimensione del CIDR BYOIP. Ad esempio, se il CIDR del pool BYOIP è /50, puoi scegliere una lunghezza della maschera di rete compresa tra /52 e /60 per il VPC. Le lunghezze possibili delle maschere di rete IPv6 sono comprese tra /44 e /60 con incrementi di /4.

7. (Facoltativo) Scegli un'opzione di tenancy. Questa opzione definisce se le istanze EC2 avviate nel VPC verranno eseguite su hardware condiviso con altri Account AWS o su hardware dedicato esclusivamente all'uso personale. Se scegli la tenancy del VPC, le istanze EC2 *`Default`* avviate in questo VPC utilizzeranno l'attributo di tenancy specificato all'avvio dell'istanza. Per ulteriori informazioni, consulta Launch an instance using defined parameters nella Amazon EC2 User Guide. Se scegli che la tenancy del VPC sia `Dedicated`, le istanze verranno sempre eseguite come Istanze dedicate su un hardware dedicato per il tuo utilizzo. Se utilizzi AWS Outposts, Outpost richiede una connettività privata; devi usare la locazione. `Default`

8. (Facoltativo) Per aggiungere un tag al VPC, scegli Aggiungi nuovo tag e immetti una chiave e un valore di tag.
9. Seleziona Crea VPC.
10. Dopo aver creato un VPC, puoi aggiungere sottoreti. Per ulteriori informazioni, consulta Creazione di una sottorete.

## Crea un VPC utilizzando il AWS CLI

La procedura seguente contiene AWS CLI comandi di esempio per creare un VPC più le risorse VPC aggiuntive necessarie per eseguire un'applicazione. Se esegui tutti i comandi di questa procedura, creerai un VPC, una sottorete pubblica, una sottorete privata, una tabella di routing per ogni sottorete, un gateway Internet, un gateway Internet egress-only e un gateway NAT pubblico. Se non hai bisogno di tutte queste risorse, puoi utilizzare solo gli esempi di comandi necessari.

Prerequisiti

Prima di iniziare, installa e configura la AWS CLI. Quando si configura AWS CLI, vengono richieste le credenziali. AWS Gli esempi in questa procedura presuppongono che tu abbia configurato una regione predefinita. In caso contrario, aggiungi l'opzione `--region` a ogni comando. Per ulteriori informazioni, consulta Installazione o aggiornamento della AWS CLI e Configurazione della AWS CLI.

Assegnazione di tag

Dopo averla creata, puoi aggiungere tag a una risorsa utilizzando il comando create-tags. In alternativa, puoi aggiungere l'opzione `--tag-specification` al comando di creazione della risorsa, come riportato di seguito.

```
--tag-specifications ResourceType=vpc,Tags=[{Key=Name,Value=my-project}]
```

Per creare un VPC più risorse VPC utilizzando il AWS CLI

1. Usa il comando create-vpc seguente per creare un VPC con il blocco CIDR IPv4 specificato.

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --query Vpc.VpcId --output text
   ```

   In alternativa, per creare un cloud privato VPC a dual-stack, aggiungi l'opzione `--amazon-provided-ipv6-cidr-block` per aggiungere un blocco CIDR IPv6 fornito da Amazon, come mostrato nell'esempio seguente.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/24 --amazon-provided-ipv6-cidr-block --
query Vpc.VpcId --output text
```

Questi comandi restituiscono l'ID del nuovo VPC. Di seguito è riportato un esempio.

```
vpc-1a2b3c4d5e6f1a2b3
```

2. [VPC dual-stack] Ottieni il blocco CIDR IPv6 associato al VPC tramite il comando describe-vpcs seguente.

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 Vpcs[].Ipv6CidrBlockAssociationSet[].Ipv6CidrBlock --output text
```

Di seguito è riportato un output di esempio.

```
2600:1f13:cfe:3600::/56
```

3. Crea una o più sottoreti, a seconda del caso d'uso. In fase produzione, è preferibile avviare le risorse in almeno due zone di disponibilità. Usa uno dei seguenti comandi per creare le sottoreti.

   - Sottorete solo IPv4: per creare una sottorete con un blocco CIDR IPv4 specifico, usa il comando create-subnet seguente.

     ```
     aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
      --availability-zone us-east-2a --query Subnet.SubnetId --output text
     ```

   - Sottorete dual stack: se hai creato un VPC dual stack, puoi utilizzare l'opzione `--ipv6-cidr-block` per creare una sottorete dual stack, come mostrato nel comando seguente.

     ```
     aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
      --ipv6-cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --
     query Subnet.SubnetId --output text
     ```

   - Sottorete solo IPv6: se hai creato un VPC dual stack, puoi utilizzare l'opzione `--ipv6-native` per creare una sottorete solo IPv6, come mostrato nel comando seguente.

     ```
     aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --ipv6-native --ipv6-
     cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --query
      Subnet.SubnetId --output text
     ```

Questi comandi restituiscono l'ID della nuova sottorete. Di seguito è riportato un esempio.

```
subnet-1a2b3c4d5e6f1a2b3
```

4. Se hai bisogno di una sottorete pubblica per i tuoi server Web o per un gateway NAT, procedi come segue:

   a. Crea un gateway Internet utilizzando il seguente comando create-internet-gateway. Il comando restituisce l'ID del nuovo gateway Internet.

   ```
   aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --
   output text
   ```

   b. Collega il gateway Internet al VPC usando il comando attach-internet-gateway seguente. Utilizza l'ID gateway Internet restituito dalla fase precedente.

   ```
   aws ec2 attach-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --internet-
   gateway-id igw-id
   ```

   c. Crea una tabella di routing personalizzata per la sottorete pubblica usando il comando create-route-table seguente. Il comando restituisce l'ID della nuova tabella di instradamento.

   ```
   aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
    RouteTable.RouteTableId --output text
   ```

   d. Crea un percorso nella tabella di routing che invia tutto il traffico IPv4 al gateway Internet usando il comando create-route seguente. Utilizza l'ID della tabella di instradamento per la sottorete pubblica.

   ```
   aws ec2 create-route --route-table-id rtb-id-public --destination-cidr-block
    0.0.0.0/0 --gateway-id igw-id
   ```

   e. Associa la tabella di routing alla sottorete pubblica usando il comando associate-route-table seguente. Utilizza l'ID della tabella di instradamento per la sottorete pubblica e l'ID della sottorete pubblica.

   ```
   aws ec2 associate-route-table --route-table-id rtb-id-public --subnet-
   id subnet-id-public-subnet
   ```

5. [IPv6] Puoi aggiungere un gateway Internet egress-only, in modo che le istanze di una sottorete privata possano accedere a Internet tramite IPv6 (ad esempio, per ottenere aggiornamenti software), senza che gli host su Internet possano accedere alle tue istanze.

   a. Crea un gateway Internet egress-only usando il comando create-egress-only-internet-gateway seguente. Il comando restituisce l'ID del nuovo gateway Internet.

   ```
   aws ec2 create-egress-only-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --
   query EgressOnlyInternetGateway.EgressOnlyInternetGatewayId --output text
   ```

   b. Crea una tabella di routing personalizzata per la sottorete privata usando il comando create-route-table seguente. Il comando restituisce l'ID della nuova tabella di instradamento.

   ```
   aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
    RouteTable.RouteTableId --output text
   ```

   c. Crea un percorso nella tabella di routing della sottorete privata che invii tutto il traffico IPv6 al gateway Internet egress-only usando il comando create-route seguente. Utilizza l'ID della tabella di instradamento restituito nella fase precedente.

   ```
   aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
   block ::/0 --egress-only-internet-gateway eigw-id
   ```

   d. Associa la tabella di routing alla sottorete privata usando il comando associate-route-table seguente.

   ```
   aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
   id subnet-id-private-subnet
   ```

6. Se hai bisogno di un gateway NAT per le risorse in una sottorete privata, procedi come segue:

   a. Crea un indirizzo IP elastico per il gateway NAT usando il comando allocate-address seguente.

   ```
   aws ec2 allocate-address --domain vpc --query AllocationId --output text
   ```

   b. Crea il gateway NAT nella sottorete pubblica utilizzando il seguente comando create-nat-gateway. Utilizza l'ID di allocazione restituito nella fase precedente.

```
aws ec2 create-nat-gateway --subnet-id subnet-id-public-subnet --allocation-
id eipalloc-id
```

c. (Facoltativo) Se hai già creato una tabella di instradamento per la sottorete privata nel passaggio 5, ignora questo passaggio. In caso contrario, usa il comando create-route-table seguente per creare una tabella di instradamento per la sottorete privata. Il comando restituisce l'ID della nuova tabella di instradamento.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

d. Crea un percorso nella tabella di routing della sottorete privata che invii tutto il traffico IPv4 al gateway NAT usando il comando create-route seguente. Utilizza l'ID della tabella di instradamento della sottorete privata creata in questo passaggio o nel passaggio 5.

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block 0.0.0.0/0 --gateway-id nat-id
```

e. (Facoltativo) Se hai già associato una tabella di instradamento alla sottorete privata nel passaggio 5, ignora questo passaggio. In caso contrario, usa il comando associate-route-table seguente per associare la tabella di instradamento alla sottorete privata. Utilizza l'ID della tabella di instradamento della sottorete privata creata in questo passaggio o nel passaggio 5.

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

# Configura il VPC

Usa le procedure seguenti per visualizzare e configurare cloud privati virtuali (VPC).

Attività

- Visualizzazione di un VPC
- Come visualizzare le risorse nel VPC
- Come aggiungere un blocco CIDR IPv4 al VPC.
- Come aggiungere un blocco CIDR IPv6 al VPC.

- Rimozione di un blocco CIDR IPv4 dal VPC
- Rimozione di un blocco CIDR IPv6 dal VPC

Per ulteriori informazioni sulla creazione di un VPC, consulta le pagine the section called “Crea un VPC” oppure the section called “Eliminazione del VPC”.

## Visualizzazione di un VPC

Seguire i passaggi seguenti per visualizzare i dettagli del proprio VPC.

Come visualizzare i dettagli del VPC tramite la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegliere VPC.
3. Seleziona il VPC, quindi scegli Visualizza dettagli per visualizzare i dettagli di configurazione del tuo VPC.

Per descrivere un VPC utilizzando AWS CLI

Usa il comando describe-tag.

Come visualizzare tutti i VPC tra tutte le regioni

Apri la console Amazon EC2 Global View all'indirizzo https://console.aws.amazon.com/ec2globalview/home. Per ulteriori informazioni, consulta Elencare e filtrare le risorse utilizzando Amazon EC2 Global View nella Amazon EC2 User Guide.

## Come visualizzare le risorse nel VPC

Completa la procedura seguente per visualizzare una rappresentazione visiva delle risorse nel tuo VPC tramite la scheda Mappa delle risorse. Le seguenti risorse sono visibili nella mappa delle risorse:

- VPC
- Sottoreti
  - La zona di disponibilità è rappresentata da una lettera.
  - Le sottoreti pubbliche sono verdi.
  - Le sottoreti private sono blu.

- Tabelle di instradamento
- Gateway Internet
- Internet Gateway egress-only
- Gateway NAT
- Endpoint gateway (Amazon S3 e Amazon DynamoDB)

La mappa delle risorse mostra le relazioni tra le risorse in un VPC e la modalità con cui il traffico fluisce da sottoreti a gateway NAT, gateway Internet ed endpoint dei gateway.

Puoi utilizzare la mappa delle risorse per comprendere l'architettura di un VPC, vedere quante sottoreti contiene, quali sottoreti sono associate a quali tabelle di instradamento e quali tabelle di instradamento includono percorsi verso gateway NAT, gateway Internet ed endpoint dei gateway.

Puoi utilizzare la mappa delle risorse anche per individuare configurazioni indesiderate o errate, ad esempio sottoreti private scollegate da gateway NAT o sottoreti private con un percorso diretto al gateway Internet. Puoi scegliere le risorse nella relativa mappa, ad esempio tabelle di instradamento, e modificare le configurazioni per tali risorse.

Come visualizzare le risorse del VPC

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegliere VPC.
3. Seleziona il VPC
4. Scegli la scheda mappa delle risorse per visualizzare una visualizzazione delle risorse.
5. Scegli Mostra dettagli per visualizzare dettagli aggiuntivi, oltre agli ID delle risorse e alle zone visualizzati per impostazione predefinita.

    - VPC: gli intervalli CIDR IPv4 e IPv6 assegnati al VPC.
    - Sottoreti: gli intervalli CIDR IPv4 e IPv6 assegnati a ciascuna sottorete.
    - Tabelle di instradamento: le associazioni delle sottoreti e il numero degli instradamenti nella tabella di routing.
    - Connessioni di rete: i dettagli relativi a ciascun tipo di connessione:
        - Se nel VPC sono presenti sottoreti pubbliche, esiste una risorsa gateway Internet con il numero di percorsi e le sottoreti di origine e destinazione per il traffico che utilizza il gateway Internet.

- Se è presente un gateway Internet egress-only, esiste una risorsa gateway Internet egress-only con il numero di route e le sottoreti di origine e destinazione per il traffico che utilizza il gateway Internet egress-only.
- Se è presente un gateway NAT, esiste una risorsa gateway NAT con il numero di interfacce di rete e indirizzi IP elastici per il gateway NAT.
- Se esiste un endpoint gateway, esiste una risorsa endpoint gateway con il nome del AWS servizio (Amazon S3 o Amazon DynamoDB) a cui è possibile connettersi utilizzando l'endpoint.

6. Passa il mouse su una risorsa per visualizzare la relazione tra le risorse. Le linee continue rappresentano le relazioni tra le risorse. Le linee tratteggiate rappresentano il traffico di rete verso le connessioni di rete.

## Come aggiungere un blocco CIDR IPv4 al VPC.

Per impostazione predefinita, il VPC può avere fino a cinque blocchi CIDR IPv4, ma il limite è regolabile. Per ulteriori informazioni, consulta Quote Amazon VPC. Per informazioni sulle restrizioni sui blocchi CIDR IPv4 di un VPC, consulta Blocchi CIDR del VPC.

Come aggiungere un blocco CIDR IPv4 a un VPC mediante la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
3. Seleziona il VPC e scegli Actions (Operazioni), Edit CIDRs (Modifica CIDR).
4. Scegli Add IPv4 CIDR (Aggiungi nuovo CIDR IPv4).
5. Per IPv4 CIDR block (Blocco CIDR IPv4), effettua una delle seguenti operazioni:
   - Scegli IPv4 CIDR manual input (Input manuale CIDR IPv4) e inserisci un blocco CIDR IPv4.
   - Scegli IPAM-allocated IPv4 CIDR (CIDR IPv4 allocato da IPAM) e selezionare un CIDR da un pool IPAM IPv4.
6. Selezionare Save (Salva), quindi Close (Chiudi).
7. Dopo avere aggiunto un blocco CIDR IPv4 al VPC, puoi creare sottoreti che utilizzano il nuovo blocco CIDR. Per ulteriori informazioni, consulta Creazione di una sottorete.

Per associare un blocco CIDR IPv4 a un VPC utilizzando AWS CLI

Usa il comando associate-vpc-cidr-block.

# Come aggiungere un blocco CIDR IPv6 al VPC.

Per impostazione predefinita, il VPC può avere fino a cinque blocchi CIDR IPv6, ma il limite è regolabile. Per ulteriori informazioni, consulta Quote Amazon VPC. Per informazioni sulle restrizioni sui blocchi CIDR IPv6 di un VPC, consulta Blocchi CIDR del VPC.

Come aggiungere un blocco CIDR IPv6 a un VPC mediante la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
3. Seleziona il VPC e scegli Actions (Operazioni), Edit CIDRs (Modifica CIDR).
4. Scegli Add new IPv6 CIDR (Aggiungi nuovo CIDR IPv6).
5. Per IPv6 CIDR block (Blocco CIDR IPv6), effettua una delle seguenti operazioni:

   - Scegli IPAM-allocated IPv6 CIDR block (Blocco CIDR IPv5 allocato tramite IPAM) se utilizzi Gestione indirizzi IP di Amazon VPC e se desideri eseguire il provisioning di un CIDR IPv6 da un pool IPAM. Sono disponibili due opzioni per eseguire il provisioning di un intervallo di indirizzi IP al VPC in CIDR block (Blocco CIDR):
     - Netmask length (Lunghezza maschera di rete): scegli questa opzione per selezionare una lunghezza della maschera di rete per il CIDR. Esegui una di queste operazioni:
       - Se è selezionata una lunghezza della maschera di rete predefinita per il pool IPAM, puoi scegliere Default to IPAM netmask length (Lunghezza predefinita della maschera di rete IPAM) per utilizzare la lunghezza della maschera di rete predefinita impostata per il pool IPAM dall'amministratore IPAM. Per ulteriori informazioni sulla regola di allocazione della lunghezza della maschera di rete predefinita opzionale, consulta Creare un pool IPv6 regionale nella Guida per l'utente IPAM di Amazon VPC.
       - Se non è selezionata alcuna lunghezza della maschera di rete predefinita per il pool IPAM, scegli una lunghezza della maschera di rete più specifica della lunghezza della maschera di rete del CIDR del pool IPAM. Ad esempio, se il CIDR del pool IPAM è /50, puoi scegliere una lunghezza della maschera di rete compresa tra /52 e /60 per il VPC. Le lunghezze possibili delle maschere di rete sono comprese tra /44 e /60 con incrementi di /4.
     - Select a CIDR (Seleziona un CIDR): scegli questa opzione per inserire manualmente un indirizzo IPv6. Puoi scegliere solo una lunghezza della maschera di rete più specifica della lunghezza della maschera di rete del CIDR del pool IPAM. Ad esempio, se il CIDR del pool IPAM è /50, puoi scegliere una lunghezza della maschera di rete compresa tra /52 e /60 per

il VPC. Le lunghezze possibili delle maschere di rete IPv6 sono comprese tra /44 e /60 con incrementi di /4.

- Scegli Blocco CIDR IPv6 fornito da Amazon per richiedere un blocco CIDR IPv6 dal pool di indirizzi IPv6 di Amazon. Per Network Border Group, seleziona il gruppo da cui AWS pubblicizza gli indirizzi IP. Amazon fornisce una dimensione fissa del blocco CIDR IPv6 /56.
- Scegli IPv6 CIDR owned by me (CIDR IPv6 di mia proprietà) per eseguire il provisioning di un CIDR IPv6 già portato in AWS. Per ulteriori informazioni su come trasferire i propri intervalli di indirizzi IP su AWS, consulta Bring your own IP address (BYOIP) in Amazon EC2 nella Amazon EC2 User Guide. Sono disponibili due opzioni per eseguire il provisioning di un intervallo di indirizzi IP al VPC in CIDR block (Blocco CIDR):
  - No preference (Nessuna preferenza): scegli questa opzione per utilizzare la lunghezza della maschera di rete /56.
  - Select a CIDR (Seleziona un CIDR): scegli questa opzione per inserire manualmente un indirizzo IPv6, quindi scegli una lunghezza della maschera di rete più specifica della dimensione del CIDR BYOIP. Ad esempio, se il CIDR del pool BYOIP è /50, puoi scegliere una lunghezza della maschera di rete compresa tra /52 e /60 per il VPC. Le lunghezze possibili delle maschere di rete IPv6 sono comprese tra /44 e /60 con incrementi di /4.

6. Scegli Seleziona CIDR, quindi scegli Chiudi.
7. Dopo avere aggiunto un blocco CIDR IPv6 al VPC, puoi creare sottoreti che utilizzano il nuovo blocco CIDR. Per ulteriori informazioni, consulta Creazione di una sottorete.

Per associare un blocco CIDR IPv6 a un VPC utilizzando AWS CLI

Usa il comando associate-vpc-cidr-block.

## Rimozione di un blocco CIDR IPv4 dal VPC

Se al VPC sono associati più blocchi CIDR IPv4, puoi rimuovere un blocco CIDR IPv4 dal VPC. Non puoi rimuovere il blocco CIDR IPv4 principale. Puoi rimuovere solo un blocco CIDR intero; non puoi rimuovere una sottorete di un blocco CIDR o un intervallo unito di blocchi CIDR. Devi prima eliminare tutte le sottoreti nel blocco CIDR.

Per rimuovere un blocco CIDR da un VPC tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).

3. Selezionare il VPC e scegliere Actions (Operazioni), Edit CIDRs (Modifica CIDR).
4. In CIDR IPv4 di VPC rimuovi il CIDR scegliendo Rimuovi.
5. Scegli Chiudi.

Per dissociare un blocco CIDR IPv4 da un VPC utilizzando AWS CLI

Usa il comando disassociate-vpc-cidr-block.

## Rimozione di un blocco CIDR IPv6 dal VPC

Se non desideri più il supporto IPv6 nel VPC, ma vuoi continuare a utilizzare il VPC per creare e comunicare con risorse IPv4, puoi rimuovere il blocco CIDR IPv6.

Per rimuovere un blocco CIDR IPv6, devi innanzitutto annullare l'assegnazione di tutti gli indirizzi IPv6 assegnati alle istanze nella sottorete.

La rimozione di un blocco CIDR IPv6 non elimina automaticamente eventuali regole dei gruppi di sicurezza, regole della lista di controllo accessi di rete o regole della tabella di instradamento che sono state configurate per le reti IPv6. Devi modificare o eliminare manualmente queste regole o route.

Rimozione di un blocco CIDR IPv6 da un VPC tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
3. Selezionare il VPC, scegliere Actions (Operazioni), Edit CIDRs (Modifica CIDR).
4. In CIDR IPv6 di VPC rimuovi il CIDR scegliendo Rimuovi.
5. Scegli Chiudi.

Per dissociare un blocco CIDR IPv6 da un VPC utilizzando AWS CLI

Usa il comando disassociate-vpc-cidr-block.

# Set di opzioni DHCP in Amazon VPC

I dispositivi di rete nel VPC utilizzano il Protocollo di configurazione per host dinamico (DHCP). È possibile utilizzare i set di opzioni DHCP per controllare i seguenti aspetti della configurazione di rete nella rete virtuale:

- È possibile controllare i server DNS, i nomi di dominio o i server Network Time Protocol (NTP) utilizzati dai dispositivi del VPC.
- Se la risoluzione DNS è abilitata nel VPC.

Indice



## Che cos'è il DHCP?

Ogni dispositivo su una rete TCP/IP richiede un indirizzo IP per comunicare sulla rete. In passato, gli indirizzi IP dovevano essere assegnati manualmente a ogni dispositivo della rete. Oggi gli indirizzi IP vengono assegnati dinamicamente dai server DHCP utilizzando il Protocollo di configurazione per host dinamico (DHCP).

Le applicazioni in esecuzione su istanze EC2 possono comunicare con i server Amazon DHCP secondo necessità per recuperare il leasing dell'indirizzo IP o altre informazioni di configurazione della rete (come l'indirizzo IP di un server Amazon DNS o l'indirizzo IP del router nel VPC).

È possibile specificare Amazon VPC consente di specificare le configurazioni di rete fornite dai server Amazon DHCP utilizzando i set di opzioni DHCP.

Se hai una configurazione VPC che richiede alle tue applicazioni di effettuare richieste dirette al server DHCP Amazon IPv6, tieni presente ciò che segue:

- Un'istanza EC2 in una sottorete dual-stack può recuperare solo il proprio indirizzo IPv6 dal server DHCP IPv6. Non è in grado di recuperare altre configurazioni di rete dal server DHCP IPv6, come i nomi dei server DNS o i nomi di dominio.
- Un'istanza EC2 in una sottorete solo IPv6 può recuperare il proprio indirizzo IPv6 dal server DHCP IPv6 e ulteriori informazioni di configurazione di rete, come i nomi dei server DNS e i nomi di dominio.
- Per un'istanza EC2 in una sottorete solo IPv6, il server DHCP IPv4 restituirà 169.254.169.253 come name server se "DNS» è esplicitamente menzionato nel set di opzioni DHCP. AmazonProvided Se "AmazonProvidedDNS» non è presente nel set di opzioni, il server DHCP

IPv4 non restituirà un indirizzo indipendentemente dal fatto che nel set di opzioni siano menzionati o meno altri name server IPv4.

I server Amazon DHCP possono anche fornire un intero prefisso IPv4 o IPv6 a un'interfaccia di rete nel tuo VPC utilizzando la delega dei prefissi (vedi Assegnazione di prefissi alle interfacce di rete Amazon EC2 nella Amazon EC2 User Guide). La delega del prefisso IPv4 non è fornita nelle risposte DHCP. I prefissi IPv4 assegnati all'interfaccia possono essere recuperati utilizzando IMDS (consulta le categorie di metadati delle istanze nella Amazon EC2 User Guide).

## Concetti relativi ai set di opzioni DHCP

Un Set di opzioni DHCP è un gruppo di impostazioni di rete utilizzate dalle risorse nel VPC, come le istanze EC2, per comunicare tramite la rete virtuale.

Per ogni regione è presente un set di opzioni DHCP predefinito. Ogni VPC utilizza il set di opzioni DHCP predefinito per la propria regione, a meno che non si crei e si associ un set di opzioni DHCP personalizzato al VPC o si configuri il VPC senza.

Se il tuo VPC non ha un set di opzioni DHCP configurato:

- Per le istanze EC2 basate sul sistema Nitro, AWS verrà configurato `169.254.169.253` come server dei nomi di dominio predefinito.
- Per le istanze EC2 basate su Xen, non verrà configurato alcun server di nomi di dominio e, poiché le istanze nel VPC non hanno accesso a un server DNS, non saranno in grado di accedere a Internet.

É possibile associare un set di opzioni DHCP con più VPC, ma ogni VPC può essere associato a un solo set.

Se elimini un VPC, viene annullata l'associazione al VPC del set di opzioni DHCP associato.

Indice



### Set di opzioni DHCP predefinito

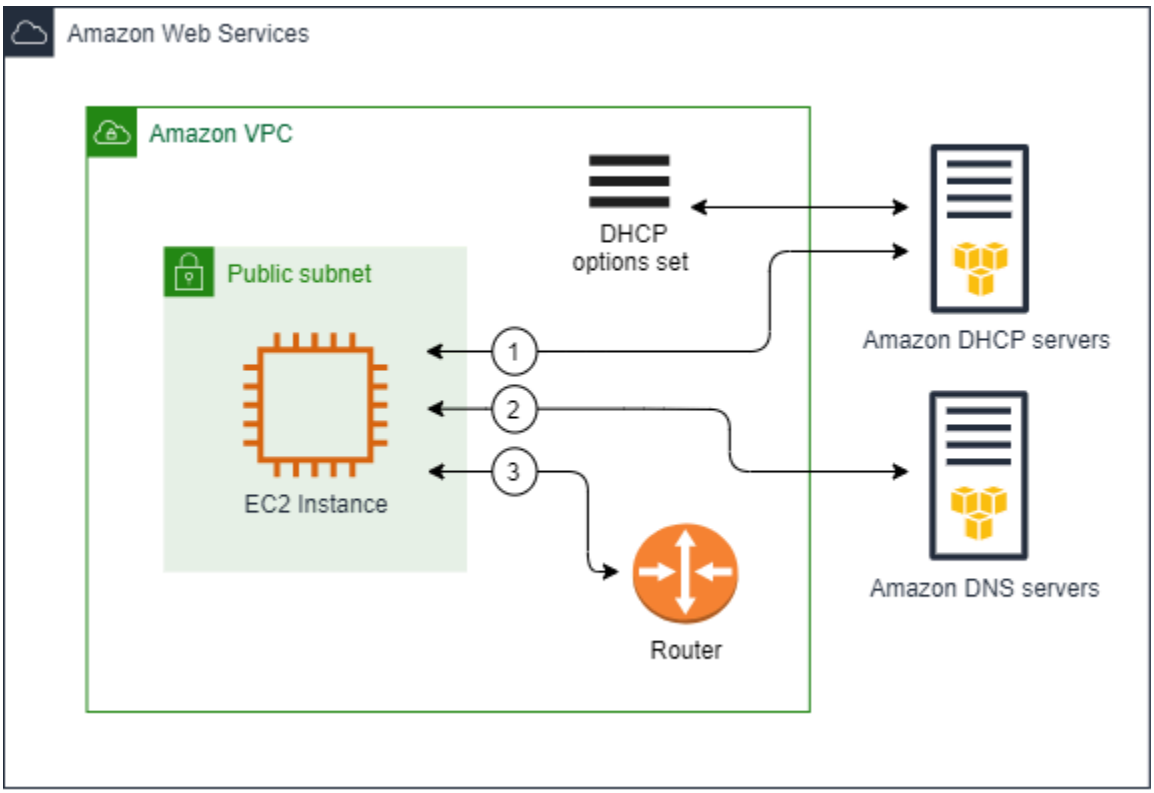
Il set di opzioni DHCP predefinito contiene le seguenti impostazioni:

- Server dei nomi di dominio: i server DNS utilizzati dalle interfacce di rete per la risoluzione dei nomi di dominio. Per un set di opzioni DHCP predefinito, questo è sempre `AmazonProvidedDNS`. Per ulteriori informazioni, consulta Server DNS Amazon.
- Nome di dominio: il nome di dominio che un client deve utilizzare per la risoluzione dei nomi host tramite il sistema dei nomi di dominio (DNS). Per ulteriori informazioni sui nomi di dominio utilizzati per le istanze EC2, consulta Nomi host delle istanze Amazon EC2.
- IPv6 Preferred Lease Time: con quale frequenza un'istanza in esecuzione a cui è assegnato un IPv6 subisce il rinnovo del lease DHCPv6. Il tempo di leasing predefinito è 140 secondi. Il rinnovo del leasing avviene in genere quando è trascorsa la metà del periodo di leasing.

Quando utilizzi un set di opzioni DHCP predefinito, non vengono utilizzate le seguenti impostazioni, ma esistono impostazioni predefinite per le istanze EC2:

- Server NTP: per impostazione predefinita, le istanze EC2 utilizzano il servizio di sincronizzazione oraria di Amazon per recuperare l'ora.
- Server di nome NetBIOS: per le istanze EC2 che eseguono Windows, il nome del computer NetBIOS è un nome descrittivo assegnato all'istanza per identificarla sulla rete. Il server di nomi NetBIOS mantiene un elenco di mappature tra i nomi di computer NetBIOS e gli indirizzi di rete per le reti che utilizzano NetBIOS come servizio di denominazione.
- Tipo di nodo NetBIOS: per le istanze EC2 che eseguono Windows, questo è il metodo utilizzato dalle istanze per risolvere i nomi NetBIOS in indirizzi IP.

Quando utilizzi il set di opzioni predefinito, il server Amazon DHCP utilizza le configurazioni di rete nel set di opzioni predefinito. Quando avvii le istanze nel VPC, esse si comporteranno come mostrato nel seguente diagramma: (1) interagiscono con il server DHCP, (2) interagiscono con il server Amazon DNS e (3) si connettono ad altri dispositivi della rete tramite il router del VPC. Le istanze possono interagire con il server Amazon DHCP in qualsiasi momento per ottenere il leasing dell'indirizzo IP e le impostazioni di rete aggiuntive.



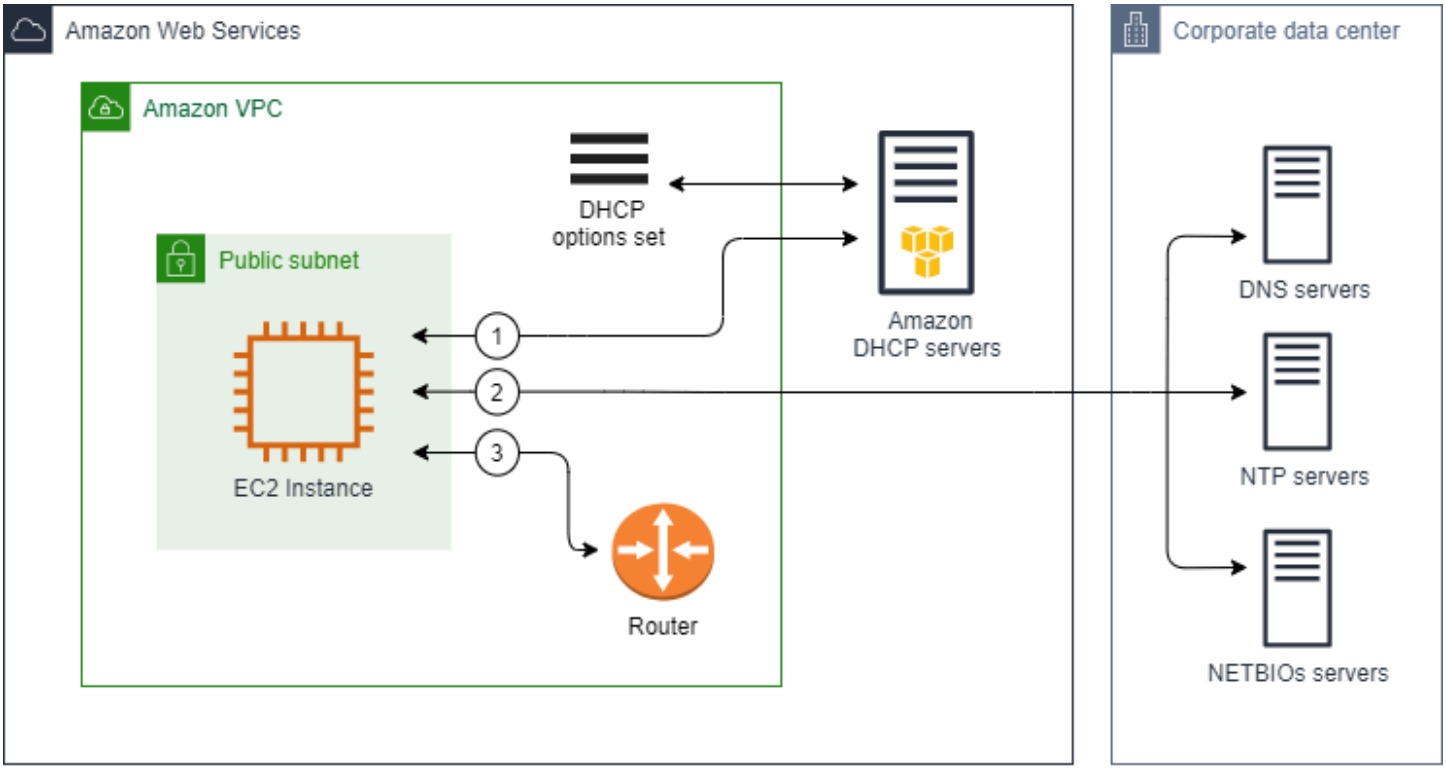

## Set di opzioni DHCP personalizzato

È possibile creare un set di opzioni DHCP personalizzato con le seguenti impostazioni e quindi associarlo a un VPC:

- Server dei nomi di dominio: i server DNS utilizzati dalle interfacce di rete per la risoluzione dei nomi di dominio.
- Nome di dominio: il nome di dominio che un client utilizza per la risoluzione dei nomi host tramite il sistema dei nomi di dominio (DNS).
- Server NTP: i server NTP che forniscono il tempo alle istanze.
- Server di nome NetBIOS: per le istanze EC2 che eseguono Windows, il nome del computer NetBIOS è un nome descrittivo assegnato all'istanza per identificarla sulla rete. Un server di nomi NetBIOS mantiene un elenco di mappature tra i nomi di computer NetBIOS e gli indirizzi di rete per le reti che utilizzano NetBIOS come servizio di denominazione.
- Tipo di nodo NetBIOS: per le istanze EC2 che eseguono Windows, è il metodo utilizzato dalle istanze per risolvere i nomi NetBIOS in indirizzi IP.
- IPv6 Preferred Lease Time (opzionale): un valore (in secondi, minuti, ore o anni) che indica la frequenza con cui un'istanza in esecuzione a cui è assegnato un IPv6 viene rinnovato il lease DHCPv6. I valori accettabili sono compresi tra 140 e 4294967295 secondi (circa 138 anni).

Se non viene immesso alcun valore, il tempo di leasing predefinito è 140 secondi. Se utilizzi l'indirizzamento a lungo termine per le istanze EC2, puoi aumentare la durata del leasing ed evitare frequenti richieste di rinnovo del leasing. Il rinnovo del leasing avviene in genere quando è trascorsa la metà del periodo di leasing.

Quando utilizzi un set di opzioni personalizzato, le istanze avviate nel VPC si comportano come illustrato nel diagramma seguente: (1) utilizzano le impostazioni di rete nel set di opzioni DHCP personalizzato, (2) interagiscono con i server DNS, NTP e NetBIOs specificato nel set di opzioni personalizzato e (3) si connettono ad altri dispositivi della rete tramite il router del VPC.




Attività correlate

- Creazione di un set di opzioni DHCP
- Modifica del set opzioni DHCP associato a un VPC

## Utilizzo dei set di opzioni DHCP

Per visualizzare e utilizzare i set di opzioni DHCP, utilizza le procedure seguenti. Per ulteriori informazioni sui set opzioni DHCP, consulta the section called “Concetti relativi ai set di opzioni DHCP”.

Attività

- Visualizza i set di opzioni DHCP
- Creazione di un set di opzioni DHCP
- Modifica del set opzioni DHCP associato a un VPC
- Eliminazione di un set di opzioni DHCP

## Visualizza i set di opzioni DHCP

È possibile visualizzare i set di opzioni DHCP come segue. Per un set di opzioni DHCP predefinito, le uniche impostazioni con valori sono i nomi di dominio e i server dei nomi di dominio.

Visualizzare i set di opzioni DHCP utilizzando la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli DHCP Options Sets (Set di opzioni DHCP).
3. Seleziona l'ID di un set di opzioni DHCP per aprirne la pagina dei dettagli.

Visualizzare i set di opzioni DHCP utilizzando la riga di comando

Per ulteriori informazioni su queste interfacce a riga di comando, consulta Uso di Amazon VPC.

- describe-dhcp-options (AWS CLI)
- Get-EC2DhcpOption (AWS Tools for Windows PowerShell)

## Creazione di un set di opzioni DHCP

Un set di opzioni DHCP personalizzato ti consente di personalizzare il VPC con il tuo server DNS, il nome di dominio e altro ancora. Puoi creare tutti i set aggiuntivi di opzioni DHCP che desideri. Tuttavia, puoi associare a un VPC solo un set di opzioni DHCP alla volta.

> **Note**
>
> Dopo aver creato un set di opzioni DHCP, non sarà possibile modificarlo. Per aggiornare le opzio9ni DHCP per il tuo VPC, è necessario creare un nuovo set di opzioni DHCP e associarlo al VPC.

Creare un set di opzioni DHCP utilizzando la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli DHCP Options Sets (Set di opzioni DHCP).
3. Seleziona Create DHCP options set (Crea set di opzioni DHCP).
4. Per Tag settings (Impostazioni tag), è possibile inserire un nome per il set di opzioni DHCP. Se inserisci un valore, viene creato automaticamente un tag Nome per il set di opzioni DHCP.
5. Per Opzioni DHCP, fornire le impostazioni di configurazione necessarie.

   - Domain name (Nome dominio): inserisci il nome di dominio che un client deve utilizzare per la risoluzione dei nomi host tramite il sistema dei nomi di dominio. Se non si utilizza il AmazonProvided DNS, i server dei nomi di dominio personalizzati devono risolvere il nome host in modo appropriato. Se utilizzi una zona ospitata privata di Amazon Route 53, puoi usare AmazonProvided DNS. Per ulteriori informazioni, consulta Attributi DNS per il VPC.

     Alcuni sistemi operativi Linux accettano più nomi di dominio separati da spazi. Tuttavia, Windows e altri sistemi operativi Linux trattano il valore come un singolo dominio, il che si traduce in un comportamento imprevisto. Se il set di opzioni DHCP è associato a un VPC con istanze che eseguono sistemi operativi che trattano il valore come un singolo dominio, specifica un solo nome di dominio.
   - Domain name servers (Server dei nomi di dominio (DNS)) (facoltativo): inserisci i server DNS che verranno utilizzati per risolvere l'indirizzo IP dei un host dal nome dell'host.

     Puoi inserire **`AmazonProvidedDNS`** o server dei nomi di dominio personalizzati. L'utilizzo di entrambe le opzioni potrebbe causare un comportamento imprevisto. È possibile inserire gli indirizzi IP di un massimo di quattro server dei nomi di dominio IPv4 (o fino a tre server dei nomi di dominio IPv4 e **`AmazonProvidedDNS`**) e quattro server dei nomi di dominio IPv6 separati da virgole. Anche se puoi specificare fino a otto server di nomi di dominio, alcuni sistemi operativi potrebbero imporre limiti più bassi. Per ulteriori informazioni su AmazonProvidedDNS e sul server Amazon DNS, consulta. Server DNS Amazon

     > **Important**
     >
     > Se il tuo VPC dispone di un gateway Internet, assicurati di specificare il tuo server DNS o un server Amazon DNS (AmazonProvidedDNS) per il valore Domain Name

servers. In caso contrario, le istanze nel VPC non potranno accedere a DNS, che disattiverà l'accesso a Internet.

- NTP servers (Server NTP) (facoltativo): inserisci l'indirizzo IP di un massimo di otto server NTP (Network Time Protocol) (quattro indirizzi IPv4 e quattro indirizzi IPv6).

  I server NTP forniscono il tempo alla rete. È possibile specificare il servizio Amazon Time Sync in un'indirizzo IPv4 `169.254.169.123` o IPv6 `fd00:ec2::123`. Di default, le istanze comunicano con Amazon Time Sync Service. Tieni presente che l'indirizzo IPv6 è accessibile solo sulle istanze EC2 costruite sul sistema Nitro.

  Per ulteriori informazioni sulle opzioni di server NTP, consulta RFC 2132. Per ulteriori informazioni sul servizio Amazon Time Sync, consulta la sezione Set the time for your istance nella Amazon EC2 User Guide.

- NetBIOS name servers (Server dei nomi NetBIOS) (facoltativo): Immettere gli indirizzi IP di un massimo di quattro server di nomi NetBIOS.

  Per le istanze EC2 che eseguono un sistema operativo Windows, il nome del computer NetBIOS è un nome descrittivo assegnato all'istanza per identificarla sulla rete. Il server di nomi NetBIOS mantiene un elenco di mappature tra i nomi di computer NetBIOS e gli indirizzi di rete per le reti che utilizzano NetBIOS come servizio di denominazione.

- NetBIOS node type (Tipo di nodo NetBIOS) (facoltativo): inserisci **1**, **2**, **4** oppure **8**. Ti consigliamo di specificare **2** (point-to-point o P-node). La trasmissione e il multicast non sono attualmente supportati. Per ulteriori informazioni su questi tipi di nodo, consulta la sezione 8.7 di RFC 2132 e la sezione 10 di RFC1001.

  Per le istanze EC2 che eseguono un sistema operativo Windows, questo è il metodo utilizzato dalle istanze per risolvere i nomi NetBIOS in indirizzi IP. Nel set di opzioni di default, non esiste alcun valore per i tipi di nodo NetBIOS.

- IPv6 Preferred Lease Time (opzionale): un valore (in secondi, minuti, ore o anni) che indica la frequenza con cui un'istanza in esecuzione a cui è assegnato un IPv6 viene rinnovato il lease DHCPv6. I valori accettabili sono compresi tra 140 e 2147483647 secondi (circa 68 anni). Se non viene immesso alcun valore, il tempo di leasing predefinito è 140 secondi. Se utilizzi l'indirizzamento a lungo termine per le istanze EC2, puoi aumentare la durata del leasing ed evitare frequenti richieste di rinnovo del leasing. Il rinnovo del leasing avviene in genere quando è trascorsa la metà del periodo di leasing.

6. Aggiungi Tags (Tag).

7. Seleziona Create DHCP options set (Crea set di opzioni DHCP). Annota il nome o l'ID del nuovo set di opzioni DHCP.
8. Per configurare il VPC perché utilizzi il nuovo set di opzioni, consulta Modifica del set opzioni DHCP associato a un VPC.

Creare un set di opzioni DHCP per il VPC utilizzando la riga di comando

Per ulteriori informazioni su queste interfacce a riga di comando, consulta Uso di Amazon VPC.

- create-dhcp-options (AWS CLI)
- New-EC2DhcpOption (AWS Tools for Windows PowerShell)

## Modifica del set opzioni DHCP associato a un VPC

Dopo aver creato un set di opzioni DHCP, è possibile associarlo a uno o più VPC. È possibile associare a un VPC solo un set di opzioni DHCP alla volta. Se non si associa un set di opzioni DHCP a un VPC, la risoluzione del nome di dominio nel VPC viene disabilitata.

Quando al VPC viene associato un nuovo set di opzioni DHCP, le nuove opzioni verranno utilizzate da tutte le nuove istanze avviate nel VPC e da quelle già esistenti. Non è necessario riavviare o rilanciare le istanze. Queste istanze rilevano automaticamente le modifiche entro poche ore, in base alla frequenza con cui l'istanza rinnova la locazione dei servizi DHCP. Se lo desideri, puoi esplicitamente rinnovare la locazione utilizzando il sistema operativo sull'istanza.

Modificare il set di opzioni DHCP associato a un VPC utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
3. Seleziona la casella di controllo del VPC, quindi scegli Actions (Operazioni), Edit VPC settings (Modifica impostazioni VPC).
4. Per DHCP options set (Set di opzioni DHCP), scegli il set di opzioni DHCP. In alternativa, scegli Nessun set di opzioni DHCP per disabilitare la risoluzione dei nomi di dominio per il VPC.
5. Selezionare Salva.

Modificare il set di opzioni DHCP associato a un VPC utilizzando la riga di comando

Per ulteriori informazioni su queste interfacce a riga di comando, consulta Uso di Amazon VPC.

- associate-dhcp-options (AWS CLI)
- Register-EC2DhcpOption (AWS Tools for Windows PowerShell)

### Eliminazione di un set di opzioni DHCP

Quando un set di opzioni DHCP non è più necessario, utilizza la seguente procedura per eliminarlo. Non è possibile eliminare un set di opzioni DHCP se è in uso. Per ogni VPC associato al set di opzioni DHCP da eliminare, è necessario associare un set di opzioni DHCP diverso al VPC o configurare il VPC in modo che non utilizzi alcun set di opzioni DHCP. Per ulteriori informazioni, consulta the section called “Modifica del set opzioni DHCP associato a un VPC”.

Eliminare un set di opzioni DHCP utilizzando la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli DHCP Options Sets (Set di opzioni DHCP).
3. Seleziona il pulsante radio per il set di opzioni DHCP, quindi scegli Operazioni, Elimina set di opzioni DHCP.
4. Quando viene richiesta la conferma, inserisci **`delete`** e scegli Elimina set di opzioni DHCP.

Eliminare un set di opzioni DHCP utilizzando la riga di comando

Per ulteriori informazioni su queste interfacce a riga di comando, consulta Uso di Amazon VPC.

- delete-dhcp-options (AWS CLI)
- Remove-EC2DhcpOption (AWS Tools for Windows PowerShell)

## Attributi DNS per il VPC

Domain Name System (DNS) è uno standard che consente di risolvere i nomi utilizzati su Internet nei corrispondenti indirizzi IP. Un nome host DNS è un nome assegnato in maniera univoca e assoluta a un computer; è costituito da un nome host e un nome di dominio. I server DNS risolvono i nomi host DNS nei corrispondenti indirizzi IP.

Gli indirizzi IPv4 pubblici consentono la comunicazione su Internet, mentre gli indirizzi IPv4 privati consentono la comunicazione all'interno della rete dell'istanza. Per ulteriori informazioni, consulta Indirizzi IP per i tuoi VPC e sottoreti.

Amazon fornisce un server DNS (l'Amazon Route 53 Resolver) per il tuo VPC. Se invece desideri utilizzare il tuo server DNS, crea un nuovo set di opzioni DHCP per il VPC. Per ulteriori informazioni, consulta Set di opzioni DHCP in Amazon VPC.

Indice



## Server DNS Amazon

Il Route 53 Resolver (chiamato anche «server Amazon DNS» o «AmazonProvidedDNS») è un servizio DNS Resolver integrato in ogni zona di disponibilità di una regione. AWS Il risolutore Route 53 è collocato su `169.254.169.253` (IPv4), `fd00:ec2::253` (IPv6) e sull'intervallo CIDR IPV4 privato primario fornito al VPC più due. Ad esempio, se hai un VPC con un CIDR IPv4 `10.0.0.0/16` e un CIDR IPv6 `fd00:ec2::253`, puoi raggiungere il risolutore Route 53 solo su `169.254.169.253` (IPv4), `fd00:ec2::253` (IPv6) o `10.0.0.2` (IPv4). Le risorse all'interno di un VPC utilizzano un indirizzo locale di collegamento per le query DNS. Queste interrogazioni vengono trasferite privatamente al Route 53 Resolver e non sono visibili sulla rete. In una sottorete solo IPv6, l'indirizzo locale del collegamento IPv4 (169.254.169.253) è ancora raggiungibile purché "DNS» sia il name server nel set di opzioni DHCP. AmazonProvided

Quando avvii un'istanza in un VPC, noi le assegniamo un nome host DNS privato. Se l'istanza è configurata con un indirizzo IPv4 pubblico e gli attributi DNS VPC sono abilitati, forniamo anche un nome host DNS pubblico.

Il formato del nome host DNS privato dipende da come si configura l'istanza EC2 al momento dell'avvio. Per ulteriori informazioni sui tipi di nomi host DNS privati, consultare Denominazione istanza EC2.

Il server Amazon DNS nel VPC viene utilizzato per risolvere i nomi di dominio DNS specificati in una zona ospitata privata di Route 53. Per ulteriori informazioni sulle zone ospitate private, consulta la

sezione relativa all'Utilizzo di zone ospitate private nella Guida per gli sviluppatori di Amazon Route 53.

### Regole e considerazioni

Se utilizzi il server DNS Amazon, si applicano le seguenti regole e considerazioni.

- Non è possibile filtrare il traffico da e verso un server Amazon DNS utilizzando le liste di controllo degli accessi di rete o i gruppi di sicurezza.
- I servizi che utilizzano il framework Hadoop, come Amazon EMR, richiedono che le istanze risolvano i propri nomi di dominio pienamente qualificati (fully qualified domain names, FQDN). In questi casi, la risoluzione DNS può avere Esito negativo se l'opzione `domain-name-servers` è impostata su un valore personalizzato. Per garantire una corretta risoluzione DNS, prendi in considerazione l'aggiunta di un server di inoltro condizionale sul server DNS per inoltrare query sul dominio *`region-name`*`.compute.internal` al server DNS Amazon. Per maggiori informazioni, consulta Impostazione di un VPC per ospitare cluster nella Guida alla gestione di Amazon EMR.
- Il risolutore Amazon Route 53 supporta solo query DNS ricorsive.

## Hostname DNS

Quando avvii un'istanza, questa riceve sempre un indirizzo IPv4 privato e un nome host DNS privato corrispondente al relativo indirizzo IPv4 privato. Se l'istanza dispone di un indirizzo IPv4 pubblico, gli attributi DNS per il VPC determinano se riceve un nome host DNS pubblico corrispondente all'indirizzo IPv4 pubblico. Per ulteriori informazioni, consulta Attributi DNS nel VPC.

Con il server DNS fornito da Amazon abilitato, i nomi host DNS vengono assegnati e risolti come segue.

Nome DNS IP privato (solo IPv4)

Puoi utilizzare il nome host DNS IP privato (solo IPv4) per la comunicazione tra istanze all'interno dello stesso VPC. È possibile risolvere i nomi host del nome DNS IP privato (solo IPv4) di altre istanze in altri VPC purché le istanze si trovino AWS nella stessa regione e il nome host dell'altra istanza sia compreso nell'intervallo dello spazio di indirizzi privato definito da RFC 1918: `10.0.0.0 - 10.255.255.255 (10/8 prefix)172.16.0.0 - 172.31.255.255 (172.16/12 prefix)`, e`192.168.0.0 - 192.168.255.255 (192.168/16 prefix)`.

Nome DNS delle risorse private

Il nome DNS basato su RBN che può essere risolto nei registri DNS A e AAAA selezionati per questa istanza. Questo nome host DNS è visibile nei dettagli dell'istanza per le istanze nelle sottoreti dual-stack e solo IPv6. Per ulteriori informazioni su RBN, consultare Tipi di nomi host delle istanze EC2.

DNS IPv4 pubblico

Un nome host DNS IPv4 (esterno) pubblico assume la forma `ec2-`*`public-ipv4-address`*`.compute-1.amazonaws.com` per la regione `us-east-1` e `ec2-`*`public-ipv4-address`*`.`*`region`*`.compute.amazonaws.com` per altre regioni. Il server Amazon DNS risolve un nome host DNS pubblico per 'indirizzo IPv4 pubblico dell'istanza al di fuori della rete dell'istanza e nell'indirizzo IPv4 privato dell'istanza all'interno della rete dell'istanza. Per ulteriori informazioni, consulta Indirizzi IPv4 pubblici e nomi host DNS esterni nella Amazon EC2 User Guide.

## Attributi DNS nel VPC

I seguenti attributi VPC determinano il supporto DNS fornito per il VPC. Se entrambi gli attributi sono abilitati e se al momento della creazione viene assegnato un indirizzo IPv4 pubblico o un indirizzo IP elastico, un'istanza avviata nel VPC riceve un nome host DNS pubblico. Se abiliti entrambi gli attributi per un VPC che in precedenza non li avevano entrambi abilitati, le istanze già avviate in quel VPC ricevono nomi host DNS pubblici, se dispongono di un indirizzo IPv4 pubblico o un indirizzo IP elastico.

Per controllare se il VPC sia abilitato per questi attributi, consulta Visualizzazione e aggiornamento degli attributi DNS per il VPC.

| Attributo | Descrizione |
| --- | --- |
| `enableDnsHostnames` | Determina se il VPC supporti l'assegnazione di nomi host DNS pubblici alle istanze con indirizzi IP pubblici.<br><br>Il valore di default per questo attributo è `false` a meno che il VPC non sia un VPC di default. Prendi nota delle regole e delle considerazioni relative a questo attributo riportate di seguito. |
| `enableDnsSupport` | Determina se il VPC supporti la risoluzione DNS tramite il server DNS fornito da Amazon.<br><br>Se questo attributo è `true`, le query al DNS fornito da Amazon hanno esito positivo. Per ulteriori informazioni, consulta Server DNS Amazon. |

| Attributo | Descrizione |
| --- | --- |
| | Il valore di default per questo attributo è `true`. Nota le regole e le considerazioni relative a questo attributo riportate di seguito. |

Regole e considerazioni

- Se Entrambi gli attributi sono impostati su `true`, si verifica quanto segue:
  - Le istanze con un indirizzo IP pubblico ricevono i nomi host DNS pubblici corrispondenti.
  - Il Amazon Route 53 Resolver server può risolvere i nomi di host DNS privati forniti da Amazon.
- Se almeno uno degli attributi è impostato su `false`, avviene quanto segue:
  - Le istanze con un indirizzo IP pubblico non ricevono nomi host DNS pubblici corrispondenti.
  - Amazon Route 53 Resolver Non è in grado di risolvere i nomi host DNS privati forniti da Amazon.
  - Le istanze ricevono nomi host DNS privati personalizzati se è presente un nome di dominio personalizzato nel set di opzioni DHCP. Se non si utilizza il server Amazon Route 53 Resolver , i server dei nomi dei domini personalizzati devono risolvere il nome host come appropriato.
- Se utilizzi nomi di dominio DNS personalizzati definiti in una zona ospitata privata in Amazon Route 53 o un DNS privato con endpoint VPC di interfaccia (AWS PrivateLink), è necessario impostare gli attributi `enableDnsHostnames` e `enableDnsSupport` su `true`.
- È in Amazon Route 53 Resolver grado di risolvere i nomi host DNS privati in indirizzi IPv4 privati per tutti gli spazi di indirizzi, incluso il caso in cui l'intervallo di indirizzi IPv4 del VPC non rientra negli intervalli di indirizzi IPv4 privati specificati da RFC 1918. Tuttavia, se il VPC è stato creato prima di ottobre 2016, Amazon Route 53 Resolver non risolve i nomi host DNS privati se l'intervallo di indirizzi IPv4 del VPC non rientra in questi intervalli. Per abilitare il supporto, contatta AWS Support.
- Se utilizzi il peering VPC, devi abilitare entrambi gli attributi per entrambi i VPC e abilitare la risoluzione DNS per la connessione peering. Per ulteriori informazioni, consulta Abilitazione della risoluzione DNS per una connessione peering VPC.

## Quote per DNS

Ciascuna istanza EC2 può inviare 1024 pacchetti al secondo per interfaccia di rete a Route 53 Resolver (in particolare l'indirizzo .2, come 10.0.0.2, e 169.254.169.253). Questa quota non può essere aumentata. Il numero di query DNS al secondo supportate da Route 53 Resolver varia in

base al tipo di query, alla dimensione della risposta e al protocollo in uso. Per ulteriori informazioni e suggerimenti sulle architetture DNS scalabili, consulta la guida tecnica DNS ibrido AWS con Active Directory.

Se raggiungi la quota, il Route 53 Resolver rifiuta il traffico. Alcune delle cause per raggiungere la quota potrebbero essere un problema di limitazione DNS o query di metadati di istanza che utilizzano l'interfaccia di rete di Route 53 Resolver. Per informazioni su come risolvere i problemi di limitazione DNS del VPC, vedere Come posso determinare se le mie query DNS verso il server DNS fornito da Amazon non stanno funzionando per via del throttling DNS del VPC. Per informazioni sul recupero dei metadati dell'istanza, consulta Recupera i metadati dell'istanza nella Amazon EC2 User Guide.

## Visualizzazione di nomi host DNS per l'istanza EC2

Puoi visualizzare i nomi host DNS per un'istanza in esecuzione o un'interfaccia di rete utilizzando la console Amazon EC2 o la riga di comando.

I campi Public DNS (IPv4) (DNS pubblico (IPv4)) e Private DNS (DNS privato) sono disponibili quando le opzioni DNS sono abilitate per il VPC associato all'istanza. Per ulteriori informazioni, consulta the section called “Attributi DNS nel VPC”.

### Istanza

Per visualizzare i nomi host DNS di un'istanza tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Selezionare l'istanza dall'elenco.
4. Nel riquadro dei dettagli, i campi Public DNS (IPv4) (DNS pubblico (IPv4)) e Private DNS (DNS privato) visualizzano i nomi host, se applicabile.

Per visualizzare i nomi host DNS di un'istanza tramite la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Uso di Amazon VPC.

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

### Interfaccia di rete

Per visualizzare il nome host DNS privato per un'interfaccia di rete tramite la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).
3. Selezionare l'interfaccia di rete dall'elenco.
4. Nel riquadro dei dettagli, il campo Private DNS (IPv4) (DNS privato (IPv4)) visualizza il nome host DNS privato.

Per visualizzare i nomi host DNS per un'interfaccia di rete tramite la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Uso di Amazon VPC.

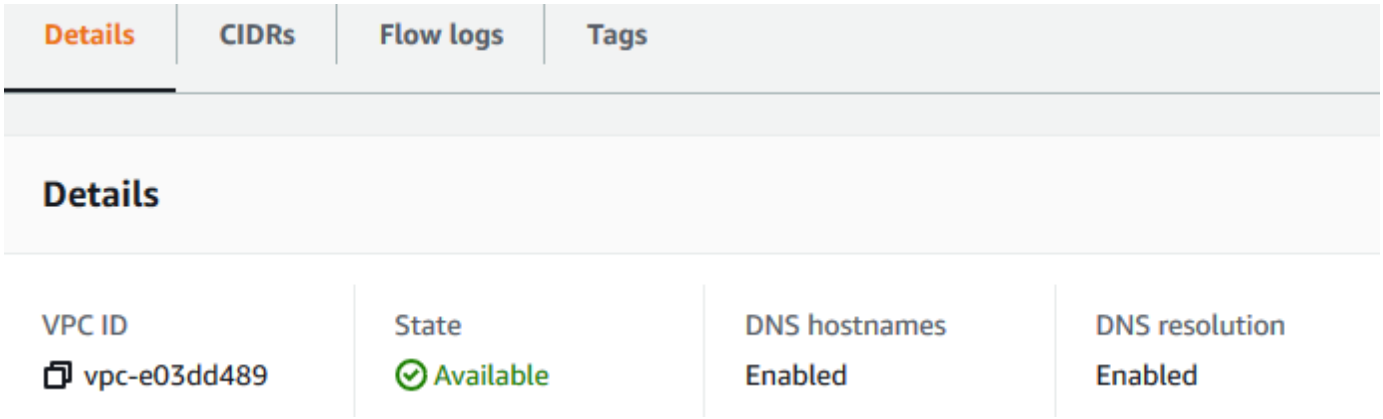
- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

## Visualizzazione e aggiornamento degli attributi DNS per il VPC

Puoi visualizzare e aggiornare gli attributi del supporto DNS per il VPC utilizzando la console Amazon VPC.

Per descrivere E aggiornare il supporto DNS per un VPC tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
3. Selezionare la casella di controllo relativa al VPC.
4. Rivedere le informazioni in Dettagli. In questo esempio, entrambe le opzioni Nomi host DNS e Risoluzione DNS sono abilitate.




5. Per aggiornare queste impostazioni, scegli Actions (Operazioni), quindi scegli Edit VPC settings (Modifica impostazioni VPC). Seleziona o deseleziona Enable (Abilita) sull'attributo DNS appropriato e scegli Save changes (Salva modifiche).

Per descrivere il supporto DNS per un VPC tramite la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Uso di Amazon VPC.

- describe-vpc-attribute (AWS CLI)
- Get-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Per aggiornare il supporto DNS per un VPC tramite la riga di comando

È possibile utilizzare uno dei seguenti comandi. Per ulteriori informazioni su queste interfacce a riga di comando, consulta Uso di Amazon VPC.

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

## Zone ospitate private

Per accedere alle risorse del tuo VPC utilizzando nomi di dominio DNS personalizzati, ad esempio`example.com`, invece di utilizzare indirizzi IPv4 privati o nomi host DNS privati AWS forniti, puoi creare una zona ospitata privata in Route 53. Una zona ospitata privata è un container che contiene informazioni su come si desidera instradare il traffico per un dominio e i relativi sottodomini all'interno di uno o più VPC senza esporre le risorse su Internet. Puoi quindi creare set di record di risorse Route 53, che determinano come Route 53 risponde a query per il dominio e per i

sottodomini. Ad esempio, se desideri che le richieste browser per example.com vengano instradate a un server Web nel VPC, crea un record A nella zona ospitata privata e specifica l'indirizzo IP di tale server Web. Per ulteriori informazioni sulla creazione di una zona ospitata privata, consulta la sezione relativa all'utilizzo di zone ospitate private nella Guida per gli sviluppatori di Amazon Route 53.

Per accedere alle risorse utilizzando nomi dominio DNS personalizzati, devi essere connesso a un'istanza all'interno del VPC. Dall'istanza, puoi verificare che la risorsa nella zona ospitata privata è accessibile dal suo nome DNS personalizzato utilizzando il comando `ping`; ad esempio, `ping mywebserver.example.com`. (Per il corretto funzionamento del comando `ping`, devi accertarti che le regole del gruppo di sicurezza dell'istanza consentano traffico ICMP in entrata.)

Le zone ospitate private non supportano relazioni transitive all'esterno del VPC; ad esempio, non puoi accedere alle risorse utilizzando i relativi nomi DNS privati personalizzati dall'altro lato di una connessione VPN.

> **Important**
>
> Se utilizzi nomi di dominio DNS personalizzati definiti in una zona ospitata privata in Amazon Route 53, devi impostare entrambi gli attributi `enableDnsHostnames` e `enableDnsSupport` su `true`.

## NAU (Network Address Usage) per il tuo VPC

Network Address Usage (NAU) è un parametro applicato alle risorse nella tua rete virtuale che consente di pianificare e monitorare le dimensioni del tuo VPC. Ogni unità NAU contribuisce a un totale che rappresenta la dimensione del VPC.

È importante comprendere il numero totale di unità che costituiscono il NAU del VPC perché le seguenti quote VPC limitano le dimensioni di un VPC:

- Network Address Usage: il numero massimo di unità NAU che può avere un singolo VPC. Per impostazione predefinita, ogni VPC può avere un massimo di 64.000 unità NAU. Puoi richiedere un aumento della quota fino a 256.000.
- Peered Network Address Usage (Network Address Usage con peering): il numero massimo di unità NAU per un VPC e tutti i relativi VPC con peering. Se un VPC è associato ad altri VPC nella stessa regione, per impostazione predefinita i VPC combinati possono avere un massimo di 128.000 unità NAU. Puoi richiedere un aumento della quota fino a 512.000. I VPC con peering in diverse regioni non contribuiscono a questo limite.

Puoi utilizzare il NAU nei modi seguenti:

- Prima di creare la rete virtuale, calcolare le unità NAU per decidere se distribuire i carichi di lavoro su più VPC.
- Dopo aver creato il tuo VPC, usa Amazon CloudWatch per monitorare l'utilizzo del VPC NAU in modo che non superi i limiti di quota NAU. Per ulteriori informazioni, consulta the section called “Metriche di CloudWatch”.

## Come viene calcolato il NAU

Se si capisce come viene calcolato il NAU, può essere d'aiuto per pianificare il dimensionamento dei VPC.

La tabella seguente spiega quali risorse costituiscono il numero di NAU in un VPC e quante unità NAU utilizza ciascuna risorsa. Alcune AWS risorse sono rappresentate come singole unità NAU e alcune risorse sono rappresentate come più unità NAU. Puoi usare la tabella per imparare a calcolare il NAU.

| Risorsa | Unità NAU |
| --- | --- |
| Ogni indirizzo IPv4 pubblico o privato e ogni indirizzo IPv6 assegnati a un'interfaccia di rete per un'istanza EC2 nel VPC | 1 |
| Interfacce di rete aggiuntive collegate a un'istanza EC2 | 1 |
| Prefissi assegnati a un'interfaccia di rete | 1 |
| Network Load Balancer per AZ | 6 |
| Gateway Load Balancer per AZ | 6 |
| Endpoint VPC per AZ | 6 |
| Collegamenti del gateway di transito | 6 |
| Funzione Lambda | 6 |
| Gateway NAT | 6 |

| Risorsa | Unità NAU |
| --- | --- |
| Obiettivo di montaggio EFS | 6 |

## Esempi NAU

Gli esempi seguenti mostrano come calcolare il NAU.

Esempio 1: due VPC collegati tramite peering di VPC

I VPC con peering che si trovano nella stessa regione contribuiscono a una quota NAU combinata.

- VPC 1
  - 50 Network Load Balancer in 2 sottoreti in zone di disponibilità separate: 600 unità NAU
  - 5.000 istanze (ciascuna con un indirizzo IPv4 e un indirizzo IPv6) in una sottorete e 5.000 istanze (ciascuna con un indirizzo IPv4 e un indirizzo IPv6) in un'altra sottorete: 20.000 unità
  - 100 funzioni Lambda: 600 unità NAU
- VPC 2
  - 50 Network Load Balancer in 2 sottoreti in zone di disponibilità separate: 600 unità NAU
  - 5.000 istanze (ciascuna con un indirizzo IPv4 e un indirizzo IPv6) in una sottorete e 5.000 istanze (ciascuna con un indirizzo IPv4 e un indirizzo IPv6) in un'altra sottorete: 20.000 unità
  - 100 funzioni Lambda: 600 unità NAU
- Numero totale di NAU con peering: 42.400 unità
- Quota NAU con peering predefinita: 128.000 unità

Esempio 2: due VPC connessi tramite un gateway di transito

I VPC connessi tramite un gateway di transito non contribuiscono a una quota NAU combinata come accade per i VPC con peering.

- VPC 1
  - 50 Network Load Balancer in 2 sottoreti in zone di disponibilità separate: 600 unità NAU
  - 5.000 istanze (ciascuna con un indirizzo IPv4 e un indirizzo IPv6) in una sottorete e 5.000 istanze (ciascuna con un indirizzo IPv4 e un indirizzo IPv6) in un'altra sottorete: 20.000 unità
  - 100 funzioni Lambda: 600 unità NAU

- VPC 2
  - 50 Network Load Balancer in 2 sottoreti in zone di disponibilità separate: 600 unità NAU
  - 5.000 istanze (ciascuna con un indirizzo IPv4 e un indirizzo IPv6) in una sottorete e 5.000 istanze (ciascuna con un indirizzo IPv4 e un indirizzo IPv6) in un'altra sottorete: 20.000 unità
  - 100 funzioni Lambda: 600 unità NAU
- Numero totale di NAU per VPC: 21.200 unità
- Quota NAU predefinita per VPC: 64.000 unità

# Condividere il VPC con altri account

La condivisione di VPC consente Account AWS a più utenti di creare le proprie risorse applicative, come istanze Amazon EC2, database Amazon Relational Database Service (RDS), cluster AWS Lambda Amazon Redshift e funzioni, in cloud privati virtuali (VPC) condivisi e gestiti centralmente. In questo modello, l'account proprietario del VPC (proprietario) condivide una o più sottoreti con altri account (partecipanti) che appartengono alla stessa organizzazione di. AWS Organizations Una volta condivisa una sottorete, i partecipanti possono visualizzare, creare, modificare ed eliminare le proprie risorse delle applicazioni nelle sottoreti condivise. Non possono invece visualizzare, modificare o eliminare le risorse che appartengono ad altri partecipanti o al proprietario del VPC.

Puoi condividere i VPC per sfruttare il routing implicito all'interno di un VPC per le applicazioni che richiedono un elevato grado di interconnessione e che si trovano all'interno degli stessi limiti di affidabilità. Questo consente di ridurre il numero di VPC creati e gestiti, utilizzando al contempo account separati per la fatturazione e il controllo degli accessi. Puoi semplificare le topologie di rete interconnettendo Amazon VPC condivisi utilizzando funzionalità di connettività AWS PrivateLink, come gateway di transito e peering VPC. Per ulteriori informazioni sui vantaggi della condivisione VPC, consulta Condivisione di VPC: un nuovo approccio a più account e gestione dei VPC.

Indice

- Quote di condivisione dei VPC
- Esempio della condivisione di sottoreti pubbliche e private

## Prerequisiti dei VPC condivisi

- Gli account del proprietario e del partecipante del VPC devono essere gestiti da. AWS Organizations
- È necessario abilitare la condivisione delle risorse nella AWS RAM console dall'account di gestione dell'organizzazione. Per ulteriori informazioni, consulta Abilitare la condivisione delle risorse AWS Organizations nella Guida AWS RAM per l'utente.
- È necessario creare una condivisione di risorse. È possibile specificare le sottoreti da condividere quando si crea la condivisione di risorse o aggiungere le sottoreti alla condivisione di risorse in un secondo momento utilizzando la procedura riportata nella sezione successiva. Per ulteriori informazioni, consulta l'argomento relativo alla creazione di una condivisione di risorse nella Guida per l'utente di AWS RAM .

## Condivisione di una sottorete

È possibile condividere sottoreti non predefinite con altri account all'interno dell'organizzazione come segue.

Per condividere una sottorete utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
3. Selezionare la sottorete e scegliere Actions (Operazioni), Share subnet (Condividi sottorete).
4. Selezionare la condivisione di risorse e scegliere Share subnet (Condividi sottorete).

Per condividere una sottorete utilizzando AWS CLI

Usare i associate-resource-sharecomandi create-resource-shareand.

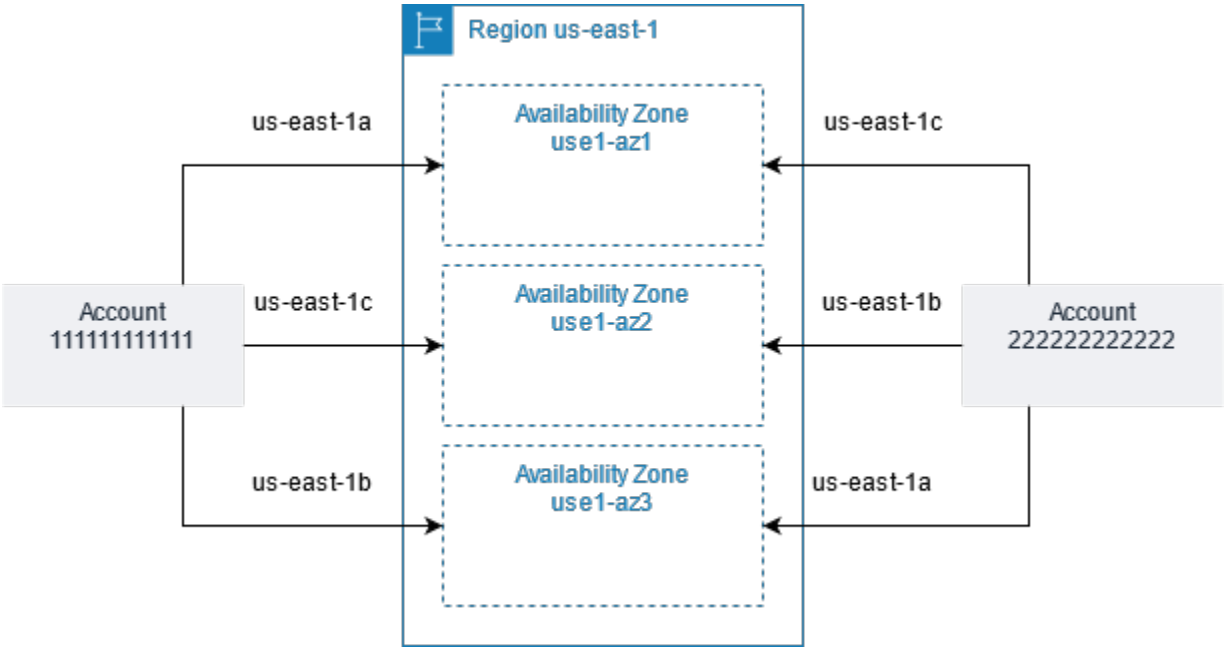
### Mappatura di sottoreti tra zone di disponibilità

Per garantire che le risorse vengano distribuite tra le zone di disponibilità di una regione, mappiamo in modo indipendente le zone di disponibilità ai nomi per ciascun account . Ad esempio, la zona `us-`

`east-1a` di disponibilità del tuo AWS account potrebbe non avere la stessa posizione `us-east-1a` di un altro AWS account.

Per coordinare le zone di disponibilità tra gli account per la condivisione VPC, è necessario utilizzare un AZ ID, un identificatore unico e invariato per una zona di disponibilità. Ad esempio, `use1-az1` è l'AZ ID per una delle zone di disponibilità della regione `us-east-1`. Utilizzare gli ID AZ per stabilire la posizione delle risorse in un account rispetto a un altro account. È possibile visualizzare l'ID AZ per ogni sottorete nella console Amazon VPC.

Il diagramma seguente illustra due account con diverse mappature del codice di zona di disponibilità per l'AZ ID.




## Annullamento della condivisione di una sottorete condivisa

Il proprietario può annullare in qualsiasi momento la condivisione di una sottorete condivisa con i partecipanti. Dopo avere annullato la condivisione di una sottorete condivisa, si applicano le regole seguenti:

- Le risorse esistenti dei partecipanti continuano a funzionare nella sottorete non condivisa. AWS i servizi gestiti (ad esempio, Elastic Load Balancing) con flussi di lavoro automatizzati/gestiti (come la scalabilità automatica o la sostituzione dei nodi) possono richiedere l'accesso continuo alla sottorete condivisa per alcune risorse.
- I partecipanti non possono più creare nuove risorse nella sottorete la cui condivisione è stata annullata.

- Possono modificare, descrivere ed eliminare le proprie risorse che si trovano nella sottorete.
- Se i partecipanti hanno ancora risorse nella sottorete di cui è stata annullata la condivisione, il proprietario non può eliminare la sottorete condivisa o il relativo VPC. Il proprietario può eliminare la sottorete o il VPC della sottorete condivisa solo dopo che i partecipanti hanno eliminato tutte le risorse nella sottorete di cui è stata annullata la condivisione.

Per annullare la condivisione di una sottorete utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
3. Selezionare la sottorete e scegliere Actions (Operazioni), Share subnet (Condividi sottorete).
4. Scegliere Actions (Operazioni), Stop sharing (Interrompi condivisione).

Per annullare la condivisione di una sottorete utilizzando AWS CLI

Utilizza il comando disassociate-resource-share.

## Identificazione del proprietario di una sottorete condivisa

I partecipanti possono visualizzare le sottoreti che sono state condivise con loro utilizzando lo strumento a riga di comando o la console Amazon VPC.

Per identificare il proprietario di una sottorete tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti). Nella colonna Owner (Proprietario) è visualizzato il proprietario della sottorete.

Per identificare il proprietario di una sottorete utilizzando il AWS CLI

Utilizzare i comandi describe-subnets e describe-vpcs, nel cui output è incluso l'ID del proprietario.

## Gestione delle risorse VPC

Proprietari e partecipanti sono responsabili delle risorse VPC di loro proprietà.

### Risorse del proprietario

I proprietari di VPC sono responsabili della creazione, della gestione e dell'eliminazione delle risorse associate a un VPC condiviso. Tali risorse includono: sottoreti, tabelle di routing, ACL di rete, connessioni peering, endpoint gateway, endpoint di interfaccia, endpoint Amazon Route 53 Resolver , gateway Internet, gateway NAT, gateway virtuali privati e collegamenti del gateway di transito.

### Risorse dei partecipanti

I partecipanti possono creare un set limitato di risorse VPC in un VPC condiviso. Ad esempio, i partecipanti possono creare interfacce e gruppi di sicurezza di rete e abilitare flussi di log VPC per le interfacce di rete di cui sono proprietari. Le risorse VPC create da un partecipante vengono conteggiate con le quote VPC dell'account del partecipante, non dell'account del proprietario. Per ulteriori informazioni, consulta Condivisione VPC.

### Fatturazione e misurazione per il proprietario e i partecipanti

- In un VPC condiviso, ogni partecipante paga per le proprie risorse applicative, tra cui istanze Amazon EC2, database Amazon Relational Database Service, cluster Amazon Redshift e funzioni. AWS Lambda I partecipanti pagano anche i costi di trasferimento dei dati associati al trasferimento dei dati tra zone di disponibilità e al trasferimento dei dati tramite connessioni peering VPC, attraverso gateway Internet e tra gateway. AWS Direct Connect
- I proprietari di VPC pagano le tariffe orarie (ove applicabile), i costi di elaborazione e trasferimento dei dati attraverso gateway NAT, gateway privati virtuali, gateway di transito ed endpoint VPC. AWS PrivateLink Inoltre, gli indirizzi IPv4 pubblici utilizzati nei VPC condivisi vengono fatturati ai proprietari di VPC. Per ulteriori informazioni sui prezzi degli indirizzi IPv4 pubblici, consulta la scheda Indirizzo IPv4 pubblico nella pagina dei prezzi di Amazon VPC.
- Un trasferimento dati nella stessa zona di disponibilità (indicata in modo univoco da un ID AZ) è gratuito, indipendentemente dalla proprietà dell'account delle risorse di comunicazione.

## Responsabilità e autorizzazioni per proprietari e partecipanti

Le seguenti responsabilità e autorizzazioni si applicano alle risorse VPC quando si lavora con sottoreti VPC condivise:

Log di flusso

- I partecipanti non possono creare, eliminare o descrivere i log di flusso in una sottorete VPC condivisa di cui non sono i proprietari.
- I partecipanti possono creare, eliminare o descrivere i log di flusso in una sottorete VPC condivisa di cui sono i proprietari.
- I proprietari di VPC non possono descrivere o eliminare i log di flusso creati da un partecipante.

Gateway Internet e gateway Internet solo in uscita

- I partecipanti non possono creare, collegare o eliminare gateway Internet e gateway Internet di sola uscita in una sottorete VPC condivisa. I partecipanti possono descrivere i gateway Internet in una sottorete VPC condivisa. I partecipanti non possono descrivere i gateway Internet di sola uscita in una sottorete VPC condivisa.

Gateway NAT

- I partecipanti non possono creare, eliminare o descrivere i gateway NAT in una sottorete VPC condivisa.

Liste di controllo degli accessi di rete (NACL)

- I partecipanti non possono creare, eliminare o descrivere le NACL in una sottorete VPC condivisa. I partecipanti possono descrivere le NACL create dai proprietari di VPC in una sottorete VPC condivisa.

Interfacce di rete

- I partecipanti possono creare interfacce di rete in una sottorete VPC condivisa. I partecipanti non possono utilizzare in altro modo le interfacce di rete create dai proprietari di VPC in una sottorete VPC condivisa, ad esempio collegando, scollegando o modificando le interfacce. I partecipanti possono modificare o eliminare le risorse in un VPC condiviso che hanno creato. Ad esempio, i partecipanti possono associare o dissociare gli indirizzi IP alle interfacce di rete create.
- I proprietari di VPC possono descrivere le interfacce di rete di proprietà dei partecipanti in una sottorete VPC condivisa. I proprietari di VPC non possono lavorare con le interfacce di rete di

proprietà dei partecipanti in nessun altro modo, ad esempio collegando, scollegando o modificando le interfacce di rete di proprietà dei partecipanti in una sottorete VPC condivisa.

Tabelle di instradamento

- I partecipanti non possono utilizzare (creare, eliminare o associare) le tabelle di routing in una sottorete VPC condivisa. I partecipanti possono descrivere le tabelle di routing in una sottorete VPC condivisa.

Gruppi di sicurezza

- I partecipanti possono lavorare con (creare, eliminare, descrivere, modificare o creare regole di ingresso e uscita per) i gruppi di sicurezza di loro proprietà in una sottorete VPC condivisa. I partecipanti non possono lavorare in alcun modo con i gruppi di sicurezza creati dai proprietari di VPC.
- I partecipanti possono creare regole nei gruppi di sicurezza di loro proprietà che fanno riferimento ai gruppi di sicurezza che appartengono ad altri partecipanti o al proprietario del VPC come segue: account-number/ security-group-id
- I partecipanti non possono avviare le istanze utilizzando i gruppi di sicurezza di proprietà di altri partecipanti o del proprietario del VPC. I partecipanti non possono avviare le istanze utilizzando il gruppo di sicurezza predefinito per il VPC, in quanto questo appartiene al proprietario.
- I partecipanti possono descrivere i gruppi di sicurezza creati dai partecipanti in una sottorete VPC condivisa. I proprietari di VPC non possono lavorare con i gruppi di sicurezza creati dai partecipanti in nessun altro modo. Ad esempio, i proprietari di VPC non possono avviare istanze utilizzando i gruppi di sicurezza creati dai partecipanti.

Sottoreti

- I partecipanti non possono modificare le sottoreti condivise o i relativi attributi. Solo il proprietario del VPC può farlo. I partecipanti possono descrivere le sottoreti in una sottorete VPC condivisa.
- I proprietari di VPC possono condividere le sottoreti solo con altri account o unità organizzative appartenenti alla stessa organizzazione di Organizations. AWS I proprietari dei VPC non possono condividere le sottoreti che si trovano in un VPC predefinito.

Gateway di transito

- Solo il proprietario del VPC può collegare un gateway di transito a una sottorete condivisa del VPC. I partecipanti non possono.

VPC

- I partecipanti non possono modificare i VPC o i relativi attributi. Solo il proprietario del VPC può farlo. I partecipanti possono descrivere i VPC, i loro attributi e i set di opzioni DHCP.
- I tag VPC e i tag per le risorse all'interno del VPC condiviso non vengono condivisi con i partecipanti.

## AWS risorse e sottoreti VPC condivise

Le seguenti risorse di Servizi AWS supporto nelle sottoreti VPC condivise. Per ulteriori informazioni su come il servizio supporta le sottoreti VPC condivise, segui i collegamenti alla documentazione del servizio corrispondente.

- Amazon Aurora
- AWS CodeBuild
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Kubernetes Service
- Sistema di bilanciamento del carico elastico
  - Application Load Balancer
  - Sistemi di bilanciamento del carico del gateway
  - Network Load Balancers
- Amazon EMR
- AWS Glue
- AWS Lambda
- AWS Network Manager
  - AWS WAN cloud
  - Strumento di analisi degli accessi alla rete
  - Reachability Analyzer

- AWS PrivateLink†
- Amazon Relational Database Service (RDS)
- Amazon Redshift
- Amazon Route 53
- AWS Transit Gateway
- Accesso verificato da AWS
- Amazon VPC
  - Peering
  - Mirroring del traffico
- Amazon VPC Lattice

† È possibile connettersi a tutti i AWS servizi che supportano PrivateLink l'utilizzo di un endpoint VPC in un VPC condiviso. Per un elenco dei servizi che supportano PrivateLink, consulta AWS i servizi che si integrano con AWS PrivateLink nella Guida.AWS PrivateLink

## Quote di condivisione dei VPC

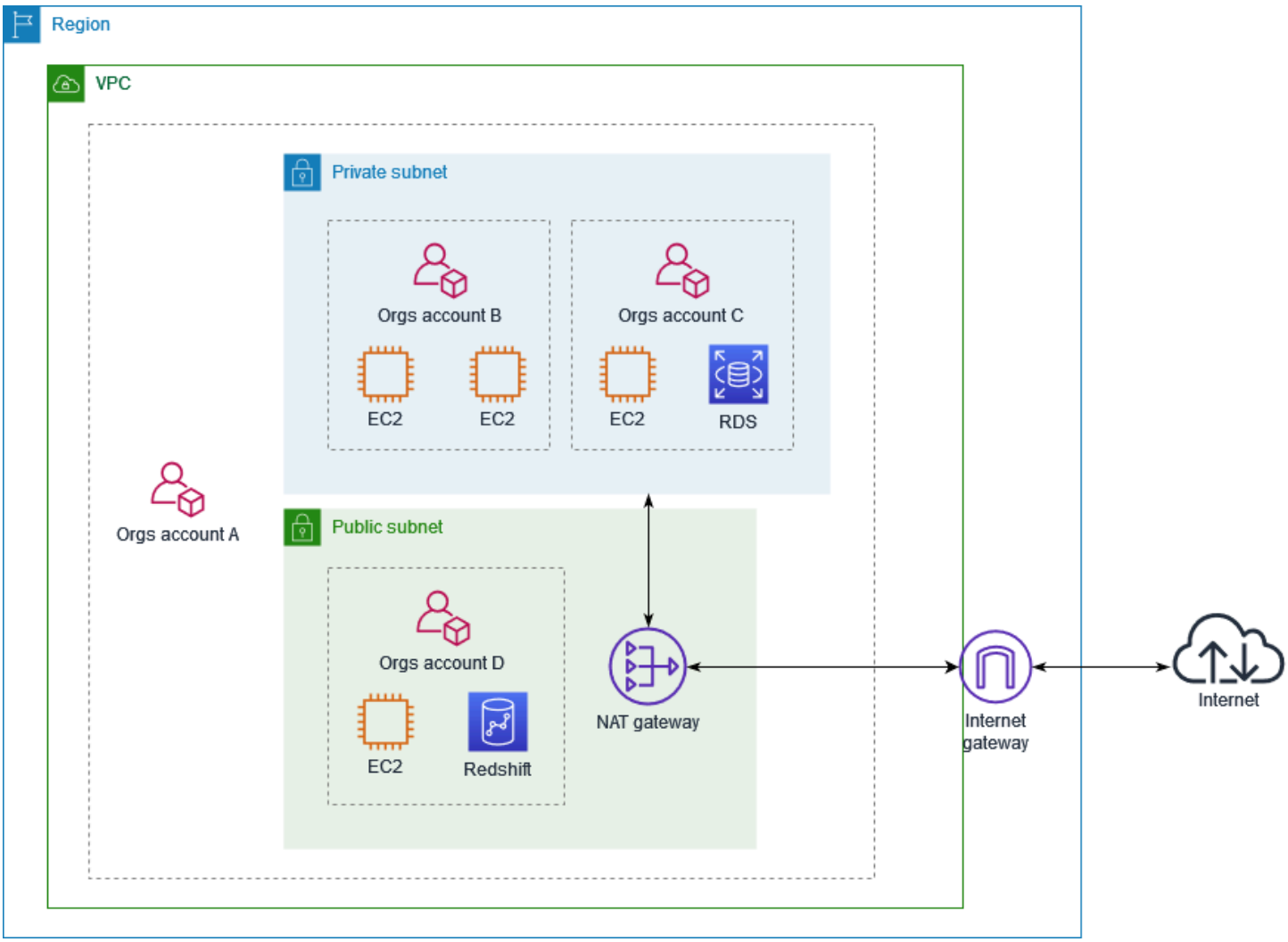
Esistono quote relative alla condivisione di VPC. Per ulteriori informazioni, consulta Condivisione VPC.

## Esempio della condivisione di sottoreti pubbliche e private

Si consideri uno scenario in cui si desidera che un account (account A) responsabile dell'infrastruttura costituita da VPC, sottoreti, tabelle di instradamento, gateway e intervalli CIDR, e altri account membri, possa utilizzare le sottoreti per le proprie applicazioni. L'account D dispone di applicazioni che devono connettersi a Internet. L'account B e l'account C dispongono di applicazioni che non devono connettersi a Internet.

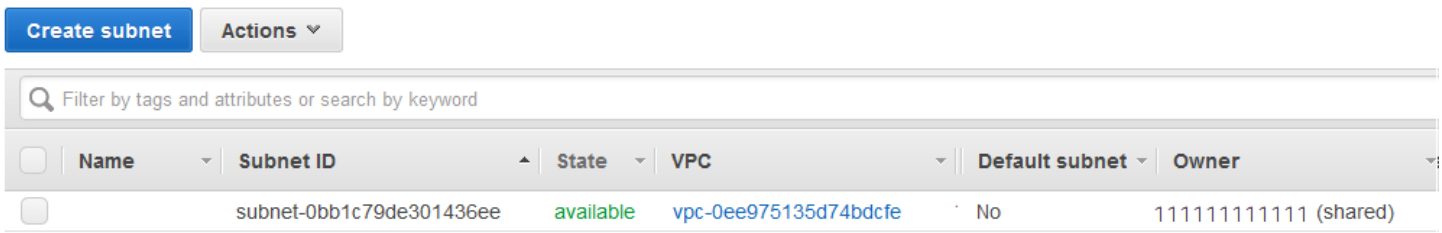
L'account A utilizza AWS Resource Access Manager per creare una condivisione di risorse per le sottoreti e condivide le sottoreti pubbliche con l'account D e le sottoreti private con l'account B e l'account C. L'account B, l'account C e l'account D possono creare risorse nelle sottoreti. Ogni account può vedere e creare risorse solo nelle sottoreti condivise con lo stesso. Ogni account può controllare le risorse che crea in queste sottoreti (ad esempio, istanze EC2 e gruppi di sicurezza).

Non è richiesta alcuna configurazione aggiuntiva per le sottoreti condivise, quindi le tabelle di routing sono identiche alle tabelle di routing delle sottoreti non condivise.




L'account A (111111111111) condivide la sottorete pubblica con l'account D (444444444444). L'account D vede la seguente sottorete e nella colonna Proprietario vengono forniti due indicatori per segnalare che la sottorete è condivisa.

- L'ID account del proprietario è l'account A (111111111111), non l'account D (444444444444).
- La parola "condivisa" viene visualizzata accanto all'ID dell'account del proprietario.



# Estendere un VPC a una zona locale, una zona Wavelength o un Outpost

È possibile ospitare risorse VPC, ad esempio sottoreti, in più posizioni in tutto il mondo. Queste posizioni sono composte da aree, zone di disponibilità, zone locali e zone Wavelength. Ciascuna regione è un'area geografica distinta.

- Le zone di disponibilità sono più posizioni isolate all'interno di ogni regione.
- Le zone locali offrono la possibilità di collocare risorse, ad esempio elaborazione e archiviazione, in più posizioni più vicine agli utenti finali.
- AWS Outposts porta i servizi AWS, l'infrastruttura e i modelli operativi praticamente in ogni data center, ambiente in co-location o struttura in locale.
- Le zone Wavelength consentono agli sviluppatori di creare applicazioni che offrono latenze molto basse a dispositivi 5G e utenti finali. Wavelength distribuisce servizi di calcolo e storage standard di AWS all'edge delle reti 5G dei provider all'avanguardia nei servizi di telecomunicazione.

AWS gestisce data center ad alta disponibilità e all'avanguardia. Anche se rari, i guasti che compromettono la disponibilità di istanze nella stessa ubicazione possono verificarsi. Se ospiti tutte le istanze in un'unica ubicazione in cui si verifica un guasto, nessuna di esse risulterà disponibile.

Per aiutarti a determinare quale distribuzione è più adatta a te, consulta le Domande frequenti su AWS Wavelength.

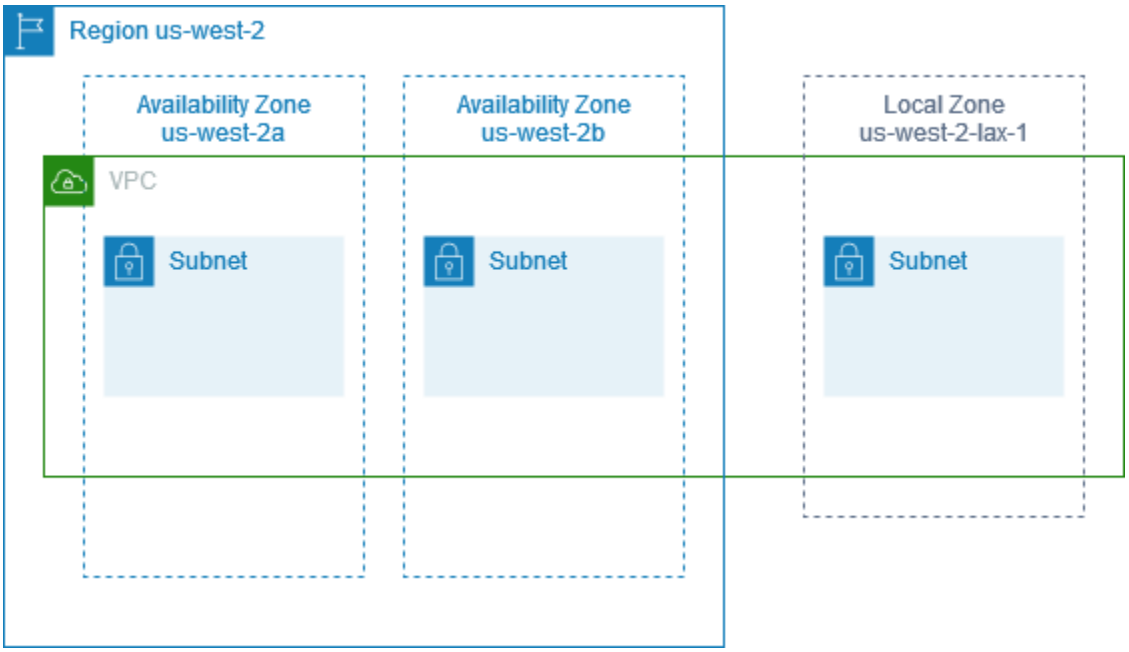
## Sottoreti nelle zone locali AWS

Le zone locali AWS consentono di posizionare le risorse più vicine agli utenti finali e di connettersi senza problemi all'intera gamma di servizi nella regione AWS che utilizza API e set di strumenti familiari. Quando si crea una sottorete in una zona locale, il VPC viene esteso anche a tale zona.

Per utilizzare una zona locale, è necessario attenersi alla seguente procedura:

- Scegli la zona locale.
- Creare una sottorete nella zona locale.
- Avvia le risorse nella sottorete della zona locale, in modo che le applicazioni siano più vicine ai tuoi utenti.

Il diagramma seguente mostra un VPC nella regione Stati Uniti occidentali (Oregon) (`us-west-2`) che comprende diverse zone di disponibilità e una zona locale.




Quando si crea un VPC, è possibile scegliere di assegnare un set di indirizzi IP pubblici forniti da Amazon al VPC. È anche possibile impostare un gruppo di confine di rete per gli indirizzi che limiti gli indirizzi al gruppo. Quando si imposta un gruppo di confine di rete, gli indirizzi IP non possono spostarsi tra i gruppi di confine di rete. Il traffico di rete della zona locale andrà direttamente a Internet o ai punti di presenza (PoP) senza attraversare la Regione madre della Zona locale, consentendo l'accesso al calcolo a bassa latenza. Per l'elenco completo delle zone locali e delle Regioni madri corrispondenti, consulta Zone locali disponibili sulla AWS Guida per l'utente delle zone locali.

Le seguenti regole si applicano alle zone locali:

- Le sottoreti della zona locale seguono le stesse regole di routing delle sottoreti della zona di disponibilità, incluse le tabelle di routing, i gruppi di sicurezza, le liste di controllo degli accessi di rete.
- Il traffico Internet in uscita lascia una zona locale dalla zona locale.
- È necessario effettuare il provisioning di indirizzi IP pubblici da utilizzare in una zona locale. Quando si allocano gli indirizzi, è possibile specificare la posizione da cui viene pubblicizzato l'indirizzo IP. Vi si fa riferimento come gruppo di confine di rete ed è possibile impostare questo parametro per limitare l'indirizzo a questa posizione. Dopo aver effettuato il provisioning degli indirizzi IP, non è possibile spostarli tra la zona locale e la Regione padre (ad esempio, da `us-west-2-lax-1a` a `us-west-2`).

- Se la zona locale supporta IPv6, puoi richiedere gli indirizzi IP forniti da Amazon IPv6 e associarli al gruppo di confine di rete per un VPC nuovo o esistente. Per l'elenco delle zone locali che supportano IPv6, consulta Considerazioni nella AWS Guida per l'utente delle zone locali
- Non puoi creare i endpoint VPC all'interno delle sottoreti della zona locale.

Per altre informazioni sull'utilizzo delle zone locali, consulta la Guida per l'utente delle zone locali AWS.

### Considerazioni per i gateway Internet

Tieni conto di quanto segue quando utilizzi i gateway Internet (nella regione padre) nelle zone locali:

- Puoi utilizzare i gateway Internet nelle zone locali con indirizzi IP elastici o indirizzi IP pubblici assegnati automaticamente da Amazon. Gli indirizzi IP elastici associati devono includere il gruppo di confine di rete della zona locale. Per ulteriori informazioni, consulta the section called “Indirizzi IP elastici”.

  Non è possibile associare un indirizzo IP elastico impostato per la regione.
- Gli indirizzi IP elastici utilizzati nelle zone locali hanno le stesse quote degli indirizzi IP elastici in una regione. Per ulteriori informazioni, consulta the section called “Indirizzi IP elastici”.
- Puoi utilizzare gateway Internet nelle tabelle di routing associate alle risorse della zona locale. Per ulteriori informazioni, consulta the section called “Routing a un Internet gateway”.

### Accesso alle zone locali mediante un gateway Direct Connect

Considerare lo scenario in cui si desidera un data center locale per accedere alle risorse che si trovano in una zona locale. Si utilizza un gateway virtuale privato per il VPC associato alla zona locale per connettersi a un gateway Direct Connect. Il gateway Direct Connect si connette a una posizione AWS Direct Connect in una regione. Il data center locale dispone di una connessione AWS Direct Connect alla posizione AWS Direct Connect.

> **Note**
>
> Il traffico all'interno degli Stati Uniti destinato a una sottorete in una zona locale che utilizza Direct Connect non attraversa la regione principale della zona locale. Al contrario, il traffico segue il percorso più breve verso la zona locale. Questo riduce la latenza e rende le applicazioni più reattive.

È possibile configurare le seguenti risorse per questa configurazione:

- Un gateway privato virtuale per il VPC associato alla sottorete della zona locale. Puoi visualizzare il VPC per la sottorete nella pagina dei dettagli della sottorete nella Amazon Virtual Private Cloud Console o utilizzare describe-subnets.

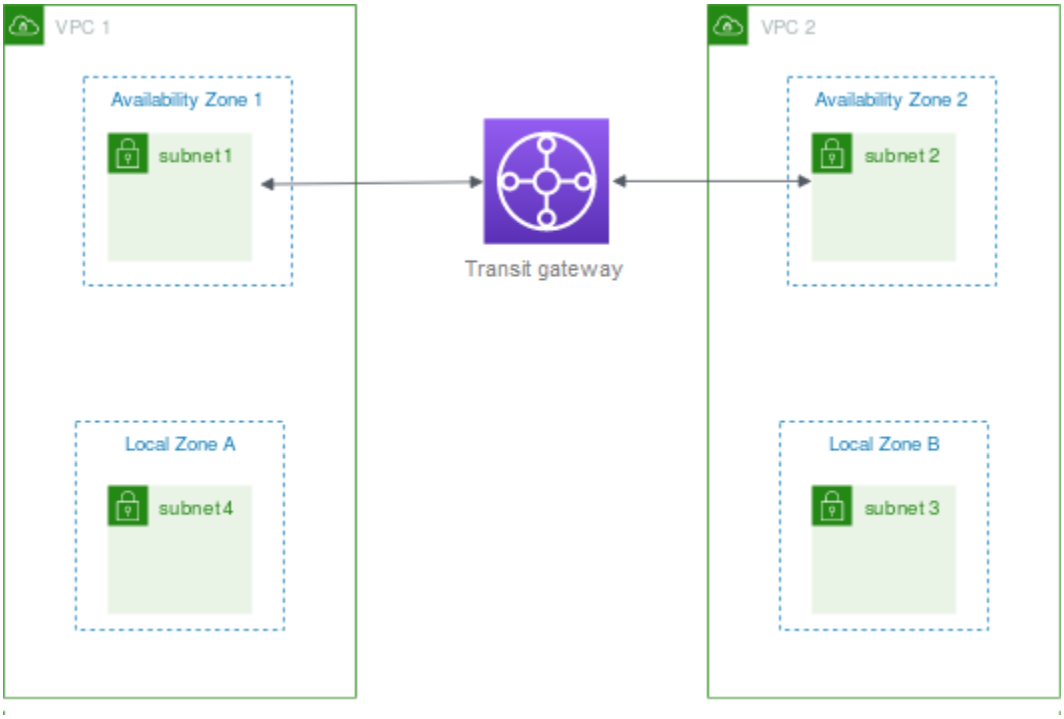
  Per informazioni su come creare un gateway virtuale privato, consulta Creazione di un gateway di destinazione nella Guida per l'utente di AWS Site-to-Site VPN.
- Una connessione Direct Connect. Per le migliori prestazioni di latenza, AWS consiglia di utilizzare la Posizione Direct Connect più vicina alla Zona locale a cui estenderai la tua sottorete.

  Per informazioni su come ordinare una connessione, consulta Interconnessioni nella Guida per l'utente di AWS Direct Connect.
- Un gateway Direct Connect. Per informazioni su come creare un gateway Direct Connect, consulta Creazione di un gateway Direct Connect nella Guida per l'utente di AWS Direct Connect.
- Un'associazione gateway privato virtuale per connettere il VPC al gateway Direct Connect. Per informazioni su come creare un'associazione a un gateway virtuale privato, consulta Associazione e annullamento dell'associazione di gateway virtuali privati nella Guida per l'utente di AWS Direct Connect.
- Una interfaccia virtuale privata sulla connessione dalla posizione AWS Direct Connect al data center On-Premise. Per informazioni su come creare un gateway Direct Connect, consulta Creazione di un'interfaccia virtuale privata al gateway Direct Connect nella Guida per l'utente di AWS Direct Connect.

## Connessione delle sottoreti delle zone locali a un gateway di transito

Non è possibile creare un collegamento del gateway di transito per una sottorete in una zona locale. Nel diagramma seguente viene illustrato come configurare la rete in modo che le sottoreti nella zona locale si connettano a un gateway di transito attraverso la zona di disponibilità padre. Crea sottoreti nelle zone locali e nelle sottoreti delle zone di disponibilità padre. Connettere le sottoreti nelle zone di disponibilità padre al gateway di transito, quindi creare un percorso nella tabella di routing per ogni VPC che instrada il traffico destinato all'altro CIDR VPC all'interfaccia di rete per il collegamento del gateway di transito.

> **Note**
>
> Il traffico destinato a una sottorete in una zona locale che ha origine da un gateway di transito attraverserà prima la regione principale.




Crea le seguenti risorse per questo scenario:

- Una sottorete nella zona di disponibilità padre. Per ulteriori informazioni, consulta the section called “Creazione di una sottorete”.
- Un gateway di transito. Per ulteriori informazioni, consulta Creare un gateway di transito in Gateway di transito di Amazon VPC.
- Un collegamento del gateway di transito per il VPC che utilizza la zona di disponibilità padre. Per ulteriori informazioni, consulta Creare un collegamento del gateway di transito a un VPC in Gateway di transito Amazon VPC.
- Una tabella di routing del gateway di transito associata al collegamento del gateway di transito. Per ulteriori informazioni, consulta Tebelle di routing del gateway di transito in Gateway di transito di Amazon VPC.
- Per ogni VPC, una voce nella tabella di routing VPC con l'altro CIDR VPC come destinazione e l'ID dell'interfaccia di rete per il collegamento del gateway di transito come destinazione. Per

trovare l'interfaccia di rete per il collegamento del gateway di transito, cercare nelle descrizioni delle interfacce di rete l'ID del collegamento del gateway di transito. Per ulteriori informazioni, consulta the section called “Routing per un gateway di transito”.

Di seguito è riportato un esempio di tabella di instradamento per VPC 1.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC 1* | *local* |
| *CIDR VPC 2* | *vpc1-attachment-network-interface-id* |

Di seguito è riportato un esempio di tabella di instradamento per VPC 2.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC 2* | *local* |
| *CIDR VPC 1* | *vpc2-attachment-network-interface-id* |

Di seguito è riportato un esempio della tabella di instradamento del gateway di transito. I blocchi CIDR per ogni VPC si propagano alla tabella di instradamento del gateway di transito.

| CIDR | Collegamento | Tipo di routing |
| --- | --- | --- |
| *CIDR VPC 1* | *Collegamento per VPC 1* | propagata |
| *CIDR VPC 2* | *Collegamento per VPC 2* | propagata |

# Sottoreti in AWS Wavelength

AWS Wavelength consente agli sviluppatori di creare applicazioni che offrono latenze molto basse a dispositivi mobili e utenti finali. Wavelength distribuisce servizi di calcolo e storage standard di AWS all'edge delle reti 5G dei provider all'avanguardia nei servizi di telecomunicazione. Gli sviluppatori possono ampliare un cloud privato virtuale (VPC) a una o più zone Wavelength, quindi usare le risorse AWS come le istanze Amazon EC2 per eseguire applicazioni che richiedono una latenza molto bassa e che si connettono ai Servizi AWS della regione.

Per utilizzare le zone Wavelength, devi prima scegliere la zona. Creare quindi una sottorete nella zona Wavelength. Puoi creare delle istanze Amazon EC2, volumi Amazon EBS e sottoreti Amazon VPC e carrier gateway in zone Wavelength. Inoltre, puoi utilizzare i servizi che orchestrano e lavorano con EC2, EBS e VPC come Amazon EC2 Auto Scaling, i cluster di Amazon EKS, i cluster di Amazon ECS, Amazon EC2 Systems Manager, Amazon CloudWatch, AWS CloudTrail e AWS CloudFormation. I servizi di Wavelength fanno parte di un VPC connesso con larghezza di banda elevata e affidabile a una regione AWS per un accesso semplice ai servizi come Amazon DynamoDB e Amazon RDS.

Le seguenti regole si applicano alle zone Wavelength:

- Un VPC si estende a una zona Wavelength quando si crea una sottorete nel VPC e la si associa alla zona Wavelength.
- Per impostazione predefinita, ogni sottorete creata in un VPC che si estende su una zona Wavelength eredita la tabella di instradamento VPC principale, incluso il routing locale.
- Quando si avvia un'istanza EC2 in una sottorete in una zona Wavelength, viene assegnato un indirizzo IP del carrier. Il gateway del carrier utilizza l'indirizzo per il traffico dall'interfaccia a Internet o ai dispositivi mobili. Il gateway del carrier utilizza NAT per tradurre l'indirizzo e quindi invia il traffico alla destinazione. Traffico proveniente dai routing di rete ei carrier di telecomunicazioni attraverso il gateway del carrier.
- È possibile impostare la destinazione di una tabella di instradamento VPC o di una tabella di instradamento della sottorete in una zona Wavelength su un gateway carrier, che consente il traffico in ingresso da una rete carrier in una posizione specifica e il traffico in uscita verso la rete del carrier e Internet. Per ulteriori informazioni sulle opzioni di routing in una zona Wavelength, consulta Routing nella AWS Wavelength Guida per lo sviluppatore.
- Le sottoreti nelle zone Wavelength hanno gli stessi componenti di rete delle sottoreti nelle zone di disponibilità, inclusi indirizzi IPv4, set di opzioni DHCP e ACL di rete.

- Non è possibile creare un collegamento del gateway di transito per una sottorete in una zona Wavelength. Creare invece l'allegato tramite una sottorete nella zona di disponibilità padre e quindi instradare il traffico alle destinazioni desiderate tramite il gateway di transito. Per un esempio, consultare la prossima sezione.

## Considerazioni sulle zone Wavelength multiple

Le istanze EC2 che si trovano in due diverse zone Wavelength nello stesso VPC non sono autorizzate a comunicare tra loro. Se avete bisogno di una comunicazione da zona Wavelength a zona Wavelength, AWS consiglia di utilizzare più VPC, uno per ogni zona Wavelength. È possibile utilizzare un gateway di transito per connettere i VPC. Questa configurazione consente la comunicazione tra istanze nelle zone Wavelength.

Il traffico da zona Wavelength a zona Wavelength viene instradato attraverso la regione AWS. Per ulteriori informazioni, consulta AWS Transit Gateway.

Nel diagramma seguente viene illustrato come configurare la rete in modo che le istanze di due diverse zone Wavelength possano comunicare. Sono presenti due zone Wavelength (Zona Wavelength A e Zona Wavelength B). È necessario creare le seguenti risorse per abilitare la comunicazione:

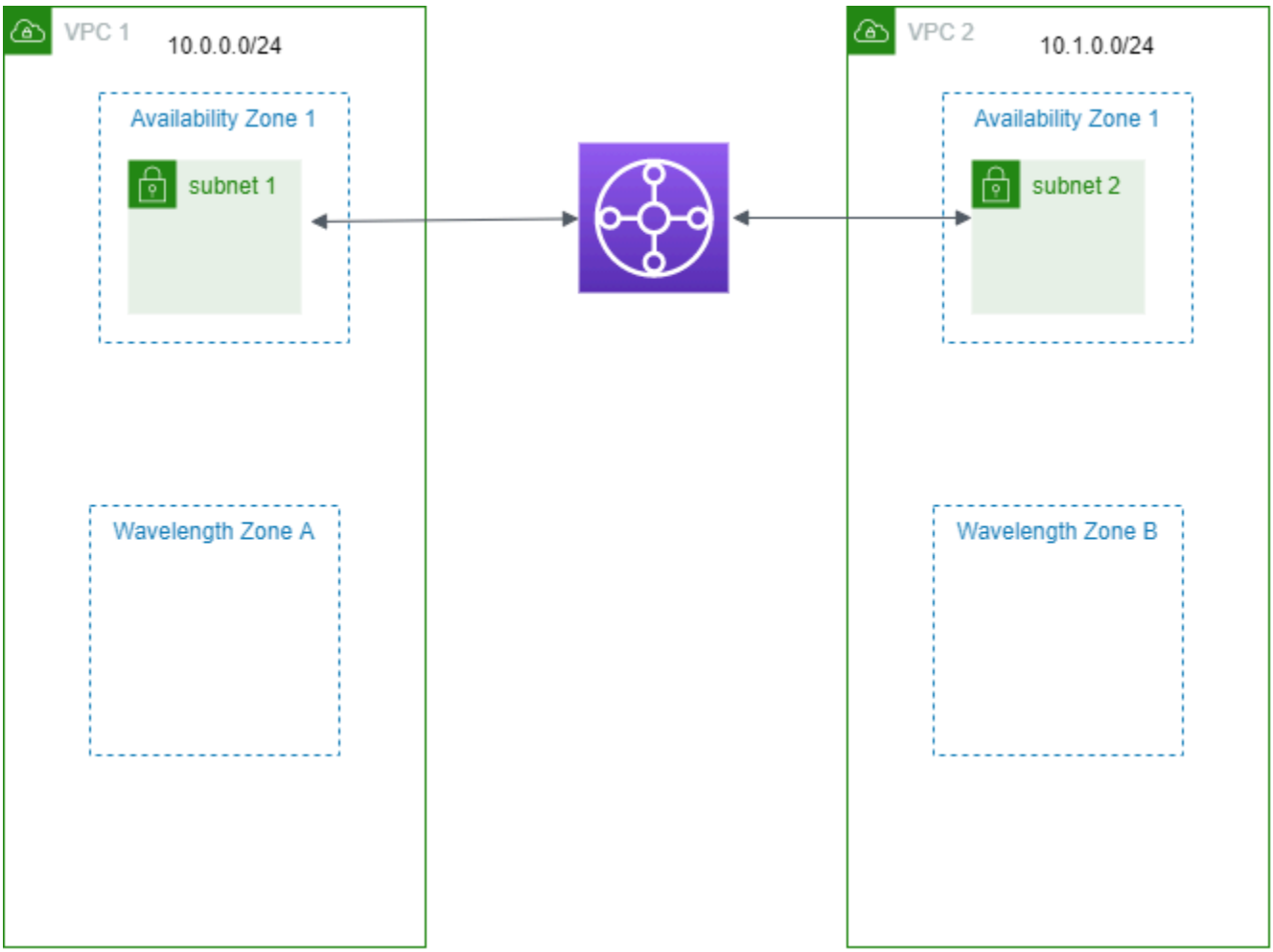
- Per ogni zona Wavelength, una sottorete in una zona di disponibilità che è la zona di disponibilità padre per la zona Wavelength. Nell'esempio viene creata la sottorete 1 e la sottorete 2. Per informazioni sulla creazione di sottoreti, vedere the section called “Creazione di una sottorete”. Utilizzare describe-availability-zones per trovare la zona padre.
- Un gateway di transito. Il gateway di transito collega i VPC. Per informazioni su come creare un gateway di transito, consulta Creazione di un gateway di transito in Guida ai gateway di transito di Amazon VPC.
- Per ogni VPC, un collegamento VPC al gateway di transito nella zona di disponibilità padre della zona Wavelength. Per ulteriori informazioni, consultare Creazione di un collegamento del gateway di transito a un VPC nella guida Gateway di transito Amazon VPC.
- Voci per ogni VPC nella tabella di routing del gateway di transito. Per informazioni su come creare routing per i gateway di transito, consulta Tabelle di routing del gateway di transito nella Guida ai gateway di transito di Amazon VPC.
- Per ogni VPC, una voce nella tabella di routing VPC con l'altro CIDR VPC come destinazione e l'ID gateway di transito come destinazione. Per ulteriori informazioni, consulta the section called “Routing per un gateway di transito”.

Nell'esempio, la tabella di instradamento per VPC 1 ha la seguente voce:

| Destinazione | Target |
| --- | --- |
| 10.1.0.0/24 | tgw-22222222222222222 |

La tabella di instradamento per VPC 2 ha la seguente voce:

| Destinazione | Target |
| --- | --- |
| 10.0.0.0/24 | tgw-22222222222222222 |



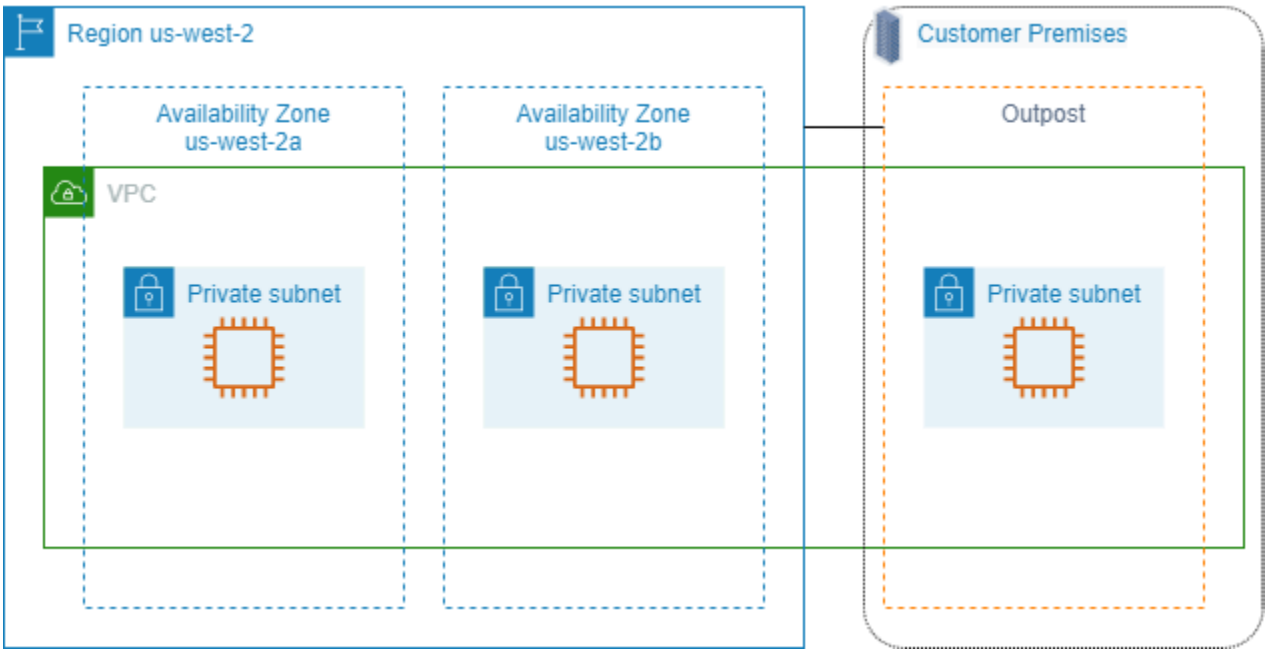
# Sottoreti in AWS Outposts

AWS Outposts ti offre la stessa infrastruttura hardware AWS, i servizi, le API e gli strumenti per creare ed eseguire le applicazioni On-Premise come nel cloud. AWS Outposts è l'ideale per carichi di lavoro che richiedono un accesso a bassa latenza ad applicazioni o sistemi On-Premise e per carichi di lavoro che devono archiviare ed elaborare i dati in locale Per ulteriori informazioni su AWS Outposts, consulta AWS Outposts.

Un VPC comprende tutte le zone di disponibilità di una regione AWS. Dopo aver collegato il tuo Outpost alla regione madre, puoi ampliare la copertura di qualsiasi VPC della regione includendo il tuo Outpost attraverso la creazione di una sottorete per l'Outpost di quel VPC.

Si applicano le seguenti regole a AWS Outposts:

- Le sottoreti devono risiedere in una posizione Outpost.
- Puoi creare una sottorete per un Outpost specificando, quando crei la sottorete, il nome della risorsa Amazon (ARN) dell'Outpost.
- Rack Outposts - il gateway locale gestisce la connettività di rete tra il VPC e le reti on-premise. Per ulteriori informazioni, consulta Gateway locali nella Guida per l'utente del rack Outposts di AWS Outposts.
- Server Outposts - l'interfaccia di rete locale gestisce la connettività di rete tra il VPC e le reti on-premise. Per ulteriori informazioni, consulta le Interfacce di rete locale nella Guida per l'utente dei server Outposts di AWS Outposts.
- Per impostazione predefinita, ogni sottorete creata in un VPC, comprese le sottoreti per gli Outposts, viene implicitamente associata alla tabella di routing principale per il VPC. Inoltre puoi associare esplicitamente una tabella di routing personalizzata alle sottoreti del VPC e disporre di un gateway locale come destinazione hop successiva per tutto il traffico che deve essere instradato per la rete on-premise.




# Eliminazione del VPC

Quando un VPC non è più necessario, è possibile eliminarlo.

Requisito

Per eliminare un VPC, devi innanzitutto terminare o eliminare tutte le risorse che hanno creato un'interfaccia di rete gestita dal richiedente nel VPC. Ad esempio, devi terminare le istanze EC2 ed eliminare i bilanciatori del carico, i gateway NAT, gli allegati del VPC del gateway di transito e gli endpoint VPC di interfaccia.

Indice



## Eliminazione di un VPC tramite la console

Se elimini un VPC tramite la console Amazon VPC, vengono eliminati anche i seguenti componenti del VPC:

- Opzioni DHCP
- Internet Gateway egress-only

- Endpoint gateway
- Gateway Internet
- Liste di controllo accessi (ACL) di rete
- Tabelle di instradamento
- Gruppi di sicurezza
- Sottoreti

Per eliminare il VPC tramite la console

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Terminare tutte le istanze nel VPC. Per ulteriori informazioni, consulta Terminate Your Instance nella Amazon EC2 User Guide.
3. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
4. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
5. Selezionare il VPC da eliminare E scegliere Actions (Operazioni), Delete VPC (Elimina VPC).
6. Verranno mostrate le eventuali risorse da eliminare o terminare per consentire l'eliminazione del cloud privato VPC. Elimina o termina queste risorse ed esegui un nuovo tentativo. In caso contrario, verranno mostrate le risorse che saranno eliminate assieme al VPC. Rivedi l'elenco e procedi con il passaggio successivo.
7. (Facoltativo) Se disponi di una connessione VPN Site-to-Site, seleziona l'opzione per eliminarla. Se previdi di utilizzare il gateway del cliente con un altro VPC, ti consigliamo di mantenere la connessione Site-to-Site VPN e i gateway. In caso contrario, è necessario configurare nuovamente il dispositivo gateway del cliente dopo aver creato una nuova connessione Site-to-Site VPN.
8. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

## Eliminazione di un VPC utilizzando la riga di comando

Prima di poter eliminare un VPC utilizzando la riga di comando, è necessario terminare o eliminare tutte le risorse che hanno creato un'interfaccia di rete gestita dal richiedente nel VPC. Inoltre, è necessario eliminare o scollegare tutte le risorse VPC create, ad esempio sottoreti, gruppi di sicurezza, ACL di rete, tabelle di routing, gateway Internet e gateway Internet egress-only. Non è necessario eliminare il gruppo di sicurezza predefinito, la tabella di routing predefinita o l'ACL di rete predefinita.

La procedura seguente illustra i comandi utilizzati per eliminare le risorse VPC comuni e quindi eliminare il VPC. Devi usare questi comandi nell'ordine seguente. Se hai creato risorse VPC aggiuntive, devi utilizzare anche il comando di eliminazione corrispondente per poter eliminare il VPC.

Per eliminare un VPC utilizzando AWS CLI

1. Elimina il gruppo di sicurezza utilizzando il comando delete-security-group.

```
aws ec2 delete-security-group --group-id sg-id
```

2. Elimina ogni ACL di rete utilizzando il comando delete-network-acl.

```
aws ec2 delete-network-acl --network-acl-id acl-id
```

3. Elimina ogni sottorete utilizzando il comando delete-subnet.

```
aws ec2 delete-subnet --subnet-id subnet-id
```

4. Elimina ogni tabella di routing personalizzata utilizzando il comando delete-route-table.

```
aws ec2 delete-route-table --route-table-id rtb-id
```

5. Scollega il gateway Internet dal VPC utilizzando il comando detach-internet-gateway.

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-id --vpc-id vpc-id
```

6. Elimina il gateway Internet utilizzando il comando delete-internet-gateway.

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-id
```

7. [VPC a dual stack] Elimina il tuo gateway Internet egress-only utilizzando il comando delete-egress-only-internet-gateway.

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-id eigw-id
```

8. Elimina il tuo VPC utilizzando il comando delete-vpc.

```
aws ec2 delete-vpc --vpc-id vpc-id
```

# Sottoreti per il VPC

una sottorete è un intervallo di indirizzi IP nel VPC; È possibile creare AWS risorse, come le istanze EC2, in sottoreti specifiche.

Indice



## Nozioni di base sulla sottorete

Ogni sottorete deve risiedere totalmente all'interno di una zona di disponibilità e non può estendersi in altre zone. Avviando AWS risorse in zone di disponibilità separate, è possibile proteggere le applicazioni dal guasto di una singola zona di disponibilità.

Indice



### Intervallo di indirizzi IP di sottorete

Quando crei una sottorete, devi specificare i relativi indirizzi IP, a seconda della configurazione del VPC:

- Solo IPv4: la sottorete ha un blocco CIDR IPv4 ma non un blocco CIDR IPv6. Le risorse in una sottorete solo IPv4 devono comunicare tramite IPv4.

- Dual-stack: la sottorete ha sia un blocco CIDR IPv4 che un blocco CIDR IPv6. Il VPC deve avere sia un blocco CIDR IPv4 che un blocco CIDR IPv6. Le risorse in una sottorete dual-stack possono comunicare tramite IPv4 e IPv6.
- Solo IPv6: la sottorete ha un blocco CIDR IPv6 ma non un blocco CIDR IPv4. Il VPC deve disporre di un blocco CIDR IPv6. Le risorse in una sottorete solo IPv6 devono comunicare tramite IPv6.

> **Note**
>
> Alle risorse nelle sottoreti solo IPv6 vengono assegnati indirizzi link-local IPv4 dal blocco CIDR `169.254.0.0/16`. Questi indirizzi vengono utilizzati per comunicare con servizi VPC come il Servizio di metadati di istanza (IMDS).

Per ulteriori informazioni, consulta Indirizzi IP per i tuoi VPC e sottoreti.

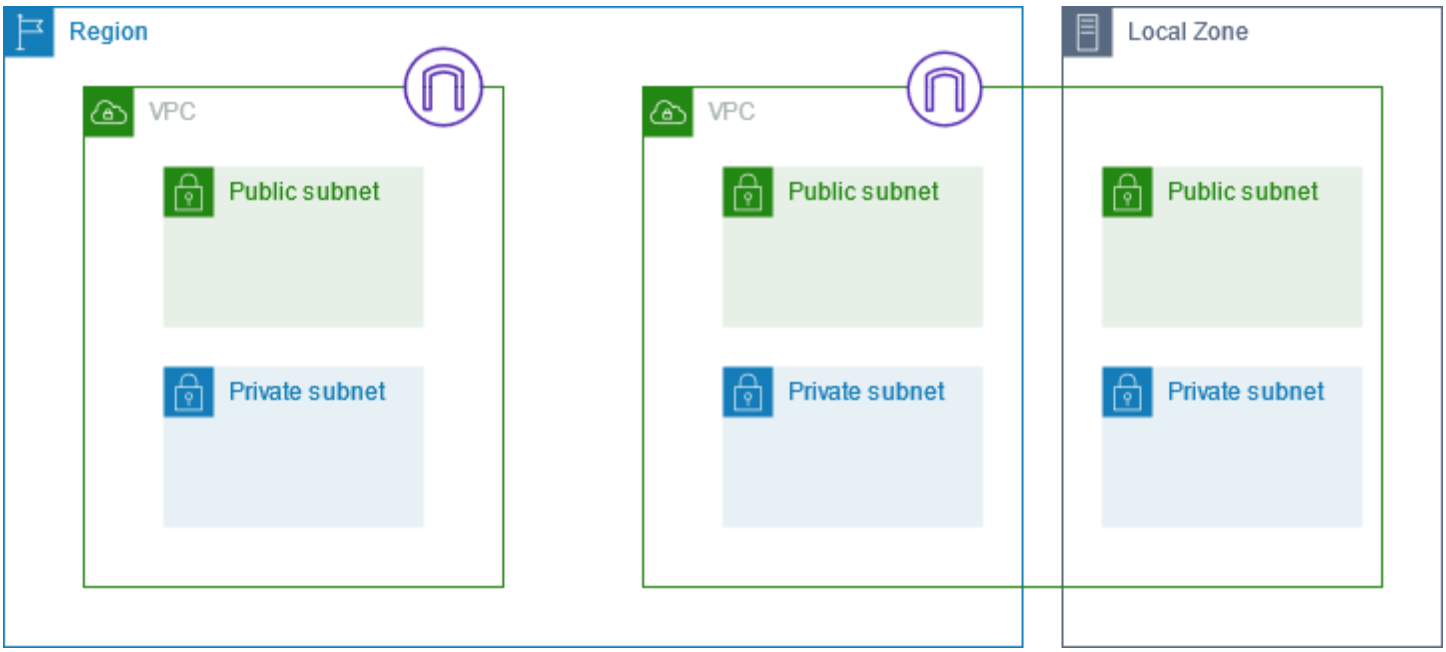
## Tipi di sottorete

Il tipo di sottorete è determinato dalla modalità di configurazione del routing per le sottoreti. Per esempio:

- Sottorete pubblica: la sottorete ha un percorso diretto a un gateway Internet. Le risorse di una sottorete pubblica possono accedere alla rete Internet pubblica.
- Sottorete privata: la sottorete non ha un instradamento diretto a un gateway Internet. Le risorse in una sottorete privata richiedono un dispositivo NAT per accedere alla rete Internet pubblica.
- Sottorete solo VPN: la sottorete ha un instradamento diretto a una connessione VPN Site-to-Site tramite un gateway privato virtuale. La sottorete pubblica non ha una route a un gateway Internet.
- Sottorete isolata: la sottorete non ha percorsi verso destinazioni esterne al suo VPC. Le risorse in una sottorete isolata possono accedere o essere accessibili solo da altre risorse nello stesso VPC.

## Diagramma sottorete

Il seguente diagramma mostra due VPC in una regione. Ogni VPC dispone di sottoreti pubbliche e private e di un gateway Internet. Facoltativamente, hai la possibilità di aggiungere sottoreti in una zona locale, come mostrato nel diagramma. Una zona locale è un'implementazione AWS dell'infrastruttura che avvicina i servizi di elaborazione, archiviazione e database agli utenti finali. Utilizzando una zona locale, gli utenti finali sono in grado di eseguire applicazioni che richiedono latenze inferiori ai 10 millisecondi. Per ulteriori informazioni, consulta AWS Zone locali.




## Routing della sottorete

Ogni sottorete deve Essere associata a una tabella di instradamento, che specifica le route consentite per il traffico in uscita che lascia la sottorete. Ogni sottorete creata viene automaticamente associata alla tabella di instradamento principale per il VPC. Puoi modificare l'associazione E modificare il contenuto della tabella di instradamento principale. Per ulteriori informazioni, consulta Configurare le tabelle di routing.

## Impostazioni sottorete

Tutte le sottoreti hanno un attributo modificabile che determina se all'interfaccia di rete creata nella sottorete viene assegnato un indirizzo IPv4 pubblico e, se possibile, un indirizzo IPv6. Questo include l'interfaccia di rete primaria (eth0) creata per l'istanza quando questa viene avviata nella sottorete. Indipendentemente dall'attributo della sottorete, puoi comunque sostituire questa impostazione per un'istanza specifica durante il suo avvio.

Una volta creata, la sottorete può essere modificata nelle seguenti impostazioni:

- Impostazioni di assegnazione automatica IP: consente di configurare le impostazioni di assegnazione automatica IP per richiedere automaticamente un indirizzo IPv4 o IPv6 pubblico per una nuova interfaccia di rete in questa sottorete.
- Impostazioni RBN (Resource-based Name): consente di specificare il tipo di nome host per le istanze EC2 in questa sottorete e di configurare il modo in cui vengono gestite le query dei registri

DNS A e AAAA. Per ulteriori informazioni, consulta i tipi di hostname delle istanze Amazon EC2 nella Amazon EC2 User Guide.

## Sicurezza della sottorete

Per proteggere AWS le tue risorse, ti consigliamo di utilizzare sottoreti private. Utilizza un host bastione o un dispositivo NAT per fornire l'accesso Internet per l'accesso Internet, ad esempio istanze EC2, in una sottorete privata.

AWS offre funzionalità che puoi utilizzare per aumentare la sicurezza delle risorse nel tuo VPC. I gruppi di sicurezza consentono il traffico in entrata e in uscita delle risorse associate, ad esempio le istanze EC2. Le ACL di rete consentono o rifiutano il traffico in entrata e in uscita a livello di sottorete. Nella maggior parte dei casi, i gruppi di sicurezza possono soddisfare le tue esigenze. Se desideri un livello di sicurezza aggiuntivo per il tuo VPC, puoi utilizzare le ACL di rete. Per ulteriori informazioni, consulta the section called “Confronto dei gruppi di sicurezza e delle liste di controllo accessi di rete”.

Per impostazione predefinita, ogni sottorete deve Essere associata a una lista di controllo accessi di rete. Ogni sottorete creata viene automaticamente associata alla lista di controllo accessi di rete predefinita del VPC. L'ACL di rete predefinita consente tutto il traffico in entrata e in uscita. È possibile aggiornare l'ACL di rete predefinita o creare ACL di rete personalizzate e associarle alle sottoreti. Per ulteriori informazioni, consulta Come controllare il traffico verso le sottoreti utilizzando le liste di controllo degli accessi di rete.

Puoi creare un log di flusso sul VPC o sulla sottorete per acquisire il flusso di traffico per e dalle interfacce di rete nel VPC o nella sottorete. Puoi anche creare un log di flusso su un'interfaccia di rete singola. Per ulteriori informazioni, consulta Registrazione del traffico IP utilizzando log di flusso VPC.

## Creazione di una sottorete

Usa la procedura seguente per creare sottoreti per il cloud privato virtuale (VPC). A seconda della connettività di cui hai bisogno, potrebbe essere necessario aggiungere gateway e tabelle di routing.

Considerazioni

- È necessario specificare un blocco CIDR IPv4 per la sottorete dalla gamma di VPC. Facoltativamente, puoi specificare un blocco CIDR IPv6 per la sottorete se esiste un blocco CIDR IPv6 associato al VPC. Per ulteriori informazioni, consulta Indirizzi IP per i tuoi VPC e sottoreti.

- Se crei una sottorete solo IPv6, tieni presente quanto segue. Un'istanza EC2 avviata in una sottorete solo IPv6 riceve un indirizzo IPv6 ma non un indirizzo IPv4. Le istanze che avvii in una sottorete solo IPv6 devono essere istanze basate su Nitro System.
- Per creare la sottorete in una zona locale o in una zona Wavelength, è necessario abilitare la zona. Per maggiori informazioni, consulta Regioni e zone di disponibilità nella Guida per l'utente di Amazon EC2.

Per aggiungere una sottorete al VPC

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
3. Scegliere Create subnet (Crea sottorete).
4. In VPC ID (ID VPC), scegli il VPC per la sottorete.
5. (Facoltativo) Per Subnet name (Nome sottorete) inserisci un nome per la sottorete. In questo modo viene creato un tag con una chiave di `Name` e il valore specificato.
6. Per Zona di disponibilità, puoi scegliere una zona per la tua sottorete o lasciare l'impostazione predefinita Nessuna preferenza per consentirti di AWS sceglierne una per te.
7. Per IPv4 CIDR block (Blocco CIDR IPv4), seleziona Manual input (Input manuale) per inserire un blocco CIDR IPv4 per la sottorete (ad esempio `10.0.1.0/24`) oppure seleziona No IPv4 CIDR (Nessun CIDR IPv4). Se utilizzi Amazon VPC IP Address Manager (IPAM) per pianificare, tracciare e monitorare gli indirizzi IP per i tuoi AWS carichi di lavoro, quando crei una sottorete hai la possibilità di allocare un blocco CIDR da IPAM (allocato tramite IPAM). Per ulteriori informazioni sulla pianificazione dello spazio degli indirizzi IP VPC per le allocazioni IP della sottorete, consulta il Tutorial: Pianificare lo spazio degli indirizzi IP VPC per allocazioni IP della sottorete nella Guida per l'utente IPAM di Amazon VPC.
8. Per IPv6 CIDR block (Blocco CIDR IPv6), seleziona Manual input (Input manuale) per scegliere il CIDR IPv6 del VPC in cui creare una sottorete. Questa opzione è disponibile solo se il VPC dispone di un blocco CIDR IPv6 associato. Se utilizzi Gestione indirizzi IP (IPAM) di Amazon VPC per pianificare, tracciare e monitorare gli indirizzi IP per i carichi di lavoro AWS , quando crei una sottorete puoi allocare un blocco CIDR da IPAM (allocato tramite IPAM). Per ulteriori informazioni sulla pianificazione dello spazio degli indirizzi IP VPC per le allocazioni IP della sottorete, consulta il Tutorial: Pianificare lo spazio degli indirizzi IP VPC per allocazioni IP della sottorete nella Guida per l'utente IPAM di Amazon VPC.
9. Scegli un IPv6 VPC CIDR block (Blocco CIDR VPC IPv6).

10. Per IPv6 subnet CIDR block (Blocco CIDR sottorete IPv6), scegli un CIDR per la sottorete che sia uguale o più specifico del CIDR VPC. Ad esempio, se il CIDR del pool VPC è /50, puoi scegliere una lunghezza della maschera di rete compresa tra /50 e /64 per la sottorete. Le lunghezze possibili delle maschere di rete IPv6 sono comprese tra /44 e /64 con incrementi di /4.
11. Scegliere Create subnet (Crea sottorete).

Per aggiungere una sottorete al VPC utilizzando il AWS CLI

Usa il comando create-subnet.

Passaggi successivi

Dopo aver creato una sottorete, è possibile configurarla come segue:

- Configurare il routing. È quindi possibile creare una tabella di instradamento personalizzata e una route per inviare il traffico a un gateway associato al VPC, ad esempio un gateway Internet. Per ulteriori informazioni, consulta Configurare le tabelle di routing.
- Modifica gli indirizzi IP della sottorete. Per ulteriori informazioni, consulta the section called “Configurazione delle sottoreti”.
- Modificare il comportamento di assegnazione di indirizzi IP. È possibile specificare se le istanze avviate in tale sottorete ricevono un indirizzo IPv4 pubblico, un indirizzo IPv6 o entrambi. Per ulteriori informazioni, consulta Impostazioni sottorete.
- Modifica le impostazioni del nome basato sulle risorse (RBN). Per ulteriori informazioni, consultare Tipi di nomi host delle istanze Amazon EC2.
- Creare o modificare le liste di controllo accessi di rete. Per ulteriori informazioni, consulta Come controllare il traffico verso le sottoreti utilizzando le liste di controllo degli accessi di rete.
- Condividere la sottorete con altri account. Per ulteriori informazioni, consulta ???.

# Configurazione delle sottoreti

Usa le procedure seguenti per configurare sottoreti per il cloud privato virtuale (VPC).

Attività

- Visualizzazione delle sottoreti
- Come aggiungere un blocco CIDR IPv6 alla sottorete
- Rimozione di un blocco CIDR IPv6 dalla sottorete

- Modifica dell'attributo di assegnazione degli indirizzi IPv4 pubblici per la sottorete
- Modifica dell'attributo di assegnazione di indirizzi IPv6 pubblici per la sottorete

## Visualizzazione delle sottoreti

Seguire i passaggi di questa sezione per visualizzare i dettagli della propria sottorete.

Per visualizzare i dettagli della sottorete tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
3. Seleziona la casella di controllo per la sottorete o scegli l'ID della sottorete per aprire la pagina prodotto.

Per descrivere una sottorete utilizzando AWS CLI

Usa il comando describe-subnets.

Visualizzazione delle sottoreti tra tutte le regioni

Apri la console Amazon EC2 Global View all'indirizzo https://console.aws.amazon.com/ec2globalview/home. Per ulteriori informazioni, consulta Elencare e filtrare le risorse utilizzando Amazon EC2 Global View nella Amazon EC2 User Guide.

## Come aggiungere un blocco CIDR IPv6 alla sottorete

Puoi associare un blocco CIDR IPv6 a una sottorete Esistente nel VPC. Non associare alla sottorete un blocco CIDR IPv6 esistente.

Aggiunta di un blocco CIDR IPv6 a una sottorete

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
3. Selezionare la sottorete e scegliere Actions (Operazioni), Edit IPv6 CIDRs (Modifica CIDR IPv6).
4. Selezionare Add IPv6 CIDR (Aggiungi CIDR IPv6).
5. Scegli un blocco CIDR VPC, inserisci un blocco CIDR della sottorete, quindi scegli una lunghezza della maschera di rete uguale o più specifica della lunghezza della maschera di rete

del CIDR VPC. Ad esempio, se il CIDR del pool VPC è /50, puoi scegliere una lunghezza della maschera di rete compresa tra /50 e /64 per la sottorete. Le lunghezze possibili delle maschere di rete IPv6 sono comprese tra /44 e /64 con incrementi di /4.

6. Selezionare Salva.

Per associare un blocco CIDR IPv6 a una sottorete utilizzando AWS CLI

Usa il comando associate-subnet-cidr-block.

## Rimozione di un blocco CIDR IPv6 dalla sottorete

Se non desideri più il supporto IPv6 nella sottorete ma vuoi continuare a utilizzare la sottorete per creare e comunicare con risorse IPv4, puoi rimuovere il blocco CIDR IPv6.

Per rimuovere un blocco CIDR IPv6, devi innanzitutto annullare l'assegnazione di qualsiasi indirizzo IPv6 che è stato assegnato a qualsiasi istanza nella sottorete.

Rimozione di un blocco CIDR IPv6 da una sottorete

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
3. Selezionare la sottorete e scegliere Actions (Operazioni), Edit IPv6 CIDRs (Modifica CIDR IPv6).
4. Trova il blocco CIDR IPv6 e scegli Remove (Rimuovi).
5. Selezionare Salva.

Per dissociare un blocco CIDR IPv6 da una sottorete utilizzando AWS CLI

Usa il comando disassociate-subnet-cidr-block.

## Modifica dell'attributo di assegnazione degli indirizzi IPv4 pubblici per la sottorete

Per impostazione predefinita, le sottoreti non predefinite hanno l'attributo di indirizzamento IP4 pubblico impostato su `false`, mentre le sottoreti predefinite lo hanno impostato su `true`. Fa eccezione la sottorete non predefinita creata dalla procedura guidata di avvio dell'istanza Amazon EC2: la procedura guidata imposta l'attributo su `true`. L'attributo è modificabile tramite la console Amazon VPC.

Per modificare il comportamento di assegnazione degli indirizzi IPv4 pubblici della sottorete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
3. Selezionare la sottorete e scegliere Actions (Operazioni), Edit subnet (Modifica sottorete).
4. La casella di controllo Enable auto-assign public IPv4 address (Abilita assegnazione automatica degli indirizzi IPv4 pubblici) richiede un indirizzo IPv4 pubblico per tutte le istanze avviate nella sottorete selezionata. Selezionare o deselezionare la casella di controllo in base alle Esigenze, quindi selezionare Save (Salva).

Per modificare un attributo di sottorete utilizzando AWS CLI

Usa il comando modify-subnet-attribute.

## Modifica dell'attributo di assegnazione di indirizzi IPv6 pubblici per la sottorete

Per impostazione predefinita, tutte le sottoreti hanno l'attributo di indirizzamento IPv6 impostato su `false`. L'attributo è modificabile tramite la console Amazon VPC. Se abiliti l'attributo di assegnazione di indirizzi IPv6 nella tua sottorete, le interfacce di rete create nella sottorete ricevono un indirizzo IPv6 compreso nell'intervallo della sottorete. Le istanze avviate nella sottorete ricevono un indirizzo IPv6 nell'interfaccia di rete primaria.

La sottorete deve Essere associata a un blocco CIDR IPv6.

> **Note**
>
> Se abiliti la funzione di assegnazione di indirizzi IPv6 nella tua sottorete, l'interfaccia di rete o l'istanza ricevono un indirizzo IPv6 solo se sono state create utilizzando la versione `2016-11-15` o successiva dell'API Amazon EC2. La console Amazon EC2 utilizza la versione più recente dell'API.

Per modificare il comportamento di assegnazione di indirizzi IPv6 della sottorete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).

3. Selezionare la sottorete e scegliere Actions (Operazioni), Edit subnet (Modifica sottorete).
4. La casella di controllo Enable auto-assign public IPv6 address (Abilita assegnazione automatica degli indirizzi IPv6 pubblici) richiede un indirizzo IPv6 pubblico per tutte le interfacce di rete create nella sottorete selezionata. Selezionare o deselezionare la casella di controllo in base alle Esigenze, quindi selezionare Save (Salva).

Per modificare un attributo di sottorete utilizzando AWS CLI

Usa il comando modify-subnet-attribute

# Prenotazioni della CIDR per la sottorete

Una prenotazione CIDR di sottorete è un intervallo di indirizzi IPv4 o IPv6 che metti da parte in modo da non AWS poterli assegnare alle interfacce di rete. Ciò consente di riservare blocchi CIDR IPv4 o IPv6 (denominati anche "prefissi") da utilizzare con le tue interfacce di rete.

Quando si crea la prenotazione CIDR della sottorete, si specifica la modalità di utilizzo dell'indirizzo IP riservato. Sono disponibili le seguenti opzioni:

- Prefisso: AWS assegna gli indirizzi dell'intervallo di indirizzi IP riservato alle interfacce di rete. Per ulteriori informazioni, consulta Assegnare prefissi alle interfacce di rete di Amazon EC2 nella Amazon EC2 User Guide.
- Esplicito — Puoi assegnare manualmente indirizzi IP a interfacce di rete.

Le seguenti regole si applicano alle prenotazioni del CIDR per la sottorete:

- Quando si crea una prenotazione CIDR di sottorete, l'intervallo di indirizzi IP può includere indirizzi già in uso. La creazione di una prenotazione di sottorete non annulla l'assegnazione di alcun indirizzo IP già in uso.
- È possibile prenotare più intervalli CIDR per sottorete. Quando si prenotano più intervalli CIDR all'interno dello stesso VPC, gli intervalli CIDR non possono sovrapporsi.
- Quando si prenota più di un intervallo in una sottorete per la delega Prefisso e la delega Prefisso è configurata per l'assegnazione automatica, viene scelto casualmente un indirizzo IP da assegnare all'interfaccia di rete.
- Quando elimini una prenotazione di sottorete, gli indirizzi IP non utilizzati sono disponibili per l'assegnazione alle interfacce di rete. AWS L'eliminazione di una prenotazione di sottorete non annulla l'assegnazione di alcun indirizzo IP in uso.

Per ulteriori informazioni sulla notazione routing interdominio senza classi (CIDR), consulta Assegnazione di indirizzi IP.

## Come lavorare con le prenotazioni del CIDR della sottorete tramite la console

Puoi creare e gestire le prenotazioni del CIDR per la sottorete nel modo seguente.

Modifica delle prenotazioni del CIDR per la sottorete

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
3. Seleziona la sottorete.
4. Scegli la scheda Prenotazioni CIDR per ottenere informazioni su eventuali prenotazioni CIDR della sottorete esistente.
5. Per aggiungere o rimuovere le prenotazioni CIDR della sottorete, scegli Operazioni, Modifica prenotazioni CIDR, quindi procedi come segue:
   - Per aggiungere una prenotazione CIDR IPv4, scegli IPv4, Add IPv4 CIDR reservation (Aggiungi la prenotazione CIDR IPv4). Scegli il tipo di prenotazione, inserisci l'intervallo CIDR e scegli Add (Aggiungi).
   - Per aggiungere una prenotazione CIDR IPv6, scegli IPv6, Add IPv6 CIDR reservation (Aggiungi la prenotazione CIDR IPv6). Scegli il tipo di prenotazione, inserisci l'intervallo CIDR e scegli Add (Aggiungi).
   - Per rimuovere una prenotazione CIDR, scegli Rimuovi per la prenotazione CIDR della sottorete.

## Lavora con le prenotazioni CIDR di sottorete utilizzando il AWS CLI

È possibile utilizzare il AWS CLI per creare e gestire le prenotazioni CIDR su sottorete.

Attività

- Creare una prenotazione della CIDR per la sottorete
- Visualizza prenotazioni della CIDR per la sottorete
- Eliminare una prenotazione della CIDR per la sottorete

### Creare una prenotazione della CIDR per la sottorete

È possibile utilizzare create-subnet-cidr-reserv per creare una prenotazione della CIDR per la sottorete.

```
aws ec2 create-subnet-cidr-reservation --subnet-id subnet-03c51e2eEXAMPLE --
reservation-type prefix --cidr 2600:1f13:925:d240:3a1b::/80
```

Di seguito è riportato un output di esempio.

```
{
    "SubnetCidrReservation": {
        "SubnetCidrReservationId": "scr-044f977c4eEXAMPLE",
        "SubnetId": "subnet-03c51e2ef5EXAMPLE",
        "Cidr": "2600:1f13:925:d240:3a1b::/80",
        "ReservationType": "prefix",
        "OwnerId": "123456789012"
    }
}
```

### Visualizza prenotazioni della CIDR per la sottorete

È possibile utilizzare get-subnet-cidr-reserv per visualizzare i dettagli di una prenotazione della CIDR per la sottorete.

```
aws ec2 get-subnet-cidr-reservations --subnet-id subnet-05eef9fb78EXAMPLE
```

### Eliminare una prenotazione della CIDR per la sottorete

È possibile utilizzare delete-subnet-cidr-reserv per eliminare una prenotazione della CIDR per la sottorete.

```
aws ec2 delete-subnet-cidr-reservation --subnet-cidr-reservation-
id scr-044f977c4eEXAMPLE
```

## Configurare le tabelle di routing

Una tabella di instradamento contiene un insieme di regole, denominato route, che consente di determinare la direzione del traffico di rete dalla sottorete o dal gateway.

Indice



## Concetti relativi alla tabella di instradamento

Di seguito sono riportati i concetti chiave per le tabelle di routing.

- Tabella di routing principale: la tabella di routing fornita automaticamente con il VPC. Controlla il routing di tutte le sottoreti che non sono state esplicitamente associate a un'altra tabella di routing.
- Tabella di routing personalizzata: una tabella di routing creata per lo specifico VPC.
- Destinazione: intervallo di indirizzi IP in cui si desidera incanalare il traffico (CIDR di destinazione). Ad esempio una rete aziendale esterna con il CIDR `172.16.0.0/12`.
- Destinazione: il gateway, l'interfaccia di rete o la connessione tramite cui inviare il traffico di destinazione, ad esempio un gateway Internet.
- Associazione di tabelle di routing: l'associazione tra una tabella di routing e una sottorete, un Internet gateway o un gateway virtuale privato.
- Tabella di routing della sottorete: una tabella di routing associata a una sottorete.
- Route locale: una route predefinita per la comunicazione all'interno del VPC.
- Propagazione: se hai collegato un gateway privato virtuale al tuo VPC e abiliti la propagazione dei percorsi, i percorsi verranno aggiunti automaticamente per la connessione della VPN alle tabelle di instradamento della tua sottorete. In tal modo, non sarà necessario aggiungere o rimuovere manualmente i percorsi della VPN. Per ulteriori informazioni, consulta Opzioni di instradamento di VPN Site-to-Site nella Guida per l'utente di VPN Site-to-Site.
- Tabella di routing del gateway: una tabella di routing associata a un Internet gateway o a un gateway virtuale privato.

- Associazione Edge : tabella di routing utilizzata per instradare il traffico VPC in ingresso a un'appliance. Associa una tabella di routing all'Internet gateway o al gateway virtuale privato, quindi specifica l'interfaccia di rete dell'appliance come target per il traffico VPC.
- Tabella di routing del Transit Gateway: una tabella di routing associata a un Transit Gateway. Per ulteriori informazioni, consulta Tebelle di routing del gateway di transito in Gateway di transito di Amazon VPC.
- Tabella di routing del gateway locale: una tabella di routing associata a un gateway locale Outposts. Per ulteriori informazioni, consultare Gateway locali nella Guida per l'utente di AWS Outposts .

## Tabelle di routing di sottoreti

Il VPC dispone di un router implicito e puoi utilizzare le tabelle di routing per controllare la direzione del traffico di rete. Ogni sottorete nel VPC deve essere associata a una tabella di instradamento, che controlla il routing per la sottorete (tabella di instradamento della sottorete). Puoi associare esplicitamente una sottorete a una particolare tabella di instradamento. In caso contrario, la sottorete è implicitamente associata alla tabella di instradamento principale. Una sottorete può essere associata a una sola tabella di instradamento alla volta, ma puoi associare più sottoreti alla stessa tabella di instradamento.

Indice



### Route

Ogni route in una tabella specifica una destinazione e un target. Ad esempio, per consentire alla sottorete di accedere a Internet tramite un Internet gateway, aggiungi la seguente route alla tabella di instradamento della sottorete. La destinazione per la route è `0.0.0.0/0`, che rappresenta tutti gli indirizzi IPv4. Il target è l'Internet gateway collegato al VPC.

| Destinazione | Target |
| --- | --- |
| 0.0.0.0/0 | *igw-id* |

I blocchi CIDR per IPv4 e IPv6 sono trattati separatamente. Ad esempio, una route con un CIDR di destinazione `0.0.0.0/0` non include automaticamente tutti gli indirizzi IPv6. Devi creare una route con un CIDR di destinazione `::/0` per tutti gli indirizzi IPv6.

Se fai spesso riferimento allo stesso set di blocchi CIDR tra AWS le tue risorse, puoi creare un elenco di prefissi gestito dal cliente per raggrupparli. È quindi possibile specificare l'elenco di prefissi come destinazione nella voce della tabella di instradamento.

Ogni tabella di instradamento contiene una route locale per la comunicazione all'interno del VPC. Questa route viene aggiunta per impostazione predefinita a tutte le tabelle di routing. Se il VPC include più blocchi CIDR IPv4, le tabelle di routing contengono una route locale per ogni blocco CIDR IPv4. Se al VPC hai associato un blocco CIDR IPv6, le tabelle di routing contengono una route locale per il blocco CIDR IPv6. Puoi sostituire o ripristinare la destinazione di ciascuna route locale in base alle esigenze.

Regole e considerazioni

- È possibile aggiungere alle tabelle di routing una route che sia più specifica della route locale. La destinazione deve corrispondere all'intero blocco CIDR IPv4 o IPv6 di una sottorete nel VPC. La destinazione deve essere un gateway NAT, un'interfaccia di rete o un endpoint Gateway Load Balancer.
- Se la tabella di instradamento ha più route, utilizziamo quella più specifica corrispondente al traffico (corrispondenza di prefisso più lunga) per determinare come instradare il traffico.
- Non è possibile aggiungere percorsi agli indirizzi IPv4 che corrispondono esattamente o un sottoinsieme del seguente intervallo: 169.254.168.0/22. Questo intervallo rientra nello spazio degli indirizzi locali del collegamento ed è riservato all'uso da parte dei servizi. AWS Ad esempio, Amazon EC2 utilizza gli indirizzi in questo intervallo per i servizi accessibili solo dalle istanze EC2, come Instance Metadata Service (IMDS) e il server Amazon DNS. È possibile utilizzare un blocco CIDR più grande ma che si sovrappone a 169.254.168.0/22, ma i pacchetti destinati agli indirizzi in 169.254.168.0/22 non verranno inoltrati.
- Non è possibile aggiungere percorsi agli indirizzi IPv6 che sono un'esatta corrispondenza o un sottoinsieme del seguente intervallo: fd00:ec2::/32. Questo intervallo rientra nello spazio degli

indirizzi locali univoci (ULA) ed è riservato all'uso da parte AWS dei servizi. Ad esempio, Amazon EC2 utilizza gli indirizzi in questo intervallo per i servizi accessibili solo dalle istanze EC2, come Instance Metadata Service (IMDS) e il server Amazon DNS. È possibile utilizzare un blocco CIDR più grande di fd00:ec2::/32, ma i pacchetti destinati agli indirizzi in fd00:ec2::/32 non verranno inoltrati.

- È possibile aggiungere appliance middlebox nei percorsi di routing per il VPC. Per ulteriori informazioni, consultare the section called “Routing per un'appliance middlebox”.

Esempio

Nel seguente diagramma, un VPC dispone sia di un blocco CIDR IPv4 che di un blocco CIDR IPv6. Il traffico IPv4 e IPv6 viene trattato separatamente, come illustrato nella seguente tabella di routing.

| Destinazione | Target |
|---|---|
| 10.0.0.0/16 | Local |
| 2001:db8:1234:1a00::/56 | Local |
| 172.31.0.0/16 | pcx-11223344556677889 |
| 0.0.0.0/0 | igw-12345678901234567 |
| ::/0 | eigw-aabbccddee1122334 |

- Il traffico IPv4 da instradare all'interno del VPC (10.0.0.0/16) è coperto dal percorso Local.
- Il traffico IPv6 da instradare all'interno del VPC (2001:db8:1234:1a00::/56) è coperto dal percorso Local.
- Il percorso per 172.31.0.0/16 invia il traffico a una connessione peering.
- Il percorso per tutto il traffico IPv4 (0.0.0.0/0) invia il traffico a un gateway Internet. Pertanto, tutto il traffico IPv4, ad eccezione del traffico all'interno del VPC e verso la connessione peering, viene indirizzato al gateway Internet.
- Il percorso per tutto il traffico IPv6 (::/0) invia il traffico a un gateway Internet di sola uscita. Pertanto, tutto il traffico IPv6, ad eccezione del traffico all'interno del VPC, viene indirizzato al gateway Internet di sola uscita.

## Tabella di routing principale

Quando crei un VPC, questo include automaticamente una tabella di instradamento principale. Se una sottorete non è esplicitamente associata a una tabella di routing, per impostazione predefinita utilizza la tabella di routing principale. Nella pagina Tabelle di instradamento della console Amazon VPC, puoi visualizzare la tabella di instradamento principale di un VPC cercando Sì nella colonna Principale.

Per impostazione predefinita, quando crei un VPC non predefinito, la tabella di instradamento principale contiene solo una route locale. Se Crea un VPC e scegli un gateway NAT , Amazon VPC aggiunge automaticamente le route alla tabella di instradamento principale per i gateway.

Le seguenti regole si applicano alla tabella di instradamento principale:

- Puoi aggiungere, rimuovere E modificare le route nella tabella di instradamento principale.
- Non puoi eliminare la tabella di instradamento principale.
- Non è possibile impostare una tabella di routing del gateway come tabella di routing principale.
- È possibile sostituire la tabella di routing principale associando una tabella di routing personalizzata a una sottorete.
- Puoi associare in modo esplicito una sottorete alla tabella di instradamento principale, anche se è già implicitamente associata.

  Questa operazione può essere utile quando cambi la tabella di instradamento principale. In questo caso, viene modificata anche la tabella predefinita per le nuove sottoreti o per qualsiasi sottorete non esplicitamente associata ad altre tabelle di routing. Per ulteriori informazioni, consulta Sostituzione della tabella di instradamento principale.

## Tabelle di routing personalizzate

Per impostazione predefinita, una tabella di routing contiene un percorso locale per la comunicazione all'interno del VPC. Se Crea un VPC e scegli una sottorete pubblica, Amazon VPC crea una tabella di instradamento personalizzata e aggiunta una route che punta al gateway Internet. Un modo per proteggere il VPC è lasciare la tabella di instradamento principale nel suo stato predefinito originale. Quindi, associare esplicitamente tutte le nuove sottoreti a una delle tabelle di routing personalizzate che hai creato. Ciò consente di controllare esplicitamente il modo in cui ogni sottorete instrada il traffico.

Puoi aggiungere, rimuovere e modificare le route in una tabella di instradamento personalizzata. Puoi eliminare una tabella di instradamento personalizzata solo se non ha associazioni.

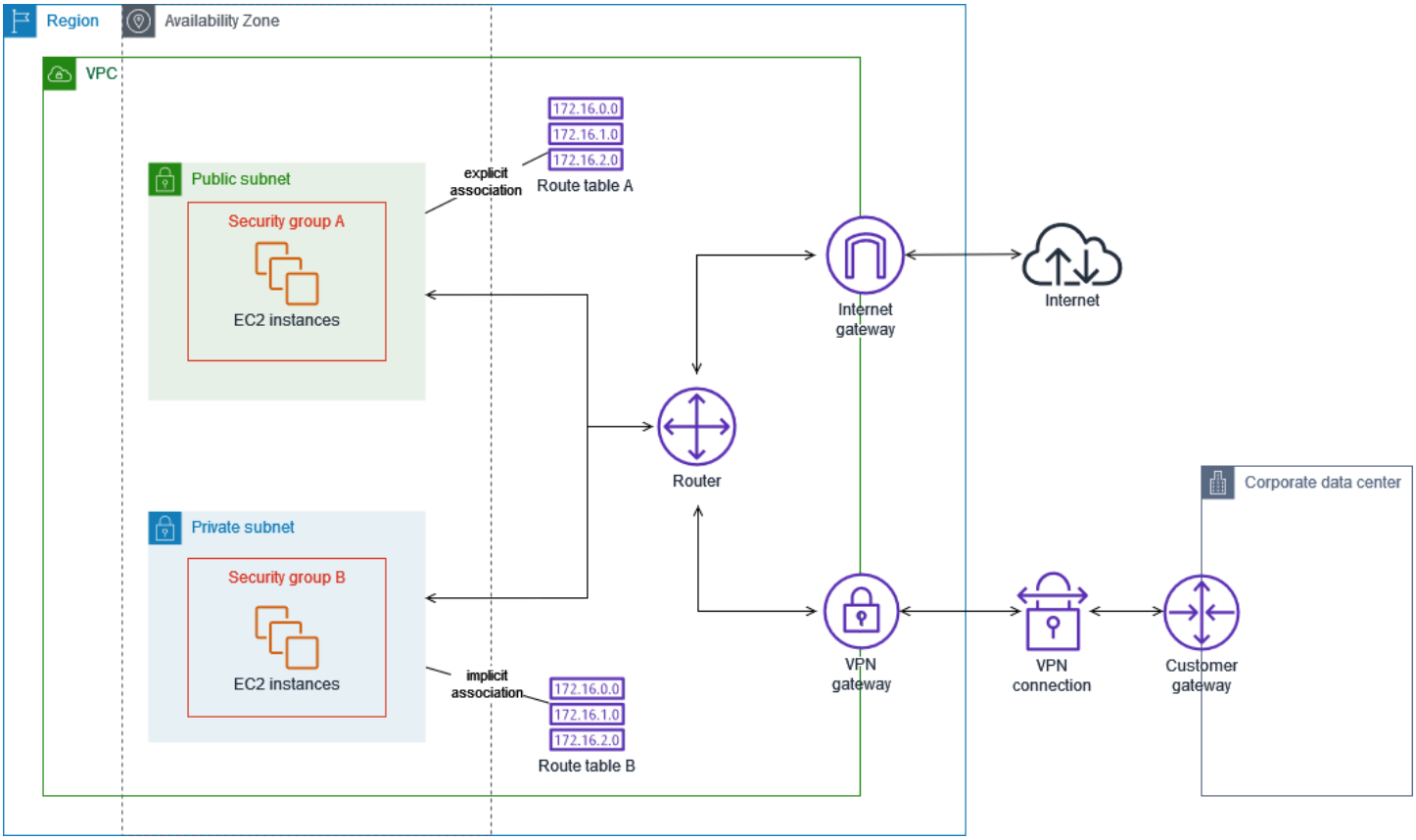
## Associazione di tabelle di routing della sottorete

Ogni sottorete nel VPC deve essere associata a una tabella di instradamento. Una sottorete può essere associata esplicitamente alla tabella di instradamento personalizzata oppure, implicitamente o esplicitamente, alla tabella di instradamento principale. Per maggiori informazioni sulla visualizzazione delle associazioni della sottorete e della tabella di instradamento, consulta Determinazione delle sottoreti o dei gateway associati esplicitamente.

Le sottoreti che si trovano in VPC associati a Outposts possono avere un tipo di target aggiuntivo per un gateway locale. Questa è l'unica differenza di routing rispetto alle sottoreti non Outposts.

Esempio 1: Associazione di sottoreti implicita ed esplicita

Il diagramma seguente mostra il routing per un VPC con un Internet gateway, un gateway virtuale privato, una sottorete pubblica e una sottorete solo VPN.



Una tabella di instradamento A è una tabella di instradamento personalizzata associata esplicitamente alla sottorete pubblica. Ha un percorso che invia tutto il traffico al gateway Internet, che è ciò che rende la sottorete una sottorete pubblica.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | Locale |
| 0.0.0.0/0 | *igw-id* |

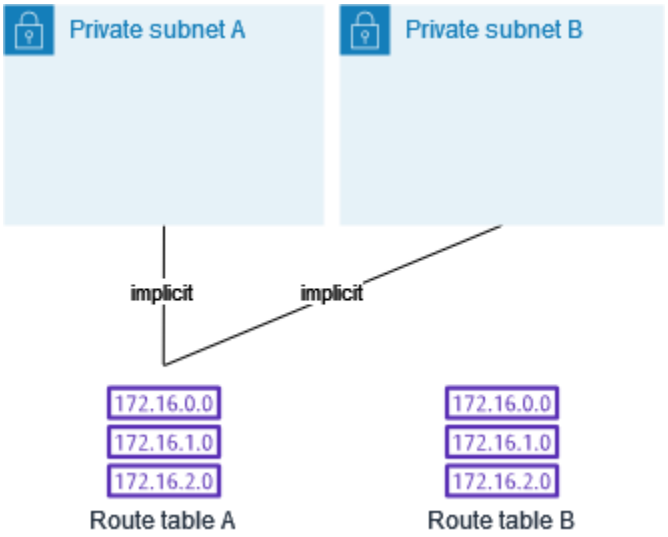
La tabella di instradamento B è la tabella di instradamento principale. È associato implicitamente alla sottorete privata. Ha un percorso che invia tutto il traffico al gateway privato virtuale ma nessun percorso verso il gateway Internet, che è ciò che rende la sottorete una sottorete solo VPN. Se crei un'altra sottorete in questo VPC e non associ una tabella di routing personalizzata, anche la sottorete verrà associata implicitamente a questa tabella di routing perché è la tabella di routing principale.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | Locale |
| 0.0.0.0/0 | *vgw-id* |

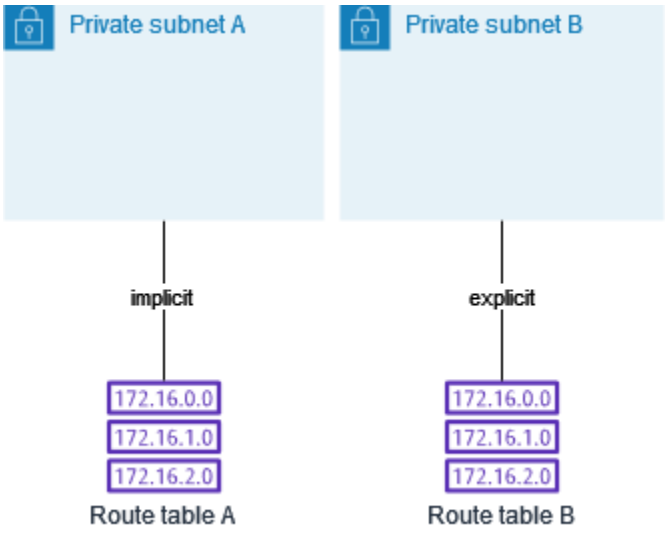
Esempio 2: Sostituzione della tabella di instradamento principale

Se vuoi apportare modifiche alla tabella di instradamento principale ed evitare qualsiasi interruzione del traffico, è consigliabile testare prima le modifiche della route utilizzando una tabella di instradamento personalizzata. Quando sei soddisfatto del risultato del test, puoi sostituire la tabella di instradamento principale con la nuova tabella personalizzata.

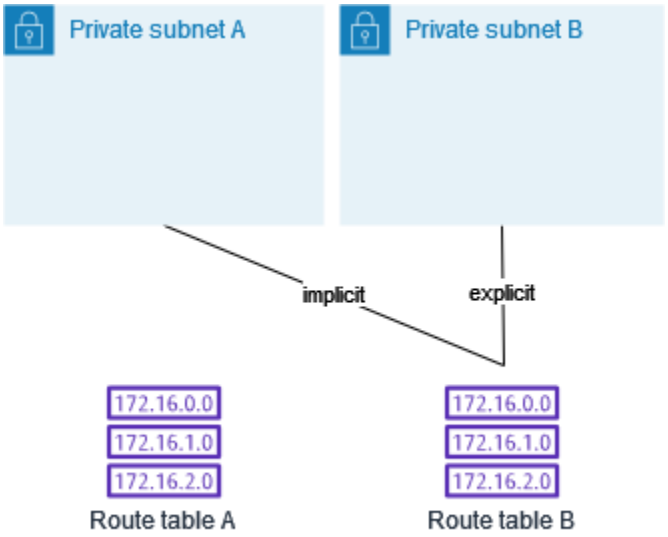
Il diagramma seguente mostra due sottoreti e due tabelle di routing. La sottorete A è associata implicitamente alla tabella di routing A, la tabella di routing principale. La sottorete B è associata implicitamente alla tabella di routing A. La tabella di routing B, una tabella di routing personalizzata, non è associata ad alcuna sottorete.



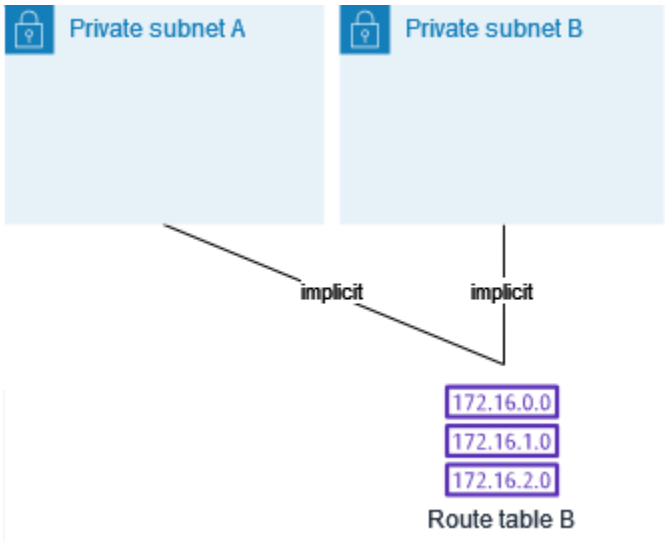

Per sostituire la tabella di routing principale, inizia creando un'associazione esplicita tra la sottorete B e la tabella di routing B. Verifica la tabella di routing B.




Dopo aver testato la tabella di routing B, puoi definirla come la tabella di routing principale. La sottorete B ha ancora un'associazione esplicita con la tabella di routing. Tuttavia la sottorete A adesso ha un'associazione implicita con la tabella di routing B in quanto questa è la nuova tabella di routing principale. La tabella di routing A non è più associata ad alcuna sottorete.




(Facoltativo) Se dissoci la sottorete B dalla tabella di routing B, si ha ancora un'associazione implicita tra la sottorete B e la tabella di routing B. Se non hai più bisogno della tabella di routing A, puoi eliminarla.




## Tabelle di routing del gateway

Puoi associare una tabella di instradamento a un Internet gateway o a un gateway virtuale privato. Quando una tabella di instradamento è associata a un gateway, viene chiamata tabella di instradamento del gateway. Puoi creare una tabella di instradamento del gateway per controllare dettagliatamente il percorso di routing del traffico che entra nel VPC. Ad esempio, puoi intercettare il traffico che entra nel VPC tramite un Internet gateway reindirizzandolo a un'appliance middlebox (come un'appliance di sicurezza) nel VPC.

Indice



## Route delle tabelle di routing del gateway

Una tabella di instradamento del gateway associata a un gateway Internet supporta le route con i seguenti target:

- La route locale di default
- Un endpoint del load balancer del gateway
- Un'interfaccia di rete per un'appliance middlebox

Una tabella di instradamento del gateway associata a un gateway virtuale privato supporta le route con i seguenti target:

- La route locale di default
- Un endpoint del load balancer del gateway
- Un'interfaccia di rete per un'appliance middlebox

Quando la destinazione è un endpoint Gateway Load Balancer o un'interfaccia di rete, sono consentite le seguenti destinazioni:

- L'intero blocco CIDR IPv4 o IPv6 del VPC. In questo caso, sostituisci il target della route locale predefinita.
- L'intero blocco CIDR IPv4 o IPv6 di una sottorete nel VPC. Si tratta di una route più specifica rispetto alla route locale predefinita.

Se modifichi il target della route locale in una tabella di instradamento del gateway su un'interfaccia di rete nel VPC, puoi ripristinarlo in seguito sul target `local` predefinito. Per ulteriori informazioni, consulta Sostituzione o ripristino della destinazione per una route locale.

Esempio

Nella tabella di instradamento del gateway seguente, il traffico destinato a una sottorete con il blocco CIDR `172.31.0.0/20` viene instradato a un'interfaccia di rete specifica. Il traffico destinato a tutte le altre sottoreti nel VPC utilizza la route locale.

| Destinazione | Target |
| --- | --- |
| 172.31.0.0/16 | Locale |
| 172.31.0.0/20 | *eni-id* |

Esempio

Nella tabella di instradamento del gateway seguente, il target per la route locale viene sostituito con un ID dell'interfaccia di rete. Il traffico destinato a tutte le sottoreti all'interno del VPC viene instradato all'interfaccia di rete.

| Destinazione | Target |
| --- | --- |
| 172.31.0.0/16 | *eni-id* |

## Regole e considerazioni

Non puoi associare una tabella di routing a un gateway se è vera una delle seguenti condizioni:

- La tabella di routing contiene instradamenti esistenti con destinazioni diverse rispetto a un'interfaccia di rete, a un endpoint Gateway Load Balancer o alla route locale di default.
- La tabella di routing contiene le route esistenti per i blocchi CIDR al di fuori degli intervalli nel VPC.
- La propagazione delle route è abilitata per la tabella di instradamento.

Inoltre, si applicano le seguenti regole e considerazioni:

- Non puoi aggiungere route ai blocchi CIDR al di fuori degli intervalli del VPC, inclusi gli intervalli maggiori dei singoli blocchi CIDR del VPC.
- Come destinazione puoi specificare soltanto `local`, un endpoint Gateway Load Balancer o un'interfaccia di rete. Non puoi specificare altri tipi di destinazioni, inclusi i singoli indirizzi IP host. Per ulteriori informazioni, consulta the section called “Opzioni di routing di esempio”.

- Non è possibile specificare un elenco di prefissi come destinazione.
- Non puoi utilizzare una tabella di instradamento del gateway per controllare o intercettare il traffico esterno al VPC, ad esempio il traffico che passa da un gateway di transito collegato. Puoi intercettare il traffico che entra nel VPC e reindirizzarlo a un altro target solo nello stesso VPC.
- Per garantire che il traffico raggiunga l'appliance middlebox, l'interfaccia di rete di destinazione deve essere collegata a un'istanza in esecuzione. Per un traffico che passa attraverso un gateway Internet, l'interfaccia di rete di destinazione deve avere anche un indirizzo IP pubblico.
- Durante la configurazione dell'accessorio middlebox, prendere nota delle considerazioni relative all'accessorio.
- Quando si instrada il traffico attraverso un'appliance middlebox, il traffico di ritorno dalla sottorete di destinazione deve essere instradato attraverso la stessa appliance. Il routing asimmetrico non è supportato.
- Le regole della tabella di instradamento si applicano a tutto il traffico che lascia una sottorete. Il traffico che lascia una sottorete è definito come traffico destinato all'indirizzo MAC del router gateway della sottorete. Il traffico destinato all'indirizzo MAC di un'altra interfaccia di rete nella sottorete utilizza il routing del collegamento dati (livello 2) anziché della rete (livello 3) in modo che le regole non si applichino a questo traffico.
- Non tutte le zone locali supportano l'associazione edge con gateway privati virtuali. Per ulteriori informazioni sulle zone disponibili, consulta Considerazioni nella AWS Guida per l'utente delle zone locali.

## Priorità della route

In generale, indirizziamo il traffico utilizzando il routing più specifico che corrisponde al traffico stesso. Ciò è noto come corrispondenza prefisso più lungo. Se la tabella di instradamento presenta routing sovrapposti o corrispondenti, si applicano le seguenti regole aggiuntive.

Indice

## Corrispondenza prefisso più lungo

Le route verso indirizzi IPv4 e IPv6 o blocchi CIDR sono indipendenti l'uno dall'altro. Per determinare come instradare il traffico, viene usato il routing più specifico che corrisponde al traffico IPv4 o IPv6.

Ad esempio, la tabella di instradamento della sottorete seguente include una route per il traffico Internet IPv4 (`0.0.0.0/0`) che punta a un Gateway Internet e una route per il traffico IPv4 `172.31.0.0/16` che punta a una connessione peering (`pcx-11223344556677889`). Il traffico dalla sottorete destinato all'intervallo di indirizzi IP `172.31.0.0/16` utilizza la connessione peering perché questa route è più specifica rispetto a quella per l'Internet gateway. Il traffico destinato a un target nel VPC (`10.0.0.0/16`) è coperto dalla route `local` ed è quindi instradato all'interno del VPC. Il resto del traffico dalla sottorete utilizza l'Internet gateway.

| Destinazione | Target |
| --- | --- |
| 10.0.0.0/16 | locale |
| 172.31.0.0/16 | pcx-11223344556677889 |
| 0.0.0.0/0 | igw-12345678901234567 |

## Priorità del routing e routing propagati

Se hai collegato un gateway virtuale privato al VPC e abilitato la propagazione delle route sulla tabella di routing della sottorete, le route che rappresentano la connessione Site-to-Site VPN vengono automaticamente visualizzate come route propagate nella tua tabella di routing.

Se la destinazione di un routing propagato si sovrappone a un route statico, il secondo ha la priorità.

Se la destinazione di un percrouting orso propagato è identica alla destinazione di un routing statico, quello statico ha la priorità se la destinazione è una delle seguenti:

- gateway Internet
- Gateway NAT
- Interfaccia di rete
- ID istanza
- Endpoint VPC del gateway

- Gateway di transito
- Connessione di peering di VPC
- Endpoint Gateway Load Balancer

Per ulteriori informazioni, consulta Tabelle di routing e priorità della route VPN nella Guida per l'utente di AWS Site-to-Site VPN .

Ad esempio, la seguente tabella di routing dispone di un routing statico a un Gateway Internet e un routing propagato a un gateway virtuale privato. La destinazione di entrambe le regole è `172.31.0.0/24`. Poiché il routing statico verso un Gateway Internet ha la priorità, tutto il traffico destinato a `172.31.0.0/24` viene indirizzato al Gateway Internet.

| Destinazione | Target | Propagato |
|---|---|---|
| 10.0.0.0/16 | locale | No |
| 172.31.0.0/24 | vgw-11223344556677889 | Sì |
| 172.31.0.0/24 | igw-12345678901234567 | No |

## Elenco di priorità di route e prefisso

Se la tabella di instradamento fa riferimento a un elenco di prefissi, si applicano le seguenti regole:

- Se la tabella di instradamento contiene un routing statico con un blocco CIDR di destinazione che si sovrappone a un routing statico con un elenco di prefissi, quello con il blocco CIDR ha la priorità.
- Se la tabella di instradamento contiene una route propagata che corrisponde a una route che fa riferimento a un elenco di prefissi, la route che fa riferimento all'elenco di prefissi avrà la priorità. Nota che per le route che si sovrappongono, le route più specifiche hanno sempre la priorità indipendentemente dal fatto che si tratti di route propagate, route statiche o route che fanno riferimento a elenchi di prefissi.
- Se la tabella di instradamento fa riferimento a più elenchi di prefissi che hanno blocchi CIDR sovrapposti a target diversi, la route che ha la priorità viene scelta in modo casuale. Successivamente, la stessa route avrà sempre la priorità.

## Quote della tabella di instradamento

Esiste una quota per il numero di tabelle di routing che possono essere create per ogni VPC. C'è anche una quota per il numero di route che possono essere aggiunte a ogni tabella di instradamento. Per ulteriori informazioni, consulta Quote Amazon VPC.

## Risolvi i problemi di raggiungibilità

Reachability Analyzer è uno strumento di analisi statica della configurazione. Usa Reachability Analyzer per analizzare ed eseguire il debug della raggiungibilità della rete tra due risorse nel tuo VPC. Reachability Analyzer hop-by-hop produce dettagli del percorso virtuale tra queste risorse quando sono raggiungibili e identifica il componente di blocco in caso contrario. Ad esempio, è in grado di identificare i percorsi mancanti o non configurati correttamente nella tabella delle rotte.

Per ulteriori informazioni, consulta la Guida di Reachability Analyzer.

## Opzioni di routing di esempio

I seguenti argomenti descrivono il routing per specifici gateway o connessioni nel VPC.

Indice

## Routing a un Internet gateway

Puoi rendere pubblica una sottorete aggiungendo una route nella tabella di instradamento della sottorete a un Internet gateway. Per farlo, crea e collega un Internet gateway al VPC, quindi aggiungi una route con una destinazione `0.0.0.0/0` per il traffico IPv4 o `::/0` per il traffico IPv6, nonché un target dell'ID dell'Internet gateway (`igw-xxxxxxxxxxxxxxxxx`).

| Destinazione | Target |
| --- | --- |
| 0.0.0.0/0 | *igw-id* |
| ::/0 | *igw-id* |

Per ulteriori informazioni, consulta Eseguire la connessione a Internet utilizzando un gateway Internet.

## Routing a un dispositivo NAT

Per abilitare le istanze di una sottorete privata per connettersi a Internet, puoi creare un gateway NAT o avviare un'istanza NAT in una sottorete pubblica. Aggiungi quindi una route per la tabella di instradamento della sottorete privata che indirizza il traffico Internet IPv4 (`0.0.0.0/0`) al dispositivo NAT.

| Destinazione | Target |
| --- | --- |
| 0.0.0.0/0 | *nat-gateway-id* |

Puoi anche creare route più specifiche verso altri target per evitare costi di elaborazione dei dati superflui per l'utilizzo di un gateway NAT o per instradare un determinato tipo di traffico privatamente. Nell'esempio seguente, il traffico Amazon S3 (pl-xxxxxxxx, un elenco di prefissi contenente intervalli di indirizzi IP per Amazon S3 in una regione specifica) viene instradato a un endpoint VPC del gateway e il traffico 10.25.0.0/16 viene instradato a una connessione peering VPC. Questi intervalli di indirizzi IP sono più specifici di 0.0.0.0/0. Quando le istanze inviano traffico ad Amazon S3 o al VPC peer, il traffico viene inviato all'endpoint VPC del gateway o alla connessione di peering VPC. Il resto del traffico viene inviato al gateway NAT.

| Destinazione | Target |
| --- | --- |
| 0.0.0.0/0 | *nat-gateway-id* |
| pl-*xxxxxxxx* | *vpce-id* |
| 10.25.0.0/16 | *pcx-id* |

Per ulteriori informazioni, consulta Dispositivi NAT.

## Routing a un gateway virtuale privato

Puoi utilizzare una AWS Site-to-Site VPN connessione per consentire alle istanze del tuo VPC di comunicare con la tua rete. Per farlo, crea e collega un gateway virtuale privato al VPC. Aggiungi quindi una route alla tabella di instradamento della sottorete specificano la rete come destinazione e il gateway virtuale privato come target (`vgw-xxxxxxxxxxxxxxxxx`).

| Destinazione | Target |
| --- | --- |
| 10.0.0.0/16 | *vgw-id* |

È quindi possibile creare e configurare la connessione Site-to-Site VPN. Per ulteriori informazioni, consulta Che cos'è AWS Site-to-Site VPN? e Tabelle di routing e priorità della route VPN nella Guida per l'utente AWS Site-to-Site VPN .

Una connessione Site-to-Site VPN su un gateway virtuale privato non supporta il traffico IPv6. Supportiamo tuttavia il traffico IPv6 instradato via un gateway virtuale privato a una connessione AWS Direct Connect . Per ulteriori informazioni, consulta la Guida per l'utente AWS Direct Connect.

## Routing verso un gateway locale AWS Outposts

Questa sezione descrive le configurazioni delle tabelle di routing per il routing verso un gateway locale. AWS Outposts

Indice

### Abilita il traffico tra le sottoreti Outpost e la rete locale

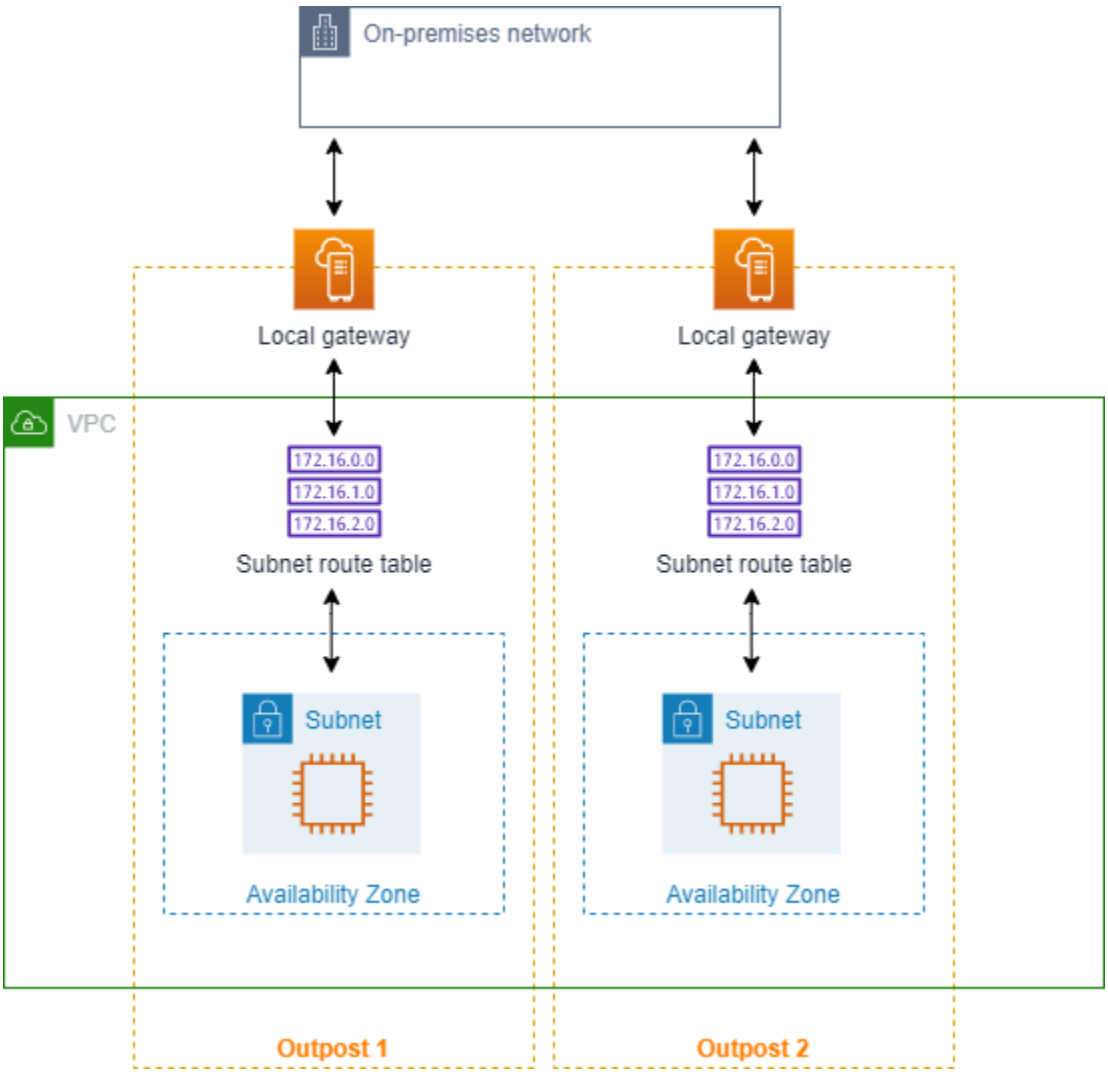
Le sottoreti associate in VPC AWS Outposts possono avere un tipo di destinazione aggiuntivo di gateway locale. Considera il caso in cui desideri che il gateway locale instradi il traffico con un indirizzo di destinazione 192.168.10.0/24 alla rete del cliente. Per farlo, aggiungi la route seguente con la rete di destinazione e un target del gateway locale (`lgw-xxxx`).

| Destinazione | Target |
| --- | --- |
| 192.168.10.0/24 | *lgw-id* |

### Abilita il traffico tra sottoreti nello stesso VPC su Outposts

Puoi stabilire una comunicazione tra le sottoreti che si trovano nello stesso VPC su diversi Outpost, utilizzando i gateway locali di Outpost e la rete locale.

È possibile utilizzare questa funzionalità per creare architetture simili alle architetture di più Zone di disponibilità (AZ) per le applicazioni locali in esecuzione sui rack Outposts stabilendo la connettività tra i rack Outposts ancorati a diverse AZ.




Per abilitare questa funzionalità, aggiungi un percorso alla tabella di routing della sottorete del rack di Outpost che sia più specifico del percorso locale in quella tabella di routing e abbia un tipo di destinazione di gateway locale. La destinazione della route deve corrispondere all'intero blocco IPv4 della sottorete nel VPC che si trova in un altro Outpost. Ripeti questa configurazione per tutte le sottoreti Outpost che devono comunicare.

**Important**

- Per utilizzare questa funzionalità, è necessario utilizzare un routing VPC diretto. Non puoi usare gli indirizzi IP di proprietà del cliente.
- La rete locale a cui sono collegati i gateway locali di Outposts deve disporre del routing richiesto in modo che le sottoreti possano accedere l'una all'altra.

- Se si desidera utilizzare i gruppi di sicurezza per le risorse nelle sottoreti, è necessario utilizzare regole che includano intervalli di indirizzi IP come origine o destinazione nelle sottoreti Outpost. Non è possibile utilizzare gli ID dei gruppi di sicurezza.
- I rack Outposts esistenti potrebbero richiedere un aggiornamento per abilitare il supporto per la comunicazione all'interno dei VPC tra più Outposts. Se questa funzionalità non funziona nel caso specifico, contatta l'assistenza AWS.

Example Esempio

Per un VPC con un CIDR di 10.0.0.0/16, una sottorete Outpost 1 con un CIDR di 10.0.1.0/24 e una sottorete Outpost 2 con un CIDR di 10.0.2.0/24, la voce per la tabella di routing della sottorete Outpost 1 sarebbe la seguente:

| Destinazione | Target |
| --- | --- |
| 10.0.0.0/16 | Locale |
| 10.0.2.0/24 | *lgw-1-id* |

La voce per la tabella di routing della sottorete Outpost 2 sarebbe la seguente:

| Destinazione | Target |
| --- | --- |
| 10.0.0.0/16 | Locale |
| 10.0.1.0/24 | *lgw-2-id* |

## Routing a una connessione peering VPC

Una connessione peering VPC è una connessione di rete tra due VPC che ti consente di instradare il traffico tra gli stessi utilizzando indirizzi IPv4 privati. Le istanze nei due VPC possono comunicare tra loro come se facessero parte della stessa rete.

Per abilitare il routing del traffico tra i VPC in una connessione peering VPC, devi aggiungere una route a una o più tabelle di routing della sottorete che punti alla connessione peering VPC. Ciò

consente di accedere in tutto o in parte al blocco CIDR dell'altro VPC nella connessione peering. Analogamente, Il proprietario dell'altro VPC deve aggiungere una route alla relativa tabella di instradamento della sottorete per instradare a sua volta il traffico al tuo VPC.

Ad esempio, hai una connessione peering VPC (`pcx-11223344556677889`) tra due VPC, con le seguenti informazioni:

- VPC A: il blocco CIDR è 10.0.0.0/16
- VPC B: il blocco CIDR è 172.31.0.0/16

Per abilitare il traffico tra i VPC e consentire l'accesso all'intero blocco CIDR IPv4 di entrambi i VPC, la tabella di instradamento di VPC A è configurata come descritto di seguito.

| Destinazione | Target |
|---|---|
| 10.0.0.0/16 | Locale |
| 172.31.0.0/16 | pcx-11223344556677889 |

La tabella di instradamento di VPC B è configurata come segue.

| Destinazione | Target |
|---|---|
| 172.31.0.0/16 | Locale |
| 10.0.0.0/16 | pcx-11223344556677889 |

La tua connessione peering VPC può supportare anche le comunicazioni IPv6 tra istanze nei VPC, purché i VPC e le istanze siano abilitate per la comunicazione IPv6. Per abilitare il routing del traffico IPv6 tra VPC, devi aggiungere una route alla tua tabella di instradamento che punta alla connessione peering VPC per accedere all'intero blocco CIDR IPv6, o a una sua parte, del VPC in peering.

Ad esempio, utilizzando la stessa connessione peering VPC vista precedentemente (`pcx-11223344556677889`), supponi che i VPC dispongano delle seguenti informazioni:

- VPC A: il blocco CIDR IPv6 è `2001:db8:1234:1a00::/56`
- VPC B: il blocco CIDR IPv6 è `2001:db8:5678:2b00::/56`

Per abilitare le comunicazioni IPv6 sulla connessione peering VPC, aggiungi la route seguente alla tabella di instradamento per VPC A.

| Destinazione | Target |
| --- | --- |
| 10.0.0.0/16 | Locale |
| 172.31.0.0/16 | pcx-11223344556677889 |
| 2001:db8:5678:2b00::/56 | pcx-11223344556677889 |

Aggiungi la route seguente alla tabella di instradamento per VPC B:

| Destinazione | Target |
| --- | --- |
| 172.31.0.0/16 | Locale |
| 10.0.0.0/16 | pcx-11223344556677889 |
| 2001:db8:1234:1a00::/56 | pcx-11223344556677889 |

Per ulteriori informazioni sulle connessioni peering VPC, consulta Guida di Amazon VPC Peering.

## Routing a un endpoint VPC del gateway

Un endpoint VPC gateway ti consente di creare una connessione privata tra il tuo VPC e un altro servizio. AWS Quando crei un endpoint del gateway, specifica le tabelle di routing della sottorete nel VPC utilizzate dall'endpoint del gateway. Una route viene aggiunta automaticamente a ciascuna delle tabelle di routing con una destinazione che specifica l'ID di elenco di prefissi del servizio (`pl-`*`xxxxxxxx`*) e un target con l'ID di endpoint (`vpce-`*`xxxxxxxxxxxxxxxxx`*). Non puoi eliminare o modificare Esplicitamente la route dell'endpoint, ma puoi modificare le tabelle di routing utilizzate dall'endpoint.

Per ulteriori informazioni sul routing degli endpoint e sulle implicazioni per i routing ai servizi AWS , consulta Routing per endpoint gateway.

## Routing a un Internet gateway egress-only

Puoi creare un Internet gateway egress-only per il VPC per consentire alle istanze in una sottorete privata di avviare la comunicazione in uscita verso Internet, impedendo nel contempo a Internet di avviare connessioni con le istanze. Un Internet gateway egress-only viene utilizzato soltanto per il traffico IPv6. Per configurare il routing per un Internet gateway egress-only, aggiungi una route nella tabella di instradamento della sottorete privata che instrada il traffico Internet IPv6 (`::/0`) all'Internet gateway egress-only.

| Destinazione | Target |
| --- | --- |
| ::/0 | *eigw-id* |

Per ulteriori informazioni, consulta Abilitazione del traffico in uscita IPv6 utilizzando un gateway Internet egress-only.

## Routing per un gateway di transito

Quando si collega un VPC a un gateway di transito, è necessario aggiungere una route alla tabella di routing della sottorete affinché il traffico sia instradato attraverso il gateway di transito.

Ipotizzare il seguente scenario in cui sono presenti tre VPC collegatI a un gateway di transito. In questo scenario, tutti gli allegati sono associati alla tabella di routing predefinita del gateway di transito e si propagano alla tabella di routing del gateway di transito. Pertanto, tutti gli allegati possono instradare i pacchetti tra di essi, con il gateway di transito che assume il ruolo di un semplice hub IP di livello 3.

Ad esempio, considerare due VPC, con le seguenti informazioni:

- VPC A: 10.1.0.0/16, ID di collegamento tgw-attach-11111111111111111
- VPC B: 10.2.0.0/16, ID di collegamento tgw-attach-22222222222222222

Per abilitare il traffico tra i VPC e consentire l'accesso al gateway di transito, la tabella di routing del VPC A è configurata come descritto di seguito.

| Destinazione | Target |
| --- | --- |
| 10.1.0.0/16 | locale |

| Destinazione | Target |
| --- | --- |
| 10.0.0.0/8 | *tgw-id* |

Qui di seguito è illustrato un esempio degli elementi della tabella di routing del gateway di transito per gli allegati del VPC.

| Destinazione | Target |
| --- | --- |
| 10.1.0.0/16 | tgw-attach-11111111111111111 |
| 10.2.0.0/16 | tgw-attach-22222222222222222 |

Per ulteriori informazioni sulle tabelle delle route del gateway di transito, consulta Routing in Gateway di transito di Amazon VPC.

## Routing per un'appliance middlebox

È possibile aggiungere appliance middlebox nei percorsi di routing per il VPC. Di seguito sono riportati alcuni casi d'uso:

- È possibile intercettare il traffico che entra nel VPC tramite un gateway Internet o un gateway virtuale privato indirizzandolo a un'appliance middlebox nel VPC. È possibile utilizzare la procedura guidata di routing middlebox per configurare AWS automaticamente le tabelle di routing appropriate per il gateway, il middlebox e la sottorete di destinazione. Per ulteriori informazioni, consulta the section called “Procedura guidata di instradamento middlebox”.
- Traffico diretto tra due sottoreti a un'appliance middlebox. A tale scopo, è possibile creare una route per una tabella di routing della sottorete che corrisponda al CIDR dell'altra sottorete e specifichi come target un endpoint del load balancer del gateway, un gateway NAT, un endpoint Network Firewall o l'interfaccia di rete per un'appliance. In alternativa, per reindirizzare tutto il traffico dalla sottorete a qualsiasi altra sottorete, sostituire il target della route locale con un endpoint del load balancer del gateway, un gateway NAT o un'interfaccia di rete.

Puoi configurare l'appliance in base alle tue esigenze. Ad esempio, puoi configurare un'appliance per la sicurezza, che schermi tutto il traffico, o un'appliance di accelerazione WAN. L'appliance viene

distribuita come istanza Amazon EC2 in una sottorete nel VPC ed è rappresentata da un'interfaccia di rete elastica (interfaccia di rete) nella sottorete.

Se la propagazione della route è stata abilitata per la tabella di routing della sottorete di destinazione, è necessario tenere conto della priorità della route. Diamo priorità alla route più specifica e se le route corrispondono, diamo priorità alle route statiche rispetto alle route propagate. Esamina i percorsi per assicurarti che il traffico venga instradato correttamente e che non ci siano conseguenze indesiderate se abiliti o disabiliti la propagazione delle rotte (ad esempio, la propagazione delle rotte è necessaria per una connessione che supporta i jumbo frame). AWS Direct Connect

Per instradare il traffico VPC in ingresso a un'appliance, puoi associare una tabella di instradamento all'Internet gateway o al gateway virtuale privato, quindi specificare l'interfaccia di rete dell'appliance come target per il traffico VPC. Per ulteriori informazioni, consulta Tabelle di routing del gateway. Puoi anche instradare il traffico in uscita dalla sottorete a un'appliance middlebox in un'altra sottorete.

Per esempi di routing middlebox, consultare Scenari middlebox.

Indice



## Considerazioni sull'appliance

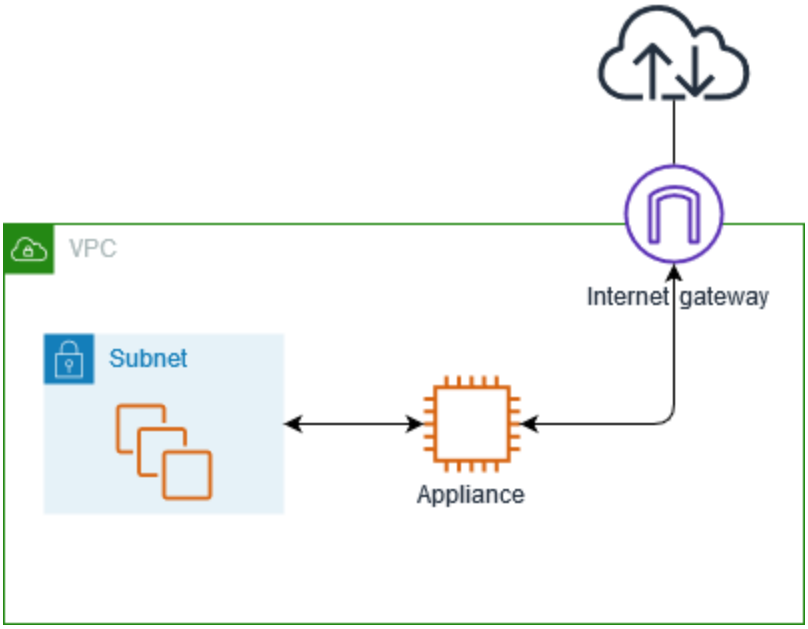
Puoi scegliere un'appliance di terze parti da Marketplace AWS oppure configurarne una personalizzata. Quando crei o configuri un'appliance, tieni presente quanto segue:

- L'appliance deve essere configurata in una sottorete separata per il traffico di origine o di destinazione.
- Devi disabilitare i controlli dell'origine/della destinazione sull'appliance. Per ulteriori informazioni, consulta Changing the Source or Destination Checking nella Amazon EC2 User Guide.
- Non puoi instradare il traffico tra host nella stessa sottorete tramite un'appliance.
- L'appliance non deve eseguire Network Address Translation (NAT).
- È possibile aggiungere alle tabelle di routing una route che sia più specifica della route locale. È possibile utilizzare route più specifiche per reindirizzare il traffico tra sottoreti all'interno di un VPC (traffico Est-Ovest) a un'appliance middlebox. La destinazione della route deve corrispondere all'intero blocco CIDR IPv4 o IPv6 di una sottorete nel VPC.

- Per intercettare il traffico IPv6, verifica che il VPC, la sottorete e l'appliance supportino IPv6. I gateway virtuali privati non supportano il traffico IPv6.

### Routing del traffico tra un gateway e un'appliance

Per instradare il traffico VPC in ingresso a un'appliance, puoi associare una tabella di instradamento all'Internet gateway o al gateway virtuale privato, quindi specificare l'interfaccia di rete dell'appliance come target per il traffico VPC. Nell'esempio seguente, il VPC dispone di un gateway Internet, un'appliance e una sottorete con istanze. Il traffico proveniente da Internet viene instradato attraverso un'appliance.




Associa questa tabella di instradamento all'Internet gateway o al gateway virtuale privato. La prima voce è la route locale. La seconda voce invia il traffico IPv4 destinato alla sottorete all'interfaccia di rete dell'appliance. Questa è una route più specifica rispetto alla route locale.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | Locale |
| *CIDR sottorete* | *ID interfaccia di rete dell'appliance* |

In alternativa, è possibile sostituire il target per la route locale con l'interfaccia di rete dell'appliance. Ciò è possibile per garantire che tutto il traffico venga instradato automaticamente all'appliance, incluso quello destinato alle sottoreti aggiunte al VPC in un secondo momento.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | *ID interfaccia di rete dell'appliance* |

Per instradare il traffico dalla sottorete a un'appliance in un'altra sottorete, aggiungi una route alla tabella di instradamento della sottorete che indirizza il traffico all'interfaccia di rete dell'appliance. La destinazione deve essere meno specifica rispetto a quella per la route locale. Ad esempio, per il traffico destinato a Internet, specifica `0.0.0.0/0` (tutti gli indirizzi IPv4) per la destinazione.

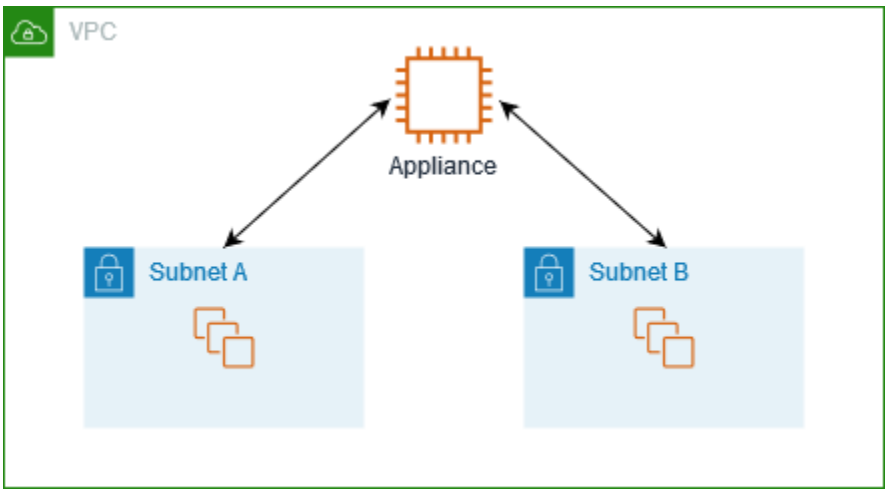
| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | Locale |
| 0.0.0.0/0 | *ID interfaccia di rete dell'appliance* |

Quindi, nella tabella di instradamento associata alla sottorete dell'appliance, aggiungere una route che restituisce il traffico al gateway Internet o al gateway virtuale privato.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | Locale |
| 0.0.0.0/0 | *igw-id* |

Routing del traffico tra sottoreti a un'appliance

È possibile instradare il traffico destinato a una sottorete specifica all'interfaccia di rete di un'appliance. Nell'esempio seguente, il VPC contiene due sottoreti e un'appliance. Il traffico tra sottoreti viene instradato tramite un'appliance.




Gruppi di sicurezza

Quando si instrada il traffico tra istanze in sottoreti diverse attraverso un'appliance middlebox, i gruppi di sicurezza per entrambe le istanze devono consentire il flusso del traffico tra le istanze. Il gruppo di sicurezza per ogni istanza deve fare riferimento all'indirizzo IP privato dell'altra istanza o all'intervallo CIDR della sottorete che contiene l'altra istanza come origine. Se si fa riferimento al gruppo di sicurezza dell'altra istanza come origine, allora il flusso del traffico tra le istanze non sarà consentito.

Routing

Di seguito è riportato un esempio di tabella di instradamento per la sottorete A. La prima voce consente alle istanze del VPC di comunicare tra loro. La seconda voce indirizza tutto il traffico dalla sottorete A alla sottorete B all'interfaccia di rete dell'appliance.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | Locale |
| *CIDR sottorete B* | *ID interfaccia di rete dell'appliance* |

Di seguito è riportato un esempio di tabella di instradamento per la sottorete B. La prima voce consente alle istanze del VPC di comunicare tra loro. La seconda voce indirizza tutto il traffico dalla sottorete B alla sottorete A all'interfaccia di rete dell'appliance.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | Locale |
| *CIDR sottorete A* | *ID interfaccia di rete dell'appliance* |

In alternativa, è possibile sostituire il target per la route locale con l'interfaccia di rete dell'appliance. Ciò è possibile per garantire che tutto il traffico venga instradato automaticamente all'appliance, incluso quello destinato alle sottoreti aggiunte al VPC in un secondo momento.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | *ID interfaccia di rete dell'appliance* |

## Routing mediante un elenco di prefissi

Se fai spesso riferimento allo stesso set di blocchi CIDR tra AWS le tue risorse, puoi creare un elenco di prefissi gestito dal cliente per raggrupparli. È quindi possibile specificare l'elenco di prefissi come destinazione nella voce della tabella di instradamento. In seguito è possibile aggiungere o rimuovere voci per l'elenco dei prefissi senza dover aggiornare le tabelle di routing.

Ad esempio, si dispone di un gateway di transito con più collegamenti VPC. I VPC devono essere in grado di comunicare con due collegamenti VPC specifici con i seguenti blocchi CIDR:

- 10.0.0.0/16
- 10.2.0.0/16

È possibile creare un elenco di prefissi con entrambe le voci. Nelle tabelle di routing della sottorete è possibile creare una route e specificare l'elenco di prefissi come destinazione e il gateway di transito come target.

| Destinazione | Target |
| --- | --- |
| 172.31.0.0/16 | Locale |

| Destinazione | Target |
| --- | --- |
| pl-123abc123abc123ab | *tgw-id* |

Il numero massimo di voci per gli elenchi di prefissi è uguale allo stesso numero di voci nella tabella di routing.

### Routing a un endpoint Gateway Load Balancer

Un Gateway Load Balancer consente di distribuire il traffico a una flotta di appliance virtuali, ad esempio i firewall. Puoi configurare il load balancer come servizio creando una configurazione di servizio per l'endpoint VPC. Puoi quindi creare un endpoint Gateway Load Balancer nel VPC e connettere il VPC al servizio.

Per indirizzare il traffico al Gateway Load Balancer (ad esempio, per una analisi della sicurezza), specifica l'endpoint Gateway Load Balancer come destinazione nelle tabelle di routing.

Per un esempio di appliance di sicurezza dietro un load balancer del gateway, consultare the section called “Ispezione del traffico utilizzando appliance di sicurezza”.

Per specificare l'endpoint Gateway Load Balancer nella tabella di routing, utilizza l'ID dell'endpoint VPC. Ad esempio, per instradare il traffico per 10.0.1.0/24 a un endpoint del load balancer del gateway, aggiungere la seguente route.

| Destinazione | Target |
| --- | --- |
| 10.0.1.0/24 | *vpc-endpoint-id* |

Per ulteriori informazioni, consultare Bilanciatori del carico del gateway.

## Utilizzo delle tabelle di routing

In questa sezione viene spiegato come lavorae con le tabelle di instradamento.

Indice

- Aggiunta e rimozione di route da una tabella di instradamento
- Abilitazione o disabilitazione della propagazione delle route
- Associazione di una sottorete a una tabella di instradamento
- Modifica della tabella di instradamento per una sottorete
- Disassociazione di una sottorete da una tabella di instradamento
- Sostituzione della tabella di instradamento principale
- Associazione di un gateway a una tabella di instradamento
- Annullamento dell'associazione di un gateway a una tabella di instradamento
- Sostituzione o ripristino della destinazione per una route locale
- Eliminazione di una tabella di instradamento

## Determinazione della tabella di instradamento per una sottorete

Puoi determinare la tabella di routing a cui una sottorete è associata esaminando i dettagli della sottorete nella console Amazon VPC.

Per determinare la tabella di routing per una sottorete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
3. Seleziona la sottorete.
4. Scegli la scheda Tabella di instradamento per visualizzare informazioni sulla tabella di instradamento e dei relativi instradamenti. Per determinare se l'associazione è alla tabella di instradamento principale e se tale associazione è esplicita, consulta Determinazione delle sottoreti o dei gateway associati esplicitamente.

## Determinazione delle sottoreti o dei gateway associati esplicitamente

Puoi determinare il numero e il tipo di sottoreti o gateway esplicitamente associati a una tabella di instradamento.

La tabella di instradamento principale può avere associazioni della sottorete esplicite e implicite. Le tabelle di routing personalizzate hanno soltanto associazioni esplicite.

Le sottoreti che non sono esplicitamente associate a una qualsiasi tabella di instradamento hanno un'associazione implicita con la tabella di instradamento principale. Puoi associare esplicitamente

una sottorete alla tabella di instradamento principale. Per uno scenario di esempio di questa opzione, consulta Sostituzione della tabella di instradamento principale.

Per determinare quali sottoreti sono esplicitamente associate utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Tabelle di routing.
3. Controlla la colonna Associazione sottorete esplicita per determinare le sottoreti associate esplicitamente e la colonna Principale per determinare se questa è la tabella di instradamento principale.
4. Seleziona la tabella di instradamento e scegli la scheda Associazioni sottorete.
5. Le sottoreti in Associazioni sottorete esplicite sono associati esplicitamente alla tabella di instradamento. Le sottoreti in Sottoreti senza associazioni esplicite appartengono allo stesso VPC della tabella di instradamento, ma non sono associate a una tabella di instradamento, per cui sono associate implicitamente alla tabella di instradamento principale per il VPC.

Per determinare quali gateway sono esplicitamente associati utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Tabelle di routing.
3. Seleziona la tabella di instradamento e scegli la scheda Associazioni edge.

Per descrivere una o più tabelle di routing e visualizzarne le associazioni utilizzando la riga di comando

- describe-route-tables (AWS CLI)
- Get-EC2RouteTable (AWS Tools for Windows PowerShell)

## Creazione di una tabella di routing personalizzata

Puoi creare una tabella di routing personalizzata per il VPC tramite la console Amazon VPC.

Per creare una tabella di routing personalizzata utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Tabelle di routing.

3. Selezionare Create route table (Crea tabella di instradamento).
4. (Facoltativo) In Name (Nome), inserisci un nome per la tabella di instradamento.
5. In VPC, seleziona il VPC.
6. (Facoltativo) Per aggiungere un tag, scegli Add new tag (Aggiungi nuovo tag) e inserisci la chiave e il valore del tag.
7. Selezionare Create route table (Crea tabella di instradamento).

Per creare una tabella di instradamento personalizzata utilizzando la riga di comando

- create-route-table (AWS CLI)
- New-EC2RouteTable (AWS Tools for Windows PowerShell)

## Aggiunta e rimozione di route da una tabella di instradamento

Puoi aggiungere, eliminare E modificare route nelle tabelle di routing. Puoi modificare soltanto le route che hai aggiunto.

Per ulteriori informazioni sull'utilizzo di route statiche per una connessione Site-to-Site VPN, consulta Modifica dei routing statici per una connessione Site-to-Site VPN nella Guida per l'utente di AWS Site-to-Site VPN .

Per aggiornare i routing per una tabella di instradamento utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Selezionare Actions (Operazioni), Edit routes (Modifica route).
4. Per aggiungere una route scegliere Add route (Aggiungi route). Per Destinazione immettere il blocco CIDR di destinazione, un singolo indirizzo IP o l'ID di un elenco di prefissi.
5. Per modificare una route esistente, sostituisci il blocco CIDR di destinazione o il singolo indirizzo IP in Destination (Destinazione). In Target scegli un target.
6. Per rimuovere una route, scegli Remove (Rimuovi).
7. Seleziona Salvataggio delle modifiche.

Aggiornare le route per una tabella di instradamento utilizzando la console

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

> **Note**
>
> Se si aggiunge una route con uno strumento a riga di comando o con l'API, il blocco CIDR di destinazione viene modificato automaticamente nella sua forma canonica. Ad esempio, se si specifica `100.68.0.18/18` per il blocco CIDR, viene creata una route con un blocco CIDR di destinazione `100.68.0.0/18`.

## Abilitazione o disabilitazione della propagazione delle route

La propagazione dei percorsi consente a un gateway privato virtuale di propagare automaticamente i percorsi alle tue tabelle di instradamento. In tal modo, non sarà necessario aggiungere o rimuovere manualmente i percorsi della VPN.

Per completare questo processo, è necessario disporre di un gateway privato virtuale.

Per ulteriori informazioni, consulta Opzioni di instradamento di VPN Site-to-Site nella Guida per l'utente di VPN Site-to-Site.

Per abilitare la propagazione della route tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Scegliere Actions (Operazioni), Edit route propagation (Modifica propatazione della route).
4. Seleziona la casella di controllo Abilita accanto al gateway virtuale privato, quindi seleziona Salva.

Per abilitare la propagazione della route utilizzando la riga di comando

- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Per disabilitare la propagazione delle route utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Scegliere Actions (Operazioni), Edit route propagation (Modifica propatazione della route).
4. Seleziona la casella di controllo Enable (Abilita) accanto al gateway virtuale privato, quindi seleziona Save (Salva).

Per disabilitare la propagazione della route utilizzando la riga di comando

- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

## Associazione di una sottorete a una tabella di instradamento

Per applicare le route delle tabelle di instradamento a una particolare sottorete, occorre associare la tabella di instradamento alla sottorete. Una tabella di instradamento possono essere associata a più sottoreti. Tuttavia, una sottorete può essere associata a una sola tabella di instradamento alla volta. Per impostazione predefinita, qualsiasi sottorete non esplicitamente associata a una tabella è implicitamente associata alla tabella di instradamento principale.

Per associare una tabella di routing a una sottorete utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Nella scheda Associazioni sottorete scegli Modifica associazioni sottorete.
4. Seleziona la casella di controllo per la sottorete da associare alla tabella di instradamento.
5. Scegli Salva associazioni.

Per associare una sottorete a una tabella di instradamento utilizzando la riga di comando

- associate-route-table (AWS CLI)
- Register-EC2RouteTable (AWS Tools for Windows PowerShell)

## Modifica della tabella di instradamento per una sottorete

Puoi modificare l'associazione della tabella di instradamento per una sottorete.

Quando si modifica la tabella di instradamento, le connessioni esistenti nella sottorete vengono eliminate a meno che la nuova tabella di instradamento non contenga una route per lo stesso traffico verso la stessa destinazione.

Per modificare un'associazione di tabelle di routing della sottorete utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti) e selezionare la sottorete.
3. Dalla scheda Route table (Tabella di instradamento) scegliere Edit route table association (Modifica associazione di tabelle di routing).
4. Per ID tabella di instradamento, seleziona la nuova tabella di instradamento.
5. Selezionare Salva.

Per modificare la tabella di instradamento associata a una sottorete utilizzando la riga di comando

- replace-route-table-association (AWS CLI)
- Set-EC2RouteTableAssociation (AWS Tools for Windows PowerShell)

## Disassociazione di una sottorete da una tabella di instradamento

Puoi disassociare una sottorete da una tabella di instradamento. Fino a che non associ la sottorete a un'altra tabella di instradamento, la sottorete è implicitamente associata alla tabella di instradamento principale.

Per annullare l'associazione di una sottorete da una tabella di routing utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Dalla scheda Subnet associations (Associazioni sottorete) scegli Edit subnet associations (Modifica associazioni sottorete).
4. Deseleziona la casella di controllo per la sottorete.
5. Scegli Salva associazioni.

Per annullare l'associazione di una sottorete da una tabella di instradamento utilizzando la riga di comando

- disassociate-route-table (AWS CLI)
- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

## Sostituzione della tabella di instradamento principale

Puoi sostituire la tabella di instradamento principale nel VPC.

Per sostituire la tabella di routing principale utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la nuova tabella di instradamento principale.
3. Scegli Actions (Azioni), Set main route table (Imposta la tabella di instradamento principale).
4. Quando viene richiesta la conferma, inserisci **`set`** e seleziona OK.

Per sostituire la tabella di instradamento principale utilizzando la riga di comando

- replace-route-table-association (AWS CLI)
- Set-EC2RouteTableAssociation (AWS Tools for Windows PowerShell)

La procedura seguente descrive come rimuovere un'associazione Esplicita tra una sottorete E la tabella di instradamento principale. Il risultato è un'associazione implicita tra la sottorete E la tabella di instradamento principale. Il processo è identico alla disassociazione di una sottorete da una tabella di instradamento.

Per rimuovere un'associazione Esplicita alla tabella di routing principale

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Dalla scheda Subnet associations (Associazioni sottorete) scegli Edit subnet associations (Modifica associazioni sottorete).
4. Deseleziona la casella di controllo per la sottorete.
5. Scegli Salva associazioni.

## Associazione di un gateway a una tabella di instradamento

Puoi associare un Internet gateway o un gateway virtuale privato a una tabella di instradamento. Per ulteriori informazioni, consulta Tabelle di routing del gateway.

Per associare un gateway a una tabella di routing utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Dalla scheda Edge associations (Associazioni edge) scegli Edit edge associations (Modifica associazioni edge).
4. Selezionare la casella di controllo relativa al gateway.
5. Seleziona Salvataggio delle modifiche.

Per associare un gateway a una tabella di routing utilizzando il AWS CLI

Utilizzare il comando associate-route-table. L'esempio seguente associa l'Internet gateway `igw-11aa22bb33cc44dd1` alla tabella di instradamento `rtb-01234567890123456`.

```
aws ec2 associate-route-table --route-table-id rtb-01234567890123456 --gateway-id
 igw-11aa22bb33cc44dd1
```

## Annullamento dell'associazione di un gateway a una tabella di instradamento

Puoi annullare l'associazione di un Internet gateway o di un gateway virtuale privato da una tabella di instradamento.

Per associare un gateway a una tabella di routing utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Dalla scheda Edge associations (Associazioni edge) scegli Edit edge associations (Modifica associazioni edge).
4. Deseleziona la casella di controllo relativa al gateway.
5. Seleziona Salvataggio delle modifiche.

Per annullare l'associazione di un gateway da una tabella di instradamento utilizzando la riga di comando

- disassociate-route-table (AWS CLI)
- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

## Sostituzione o ripristino della destinazione per una route locale

È possibile modificare la destinazione della route locale di default. Se sostituisci il target di una route locale, puoi ripristinarlo in seguito con il target `local` predefinito. Se il VPC dispone di più blocchi CIDR, le tabelle di routing hanno più route locali, una per ogni blocco CIDR. Puoi sostituire o ripristinare il target di ciascuna delle route locali in base alle esigenze.

Aggiornare l'instradamento locale utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Nella scheda Routes (Instradamento), scegli Edit routes (Modifica instradamenti).
4. Per l'instradamento locale, deseleziona Target (Destinazione) e scegli una nuova destinazione.
5. Seleziona Salvataggio delle modifiche.

Per ripristinare il target per una route locale utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Selezionare Actions (Operazioni), Edit routes (Modifica route).
4. Per l'instradamento, deseleziona Target (Destinazione) e scegli local (locale).
5. Seleziona Salvataggio delle modifiche.

Per sostituire la destinazione di una rotta locale utilizzando il AWS CLI

Utilizzare il comando replace-route. L'esempio seguente sostituisce il target della route locale con `eni-11223344556677889`.

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block
 10.0.0.0/16 --network-interface-id eni-11223344556677889
```

Per ripristinare la destinazione di una rotta locale utilizzando il AWS CLI

L'esempio seguente ripristina il target locale per la tabella di instradamento `rtb-01234567890123456`.

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block
 10.0.0.0/16 --local-target
```

## Eliminazione di una tabella di instradamento

Puoi eliminare una tabella di instradamento solo se non è associata ad alcuna sottorete. Non puoi eliminare la tabella di instradamento principale.

Per eliminare una tabella di routing utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Selezionare Actions (Operazioni), Delete route table (Elimina tabella di instradamento).
4. Quando viene richiesta la conferma, inserisci **`delete`** e scegli Delete (Elimina).

Per eliminare una tabella di instradamento utilizzando la riga di comando

- delete-route-table (AWS CLI)

- Remove-EC2RouteTable (AWS Tools for Windows PowerShell)

## Procedura guidata di instradamento middlebox

Se si desidera configurare il controllo granulare sul percorso di routing del traffico che entra o esce dal VPC, ad esempio reindirizzando il traffico a un'appliance di sicurezza, è possibile utilizzare la procedura guidata di routing middlebox nella console VPC. La procedura guidata di routing middlebox consente di creare automaticamente le tabelle di routing e le route (hop) necessarie per reindirizzare il traffico in base alle esigenze.

La procedura guidata di routing middlebox consente di configurare il routing per i seguenti scenari:

- Routing del traffico a un'appliance middlebox, ad esempio un'istanza Amazon EC2 configurata come appliance di sicurezza.
- Routing del traffico a un load balancer del gateway Per ulteriori informazioni, consulta la Guida per l'utente dei bilanciatori del carico Gateway.

Per ulteriori informazioni, consulta the section called “Scenari middlebox”.

Indice



### Prerequisiti della procedura guidata per il routing middlebox

Verificare the section called “Considerazioni sulla procedura guidata di routing middlebox”. Assicurarsi quindi di disporre delle informazioni seguenti prima di utilizzare la procedura guidata di routing middlebox.

- Il VPC.
- La risorsa da cui il traffico proviene o entra nel VPC, ad esempio, un gateway Internet, un gateway virtuale privato o un'interfaccia di rete.
- L'interfaccia di rete middlebox o l'endpoint del load balancer del gateway.

- La sottorete di destinazione per il traffico.

## Gestione di instradamenti middlebox

La procedura guidata di routing middlebox è disponibile nella Amazon Virtual Private Cloud Console.

Indice



### Creazione di route utilizzando la procedura guidata di routing middlebox

Come creare route utilizzando la procedura guidata di routing middlebox

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
3. Selezionare il VPC, quindi scegliere Operazioni,Gestione di route middlebox.
4. Selezionare Crea route.
5. Nella pagina Specifica route, procedere come segue:
   - Per Origine, scegliere l'origine del traffico. Se si sceglie un gateway virtuale privato, per CIDR IPv4 destinazione, immettere il CIDR per il traffico on-premise che entra nel VPC dal gateway virtuale privato.
   - Per Middlebox, scegliere l'ID dell'interfaccia di rete associata all'appliance middlebox oppure, se si utilizza un endpoint del load balancer del gateway, scegliere l'ID endpoint VPC.
   - Per Sottorete di destinazione, scegliere la sottorete di destinazione.
6. (Facoltativo) Per aggiungere un'altra sottorete di destinazione, scegliere Aggiungi altra sottorete, quindi completare le seguenti operazioni:
   - Per Middlebox, scegliere l'ID dell'interfaccia di rete associata all'appliance middlebox oppure, se si utilizza un endpoint del load balancer del gateway, scegliere l'ID endpoint VPC.

     È necessario utilizzare la stessa appliance middlebox per più sottoreti.
   - Per Sottorete di destinazione, scegliere la sottorete di destinazione.

7. (Facoltativo) Per aggiungere un'altra origine, scegliereAggiungi origine, quindi ripetere i passaggi precedenti.
8. Seleziona Successivo.
9. Nella pagina Rivedi e crea verificare le route, quindi selezionare Crea route.

### Modifica delle route middlebox

È possibile modificare la configurazione delle route modificando il gateway, il middlebox o la sottorete di destinazione.

Quando si apportano modifiche, la procedura guidata di routing middlebox esegue automaticamente le operazioni seguenti:

- Crea nuove tabelle di routing per il gateway, il middlebox e la sottorete di destinazione.
- Aggiunge le route necessarie alle nuove tabelle di routing.
- Dissocia le tabelle di routing correnti associate alle risorse dalla procedura guidata di routing middlebox.
- Associa alle risorse le nuove tabelle di routing create dalla procedura guidata di routing middlebox.

#### Come modificare route middlebox utilizzando la procedura guidata di routing middlebox

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
3. Selezionare il VPC, quindi scegliere Operazioni,Gestione di route middlebox.
4. Selezionare Modifica route.
5. Per modificare il gateway, in Origine, scegliere il gateway attraverso il quale il traffico entra nel VPC. Se si sceglie un gateway virtuale privato, per CIDR IPv4 destinazione, specificare la sottorete CIDR di destinazione.
6. Per aggiungere un'altra sottorete di destinazione, scegliere Aggiungi altra sottorete, quindi completare le seguenti operazioni:

   - Per Middlebox, scegliere l'ID dell'interfaccia di rete associata all'appliance middlebox oppure, se si utilizza un endpoint del load balancer del gateway, scegliere l'ID endpoint VPC.

     È necessario utilizzare la stessa appliance middlebox per più sottoreti.
   - Per Sottorete di destinazione, scegliere la sottorete di destinazione.

7. Seleziona Successivo.
8. Nella pagina Rivedi e aggiorna, viene riportato un elenco delle tabelle di routing e delle relative route che verranno create dalla procedura guidata di routing middlebox. Verificare le route, quindi nella finestra di dialogo di conferma selezionare Aggiorna route.

Visualizzazione delle tabelle di routing della procedura guidata di routing middlebox

Come visualizzare le tabelle di routing della procedura guidata di routing middlebox

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
3. Selezionare il VPC, quindi scegliere Operazioni,Gestione di route middlebox.
4. In Tabelle di routing middlebox, il numero indica il numero di route create dalla procedura guidata di routing middlebox. Selezionare il numero per visualizzare le route.

Le route della procedura guidata di routing middlebox saranno visualizzate in una pagina diversa della tabella di routing.

Eliminazione della configurazione della procedura guidata di routing middlebox

Se si decide di non voler più utilizzare la configurazione guidata di routing middlebox, è necessario eliminare manualmente le tabelle di routing.

Come eliminare la configurazione guidata di routing middlebox

1. Visualizzare le tabelle di routing della procedura guidata di routing middlebox. Per ulteriori informazioni, consulta the section called “Visualizzazione delle tabelle di routing della procedura guidata di routing middlebox”.

   Dopo aver eseguito l'operazione, le tabelle di routing create dalla procedura guidata di routing middlebox vengono visualizzate in una pagina distinta della tabella di routing.
2. Eliminare ogni tabella di routing visualizzata. Per ulteriori informazioni, consulta the section called “Eliminazione di una tabella di instradamento”.

## Considerazioni sulla procedura guidata di routing middlebox

Quando si utilizza la procedura guidata di routing middlebox, tenere in considerazione quanto segue:

- Se si desidera ispezionare il traffico, è possibile utilizzare un gateway Internet o un gateway virtuale privato per l'origine.
- Se si utilizza lo stesso middlebox in una configurazione middlebox multipla all'interno dello stesso VPC, assicurarsi che il middlebox si trovi nella stessa posizione hop per entrambe le sottoreti.
- L'appliance deve essere configurata in una sottorete separata da quella di origine o di destinazione.
- Devi disabilitare i controlli dell'origine/della destinazione sull'appliance. Per ulteriori informazioni, consulta Changing the Source or Destination Checking nella Guida per l'utente di Amazon EC2.
- Le tabelle di routing e le route create dalla procedura guidata di routing middlebox sono conteggiate per le quote. Per ulteriori informazioni, consulta the section called “Tabelle di instradamento”.
- Se si elimina una risorsa, ad esempio un'interfaccia di rete, le associazioni della tabella di instradamento con la risorsa saranno rimosse. Se la risorsa è una destinazione, la destinazione della route è impostata su blackhole. Le tabelle di routing non vengono eliminate.
- La sottorete middlebox e la sottorete di destinazione devono essere associate a una tabella di routing non predefinita.

> **Note**
>
> Si consiglia di utilizzare la procedura guidata di routing middlebox per modificare o eliminare le tabelle di routing create utilizzando la procedura guidata di routing middlebox.

## Scenari middlebox

Gli esempi seguenti descrivono gli scenari per la procedura guidata di instradamento middlebox.

Indice



### Ispezione del traffico destinato a una sottorete

Si consideri lo scenario in cui il traffico entra nel VPC attraverso un gateway Internet e si desidera ispezionare tutto il traffico destinato a una sottorete, ad esempio la sottorete B, utilizzando

un'appliance firewall installata su un'istanza EC2. L'appliance firewall deve essere installata e configurata su un'istanza EC2 in una sottorete separata dalla sottorete B nel VPC, ad esempio la sottorete C. È quindi possibile utilizzare la procedura guidata di routing middlebox per configurare le route per il traffico tra la sottorete B e il gateway Internet.

La procedura guidata di routing middlebox esegue automaticamente le operazioni seguenti:

- Crea le tabelle di routing seguenti:
  - Una tabella di instradamento per il gateway Internet
  - Una tabella di instradamento per la sottorete di destinazione
  - Una tabella di instradamento per la sottorete middlebox
- Aggiunge le route necessarie alle nuove tabelle di routing, come descritto nelle sezioni seguenti.
- Dissocia le tabelle di routing correnti associate al gateway Internet, alla sottorete B e alla sottorete C.
- Associa la tabella di routing A al gateway Internet (l'elemento Source (origine) nella procedura guidata di routing middlebox), la tabella di routing C alla sottorete C (l'elemento Middlebox nella procedura guidata di routing middlebox) e la tabella di routing B alla sottorete B (l'elemento Destination (destinazione) nella procedura guidata di routing middlebox).
- Crea un tag che indica che è stato creato dalla procedura guidata di routing middlebox e un tag che indica la data di creazione.

La procedura guidata di routing middlebox non modifica le tabelle di routing esistenti. Crea nuove tabelle di routing e quindi le associa alle risorse del gateway e della sottorete. Se le risorse sono già associate esplicitamente a tabelle di routing esistenti, le tabelle di routing esistenti vengono prima dissociate e quindi le nuove tabelle di routing vengono associate alle risorse. Le tabelle di routing esistenti non vengono eliminate.

Se non si utilizza la procedura guidata di routing middlebox, è necessario configurare manualmente e quindi assegnare le tabelle di routing alle sottoreti e al gateway Internet.

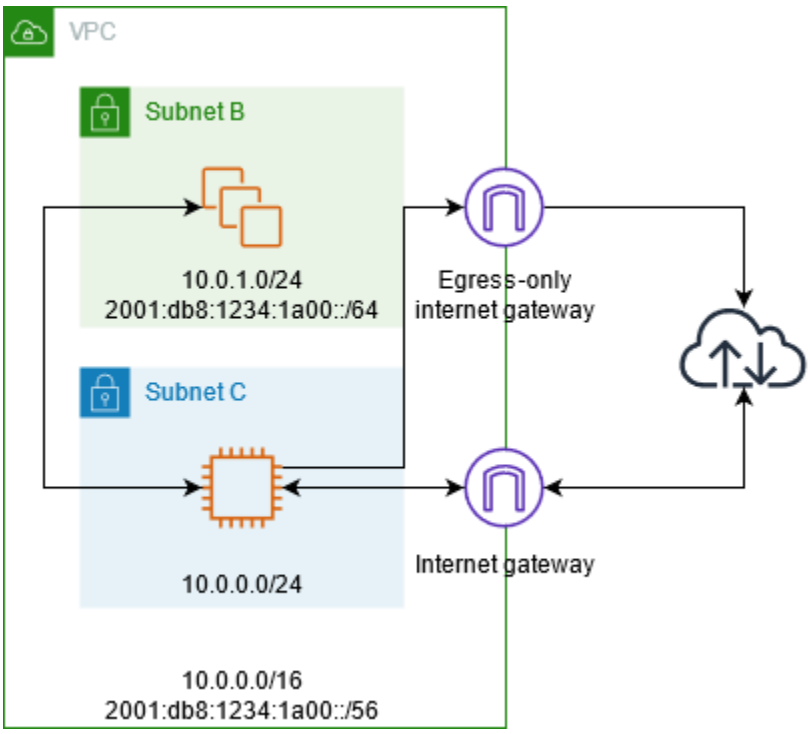



Tabella di routing del gateway Internet

Aggiungi le seguenti route alla tabella di routing per il gateway Internet.

| Destinazione | Target | Scopo |
| --- | --- | --- |
| 10.0.0.0/16 | Locale | Route locale per IPv4 |
| 10.0.1.0/24 | *appliance-eni* | Indirizza il traffico IPv4 destinato alla sottorete B al middlebox |
| *2001:db8:1234:1a00::/56* | Locale | Route locale per IPv6 |
| *2001:db8:1234:1a00::/64* | *appliance-eni* | Indirizza il traffico IPv6 destinato alla sottorete B al middlebox |

Esiste un'associazione Edge tra il gateway Internet e il VPC.

Quando utilizzi la procedura guidata di instradamento middlebox, alla tabella di instradamento sono associati i tag seguenti:

- La chiave è “Origin” e il valore è “Middlebox wizard”
- La chiave è “date_created” e il valore è l'ora di creazione (ad esempio "2021-02-18T22:25:49.137Z")

Tabella di routing della sottorete di destinazione

Aggiungi le seguenti route alla tabella di instradamento per la sottorete di destinazione (l'elemento subnet B (sottorete B) nel diagramma di esempio).

| Destinazione | Target | Scopo |
| --- | --- | --- |
| 10.0.0.0/16 | Locale | Route locale per IPv4 |
| 0.0.0.0/0 | *appliance-eni* | Indirizza il traffico IPv4 destinato a Internet al middlebox |
| *2001:db8:1234:1a00::/56* | Locale | Route locale per IPv6 |
| ::/0 | *appliance-eni* | Instradamento del traffico IPv6 destinato a Internet al middlebox |

La sottorete ha un'associazione con la sottorete middlebox.

Quando utilizzi la procedura guidata di instradamento middlebox, alla tabella di instradamento sono associati i tag seguenti:

- La chiave è “Origin” e il valore è “Middlebox wizard”
- La chiave è “date_created” e il valore è l'ora di creazione (ad esempio "2021-02-18T22:25:49.137Z")

Tabella di routing della sottorete middlebox

Aggiungi le seguenti route alla tabella di instradamento per la sottorete middlebox (l'elemento subnet C (sottorete C) nel diagramma di esempio).

| Destinazione | Target | Scopo |
| --- | --- | --- |
| 10.0.0.0/16 | Locale | Route locale per IPv4 |
| 0.0.0.0/0 | *igw-id* | Indirizza il traffico IPv4 al gateway Internet |
| *2001:db8:1234:1a00::/56* | Locale | Route locale per IPv6 |
| ::/0 | *eigw-id* | Instradamento del traffico IPv6 a un gateway Internet egress-only |

La sottorete ha un'associazione con la sottorete di destinazione.

Quando utilizzi la procedura guidata di instradamento middlebox, alla tabella di instradamento sono associati i tag seguenti:

- La chiave è “Origin” e il valore è “Middlebox wizard”
- La chiave è “date_created” e il valore è l’ora di creazione (ad esempio "2021-02-18T22:25:49.137Z")

Ispezione del traffico utilizzando appliance in un VPC di sicurezza

Considera lo scenario in cui devi ispezionare il traffico che entra in un VPC dal gateway Internet ed è destinato alla sottorete utilizzando un parco istanze di appliance di sicurezza configurate con un Gateway Load Balancer. Il proprietario del VPC del consumer del servizio crea un endpoint Gateway Load Balancer in una sottorete nel suo VPC (rappresentato da un'interfaccia di rete dell'endpoint). Tutto il traffico che entra nel VPC attraverso il gateway Internet viene instradato all'endpoint Gateway Load Balancer per l’ispezione prima di essere instradato nella sottorete dell’applicazione. Analogamente, tutto il traffico che esce dalla sottorete dell’applicazione viene instradato sull'endpoint Gateway Load Balancer per l’ispezione prima di essere instradato su Internet.

La procedura guidata di routing middlebox esegue automaticamente le operazioni seguenti:

- Crea le tabelle di routing.
- Aggiunge le route necessarie alle nuove tabelle di routing.

- Dissocia le tabelle di routing correnti associate alle sottoreti.
- Associa alle sottoreti le tabelle di routing create dalla procedura guidata di routing middlebox.
- Crea un tag che indica che è stato creato dalla procedura guidata di routing middlebox e un tag che indica la data di creazione.

La procedura guidata di routing middlebox non modifica le tabelle di routing esistenti. Crea nuove tabelle di routing e quindi le associa alle risorse del gateway e della sottorete. Se le risorse sono già associate esplicitamente a tabelle di routing esistenti, le tabelle di routing esistenti vengono prima dissociate e quindi le nuove tabelle di routing vengono associate alle risorse. Le tabelle di routing esistenti non vengono eliminate.

Se non si utilizza la procedura guidata di routing middlebox, è necessario configurare manualmente e quindi assegnare le tabelle di routing alle sottoreti e al gateway Internet.

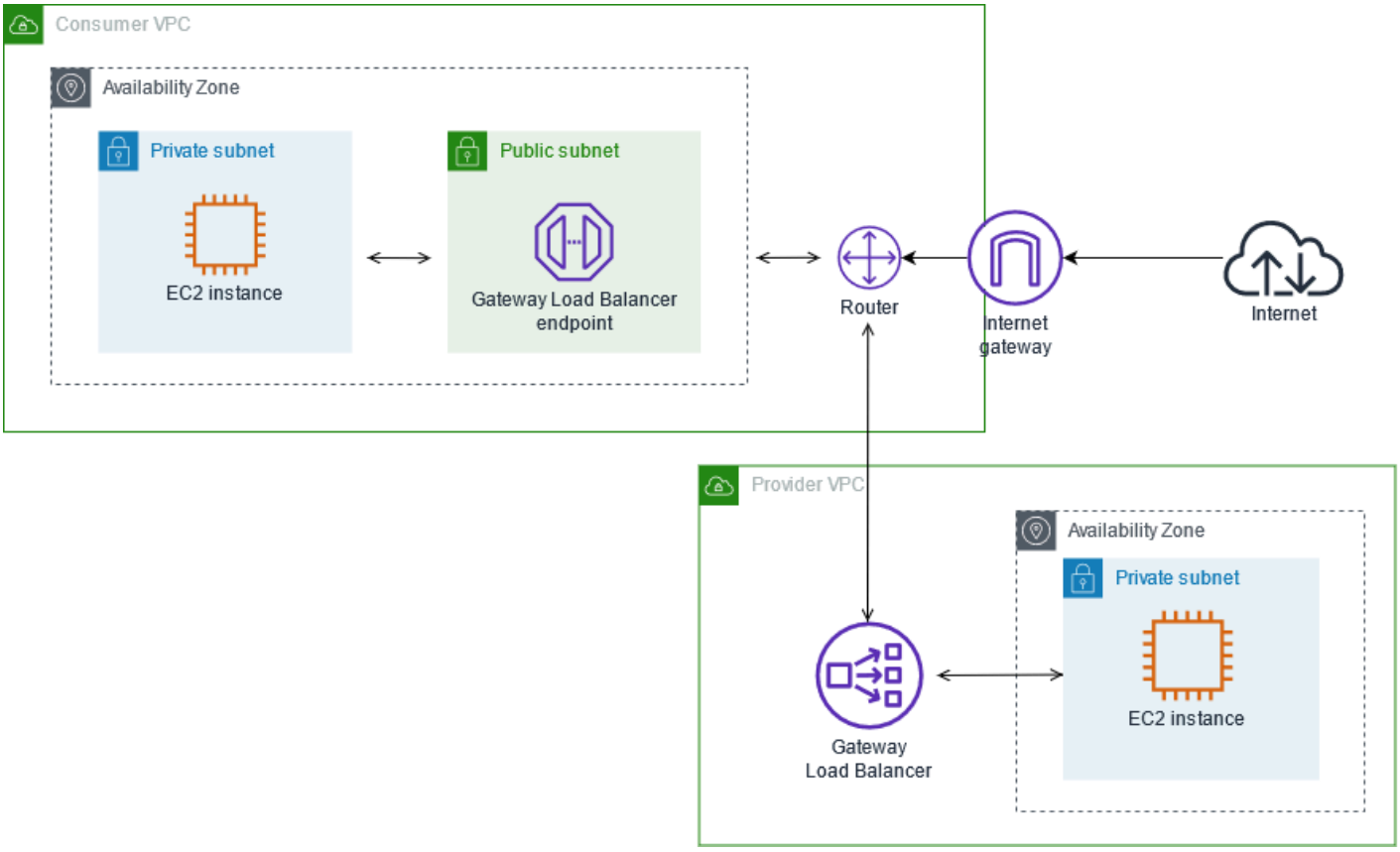



Tabella di routing del gateway Internet

La tabella di instradamento del gateway Internet ha gli instradamenti seguenti:

| Destinazione | Target | Scopo |
| --- | --- | --- |
| *CIDR VPC consumer* | Locale | Route locale |
| *CIDR sottorete applicazione* | *ID endpoint* | Indirizza il traffico destinato alla sottorete dell'applicazione all'endpoint Gateway Load Balancer. |

Esiste un'associazione edge con il gateway.

Quando utilizzi la procedura guidata di instradamento middlebox, alla tabella di instradamento sono associati i tag seguenti:

- La chiave è "Origin" e il valore è "Middlebox wizard"
- La chiave è "date_created" e il valore è l'ora di creazione (ad esempio "2021-02-18T22:25:49.137Z")

Tabella di instradamento della sottorete

La tabella di instradamento per la sottorete dell'applicazione ha gli instradamenti seguenti.

| Destinazione | Target | Scopo |
| --- | --- | --- |
| *CIDR VPC consumer* | Locale | Route locale |
| 0.0.0.0/0 | *ID endpoint* | Instrada il traffico dai server dell'appl icazione all'endpoint Gateway Load Balancer prima di instradarlo su Internet. |

Quando utilizzi la procedura guidata di instradamento middlebox, alla tabella di instradamento sono associati i tag seguenti:

- La chiave è "Origin" e il valore è "Middlebox wizard"
- La chiave è "date_created" e il valore è l'ora di creazione (ad esempio "2021-02-18T22:25:49.137Z")

Tabella di instradamento della sottorete del provider

La tabella di instradamento per la sottorete del provider ha gli instradamenti seguenti:

| Destinazione | Target | Scopo |
| --- | --- | --- |
| *CIDR VPC provider* | Locale | Instradamento locale. Assicura che il traffico proveniente da Internet venga instradato ai server delle applicazioni. |
| 0.0.0.0/0 | *igw-id* | Indirizza tutto il traffico al gateway Internet. |

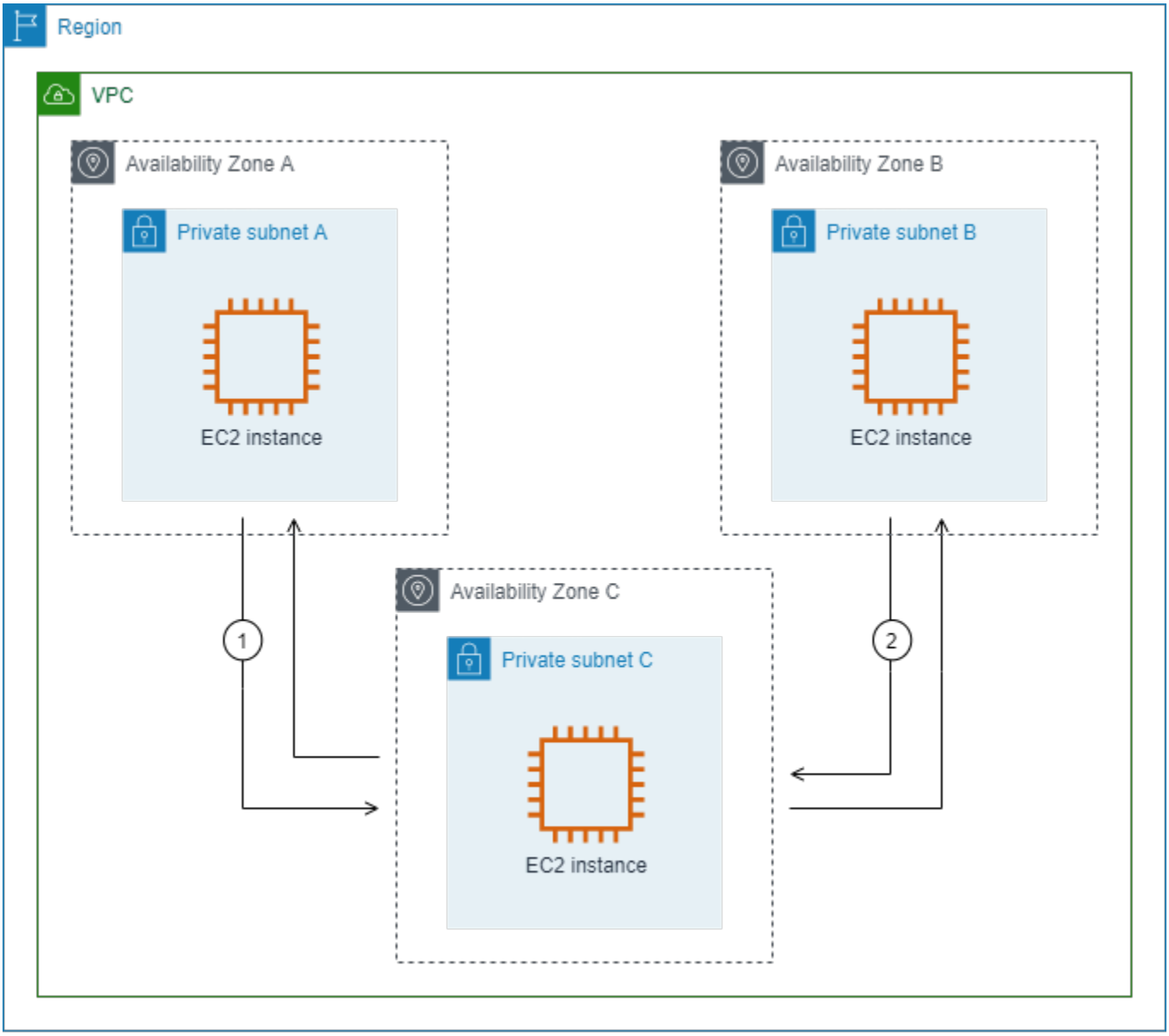
Quando utilizzi la procedura guidata di instradamento middlebox, alla tabella di instradamento sono associati i tag seguenti:

- La chiave è “Origin” e il valore è “Middlebox wizard”
- La chiave è “date_created” e il valore è l’ora di creazione (ad esempio "2021-02-18T22:25:49.137Z")

Controllo del traffico tra sottoreti

Considera lo scenario in cui hai più sottoreti in un VPC e desideri controllare il traffico tra tali sottoreti utilizzando un'appliance firewall. Configura e installa l'appliance firewall in un'istanza EC2 in una sottorete separata nel VPC.

Nel diagramma seguente viene illustrata un'appliance firewall installata su un'istanza EC2 nella sottorete C. L'appliance ispeziona tutto il traffico che viaggia dalla sottorete A alla sottorete B (vedi 1) e dalla sottorete B alla sottorete A (vedi 2).




Puoi utilizzare la tabella di instradamento principale per il VPC e la sottorete middlebox. Le sottoreti A e B hanno ognuna una tabella di instradamento personalizzata.

La procedura guidata di routing middlebox esegue automaticamente le operazioni seguenti:

- Crea le tabelle di routing.
- Aggiunge le route necessarie alle nuove tabelle di routing.
- Dissocia le tabelle di routing correnti associate alle sottoreti.
- Associa alle sottoreti le tabelle di routing create dalla procedura guidata di routing middlebox.

- Crea un tag che indica che è stato creato dalla procedura guidata di routing middlebox e un tag che indica la data di creazione.

La procedura guidata di routing middlebox non modifica le tabelle di routing esistenti. Crea nuove tabelle di routing e quindi le associa alle risorse del gateway e della sottorete. Se le risorse sono già associate esplicitamente a tabelle di routing esistenti, le tabelle di routing esistenti vengono prima dissociate e quindi le nuove tabelle di routing vengono associate alle risorse. Le tabelle di routing esistenti non vengono eliminate.

Se non si utilizza la procedura guidata di routing middlebox, è necessario configurare manualmente e quindi assegnare le tabelle di routing alle sottoreti e al gateway Internet.

Tabella di instradamento personalizzata per la sottorete A

La tabella di instradamento per la sottorete A ha gli instradamenti seguenti.

| Destinazione | Target | Scopo |
|---|---|---|
| *CIDR VPC* | Locale | Route locale |
| *CIDR sottorete B* | *appliance-eni* | Instradare il traffico destinato alla sottorete B al middlebox |

Quando utilizzi la procedura guidata di instradamento middlebox, alla tabella di instradamento sono associati i tag seguenti:

- La chiave è “Origin” e il valore è “Middlebox wizard”
- La chiave è “date_created” e il valore è l'ora di creazione (ad esempio "2021-02-18T22:25:49.137Z")

Tabella di instradamento personalizzata per la sottorete B

La tabella di instradamento per la sottorete B ha gli instradamenti seguenti.

| Destinazione | Target | Scopo |
|---|---|---|
| *CIDR VPC* | Locale | Route locale |

| Destinazione | Target | Scopo |
| --- | --- | --- |
| *CIDR sottorete A* | *appliance-eni* | Instradare il traffico destinato alla sottorete A al middlebox |

Quando utilizzi la procedura guidata di instradamento middlebox, alla tabella di instradamento sono associati i tag seguenti:

- La chiave è “Origin” e il valore è “Middlebox wizard”
- La chiave è “date_created” e il valore è l'ora di creazione (ad esempio "2021-02-18T22:25:49.137Z")

Tabella di routing principale

La sottorete C utilizza la tabella di instradamento principale. La tabella di instradamento principale ha l'instradamento seguente.

| Destinazione | Target | Scopo |
| --- | --- | --- |
| *CIDR VPC* | Locale | Route locale |

Quando utilizzi la procedura guidata di instradamento middlebox, alla tabella di instradamento sono associati i tag seguenti:

- La chiave è “Origin” e il valore è “Middlebox wizard”
- La chiave è “date_created” e il valore è l'ora di creazione (ad esempio "2021-02-18T22:25:49.137Z")

## Eliminare una sottorete

Se una sottorete non è più necessaria, è possibile eliminarla. Non è possibile eliminare una sottorete se contiene interfacce di rete. Ad esempio, è necessario terminare tutte le istanze in una sottorete prima di poterla eliminare.

### Eliminazione di una sottorete tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Terminare tutte le istanze nella sottorete. Per ulteriori informazioni, consulta la sezione relativa alla terminazione dell'istanza nella Guida per l'utente di Amazon EC2.
3. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
4. Nel riquadro di navigazione, scegliere Subnets (Sottoreti).
5. Selezionare la sottorete e scegliere Actions (Operazioni), Delete Subnet (Elimina sottorete).
6. Quando viene richiesta la conferma, digitare **`delete`** e quindi scegliere Delete (Elimina).

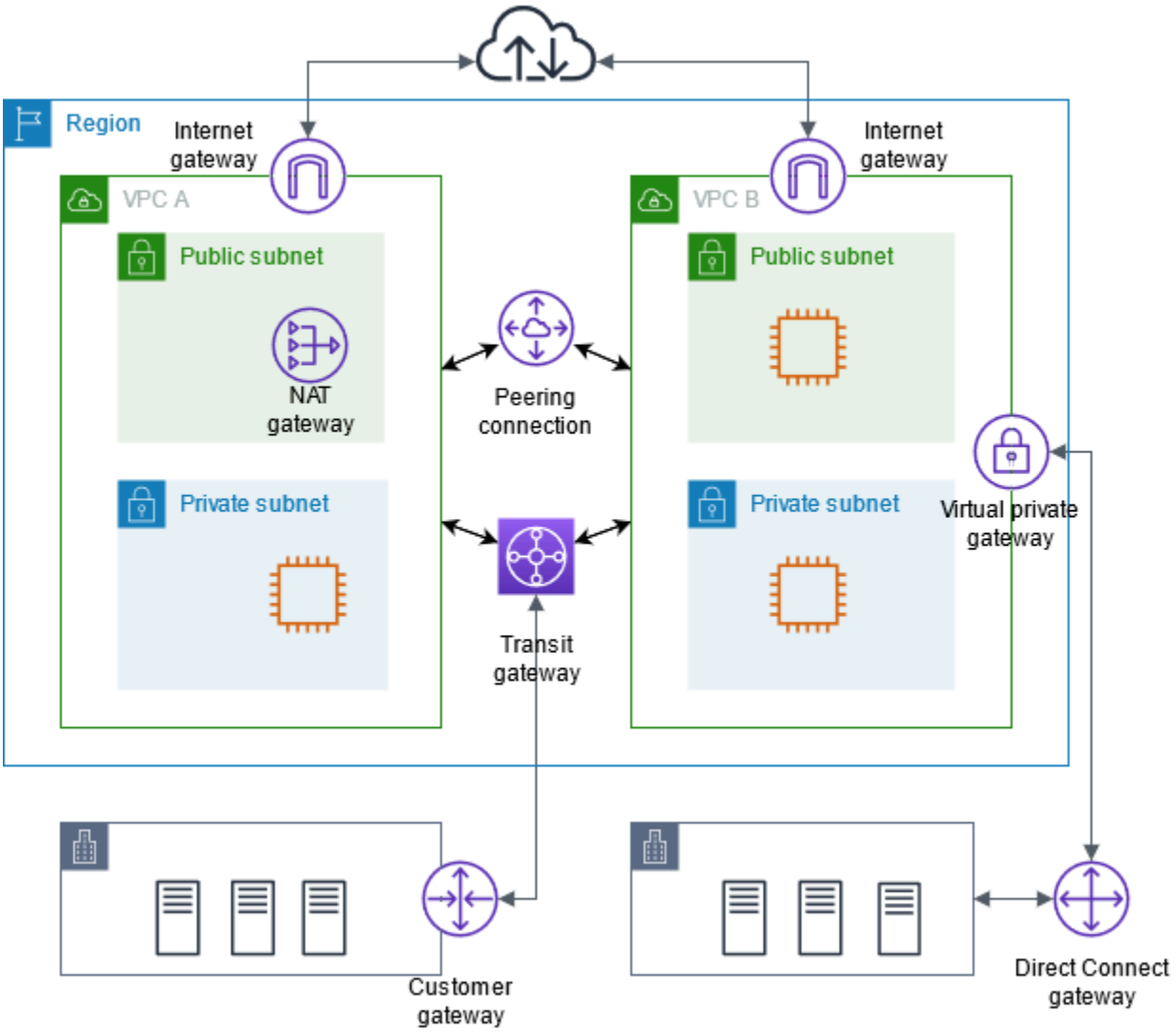
### Eliminazione di una sottorete tramite AWS CLI

Usa il comando delete-subnet.

# Connetti il tuo VPC ad altre reti

È possibile connettere il cloud privato virtuale (VPC) ad altre reti. Ad esempio, ad altri VPC, a Internet o alla rete locale.

Il seguente diagramma illustra alcune di queste opzioni di connettività. VPC A è connesso a Internet tramite un gateway Internet. L'istanza EC2 nella sottorete privata del VPC A può connettersi a Internet utilizzando il gateway NAT nella sottorete pubblica del VPC A. Il VPC B è connesso a Internet tramite un gateway Internet. L'istanza EC2 nella sottorete pubblica del VPC B può connettersi a Internet utilizzando il gateway Internet. Il VPC A e il VPC B sono collegati tra loro tramite una connessione peering VPC e un gateway di transito. Il gateway di transito ha un collegamento VPN a un data center. Il VPC B dispone di una AWS Direct Connect connessione a un data center.



Per ulteriori informazioni, consulta Opzioni di connettività di Amazon Virtual Private Cloud.

Indice



# Eseguire la connessione a Internet utilizzando un gateway Internet

Un gateway Internet è un componente VPC scalato orizzontalmente, ridondante e ad alta disponibilità che consente la comunicazione tra il VPC e Internet. Supporta traffico IPv4 e IPv6. Non causa rischi di disponibilità o vincoli di larghezza di banda nel traffico di rete.

Un gateway Internet consente alle risorse nelle sottoreti pubbliche (ad es. istanze EC2) di collegarsi a Internet se la risorsa ha un indirizzo IPv4 pubblico o un indirizzo IPv6. Analogamente, le risorse su Internet possono avviare una connessione alle risorse nella sottorete utilizzando l'indirizzo IPv4 pubblico o IPv6 pubblico. Ad esempio, un gateway Internet consente di connettersi a un'istanza EC2 AWS utilizzando il computer locale.

Un gateway Internet fornisce una destinazione nelle tabelle di instradamento del VPC per il traffico instradabile su Internet. Per le comunicazioni tramite IPv4, il gateway Internet esegue anche Network Address Translation (NAT). Per la comunicazione tramite IPv6, NAT non è necessario perché gli indirizzi IPv6 sono pubblici. Per ulteriori informazioni, consulta Indirizzi IP e NAT.

## Configurazione per l'accesso a Internet

Per consentire alle istanze di ricevere o inviare traffico da Internet, effettua le seguenti operazioni:

- Crea un gateway Internet e collegalo al tuo VPC.
- Aggiungi un instradamento alla tabella di routing per la sottorete che indirizza il traffico di Internet al gateway Internet.

- Accertati che le istanze nella sottorete hanno un indirizzo IPv4 pubblico o un indirizzo IPv6. Per ulteriori informazioni, consulta Indirizzamento IP dell'istanza nella Guida per l'utente di Amazon EC2.
- Accertati che i gruppi di sicurezza e le liste di controllo accessi alla rete consentano il flusso del traffico Internet desiderato da/verso le tue istanze.

Per fornire alle istanze l'accesso a Internet senza assegnare indirizzi IP pubblici a tali istanze, utilizza un dispositivo NAT. Un dispositivo NAT consente alle istanze di una sottorete privata di connettersi a Internet, ma impedisce agli host su Internet di avviare connessioni con le istanze. Per ulteriori informazioni, consulta Dispositivi NAT.

Sottoreti pubbliche e private

Se la sottorete è associata a una tabella di routing che ha una route a un Internet Gateway, è nota come una sottorete pubblica. Se una sottorete è associata a una tabella di routing che non dispone di una route a un Internet Gateway, è nota come una sottorete privata.

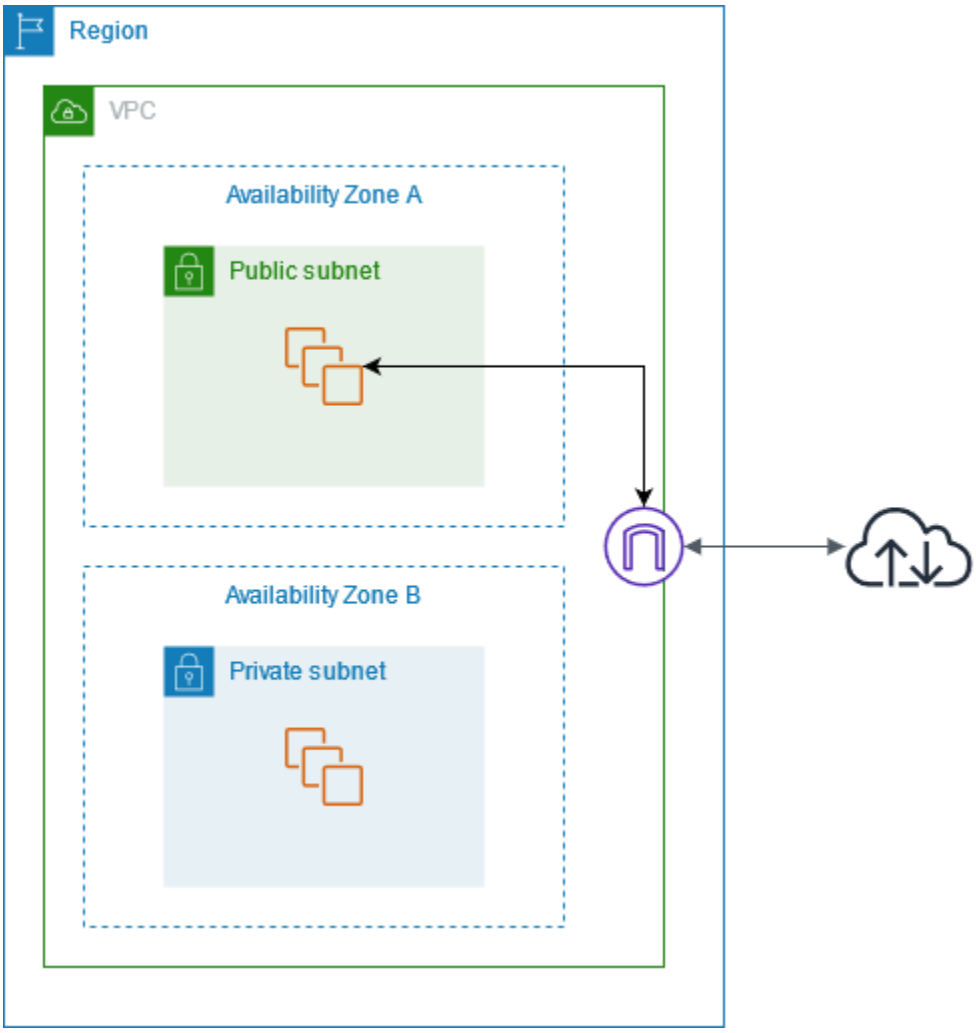
Nella tabella di routing della sottorete, puoi specificare una route per il gateway Internet a tutte le destinazioni non esplicitamente note alla tabella di routing (`0.0.0.0/0` per IPv4 o `::/0` per IPv6). In alternativa, puoi estendere il percorso a un intervallo più ristretto di indirizzi IP; ad esempio, gli indirizzi IPv4 pubblici degli endpoint pubblici della tua azienda esterni o gli indirizzi IP elastici di AWS altre istanze Amazon EC2 esterne al tuo VPC.

Indirizzi IP e NAT

Per abilitare la comunicazione via Internet per IPv4, l'istanza deve avere un indirizzo IPv4 pubblico. Puoi configurare il VPC per l'assegnazione automatica degli indirizzi IPv4 pubblici alle istanze o puoi assegnare indirizzi IP elastici alle istanze. L'istanza conosce soltanto lo spazio degli indirizzi IP (interni) privati definito nel VPC e nella sottorete. Il gateway Internet fornisce logicamente il one-to-one NAT per conto dell'istanza, in modo che quando il traffico lascia la sottorete VPC e va a Internet, il campo dell'indirizzo di risposta viene impostato sull'indirizzo IPv4 pubblico o sull'indirizzo IP elastico dell'istanza e non sul suo indirizzo IP privato. Inversamente, l'indirizzo di destinazione del traffico destinato all'indirizzo IPv4 pubblico o all'indirizzo IP elastico dell'istanza viene convertito nell'indirizzo IPv4 privato dell'istanza prima che il traffico sia distribuito al VPC.

Per abilitare la comunicazione via Internet per IPv6, il VPC e la sottorete devono avere un blocco CIDR IPv6 associato e all'istanza deve Essere assegnato un indirizzo IPv6 dell'intervallo della sottorete. Gli indirizzi IPv6 sono globalmente univoci e sono pertanto pubblici per impostazione predefinita.

Nel diagramma seguente, la sottorete situata in zona di disponibilità A è una sottorete pubblica. La tabella di routing per questa sottorete ha una route che instrada tutto il traffico IPv4 legato a Internet al gateway Internet. Le istanze nella sottorete pubblica devono avere indirizzi IP pubblici o indirizzi IP elastici per consentire la comunicazione con Internet tramite il gateway Internet. Per fare un confronto, la sottorete nella zona di disponibilità B è una sottorete privata perché la tabella di routing non dispone di un routing al gateway Internet. Poiché non esiste un percorso verso il gateway Internet, le istanze nella sottorete privata non possono comunicare con Internet anche se dispongono di indirizzi IP pubblici.




Accesso a Internet per VPC predefiniti e non predefiniti

La tabella seguente indica se il tuo VPC include dei componenti necessari per l'accesso a Internet via IPv4 o IPv6.

| Componente | VPC predefinito | VPC non predefinito |
| --- | --- | --- |
| Internet Gateway | Sì | No |
| Tabella di routing con route all'Internet Gateway per il traffico IPv4 (0.0.0.0/0) | Sì | No |
| Tabella di routing con route all'Internet Gateway per il traffico IPv6 (::/0) | No | No |
| Indirizzo IPv4 pubblico assegnato automaticamente all'istanza avviata nella sottorete | Sì (sottorete predefinita) | No (sottorete non predefinita) |
| Indirizzo IPv6 assegnato automaticamente all'istanza avviata nella sottorete | No (sottorete predefinita) | No (sottorete non predefinita) |

Per ulteriori informazioni sui VPC predefiniti, consulta VPC di default. Per ulteriori informazioni sulla creazione di un VPC, consulta Crea un VPC.

## Gestione dei gateway Internet

Di seguito viene descritto come supportare l'accesso a Internet da una sottorete nel proprio VPC utilizzando un gateway Internet. Per rimuovere l'accesso a Internet, è possibile distaccare il gateway Internet dal VPC e quindi eliminarlo.

Attività

- Creazione di un Internet Gateway
- Collegamento di un Internet Gateway a un VPC
- Scollegamento di un gateway Internet dal VPC
- Eliminazione di un Internet Gateway

## Creazione di un Internet Gateway

Usa la procedura seguente per creare un gateway Internet.

Creare un gateway Internet

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Internet gateways (Gateway Internet).
3. Scegliere Crea gateway Internet.
4. (Facoltativo) Inserisci un nome per il gateway Internet.
5. (Facoltativo) Per aggiungere un tag, scegli Add new tag (Aggiungi nuovo tag) e immetti la chiave e il valore del tag.
6. Scegliere Crea gateway Internet.
7. (Facoltativo) Per collegare immediatamente il gateway Internet a un VPC, scegli Attach to a VPC (Collega a un VPC) dal banner nella parte superiore dello schermo, seleziona un VPC disponibile e scegli Attach internet gateway (Collega un gateway Internet). In alternativa, puoi collegare il gateway Internet a un VPC in un altro momento.

## Collegamento di un Internet Gateway a un VPC

Per utilizzare un gateway Internet, devi collegarlo a un VPC.

Collegamento di un gateway Internet a un VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Internet gateways (Gateway Internet).
3. Seleziona la casella di controllo accanto al gateway Internet.
4. Scegli Actions (Azioni), Attach to VPC (Collega a un VPC).
5. Seleziona un VPC disponibile.
6. Scegli Attach internet gateway (Collega un gateway Internet).

## Scollegamento di un gateway Internet dal VPC

Se non hai più bisogno dell'accesso a Internet per le istanze che avvii in un VPC, puoi scollegare un Internet Gateway da un VPC. Non puoi scollegare un Internet Gateway se il VPC ha risorse con indirizzi IP pubblici o indirizzi IP elastici associati.

Per scollegare un Internet Gateway

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Internet gateways (Gateway Internet).
3. Seleziona la casella di controllo accanto al gateway Internet.
4. Scegli Actions, Detach from VPC (Azioni, Scollega da VPC).
5. Quando viene chiesta la conferma, seleziona Detach internet gateway (Scollega gateway Internet).

### Eliminazione di un Internet Gateway

Se non hai più bisogno di un Internet Gateway, puoi eliminarlo. Non puoi tuttavia svolgere questa operazione se un Internet Gateway è ancora collegato a un VPC.

Per eliminare un Internet Gateway

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Internet gateways (Gateway Internet).
3. Seleziona la casella di controllo accanto al gateway Internet.
4. Scegli Actions (Azioni) Delete internet gateway (Elimina gateway Internet).
5. Quando viene richiesta la conferma, inserisci **`delete`** e scegli Delete internet gateway (Elimina gateway Internet).

## Panoramica sulle API e sui comandi

Puoi eseguire le attività descritte in questa pagina tramite la riga di comando o un'API. Per ulteriori informazioni sulle interfacce a riga di comando e per un elenco delle operazioni API disponibili, consulta Uso di Amazon VPC.

Creazione di un Internet Gateway

- create-internet-gateway (AWS CLI)
- New-EC2InternetGateway (AWS Tools for Windows PowerShell)

Collegamento di un Internet Gateway a un VPC

- attach-internet-gateway (AWS CLI)
- Add-EC2InternetGateway (AWS Tools for Windows PowerShell)

Descrizione di un Internet Gateway

- describe-internet-gateways (AWS CLI)
- Get-EC2InternetGateway (AWS Tools for Windows PowerShell)

Scollegamento di un Internet Gateway da un VPC

- detach-internet-gateway (AWS CLI)
- Dismount-EC2InternetGateway (AWS Tools for Windows PowerShell)

Eliminazione di un Internet Gateway

- delete-internet-gateway (AWS CLI)
- Remove-EC2InternetGateway (AWS Tools for Windows PowerShell)

## Prezzi

Non sono previsti costi per un gateway Internet ma sono previsti costi di trasferimento dati per le istanze EC2 che lo utilizzano. Per ulteriori informazioni, consulta Prezzi di Amazon EC2 on demand.

# Abilitazione del traffico in uscita IPv6 utilizzando un gateway Internet egress-only

Un gateway Internet egress-only è un componente VPC aggiunto in parallelo, ridondante e ad alta disponibilità che permette la comunicazione in uscita su IPv6 da istanze nel VPC a Internet e impedisce a Internet di avviare una connessione IPv6 con le istanze.

> **Note**
>
> Un gateway Internet egress-only è destinato all'utilizzo solo con traffico IPv6. Per abilitare la comunicazione Internet solo in uscita su IPv4, utilizza invece un gateway NAT. Per ulteriori informazioni, consult Gateway NAT.

Indice



## Nozioni di base sull'Internet Gateway egress-only

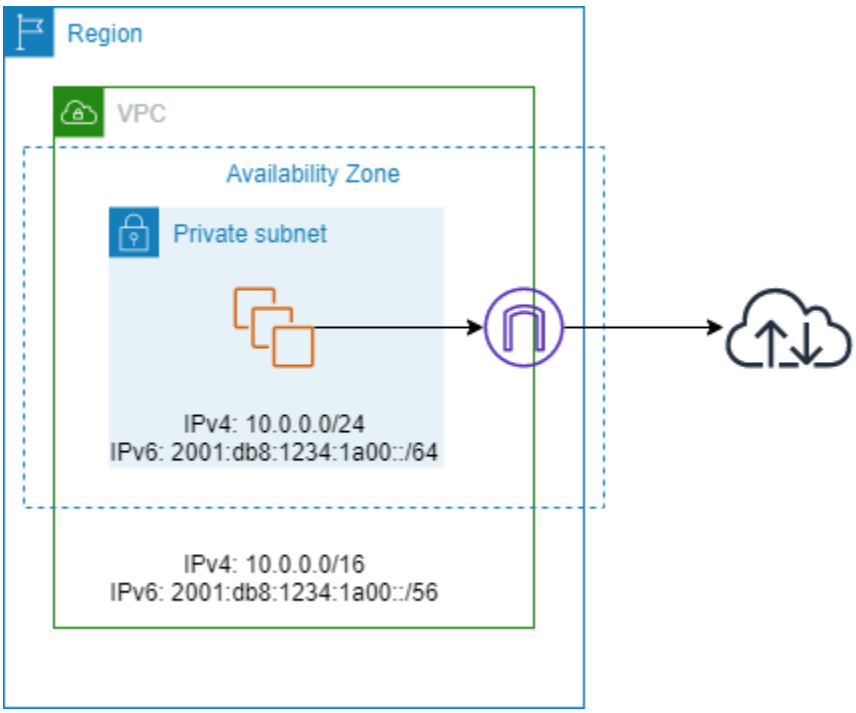
Gli indirizzi IPv6 sono globalmente univoci e sono pertanto pubblici per impostazione predefinita. Se l'istanza deve essere in grado di accedere a Internet, ma desideri impedire a risorse su Internet di avviare una comunicazione con l'istanza, puoi utilizzare un Internet Gateway egress-only. Per farlo, crea un gateway Internet egress-only nel VPC, quindi aggiungi una route alla tabella di routing che punta tutto il traffico IPv6 (`::/0`) o un intervallo specifico di indirizzi IPv6 al gateway Internet egress-only. Il traffico IPv6 nella sottorete associata alla tabella di routing viene instradato al gateway Internet egress-only.

Un gateway Internet solo in uscita è stateful: inoltra il traffico dalle istanze nella sottorete a Internet o ad altri AWS servizi, quindi invia la risposta alle istanze.

Un gateway Internet egress-only dispone delle seguenti caratteristiche:

- Non puoi associare un gruppo di sicurezza a un gateway Internet egress-only. Puoi utilizzare gruppi di sicurezza per istanze nella sottorete privata per controllare il traffico verso e da tale istanze.
- Puoi utilizzare una lista di controllo degli accessi di rete per controllare il traffico verso e dalla sottorete per la quale il gateway Internet egress-only instrada il traffico.

Nel diagramma seguente, il VPC ha sia blocchi CIDR IPv4 che IPv6 e la sottorete sia blocchi CIDR IPv4 che IPv6. Il VPC ha un gateway Internet egress-only.




Di seguito è riportata la tabella di routing associata alla sottorete. Esiste una route che invia tutto il traffico IPv6 (::/0) che punta a un gateway Internet egress-only.

| Destinazione | Target |
| --- | --- |
| 10.0.0.0/16 | Locale |
| 2001:db8:1234:1a00:/64 | Locale |
| ::/0 | *eigw-id* |

## Utilizzo di gateway Internet egress-only

Nelle sezioni seguenti viene descritto come creare un gateway Internet egress-only per la sottorete privata e come configurare il routing per la sottorete.

Attività

- Creazione di un gateway Internet egress-only
- Visualizzazione del gateway Internet egress-only
- Creazione di una tabella di routing personalizzata

- Eliminazione di un gateway Internet egress-only

## Creazione di un gateway Internet egress-only

Puoi creare un Internet Gateway egress-only per il VPC utilizzando la console Amazon VPC.

Per creare un gateway internet egress-only

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Egress Only Internet Gateways (Internet Gateway Egress-Only).
3. Selezionare Create Egress Only Internet Gateway (Crea Internet Gateway Egress-Only).
4. (Facoltativo) Aggiungere o rimuovere un tag.

   [Aggiunta di un tag] Scegli Aggiungi nuovo tag e procedi come segue:

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

   [Rimuovi un tag] Scegli Rimuovi a destra della Chiave e del Valore del tag.
5. Selezionare il VPC nel quale creare l'Internet Gateway egress-only.
6. Seleziona Crea.

## Visualizzazione del gateway Internet egress-only

Puoi visualizzare informazioni sull'Internet Gateway egress-only nella console Amazon VPC.

Per visualizzare informazioni relative a un gateway Internet egress-only

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Egress Only Internet Gateways (Internet Gateway Egress-Only).
3. Selezionare il gateway Internet egress-only per visualizzare le relative informazioni nel riquadro dei dettagli.

## Creazione di una tabella di routing personalizzata

Per inviare traffico destinato all'esterno del VPC al gateway Internet egress-only, devi creare una tabella di routing personalizzata, aggiungere una route che invia il traffico al gateway, quindi associarla alla sottorete.

Per creare una tabella di routing personalizzata e aggiungere una route al gateway Internet egress-only

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Tabelle di routing, Crea tabella di routing.
3. Nella finestra di dialogo Crea tabella di routing, assegna facoltativamente un nome alla tabella di routing, quindi seleziona il VPC e scegli Crea tabella di routing.
4. Selezionare la tabella di routing personalizzata appena creata. Nel riquadro dei dettagli sono visualizzate le schede per utilizzare la route, le associazioni e la propagazione della route.
5. Nella scheda Route, seleziona Modifica route, specifica `::/0` nella casella Destinazione, seleziona l'ID del gateway Internet egress-only nell'elenco Target, quindi seleziona Salva modifiche.
6. Nella scheda Associazioni sottorete, scegli Modifica associazioni sottorete e seleziona la casella di controllo della sottorete. Selezionare Salva.

In alternativa, è possibile aggiungere una route a una tabella di routing esistente associata alla sottorete. Selezionare la tabella di routing esistente e seguire le fasi 5 e 6 precedenti per aggiungere una route per il gateway Internet egress-only.

Per ulteriori informazioni sulle tabelle di routing, consulta Configurare le tabelle di routing.

## Eliminazione di un gateway Internet egress-only

Se non hai più bisogno di un gateway Internet egress-only, puoi eliminarlo. L'eventuale route in una tabella di routing che fa riferimento al gateway Internet egress-only eliminato rimane in uno stato `blackhole` finché la route non viene eliminata o aggiornata manualmente.

Per eliminare un gateway Internet egress-only

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Gateway Internet egress-only e selezionare il gateway Internet egress-only.

3. Scegliere Delete (Elimina).
4. Nella finestra di dialogo di conferma, scegliere Delete Egress Only Internet Gateway (Elimina Internet Gateway Egress-Only).

## Panoramica su API e CLI

Puoi eseguire le attività descritte in questa pagina tramite la riga di comando o un'API. Per ulteriori informazioni sulle interfacce a riga di comando e per un elenco delle operazioni API disponibili, consulta Uso di Amazon VPC.

Creazione di un gateway Internet egress-only

- create-egress-only-internet AWS CLI-gateway ()
- New-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

Descrizione di un gateway Internet egress-only

- describe-egress-only-internet-gateway ()AWS CLI
- Get-EC2EgressOnlyInternetGatewayList (AWS Tools for Windows PowerShell)

Eliminazione di un gateway Internet egress-only

- delete-egress-only-internet-gateway ()AWS CLI
- Remove-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

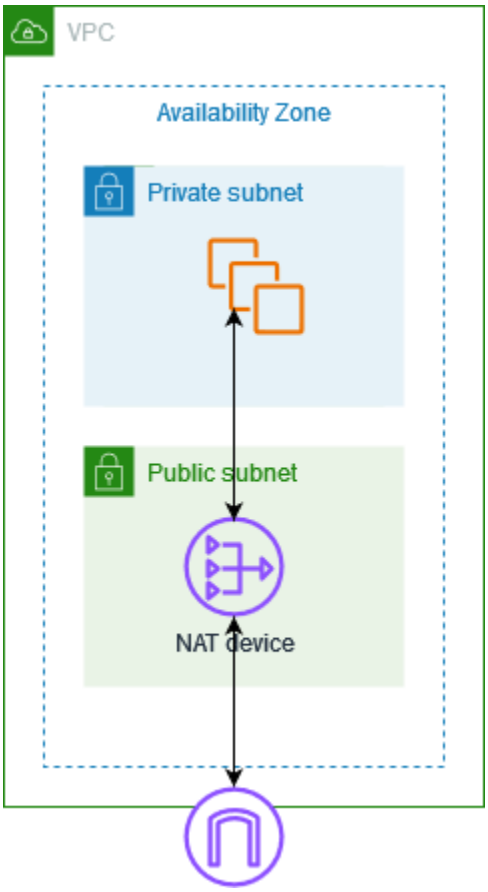
## Prezzi

Non sono previsti costi per un gateway Internet egress-only ma sono previsti costi di trasferimento dati per le istanze EC2 che lo utilizzano. Per ulteriori informazioni, consulta Prezzi di Amazon EC2 on demand.

# Eseguire la connessione a Internet o ad altri VPC utilizzando dispositivi NAT

È possibile utilizzare un dispositivo NAT per consentire alle risorse di sottoreti private di connettersi a Internet, ad altri VPC o a reti On-Premise. Queste istanze possono comunicare con servizi esterni al VPC, ma non possono ricevere richieste di connessione non richieste.

Ad esempio, il diagramma seguente mostra un dispositivo NAT in una sottorete pubblica che consente alle istanze EC2 in una sottorete privata di connettersi a Internet tramite un gateway Internet. Il dispositivo NAT sostituisce l'indirizzo IPv4 di origine delle istanze con l'indirizzo del dispositivo NAT. Quando si invia il traffico di risposta alle istanze, il dispositivo NAT converte gli indirizzi negli indirizzi IPv4 di origine iniziali.




**Important**

- Il termine NAT è utilizzato in questa documentazione per seguire la terminologia IT comune, sebbene la funzione effettiva di un dispositivo NAT sia la conversione degli indirizzi e la conversione degli indirizzi delle porte (PAT).

- Puoi utilizzare un dispositivo NAT gestito offerto da AWS, chiamato gateway NAT, oppure puoi creare il tuo dispositivo NAT su un'istanza EC2, chiamata istanza NAT. Si consiglia di utilizzare i gateway NAT perché offrono una maggiore disponibilità e larghezza di banda e richiedono meno sforzi di amministrazione per l'utente.

Indice



## Gateway NAT

Un gateway NAT è un servizio Network Address Translation (NAT). È possibile utilizzare un gateway NAT in modo che le istanze di una sottorete privata possano connettersi a servizi esterni al VPC, ma i servizi esterni non possono avviare una connessione con tali istanze.

Quando crei un gateway NAT, devi specificare uno dei seguenti tipi di connettività:

- Pubblico: (impostazione predefinita) le istanze nelle sottoreti private possono connettersi a Internet tramite un gateway NAT pubblico, ma non possono ricevere connessioni in ingresso non richieste da Internet. Puoi creare un gateway NAT pubblico in una sottorete pubblica e associare un indirizzo IP elastico al gateway NAT al momento della creazione. Puoi instradare il traffico dal gateway NAT al gateway Internet per il VPC. In alternativa, puoi usare un gateway NAT pubblico per connetterti ad altri VPC o alla rete locale. In questo caso, il traffico viene instradato dal gateway NAT attraverso un gateway di transito o un gateway virtuale privato.
- Privato: le istanze nelle sottoreti private possono connettersi ad altri VPC o alla rete locale tramite un gateway NAT privato. Puoi instradare il traffico dal gateway NAT attraverso un gateway di transito o un gateway virtuale privato. Non puoi associare un indirizzo IP elastico a un gateway NAT privato. Puoi collegare un gateway Internet a un VPC con un gateway NAT privato, ma se instradi il traffico dal gateway NAT privato al gateway Internet, il gateway Internet interrompe il traffico.

I gateway NAT sia privati sia pubblici associano l'indirizzo IPv4 privato di origine delle istanze all'indirizzo IPv4 privato del gateway NAT. Tuttavia, nel caso di un gateway NAT pubblico, il gateway Internet associa l'indirizzo IPv4 privato del gateway NAT pubblico all'indirizzo IP elastico associato

al gateway NAT. Quando invia traffico di risposta alle istanze, il gateway NAT converte l'indirizzo nell'indirizzo IP iniziale dell'origine, a prescindere dal fatto che il gateway NAT sia pubblico o privato.

> **Important**
>
> È possibile utilizzare un gateway NAT pubblico o privato per indirizzare il traffico verso i gateway di transito e i gateway privati virtuali.
> Se utilizzi un gateway NAT privato per connetterti a un gateway di transito o a un gateway privato virtuale, il traffico verso la destinazione proverrà dall'indirizzo IP privato del gateway NAT privato.
> Se utilizzi un gateway NAT pubblico per connetterti a un gateway di transito o a un gateway privato virtuale, il traffico verso la destinazione proverrà dall'indirizzo IP privato del gateway NAT pubblico, a meno che non utilizzi un gateway Internet. Il gateway NAT pubblico utilizzerà il suo EIP come indirizzo IP di origine solo se utilizzato insieme a un gateway Internet.

Indice



## Nozioni di base sul gateway NAT

Ogni gateway NAT viene creato in una zona di disponibilità specifica e implementato con ridondanza in tale zona. Esiste una quota per il numero di gateway NAT che possono essere creati in una zona di disponibilità. Per ulteriori informazioni, consulta Quote Amazon VPC.

Se disponi di risorse in più zone di disponibilità che condividono un gateway NAT e la zona di disponibilità del gateway NAT non è disponibile, le risorse nelle altre zone di disponibilità perdono

l'accesso a Internet. Per migliorare la resilienza, crea un gateway NAT in ogni zona di disponibilità e configura l'instradamento per garantire che le risorse utilizzino il gateway NAT nella stessa zona di disponibilità.

Ai gateway NAT si applicano le seguenti caratteristiche e regole:

- Un gateway NAT supporta i seguenti protocolli: TCP, UDP e ICMP.
- I gateway NAT sono supportati per il traffico IPv4 o IPv6. Per il traffico IPv6, il gateway NAT esegue NAT64. Usandolo insieme a DNS64 (disponibile su Route 53 resolver), i carichi di lavoro IPv6 in una sottorete di Amazon VPC possono comunicare con le risorse IPv4. Questi servizi IPv4 possono essere presenti nello stesso VPC (in una sottorete separata) o in un VPC diverso, nell'ambiente on-premise o su Internet.
- Un gateway NAT supporta 5 Gbps di larghezza di banda e può aumentare automaticamente fino a 100 Gbps. Se è necessaria più larghezza di banda, puoi suddividere le tue risorse in più sottoreti e creare un gateway NAT in ogni sottorete.
- Un gateway NAT può elaborare un milione di pacchetti al secondo e aumentare automaticamente fino a dieci milioni di pacchetti al secondo. Oltre questo limite, un gateway NAT rilascerà i pacchetti. Per evitare la perdita di pacchetti, suddividere le risorse in più sottoreti e creare un gateway NAT separato per ogni sottorete.
- Ogni indirizzo IPv4 può supportare fino a 55.000 connessioni simultanee verso una destinazione univoca. Una destinazione univoca è identificata da una combinazione univoca di indirizzo IP di destinazione, porta di destinazione e protocollo (TCP/UDP/ICMP). Puoi aumentare questo limite associando fino a 8 indirizzi IPv4 ai tuoi gateway NAT (1 indirizzo IPv4 principale e 7 indirizzi IPv4 secondari). Per impostazione predefinita, puoi associare fino a 2 indirizzi IP elastici al tuo gateway NAT pubblico. Puoi aumentare questo limite chiedendo un adeguamento delle quote. Per ulteriori informazioni, consulta Indirizzi IP elastici.
- Puoi scegliere l'indirizzo IPv4 privato da assegnare al gateway NAT oppure assegnarlo automaticamente dall'intervallo di indirizzi IPv4 della sottorete. L'indirizzo IPv4 privato assegnato persiste fino all'eliminazione del gateway NAT privato. Non puoi scollegare l'indirizzo IPv4 privato e non puoi collegare ulteriori indirizzi IPv4 privati.
- Non puoi associare un gruppo di sicurezza a un gateway NAT. Puoi associare i gruppi di sicurezza alle tue istanze per controllare il traffico in entrata e in uscita.
- Puoi utilizzare una lista di controllo degli accessi di rete per controllare il traffico verso e dalla sottorete in cui si trova il gateway NAT. I gateway NAT utilizzano le porte 1024 - 65535. Per ulteriori informazioni, consulta Come controllare il traffico verso le sottoreti utilizzando le liste di controllo degli accessi di rete.

- Un gateway NAT riceve un'interfaccia di rete. Puoi scegliere l'indirizzo IPv4 privato da assegnare all'interfaccia o assegnarlo automaticamente dall'intervallo di indirizzi IPv4 della sottorete. Puoi visualizzare l'interfaccia di rete del gateway NAT nella console Amazon EC2. Per ulteriori informazioni, consulta la sezione relativa alla Visualizzazione dei dettagli relativi a un'interfaccia virtuale. Non puoi modificare gli attributi di questa interfaccia di rete.
- Non è possibile indirizzare il traffico verso un gateway NAT tramite una connessione peering VPC. Non è possibile indirizzare il traffico attraverso un gateway NAT quando il traffico arriva tramite una connessione ibrida (VPN da sito a sito o connessione diretta) tramite un gateway privato virtuale. È possibile instradare il traffico attraverso un gateway NAT quando il traffico arriva tramite una connessione ibrida (VPN da sito a sito o Direct Connect) tramite un gateway di transito.
- I gateway NAT supportano il traffico con un'unità di trasmissione massima (MTU) di 8500, ma è importante tenere presente quanto segue:
  - Per evitare la potenziale perdita di pacchetti durante la comunicazione con le risorse su Internet utilizzando un gateway NAT pubblico, l'impostazione MTU per le istanze EC2 non deve superare i 1500 byte. Per ulteriori informazioni sul controllo e l'impostazione dell'MTU su un'istanza, consulta Verifica e imposta l'MTU sulla tua istanza Linux nella Amazon EC2 User Guide.
  - I gateway NAT supportano Path MTU Discovery (PMTUD) tramite pacchetti ICMPv4 FRAG_NEEDED e pacchetti ICMPv6 Packet Too Big (PTB).
  - I gateway NAT applicano il clamping MSS (Maximum Segment Size) per tutti i pacchetti. Per maggiori informazioni, consulta RFC879.

## Controllo dell'uso dei gateway NAT

Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per utilizzare gateway NAT. Puoi creare un ruolo IAM con una policy collegata che concede agli utenti le autorizzazioni per creare, descrivere ed eliminare gateway NAT. Per ulteriori informazioni, consulta Identity and Access Management per Amazon VPC.

## Utilizzo dei gateway NAT

Puoi utilizzare la console Amazon VPC per creare e gestire i gateway NAT.

Attività

- Creazione di un gateway NAT
- Come modificare le associazioni di indirizzi IP secondari
- Tagging di un gateway NAT

- Eliminazione di un gateway NAT

### Creazione di un gateway NAT

Utilizza la procedura seguente per creare un gateway NAT.

#### Quote correlate

- Non potrai creare un gateway NAT pubblico se hai esaurito il numero di EIP assegnati al tuo account. Per ulteriori informazioni sulle quote EIP e su come modificarle, consulta Indirizzi IP elastici.
- Puoi assegnare fino a 8 indirizzi IPv4 privati al tuo gateway NAT privato. Questo limite non è regolabile.
- Per impostazione predefinita, puoi associare fino a 2 indirizzi IP elastici al tuo gateway NAT pubblico. Puoi aumentare questo limite chiedendo un adeguamento delle quote. Per ulteriori informazioni, consulta Indirizzi IP elastici.

#### Per creare un gateway NAT

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Gateway NAT.
3. Scegli Crea gateway NAT.
4. (Facoltativo) Specifica un nome per il gateway NAT. In questo modo viene creato un tag dove si trova la chiave **`Name`** e il valore è il nome specificato.
5. Seleziona la sottorete in cui creare il gateway NAT.
6. Per Tipo di connettività lascia la selezione Pubblico predefinita per creare un gateway NAT pubblico oppure scegli Privato per creare un gateway NAT privato. Per ulteriori informazioni sulla differenza tra un gateway NAT pubblico e uno privato, consulta Gateway NAT.
7. Se hai scelto Pubblico, procedi come segue; in caso contrario, salta al passaggio 8:

    1. Scegli un ID allocazione indirizzo IP elastico per assegnare un EIP al gateway NAT oppure scegli Alloca IP elastico per allocare automaticamente un EIP per il gateway NAT pubblico. Per impostazione predefinita, puoi associare fino a 2 indirizzi IP elastici al tuo gateway NAT pubblico. Puoi aumentare questo limite chiedendo un adeguamento delle quote. Per ulteriori informazioni, consulta Indirizzi IP elastici.

> **Important**
>
> Quando assegni un EIP a un gateway NAT pubblico, il gruppo di confini di rete dell'EIP deve corrispondere al gruppo di confini di rete della zona di disponibilità (AZ) in cui avvii il gateway NAT pubblico. Se non è lo stesso, non sarà possibile avviare il gateway NAT. Puoi visualizzare il gruppo di confini di rete per la AZ della sottorete visualizzando i dettagli della sottorete. Analogamente, puoi visualizzare il gruppo di confini di rete di un EIP visualizzando i dettagli dell'indirizzo EIP. Per ulteriori informazioni sui gruppi di confine di rete e sugli EIP, consulta Allocare un indirizzo IP elastico.

2. (Facoltativo) Scegli Impostazioni aggiuntive e in Indirizzo IP privato - facoltativo inserisci un indirizzo IPv4 privato per il gateway NAT. Se non inserisci un indirizzo, AWS assegnerà automaticamente un indirizzo IPv4 privato al tuo gateway NAT a caso dalla sottorete in cui si trova il gateway NAT.
3. Passa alla fase 11.

8. Se hai scelto Privato, per Impostazioni aggiuntive e Metodo di assegnazione indirizzo IPv4 privato scegli una delle seguenti opzioni:

   - Assegnazione automatica: AWS sceglie l'indirizzo IPv4 privato principale per il gateway NAT. Per Numero di indirizzi IPv4 privati assegnati automaticamente, puoi facoltativamente specificare il numero di indirizzi IPv4 privati secondari per il gateway NAT. AWS sceglie questi indirizzi IP a caso dalla sottorete per il gateway NAT.
   - Personalizzato: per Indirizzo IPv4 privato primario scegli l'indirizzo IPv4 privato primario per il gateway NAT. Per Indirizzi IPv4 privati secondari, puoi specificare facoltativamente fino a 7 indirizzi IPv4 privati secondari per il gateway NAT.

9. Se nel passaggio 8 hai scelto Personalizzato, ignora questo passaggio. Se hai scelto Assegnazione automatica, in Numero di indirizzi IP privati assegnati automaticamente, scegli il numero di indirizzi IPv4 secondari che desideri AWS assegnare a questo gateway NAT privato. Puoi scegliere fino a 7 indirizzi IPv4.

> **Note**
>
> Gli indirizzi IPv4 secondari sono facoltativi e devono essere assegnati o allocati quando i carichi di lavoro che utilizzano un gateway NAT superano 55.000 connessioni simultanee a una singola destinazione (stessi IP di destinazione, porta di destinazione e protocollo).

Gli indirizzi IPv4 secondari incrementano il numero di porte disponibili e, di conseguenza, la quantità massima di connessioni simultanee che i carichi di lavoro possono stabilire utilizzando un gateway NAT.

10. Se nel passaggio 9 hai scelto Assegnazione automatica, ignora questo passaggio. Se hai scelto Personalizzato, procedi come segue:
    1. In Indirizzo IPv4 privato primario inserisci un indirizzo IPv4 privato.
    2. In Indirizzo IPv4 privato secondario inserisci fino a 7 indirizzi IPv4 privati secondari.
11. (Facoltativo) Per aggiungere un tag al gateway NAT, scegli Add new tag (Aggiungi nuovo tag) e immetti la chiave e il valore del tag. Puoi aggiungere fino a 50 tag.
12. Scegli Crea un gateway NAT.
13. Lo stato iniziale del gateway NAT è `Pending`. Dopo che lo stato viene modificato in `Available`, il gateway NAT è pronto per l'utilizzo. Assicurati di aggiornare le tabelle di instradamento secondo necessità. Per alcuni esempi, consulta the section called “Casi d'uso”.

Se lo stato del gateway NAT cambia in `Failed`, significa che durante la creazione si è verificato un errore. Per ulteriori informazioni, consulta Creazione gateway NAT non riuscita.

Come modificare le associazioni di indirizzi IP secondari

Ogni indirizzo IPv4 può supportare fino a 55.000 connessioni simultanee a una destinazione univoca. Una destinazione univoca è identificata da una combinazione univoca di indirizzo IP di destinazione, porta di destinazione e protocollo (TCP/UDP/ICMP). Puoi aumentare questo limite associando fino a 8 indirizzi IPv4 ai tuoi gateway NAT (1 indirizzo IPv4 principale e 7 indirizzi IPv4 secondari). Per impostazione predefinita, puoi associare fino a 2 indirizzi IP elastici al tuo gateway NAT pubblico. Puoi aumentare questo limite chiedendo un adeguamento delle quote. Per ulteriori informazioni, consulta Indirizzi IP elastici.

Puoi utilizzare le CloudWatchmetriche del gateway NAT ErrorPort Allocation and PacketsDrop Count per determinare se il gateway NAT genera errori di allocazione delle porte o sta eliminando pacchetti. Per risolvere questo problema, aggiungi indirizzi IPv4 secondari al tuo gateway NAT.

Considerazioni

- Puoi aggiungere indirizzi IPv4 secondari privati quando crei un gateway NAT privato o dopo aver creato il gateway NAT seguendo la procedura descritta in questa sezione. Puoi aggiungere

indirizzi EIP secondari ai gateway NAT pubblici solo dopo aver creato il gateway NAT seguendo la procedura descritta in questa sezione.

- Al tuo gateway NAT puoi associare fino a 8 indirizzi IPv4 (1 indirizzo IPv4 primario e 7 indirizzi IPv4 secondari). Puoi assegnare fino a 8 indirizzi IPv4 privati al tuo gateway NAT privato. Per impostazione predefinita, puoi associare fino a 2 indirizzi IP elastici al tuo gateway NAT pubblico. Puoi aumentare questo limite chiedendo un adeguamento delle quote. Per ulteriori informazioni, consulta Indirizzi IP elastici.

Come modificare le associazioni di indirizzi IPv4 secondari

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Gateway NAT.
3. Seleziona il gateway NAT di cui modificare le associazioni di indirizzi IPv4 secondari.
4. Scegli Operazioni, quindi scegli Modifica delle associazioni degli indirizzi IP secondari.
5. Se modifichi le associazioni di indirizzi IPv4 secondari di un gateway NAT privato, in Operazione scegli Assegna nuovi indirizzi IPv4 o Annulla assegnazione di indirizzi IPv4 esistenti. Se modifichi le associazioni di indirizzi IPv4 secondari di un gateway NAT pubblico, in Operazione scegli Associa nuovi indirizzi IPv4 o Annulla associazione di indirizzi IPv4 esistenti.
6. Esegui una di queste operazioni:

   - Se hai scelto di assegnare o associare nuovi indirizzi IPv4, procedi come segue:

     1. Questo passaggio è obbligatorio. Devi selezionare un indirizzo IPv4 privato. Scegli il Metodo di assegnazione di un indirizzo IPv4 privato:

        - Assegnazione automatica: sceglie AWS automaticamente un indirizzo IPv4 privato principale e scegli se vuoi assegnare fino a 7 indirizzi IPv4 privati secondari AWS da assegnare al gateway NAT. AWS li sceglie e li assegna automaticamente a caso dalla sottorete in cui si trova il gateway NAT.
        - Personalizzato: scegli l'indirizzo IPv4 privato primario e fino a 7 indirizzi IPv4 privati secondari da assegnare al gateway NAT.

     2. In ID allocazione IP elastico scegli un EIP da aggiungere come indirizzo IPv4 secondario. Questo passaggio è obbligatorio. Devi selezionare un EIP e un indirizzo IPv4 privato. Se per il Metodo di assegnazione di un indirizzo IP privato hai scelto Personalizzato, devi inserire anche un indirizzo IPv4 privato per ogni EIP che aggiungi.

> **Important**
>
> Quando assegni un EIP secondario a un gateway NAT pubblico, il gruppo di confini di rete dell'EIP deve corrispondere al gruppo di confini di rete della zona di disponibilità (AZ) in cui si trova il gateway NAT pubblico. Se non è lo stesso, non sarà possibile assegnare l'EIP. Puoi visualizzare il gruppo di confini di rete per la AZ della sottorete visualizzando i dettagli della sottorete. Analogamente, puoi visualizzare il gruppo di confini di rete di un EIP visualizzando i dettagli dell'indirizzo EIP. Per ulteriori informazioni sui gruppi di confine di rete e sugli EIP, consulta Allocare un indirizzo IP elastico.

Al tuo gateway NAT puoi associare fino a 8 indirizzi IP. Se il gateway NAT è pubblico, gli EIP elastici sono soggetti a un limite di quota predefinito per ogni regione. Per ulteriori informazioni, consulta Indirizzi IP elastici.

- Se hai scelto di annullare l'assegnazione o l'associazione di nuovi indirizzi IPv4, procedi come indicato di seguito:
  1. In Indirizzo IP secondario esistente di cui annullare l'assegnazione, seleziona gli indirizzi IP secondari per cui annullare l'assegnazione.
  2. (Facoltativo) In Durata dello svuotamento della connessione, inserisci il tempo massimo di attesa (in secondi) prima del rilascio forzato degli indirizzi IP se le connessioni sono ancora in corso. Se non inserisci un valore, il valore predefinito è 350 secondi.

7. Seleziona Salvataggio delle modifiche.

Se lo stato del gateway NAT cambia in `Failed`, significa che durante la creazione si è verificato un errore. Per ulteriori informazioni, consulta Creazione gateway NAT non riuscita.

Tagging di un gateway NAT

Puoi contrassegnare il gateway NAT per identificarlo o classificarlo più facilmente in base alle Esigenze dell'organizzazione. Per informazioni sull'utilizzo dei tag, consulta Tagging your Amazon EC2 resources nella Amazon EC2 User Guide.

I tag di allocazione dei costi sono supportati per i gateway NAT. Pertanto, puoi utilizzare i tag anche per organizzare la AWS fattura e rispecchiare la tua struttura dei costi. Per ulteriori informazioni, consulta Utilizzo dei tag per l'allocazione dei costi nella AWS Billing Guida per l'utente. Per ulteriori

informazioni sulla configurazione di un rapporto di allocazione dei costi con tag, consulta il rapporto mensile sull'allocazione dei costi in Informazioni sulla fatturazione AWS dell'account.

Come aggiungere tag a un gateway NAT

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegliere NAT Gateways (Gateway NAT).
3. Seleziona il gateway NAT a cui aggiungere tag e scegli Operazioni. Scegli, quindi, Gestisci tag.
4. Scegli Aggiungi nuovo tag e definisci una Chiave e un Valore per il tag. Puoi aggiungere fino a 50 tag.
5. Selezionare Salva.

Eliminazione di un gateway NAT

Se un gateway NAT non è più necessario, puoi eliminarlo. Dopo aver eliminato un gateway NAT, la relativa voce rimane visibile nella console Amazon VPC per un breve periodo di tempo (in genere un'ora) prima di essere rimossa automaticamente. Non puoi rimuovere questa voce manualmente.

L'eliminazione di un gateway NAT annulla l'associazione al relativo indirizzo IP elastico, ma non rilascia l'indirizzo dall'account. Se Elimini un gateway NAT, le route del gateway NAT rimangono in uno stato `blackhole` finché le route non vengono eliminate o aggiornate.

Per eliminare un gateway NAT

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare NAT Gateways (Gateway NAT).
3. Seleziona il pulsante di opzione per il gateway NAT, quindi scegli Operazioni, Elimina gateway NAT.
4. Quando viene richiesta la conferma, immetti **`delete`** e seleziona Elimina.
5. Se l'indirizzo IP elastico associato al gateway NAT non è più necessario, si consiglia di rilasciarlo. Per ulteriori informazioni, consulta Rilascio di un indirizzo IP elastico.

## Panoramica su API e CLI

Puoi eseguire le attività descritte in questa pagina tramite la riga di comando o l'API. Per ulteriori informazioni sulle interfacce a riga di comando e per un elenco delle operazioni API disponibili, consulta Uso di Amazon VPC.

Come assegnare un indirizzo IPv4 privato a un gateway NAT privato

- assign-private-nat-gateway-address (AWS CLI)
- Register-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)
- AssignPrivateNatGatewayIndirizzo (API di interrogazione Amazon EC2)

Come associare indirizzi IP elastici (EIP) e indirizzi IPv4 privati a un gateway NAT pubblico

- associate-nat-gateway-address (AWS CLI)
- Register-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)
- AssociateNatGatewayAddress(API di interrogazione Amazon EC2)

Creazione di un gateway NAT

- create-nat-gateway (AWS CLI)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)
- CreateNatGateway (API di interrogazione Amazon EC2)

Eliminazione di un gateway NAT

- delete-nat-gateway (AWS CLI)
- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)
- DeleteNatGateway (API di interrogazione Amazon EC2)

Descrizione di un gateway NAT

- describe-nat-gateways (AWS CLI)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)
- DescribeNatGateway (API di interrogazione Amazon EC2)

Come annullare l'associazione di indirizzi IP elastici (EIP) secondari da un gateway NAT pubblico

- disassociate-nat-gateway-address (AWS CLI)
- Unregister-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

- DisassociateNatGatewayAddress(API di interrogazione Amazon EC2)

Tagging di un gateway NAT

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)
- CreateTags(API di interrogazione Amazon EC2)

Come annullare l'assegnazione di indirizzi IPv4 secondari da un gateway NAT privato

- unassign-private-nat-gateway-address (AWS CLI)
- Unregister-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)
- UnassignPrivateNatGatewayIndirizzo (API di interrogazione Amazon EC2)

## Casi d'uso di API Gateway

Di seguito sono riportati casi di utilizzo di esempio per gateway NAT pubblici e privati.

Scenari

- Accesso a Internet da una sottorete privata
- Accedere alla rete utilizzando gli indirizzi IP consentiti riportati
- Abilitare la comunicazione tra reti sovrapposte

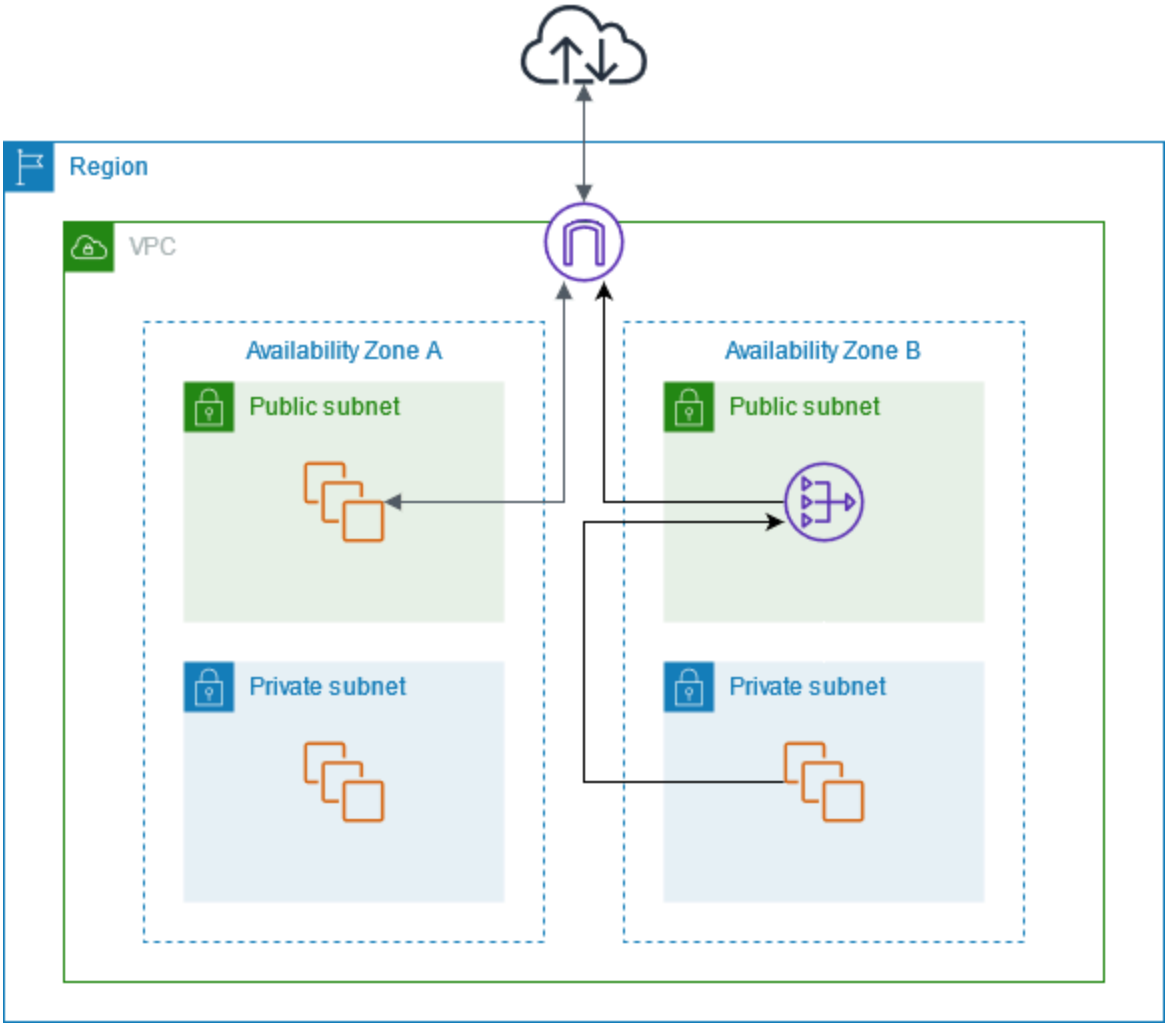
Accesso a Internet da una sottorete privata

È possibile utilizzare un gateway NAT pubblico per consentire alle istanze in una sottorete privata di inviare il traffico in uscita a Internet, e, allo stesso tempo, impedire a Internet di stabilire connessioni alle istanze.

Indice

## Panoramica

Il diagramma seguente illustra questo caso d'uso. Ci sono due zone di disponibilità, con due sottoreti in ciascuna di esse. La tabella di instradamento per ogni sottorete determina il modo in cui viene instradato il traffico. Nella zona di disponibilità A, le istanze nella sottorete pubblica possono connettersi a Internet attraverso un routing al gateway Internet, mentre le istanze nella sottorete privata non possiedono alcun routing verso Internet. Nella zona di disponibilità B, la sottorete pubblica contiene un gateway NAT. Le istanze nella sottorete privata possono raggiungere Internet attraverso un routing che le conduce al gateway NAT nella sottorete pubblica. I gateway NAT sia privati sia pubblici associano l'indirizzo IPv4 privato di origine delle istanze all'indirizzo IPv4 privato del gateway NAT privato, tuttavia nel caso di un gateway NAT pubblico, il gateway Internet associa l'indirizzo IPv4 privato del gateway NAT pubblico all'indirizzo IP elastico associato al gateway NAT. Quando invia traffico di risposta alle istanze, il gateway NAT converte l'indirizzo nell'indirizzo IP iniziale dell'origine, a prescindere dal fatto che il gateway NAT sia pubblico o privato.



Tieni presente che se le istanze nella sottorete privata nella zona di disponibilità A devono raggiungere anche Internet, puoi creare un percorso da questa sottorete al gateway NAT nella zona di disponibilità B. In alternativa, puoi migliorare la resilienza creando un gateway NAT in ogni zona di disponibilità contenente le risorse che richiedono l'accesso a Internet. Per un diagramma di esempio, consulta la pagina the section called “Server privati”.

Routing

Di seguito è riportata la tabella di instradamento associata alla sottorete pubblica nella zona di disponibilità A. La prima voce si riferisce al routing locale, che consente alle istanze nella sottorete di comunicare con altre istanze nel VPC utilizzando indirizzi IP privati. La seconda voce invia tutto il traffico rimanente della sottorete al gateway Internet. In questo modo le istanze della sottorete possono accedere a Internet.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | locale |
| 0.0.0.0/0 | *internet-gateway-id* |

Di seguito è riportata la tabella di instradamento associata alla sottorete privata nella zona di disponibilità A. La voce è la route locale, che consente alle istanze nella sottorete di comunicare con altre istanze nel VPC utilizzando gli indirizzi IP privati. Le istanze in questa sottorete non hanno accesso a Internet.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | local |

Di seguito è riportata la tabella di instradamento associata alla sottorete pubblica nella zona di disponibilità B. La prima voce si riferisce alla route locale, che consente alle istanze nella sottorete di comunicare tra loro nel VPC utilizzando indirizzi IP privati. La seconda voce invia tutto il traffico rimanente della sottorete al gateway Internet. In questo modo il gateway NAT può accedere a Internet.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | locale |
| 0.0.0.0/0 | *internet-gateway-id* |

Di seguito è riportata la tabella di instradamento associata alla sottorete privata nella zona di disponibilità B. La prima voce è quella predefinita per il routing locale, che consente alle istanze nella sottorete di comunicare tra loro nel VPC utilizzando indirizzi IP privati. La seconda voce invia tutto il traffico rimanente della sottorete al gateway NAT.

| Destinazione | Target |
| --- | --- |
| *CIDR VPC* | locale |
| 0.0.0.0/0 | *nat-gateway-id* |

Per ulteriori informazioni, consulta the section called “Utilizzo delle tabelle di routing”.

Test del gateway NAT pubblico

Dopo aver creato il gateway NAT e aggiornato le tabelle di routing, puoi eseguire il ping di alcuni indirizzi remoti su Internet da un'istanza nella sottorete privata per verificare se può connettersi a Internet. Per un esempio su come Eseguire questa operazione, consulta Test della connessione Internet.

Se è disponibile una connessione a Internet, puoi anche verificare se il traffico Internet viene instradato attraverso il gateway NAT:

- Puoi monitorare il routing del traffico da un'istanza nella sottorete privata. A questo scopo, esegui il comando `traceroute` da un'istanza Linux nella sottorete privata. Nell'output, l'indirizzo IP privato del gateway NAT dovrebbe essere visibile in uno degli hop (di solito il primo).
- Quando esegui la connessione da un'istanza nella sottorete privata, utilizza un sito Web o uno strumento di terze parti che visualizza l'indirizzo IP di origine. L'indirizzo IP di origine deve essere l'indirizzo IP elastico del gateway NAT.

Se questi test non vanno a buon fine, consulta Risoluzione dei problemi relativi ai gateway NAT.

Test della connessione Internet

Nell'esempio seguente viene illustrato come eseguire il test se un'istanza in una sottorete privata può connettersi a Internet.

1. Avvia un'istanza nella sottorete pubblica (utilizzala come un host bastione). Nella procedura guidata di avvio, assicurati di selezionare un'AMI Amazon Linux e assegna un indirizzo IP pubblico all'istanza. Verifica che le regole del gruppo di sicurezza consentano il traffico SSH in entrata da un intervallo di indirizzi IP per la rete locale SSH in uscita all'intervallo di indirizzi IP della sottorete privata (puoi anche utilizzare `0.0.0.0/0` per il traffico SSH in entrata e in uscita di questo test)..
2. Avvia un'istanza nella sottorete privata. Nella procedura guidata di avvio, assicurati di selezionare un'AMI Amazon Linux. Non assegnare un indirizzo IP pubblico all'istanza. Verifica che le regole del gruppo di sicurezza consentano il traffico SSH in entrata dall'indirizzo IP privato all'istanza avviata nella sottorete pubblica e tutto il traffico ICMP in uscita. Devi scegliere la coppia di chiavi utilizzata per avviare l'istanza nella sottorete pubblica.
3. Configura l'inoltro agente SSH sul computer locale ed esegui la connessione all'host bastione nella sottorete pubblica. Per ulteriori informazioni, consulta Per configurare l'inoltro agente SSH per Linux o macOS o Per configurare l'inoltro agente SSH per Windows.
4. Dall'host bastione, esegui la connessione all'istanza nella sottorete privata, quindi esegui il test della connessione Internet dall'istanza nella sottorete privata. Per ulteriori informazioni, consulta Per eseguire il test della connessione Internet.

Per configurare l'inoltro agente SSH per Linux o macOS

1. Dal computer locale, aggiungere la chiave privata all'agente di autenticazione.

   Per Linux, utilizzare il comando seguente:

   ```
   ssh-add -c mykeypair.pem
   ```

   Per macOS, utilizzare il comando seguente:

   ```
   ssh-add -K mykeypair.pem
   ```
2. Eseguire la connessione all'istanza nella sottorete pubblica utilizzando l'opzione `-A` per abilitare l'inoltro agente SSH e utilizzare l'indirizzo pubblico dell'istanza, come indicato nell'esempio seguente.

```
ssh -A ec2-user@54.0.0.123
```

Per configurare l'inoltro agente SSH per Windows

È possibile utilizzare il client OpenSSH, disponibile in Windows, o installare il client SSH preferito (ad esempio PuTTY).

OpenSSH

Installa OpenSSH per Windows come descritto in questo articolo: Guida introduttiva a OpenSSH per Windows. Quindi aggiungi la tua chiave all'agente di autenticazione. Per ulteriori informazioni, consulta Autenticazione basata su chiavi in OpenSSH per Windows.

PuTTY

1. Scaricare e installare Pageant dalla pagina di download PuTTY, se non è già installato.
2. Convertire la chiave privata in formato .ppk. Per ulteriori informazioni, consulta Conversione della chiave privata utilizzando PuTTYgen nella Guida per l'utente di Amazon EC2.
3. Avviare Pageant, fare clic con il tasto destro del mouse del mouse sull'icona Pageant nella barra delle applicazioni (potrebbe Essere nascosta), quindi selezionare Add Key (Aggiungi chiave). Selezionare il file .ppk creato, digitare la passphrase se necessario e scegliere Open (Apri).
4. Avviare una sessione PuTTY e connettersi all'istanza nella sottorete pubblica utilizzando il suo indirizzo IP pubblico. Per ulteriori informazioni, consulta Connessione all'istanza Linux. Nella categoria Auth, accertarsi di selezionare l'opzione Allow agent forwarding (Consenti inoltro agente) e lasciare vuota la casella Private key file for authentication (File chiave privata per autenticazione).

Per eseguire il test della connessione Internet

1. Dall'istanza nella sottorete pubblica, connettersi all'istanza nella sottorete privata utilizzando il relativo indirizzo IP privato, come indicato nell'esempio seguente.

```
ssh ec2-user@10.0.1.123
```

2. Dall'istanza privata, verificare che sia possibile connettersi a Internet eseguendo il comando `ping` per un sito Web con ICMP abilitato.

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=47 time=86.0 ms
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=47 time=75.6 ms
...
```

Premere Ctrl+C sulla tastiera per annullare il comando `ping`. Se il comando `ping` non riesce, consulta Le istanze non possono accedere a Internet.

3. (Facoltativo) Se le istanze non sono più richieste, terminarle. Per ulteriori informazioni, consulta la sezione relativa alla terminazione dell'istanza nella Guida per l'utente di Amazon EC2.

## Accedere alla rete utilizzando gli indirizzi IP consentiti riportati

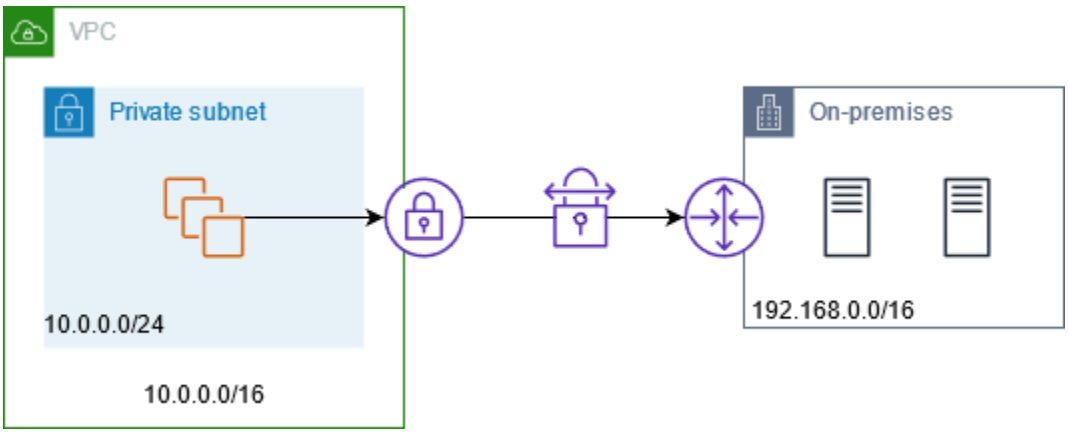
È possibile utilizzare un gateway NAT privato per abilitare la comunicazione dai VPC alla rete locale utilizzando un pool di indirizzi consentiti. Anziché assegnare a ciascuna istanza un indirizzo IP indipendente dall'intervallo di indirizzi IP consentito, è possibile instradare il traffico dalla sottorete destinata alla rete locale attraverso un gateway NAT privato con un indirizzo IP dall'intervallo di indirizzi IP consentito.

Indice

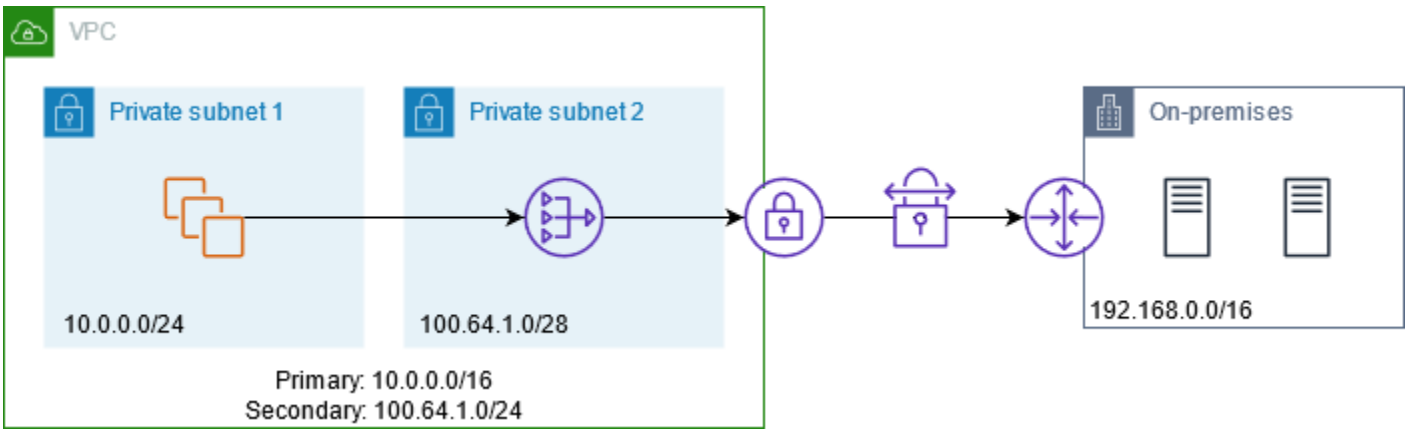


### Panoramica

Il diagramma seguente mostra come le istanze possono accedere alle risorse locali tramite. AWS VPN Il traffico proveniente dalle istanze viene instradato verso un gateway virtuale privato, tramite la connessione VPN, al gateway del cliente e quindi alla destinazione nella rete locale. Tuttavia, supponiamo che la destinazione consenta il traffico solo da un intervallo di indirizzi IP specifico, ad esempio 100.64.1.0/28. Ciò impedirebbe al traffico proveniente da queste istanze di raggiungere la rete locale.




Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. Il VPC ha il proprio intervallo di indirizzi IP originale e l'intervallo di indirizzi IP consentito. Il VPC ha una sottorete dall'intervallo di indirizzi IP consentito con un gateway NAT privato. Il traffico proveniente dalle istanze destinate alla rete locale viene inviato al gateway NAT prima di essere instradato alla connessione VPN. La rete in locale riceve il traffico dalle istanze con l'indirizzo IP di origine del gateway NAT, che proviene dall'intervallo di indirizzi IP consentito.




Risorse

Creare o aggiornare le risorse come di seguito:

- Associare l'intervallo di indirizzi IP consentito al VPC.
- Creare una sottorete nel VPC dall'intervallo di indirizzi IP consentito.
- Creare un gateway NAT privato nella nuova sottorete.
- Aggiornare la tabella di instradamento per la sottorete con le istanze per inviare il traffico destinato alla rete locale al gateway NAT. Aggiungere una route alla tabella di instradamento per la sottorete con il gateway NAT privato che invia il traffico destinato alla rete locale al gateway virtuale privato.

Routing

Di seguito è riportata la tabella di instradamento associata alla prima sottorete. Esiste un routing locale per ciascun CIDR VPC. Le route locali consentono alle risorse nella sottorete di comunicare con altre risorse nel VPC tramite gli indirizzi IP privati. La terza voce invia il traffico destinato alla rete locale al gateway NAT privato.

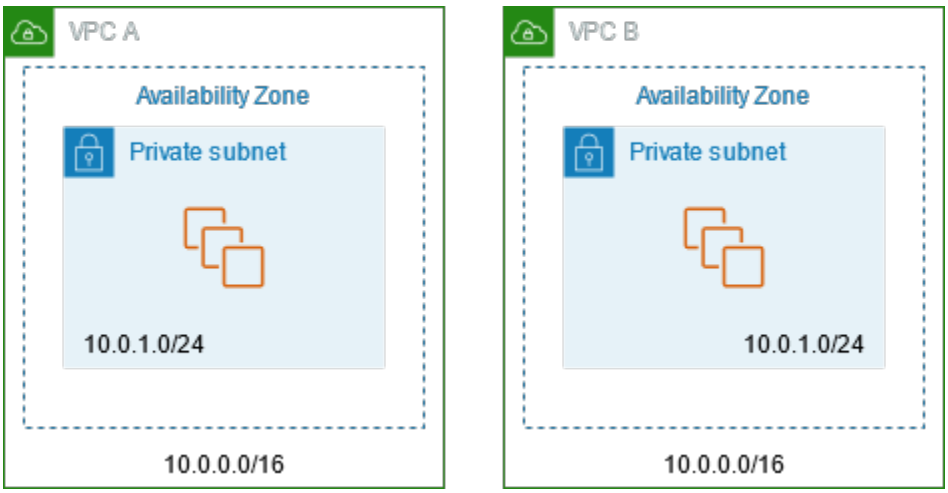
| Destinazione | Target |
| --- | --- |
| *10.0.0.0/16* | locale |
| *100,64,1,0/24* | local |
| *192.168.0.0/16* | *nat-gateway-id* |

Di seguito è riportata la tabella di instradamento associata alla seconda sottorete. Esiste un routing locale per ciascun CIDR VPC. Le route locali consentono alle risorse nella sottorete di comunicare con altre risorse nel VPC tramite gli indirizzi IP privati. La terza voce invia il traffico destinato alla rete locale al gateway virtuale privato.

| Destinazione | Target |
| --- | --- |
| *10,0,0/16* | locale |
| *100,64,1,0/24* | local |
| *192.168.0.0/16* | *vgw-id* |

Abilitare la comunicazione tra reti sovrapposte

È possibile utilizzare un gateway NAT privato per abilitare la comunicazione tra le reti anche se hanno intervalli CIDR sovrapposti. Ad esempio, supponiamo che le istanze in VPC A debbano accedere ai servizi forniti dalle istanze in VPC B.




Indice



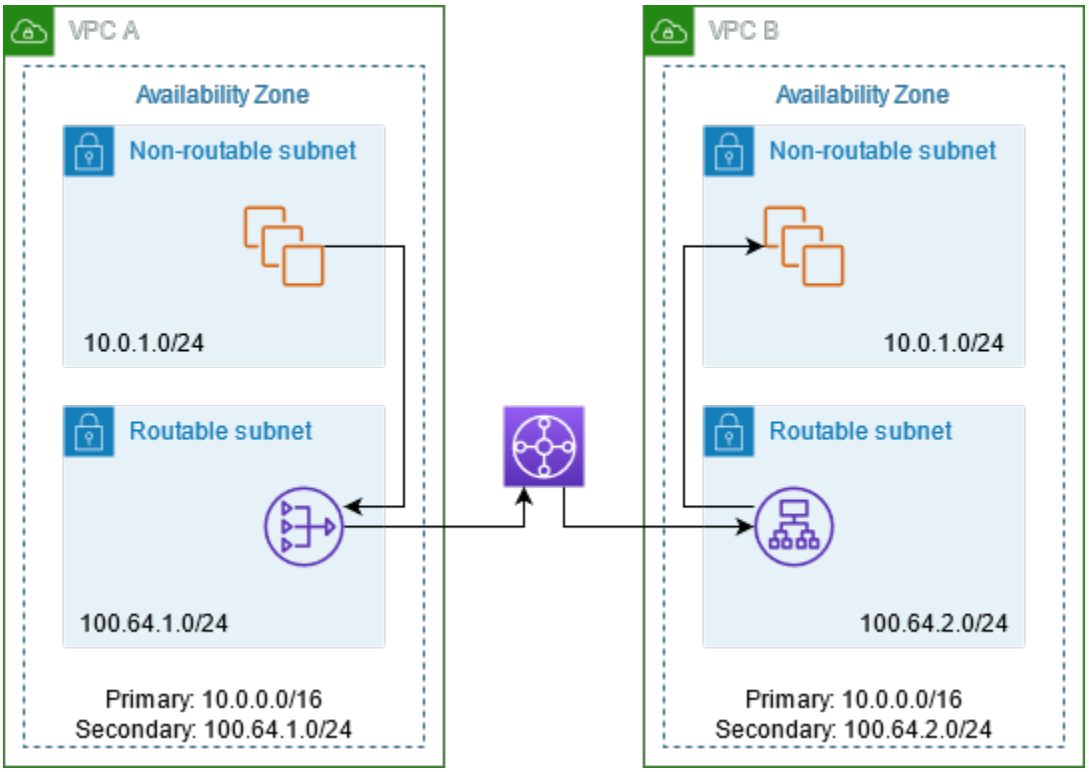
## Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. Innanzitutto, il team di gestione IP determina quali intervalli di indirizzi possono sovrapporsi (intervalli di indirizzi non instradabili) e quali no (intervalli di indirizzi instradabili). Il team di gestione IP assegna intervalli di indirizzi dal pool di intervalli di indirizzi instradabili ai progetti su richiesta.

Ogni VPC ha il suo intervallo di indirizzi IP originale, che non è instradabile, oltre all'intervallo di indirizzi IP instradabili assegnato dal team di gestione IP. VPC A ha una sottorete dal suo intervallo instradabile con un gateway NAT privato. Il gateway NAT privato ottiene il suo indirizzo IP dalla sottorete. VPC B ha una sottorete dal suo intervallo instradabile tramite Application Load Balancer. Application Load Balancer ottiene gli indirizzi IP dalle sottoreti.

Il traffico proveniente da un'istanza nella sottorete non instradabile del VPC A destinata alle istanze nella sottorete non instradabile di VPC B viene inviato attraverso il gateway NAT privato e quindi instradato al gateway di transito. Il gateway di transito invia il traffico all'Application Load Balancer, che instrada il traffico verso una delle istanze di destinazione nella sottorete non instradabile di VPC B. Il traffico dal gateway di transito al sistema di bilanciamento del carico dell'applicazione ha l'indirizzo IP di origine del gateway NAT privato. Pertanto, il traffico di risposta proveniente dal load balancer utilizza l'indirizzo del gateway NAT privato come destinazione. Il traffico di risposta viene

inviato al gateway di transito e quindi instradato al gateway NAT privato, che converte la destinazione nell'istanza nella sottorete non instradabile di VPC A.




Risorse

Creare o aggiornare risorse nel modo seguente:

- Associare gli intervalli di indirizzi IP instradabili assegnati ai rispettivi VPC.
- Creare una sottorete in VPC A dal suo intervallo di indirizzi IP instradabili e creare un gateway NAT privato in questa nuova sottorete.
- Creare una sottorete in VPC B dall'intervallo di indirizzi IP instradabili e creare un Application Load Balancer in questa nuova sottorete. Registrare le istanze nella sottorete non instradabile con il gruppo di destinazione per il load balancer.
- Creare un gateway di transito per connettere i VPC. Accertarsi di disabilitare la propagazione di route. Quando si connette ciascun VPC al gateway di transito, utilizzare l'intervallo di indirizzi instradabili del VPC.
- Aggiornare la tabella di instradamento della sottorete non instradabile in VPC A per inviare tutto il traffico destinato all'intervallo di indirizzi instradabili di VPC B al gateway NAT privato. Aggiornare la tabella di instradamento della sottorete instradabile in VPC A per inviare tutto il traffico destinato all'intervallo di indirizzi instradabili del VPC B al gateway di transito.

- Aggiornare la tabella di instradamento della sottorete instradabile in VPC B per inviare tutto il traffico destinato all'intervallo di indirizzi instradabili del VPC A al gateway di transito.

Routing

La seguente è la tabella di instradamento per la sottorete non instradabile nel VPC A.

| Destinazione | Target |
| --- | --- |
| *10,0,0/16* | locale |
| *100,64,1,0/24* | local |
| *100,64,2,0/24* | *nat-gateway-id* |

La seguente è la tabella di instradamento per la sottorete instradabile nel VPC A.

| Destinazione | Target |
| --- | --- |
| *10,0,0/16* | locale |
| *100,64,1,0/24* | local |
| *100,64,2,0/24* | *transit-gateway-id* |

La seguente è la tabella di instradamento per la sottorete non instradabile nel VPC B.

| Destinazione | Target |
| --- | --- |
| *10,0,0/16* | locale |
| *100,64,2,0/24* | local |

La seguente è la tabella di instradamento per la sottorete instradabile nel VPC B.

| Destinazione | Target |
| --- | --- |
| *10,0,0/16* | locale |
| *100,64,2,0/24* | local |
| *100,64,1,0/24* | *transit-gateway-id* |

Di seguito è riportata la tabella di instradamento del gateway di transito.

| CIDR | Collegamento | Tipo di routing |
| --- | --- | --- |
| *100,64,1,0/24* | *Collegamento per VPC A* | Statico |
| *100,64,2,0/24* | *Collegamento per VPC B* | Statico |

## DNS64 e NAT64

Un gateway NAT supporta la traduzione degli indirizzi di rete da IPv6 a IPv4, comunemente nota come NAT64. NAT64 aiuta le risorse IPv6 a comunicare con AWS le risorse IPv4 nello stesso VPC o in un VPC diverso, nella rete locale o su Internet. È possibile utilizzare NAT64 con DNS64 sul risolutore Amazon Route 53 o utilizzare il proprio server DNS64.

Indice



### Che cos'è DNS64?

I carichi di lavoro solo IPv6 in esecuzione su VPC possono inviare e ricevere solo pacchetti di rete IPv6. Senza DNS64, una query DNS per un servizio solo IPv4 restituirà un indirizzo di destinazione IPv4 in risposta e il servizio solo IPv6 non può comunicare con esso. Per colmare questa lacuna di comunicazione, è possibile abilitare il DNS64 per una sottorete e si applica a tutte le risorse all'interno di quella sottorete. AWS Con DNS64, il risolutore Amazon Route 53 cerca il registro DNS per il servizio richiesto ed effettua una delle seguenti operazioni:

- Se il registro contiene un indirizzo IPv6, restituisce il registro originale e la connessione viene stabilita senza alcuna traduzione su IPv6.
- Se non è presente un indirizzo IPv6 associato alla destinazione nel record DNS, il Route 53 Resolver ne sintetizza uno prependendo il noto prefisso `/96`, definito in RFC6052 (`64:ff9b::/96`), all'indirizzo IPv4 nel registro. Il servizio solo IPv6 invia pacchetti di rete all'indirizzo IPv6 sintetizzato. Sarà quindi necessario instradare questo traffico attraverso il gateway NAT, che esegue la traduzione necessaria sul traffico per consentire ai servizi IPv6 della sottorete di accedere ai servizi IPv4 al di fuori di tale sottorete.

È possibile abilitare o disabilitare DNS64 su una sottorete utilizzando l'attributo modify-subnet utilizzando la AWS CLI o con la console VPC selezionando una sottorete e scegliendo Azioni > Modifica impostazioni sottorete.

Che cos'è NAT64?

NAT64 consente ai servizi solo IPv6 in Amazon VPC di comunicare con i servizi solo IPv4 all'interno dello stesso VPC (in sottoreti diverse) o dei VPC connessi, nelle reti on-premise o su Internet.

NAT64 è automaticamente disponibile sui gateway NAT esistenti o su tutti i nuovi gateway NAT creati. Non è possibile abilitare o disabilitare questa funzionalità. La sottorete in cui si trova il gateway NAT non deve essere necessariamente una sottorete dual-stack per il funzionamento di NAT64.

Dopo aver abilitato DNS64, se il servizio solo IPv6 invia pacchetti di rete a un indirizzo IPv6 sintetizzato tramite il gateway NAT, si verifica quanto segue:

- Dal prefisso `64:ff9b::/96`, il gateway NAT riconosce che la destinazione originale è IPv4 e traduce i pacchetti IPv6 in IPv4 sostituendo:
  - L'origine IPv6 con un proprio IP privato che viene tradotto in un indirizzo IP elastico dal Gateway Internet.
  - La destinazione da IPv6 a IPv4 troncando il prefisso `64:ff9b::/96`.
- Il gateway NAT invia i pacchetti IPv4 tradotti alla destinazione attraverso il gateway Internet, il gateway privato virtuale o il gateway di transito e avvia una connessione.
- L'host solo IPv4 invia i pacchetti di risposta IPv4. Una volta stabilita una connessione, il gateway NAT accetta i pacchetti IPv4 di risposta dagli host esterni.
- I pacchetti IPv4 di risposta sono destinati al gateway NAT, che riceve i pacchetti e li decodifica sostituendo il suo IP (IP di destinazione) con l'indirizzo IPv6 dell'host e anteponendo

64:ff9b::/96 all'indirizzo IPv4 di origine. Il pacchetto quindi scorre verso l'host seguendo il routing locale.

In tal modo, il gateway NAT consente ai carichi di lavoro solo IPv6 in una sottorete di comunicare con i servizi solo IPv4 all'esterno della sottorete.

Configurazione di DNS64 e NAT64

Segui i passaggi descritti in questa sezione per configurare DNS64 e NAT64 per abilitare la comunicazione con i servizi solo IPv4.

Indice



Abilitare la comunicazione con i servizi solo IPv4 su internet con CLI di AWS

Se si dispone di una sottorete con carichi di lavoro solo IPv6 che deve comunicare con servizi solo IPv4 al di fuori della sottorete, in questo esempio viene illustrato come abilitare questi servizi solo IPv6 per comunicare con i servizi solo IPv4 su internet.

È innanzitutto necessario configurare un gateway NAT in una sottorete pubblica (separata dalla sottorete contenente i carichi di lavoro solo IPv6). Ad esempio, la sottorete contenente il gateway NAT deve avere un percorso che punti al gateway Internet. 0.0.0.0/0

Completare questi passaggi per consentire a questi servizi solo IPv6 di connettersi ai servizi solo IPv4 su Internet:

1. Aggiungere i seguenti tre percorsi alla tabella dei percorsi della sottorete contenente i carichi di lavoro solo IPv6:
   - Routing IPv4 (se presente) che punta al gateway NAT.
   - Routing 64:ff9b::/96 che punta al gateway NAT. Ciò consentirà di instradare il traffico proveniente dai carichi di lavoro solo IPv6 destinati ai servizi solo IPv4 attraverso il gateway NAT.
   - Routing ::/0 IPv6 che punta al gateway Internet egress-only (o al gateway Internet).

Nota: `::/0` al gateway Internet consentirà agli host IPv6 esterni (al di fuori del VPC) di avviare la connessione tramite IPv6.

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-cidr-block
0.0.0.0/0 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
64:ff9b::/96 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
::/0 --egress-only-internet-gateway-id eigw-c0a643a9
```

2. Abilitare la funzionalità DNS64 nella sottorete contenente i carichi di lavoro solo IPv6.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --enable-dns64
```

Ora, le risorse nella sottorete privata possono stabilire connessioni con stato con i servizi IPv4 e IPv6 su Internet. Configurare il gruppo di sicurezza e i NACL in modo appropriato per consentire l'uscita e l'ingresso del traffico verso il traffico `64:ff9b::/96`.

Abilitare la comunicazione con i servizi IPv4 nell'ambiente on premise

Il risolutore Amazon Route 53 consente di inoltrare le query DNS dal VPC a una rete on-premise e viceversa. Si può fare eseguendo le seguenti operazioni:

- Creare un endpoint Route 53 Resolver in uscita in un VPC e assegnargli gli indirizzi IPv4 da cui si desidera inoltrare le query da Route 53 Resolver. Per il resolver DNS on-premise, questi sono gli indirizzi IP da cui hanno origine le query DNS e, pertanto, devono essere indirizzi IPv4.
- Creare una o più regole che specificano i nomi di dominio delle query DNS che si vuole vengano inoltrate dal Route 53 Resolver ai resolver on-premise. Specificare anche gli indirizzi IPv4 dei resolver on-premise.
- Dopo aver configurato un endpoint in uscita di Route 53 Resolver, è necessario abilitare DNS64 sulla sottorete contenente i carichi di lavoro solo IPv6 e instradare tutti i dati destinati alla rete locale tramite un gateway NAT.

Come funziona DNS64 per le destinazioni solo IPv4 nelle reti on-premise:

1. Assegnare un indirizzo IPv4 all'endpoint in uscita Route 53 Resolver nel VPC.
2. La query DNS del servizio IPv6 va a Route 53 Resolver su IPv6. Route 53 Resolver corrisponde alla query con la regola di inoltro e ottiene un indirizzo IPv4 per il resolver on-premise.
3. Route 53 Resolver converte il pacchetto di query da IPv6 in IPv4 e lo inoltra all'endpoint in uscita. Ogni indirizzo IP dell'endpoint rappresenta un ENI che inoltra la richiesta all'indirizzo IPv4 on-premise del resolver DNS.
4. Il resolver on-premise invia nuovamente il pacchetto di risposta su IPv4 attraverso l'endpoint in uscita a Route 53 Resolver.
5. Supponendo che la query sia stata effettuata da una sottorete abilitata per DNS64, Route 53 Resolver fa due cose:

    a. Controlla il contenuto del pacchetto di risposta. Se nel registro è presente un indirizzo IPv6, mantiene il contenuto così com'è, ma se contiene solo un registro IPv4. Sintetizza anche un registro IPv6 anteponendo `64:ff9b::/96` all'indirizzo IPv4.

    b. Ricompila il contenuto e lo invia al servizio nel tuo VPC tramite IPv6.

## Monitora i gateway NAT con Amazon CloudWatch

Puoi monitorare il tuo gateway NAT utilizzando CloudWatch, che raccoglie informazioni dal gateway NAT e crea metriche leggibili quasi in tempo reale. Puoi utilizzare questa informazioni per monitorare E risolvere i problemi relativi al gateway NAT. I dati dei parametri del gateway NAT sono forniti ogni minuto e le statistiche sono registrate per un periodo di 15 mesi.

Per ulteriori informazioni su Amazon CloudWatch, consulta la Amazon CloudWatch User Guide. Per ulteriori informazioni sui prezzi, consulta la pagina CloudWatch dei prezzi di Amazon.

Parametri e dimensioni del gateway NAT

I seguenti parametri sono disponibili per i gateway NAT. La colonna Descrizione include una descrizione di ciascun parametro, unità e statistica.

| Parametro | Descrizione |
| --- | --- |
| `ActiveConnectionCount` | Il numero totale delle connessioni simultanee TCP attive attraverso il gateway NAT. |

| Parametro | Descrizione |
| --- | --- |
| | Un valore pari a zero indica che non ci sono connessioni attive attraverso il gateway NAT.<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è `Max`. |
| `BytesInFromDestination` | Il numero di byte ricevuti dal gateway NAT e provenienti dalla destinazione.<br><br>Se il valore per `BytesOutToSource` è inferiore al valore per `BytesInFromDestination`, vi potrebbe essere una perdita di dati durante l'esecuzione del gateway NAT o il traffico potrebbe essere attivamente bloccato dal gateway NAT.<br><br>Unità: byte<br><br>Statistiche: la statistica più utile è `Sum`. |
| `BytesInFromSource` | Il numero di byte ricevuti dal gateway NAT e provenienti dai clienti nel tuo VPC.<br><br>Se il valore per `BytesOutToDestination` è inferiore al valore per `BytesInFromSource`, vi potrebbe essere una perdita di dati durante l'esecuzione del gateway NAT.<br><br>Unità: byte<br><br>Statistiche: la statistica più utile è `Sum`. |

| Parametro | Descrizione |
| --- | --- |
| `BytesOutToDestination` | Il numero di byte inviati per mezzo del gateway NAT verso la destinazione.<br><br>Un valore superiore a zero indica che vi è un traffico verso la rete dai clienti che sono dietro il gateway NAT. Se il valore per `BytesOutToDestination` è inferiore al valore per `BytesInFromSource`, vi potrebbe essere una perdita di dati durante l'esecuzione del gateway NAT.<br><br>Unità: byte<br><br>Statistiche: la statistica più utile è `Sum`. |
| `BytesOutToSource` | Il numero di byte inviati per mezzo del gateway NAT verso i clienti nel tuo VPC.<br><br>Un valore superiore a zero indica che vi è un traffico proveniente dalla rete verso i clienti che sono dietro il gateway NAT. Se il valore per `BytesOutToSource` è inferiore al valore per `BytesInFromDestination`, vi potrebbe essere una perdita di dati durante l'esecuzione del gateway NAT o il traffico potrebbe essere attivamente bloccato dal gateway NAT.<br><br>Unità: byte<br><br>Statistiche: la statistica più utile è `Sum`. |

| Parametro | Descrizione |
| --- | --- |
| `ConnectionAttemptCount` | In numero di tentativi di connessione attraverso il gateway NAT.<br><br>Se il valore per `ConnectionEstablishedCount` è inferiore del valore per `ConnectionAttemptCount`, ciò indica che i clienti dietro il gateway NAT hanno tentato di stabilire nuove connessioni per le quali non vi era risposta.<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è `Sum`. |
| `ConnectionEstablishedCount` | In numero di connessioni stabilite attraverso il gateway NAT.<br><br>Se il valore per `ConnectionEstablishedCount` è inferiore del valore per `ConnectionAttemptCount`, ciò indica che i clienti dietro il gateway NAT hanno tentato di stabilire nuove connessioni per le quali non vi era risposta.<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è `Sum`. |
| `ErrorPortAllocation` | Il numero di volte che il gateway NAT potrebbe non allocare una porta di origine.<br><br>Un valore superiore a zero indica che sono aperte troppe connessioni simultanee sono attraverso il gateway NAT.<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è `Sum`. |

| Parametro | Descrizione |
| --- | --- |
| `IdleTimeoutCount` | Numero di connessioni che sono transitat e dallo stato attivo a quello inattivo. Una connessione attiva passa allo stato inattivo se non è stata correttamente chiusa e se non c'è stata attività negli ultimi 350 secondi.<br><br>Un valore superiore a zero indica che vi sono connessioni che sono state spostate a uno stato inattivo. Se il valore per `IdleTimeo utCount` aumenta, ciò potrebbe indicare che i clienti dietro al gateway NAT stanno usando connessioni obsolete.<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è `Sum`. |
| `PacketsDropCount` | Il numero di pacchetti consegnati dal gateway NAT.<br><br>Per calcolare il numero di pacchetti persi come percentuale del traffico complessivo di pacchetti, usa questa formula:. `PacketsDr opCount/(PacketsInFromSource +PacketsInFromDestination)*100` Se questo valore supera lo 0,01% del traffico totale sul gateway NAT, potrebbe esserci un problema con il servizio Amazon VPC. Utilizza il pannello di controllo dello stato del AWS servizio per identificare eventuali problemi relativi al servizio che potrebbero causare il rilascio di pacchetti da parte dei gateway NAT.<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è `Sum`. |

| Parametro | Descrizione |
| --- | --- |
| PacketsInFromDestination | Il numero di pacchetti ricevuti dal gateway NAT e provenienti dalla destinazione.<br><br>Se il valore per PacketsOutToSource è inferiore al valore per PacketsInFromDestination, vi potrebbe essere una perdita di dati durante l'esecuzione del gateway NAT o il traffico potrebbe essere attivamente bloccato dal gateway NAT.<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è Sum. |
| PacketsInFromSource | Il numero di pacchetti ricevuti dal gateway NAT e provenienti dai clienti nel tuo VPC.<br><br>Se il valore per PacketsOutToDestination è inferiore al valore per PacketsInFromSource, vi potrebbe essere una perdita di dati durante l'esecuzione del gateway NAT.<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è Sum. |

| Parametro | Descrizione |
| --- | --- |
| PacketsOutToDestination | Il numero di pacchetti inviati per mezzo del gateway NAT verso la destinazione.<br><br>Un valore superiore a zero indica che vi è un traffico verso la rete dai clienti che sono dietro il gateway NAT. Se il valore per PacketsOutToDestination è inferiore al valore per PacketsInFromSource, vi potrebbe essere una perdita di dati durante l'esecuzione del gateway NAT.<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è Sum. |
| PacketsOutToSource | Il numero di pacchetti inviati per mezzo del gateway NAT verso i clienti nel tuo VPC.<br><br>Un valore superiore a zero indica che vi è un traffico proveniente dalla rete verso i clienti che sono dietro il gateway NAT. Se il valore per PacketsOutToSource è inferiore al valore per PacketsInFromDestination, vi potrebbe essere una perdita di dati durante l'esecuzione del gateway NAT o il traffico potrebbe essere attivamente bloccato dal gateway NAT.<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è Sum. |

| Parametro | Descrizione |
| --- | --- |
| `PeakBytesPerSecond` | Questo parametro riporta la media più alta di 10 secondi di byte al secondo in un dato minuto.<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è `Maximum`. |
| `PeakPacketsPerSecond` | Questo parametro calcola la velocità media dei pacchetti (elaborati al secondo) ogni 10 secondi per 60 secondi, quindi riporta il valore massimo delle sei velocità (la velocità media dei pacchetti più alta).<br><br>Unità: numero<br><br>Statistiche: la statistica più utile è `Maximum`. |

Per filtrare i dati dei parametri, usa le seguenti dimensioni.

| Dimensione | Descrizione |
| --- | --- |
| `NatGatewayId` | Consente di filtrare i dati del parametro in base all'ID del gateway NAT. |

Visualizza le metriche del gateway NAT CloudWatch

Le metriche del gateway NAT vengono inviate a CloudWatch intervalli di 1 minuto. 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 di nomi. È possibile visualizzare i parametri dei gateway NAT come segue.

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, seleziona Metrics (Parametri), All metrics (Tutti i parametri).
3. Seleziona lo spazio dei nomi del parametro NatGateway.

4. Scegli la dimensione del dei parametri.

Per visualizzare le metriche utilizzando AWS CLI

Al prompt dei comandi, utilizzare il comando seguente per elencare i parametri disponibili per il servizio di gateway NAT.

```
aws cloudwatch list-metrics --namespace "AWS/NATGateway"
```

Crea CloudWatch allarmi per monitorare un gateway NAT

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 che monitora il volume di traffico in entrata o in uscita del gateway NAT. L'allarme seguente monitora il volume di traffico in uscita dai client nel VPC verso internet via il gateway NAT. Invia una notifica quando viene raggiunta la soglia di 5.000.000 di byte per un periodo di 15 minuti.

Per creare un allarme per il traffico in uscita via il gateway NAT

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, scegli Alarms (Allarmi), All alarms (Tutti gli allarmi).
3. Scegli Crea allarme.
4. Scegli Select Metric (Seleziona parametro).
5. Seleziona lo spazio dei nomi del parametro NatGateway, quindi una dimensione per il parametro. Quando arrivi alle metriche, seleziona la casella di controllo accanto alla BytesOutToDestinationmetrica per il gateway NAT, quindi scegli Seleziona metrica.
6. Configura l'allarme come segue, quindi scegli Next (Successivo):
   - Per Statistic (Statistica), scegliere Sum (Somma).
   - Alla voce Period (Periodo), scegli 15 minutes (15 minuti).
   - Per Whenever (Ogni volta che) , scegli Greater/Equal (Maggiore di/Uguale a) e inserisci `5000000` come soglia.

7. Per Notification (Notifica) scegli un argomento SNS esistente oppure Create new topic (Crea nuovo argomento), per crearne uno nuovo. Seleziona Avanti.
8. Inserisci un nome e una descrizione per l'allarme, quindi scegli Next (Successivo).
9. Quando hai finito di configurare l'allarme, scegli Create alarm (Crea allarme).

Come altro esempio, puoi creare un allarme che controlli gli errori di assegnazione delle porte e invii una notifica quando il valore è maggiore di zero (0) per tre periodi consecutivi di 5 minuti.

Per creare un allarme con cui monitorare gli errori di allocazione delle porte

1. Apri la console all'indirizzo https://console.aws.amazon.com/cloudwatch/ CloudWatch .
2. Nel pannello di navigazione, scegli Alarms (Allarmi), All alarms (Tutti gli allarmi).
3. Scegli Crea allarme.
4. Scegli Select Metric (Seleziona parametro).
5. Seleziona lo spazio dei nomi del parametro NatGateway, quindi una dimensione per il parametro. Quando arrivi alle metriche, seleziona la casella di controllo accanto alla ErrorPortAllocationmetrica per il gateway NAT, quindi scegli Seleziona metrica.
6. Configura l'allarme come segue, quindi scegli Next (Successivo):
   - Per Statistic (Statistica), scegli Maximum (Massima).
   - Alla voce Period (Periodo), scegli 5 minutes (5 minuti).
   - Per Whenever (Ogni volta che) , scegli Greater (Maggiore di) e inserisci 0 come soglia.
   - In Additional configuration (Configurazione aggiuntiva), Datapoints to alarm (Punti dati ad allarme), inserisci 3.
7. Per Notification (Notifica) scegli un argomento SNS esistente oppure Create new topic (Crea nuovo argomento), per crearne uno nuovo. Seleziona Avanti.
8. Inserisci un nome e una descrizione per l'allarme, quindi scegli Next (Successivo).
9. Al termine della configurazione dell'allarme, scegli Create alarm (Crea allarme).

Per ulteriori informazioni, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.

# Risoluzione dei problemi relativi ai gateway NAT

I seguenti argomenti consentono di risolvere alcuni problemi comuni che si possono verificare durante la creazione o l'utilizzo di un gateway NAT.

Problemi



## Creazione gateway NAT non riuscita

### Problema

Si crea un gateway NAT che passa allo stato `Failed`.

> **Note**
>
> Un gateway NAT non riuscito viene eliminato automaticamente, solitamente in circa un'ora.

### Causa

Si è verificato un errore al momento della creazione del gateway NAT. Il messaggio di stato restituito fornisce il motivo dell'errore.

### Soluzione

Per visualizzare il messaggio di errore, passa alla console Amazon VPC e seleziona Gateway NAT. Seleziona il pulsante di opzione per il gateway NAT, quindi cerca Messaggio di stato nella scheda Dettagli .

Nella seguente tabella vengono elencate le possibili cause di errore come indicato nella console Amazon VPC. Dopo aver applicato le procedure indicate per correggere il problema, puoi provare a creare nuovamente un gateway NAT.

| Errore visualizzato | Causa | Soluzione |
| --- | --- | --- |
| La sottorete non dispone di indirizzi liberi sufficienti per creare questo gateway NAT | La sottorete specificata non dispone di indirizzi IP privati liberi. Il gateway NAT richiede un'interfaccia di rete con un indirizzo IP privato allocato dall'intervallo della sottorete. | Verificare quanti indirizzi IP sono disponibili nella sottorete andado alla pagina Subnets (Sottoreti) nella console Amazon VPC. Si possono visualizzare gli Available IPs (IP disponibili nel riquadro dei dettagli della sottorete. Per creare indirizzi IP liberi nella sottorete, puoi eliminare interfacce di rete non utilizzat e o terminare istanze non richieste. |
| Rete vpc-xxxxxxxx senza Internet Gateway collegato | Un gateway NAT deve Essere creato in un VPC con un Internet Gateway. | Creare E collegare un Internet Gateway al VPC. Per ulteriori informazioni, consulta Gestione dei gateway Internet. |
| L'indirizzo IP elastico eipalloc-xxxxxxxx è già associato | L'indirizzo IP elastico specifica to è già associato a un'altra risorsa e non può essere associato al gateway NAT. | Controlla quale risorsa è associata all'indirizzo IP elastico. Vai alla pagina Elastic IPs (IP elastici) nella console Amazon VPC e visualizza i valori specificati per l'ID istanza o l'ID interfacc ia di rete. Se l'indirizzo IP elastico per tale risorsa non |

| Errore visualizzato | Causa | Soluzione |
| --- | --- | --- |
| | | è richiesto, puoi annullare l'associazione. In alternati va, alloca un nuovo indirizzo IP elastico nell'account. Per ulteriori informazioni, consulta Utilizzo degli indirizzi IP elastici. |

Quota gateway NAT

Quando provi a creare un gateway NAT, ricevi il seguente errore.

```
Performing this operation would exceed the limit of 5 NAT gateways
```

Causa

Hai raggiunto la quota di gateway NAT per l'account in quella zona di disponibilità.

Soluzione

Se hai raggiunto questa quota di gateway NAT per il tuo account, puoi effettuare una delle seguenti operazioni:

- Richiedere un aumento dei gateway NAT per quota di zona di disponibilità utilizzando la console Service Quotas.
- Verifica lo stato del gateway NAT. Lo stato `Pending`, `Available` o `Deleting` conta ai fini del raggiungimento della quota. Se recentemente hai eliminato un gateway NAT, attendi alcuni minuti finché lo stato passa da `Deleting` a `Deleted`. Prova quindi a creare un nuovo gateway NAT.
- Se il gateway NAT non è necessario in una zona di disponibilità specifica, prova a creare un gateway NAT in una zona di disponibilità in cui la quota non è stata raggiunta.

Per ulteriori informazioni, consulta Quote Amazon VPC.

Quota degli indirizzi IP elastici

Problema

Quando si prova ad allocare un indirizzo IP elastico per il gateway NAT pubblico, viene visualizzato il seguente errore.

```
The maximum number of addresses has been reached.
```

Causa

Hai raggiunto la quota di indirizzi IP elastici per l'account in quella regione.

Soluzione

Se è stata raggiunta la quota di indirizzi IP elastici, puoi disassociare un indirizzo IP elastico da un'altra risorsa. In alternativa, è possibile richiedere un aumento della quota degli IP elastici dalla console Service Quotas.

La zona di disponibilità non è supportata

Problema

Quando provi a creare un gateway NAT, ricevi il seguente error: `NotAvailableInZone`.

Causa

Può darsi che tu stia provando a creare il gateway NAT in una zona di disponibilità vincolata, ovvero una zona in cui la capacità di espansione è vincolata.

Soluzione

Non siamo in grado di supportare gateway NAT in queste zone di disponibilità.. Puoi creare un gateway NAT in un'altra zona di disponibilità e utilizzarla per sottoreti private nella zona vincolata. Puoi anche spostare le risorse in una zona di disponibilità non vincolata in modo che le risorse e il gateway NAT si trovino nella stessa zona di disponibilità.

Il gateway NAT non è più visibile

Problema

Hai creato un gateway NAT, ma non è più visibile nella console Amazon VPC.

Causa

Potrebbe essersi verificato un errore durante la creazione del gateway NAT e la creazione non è riuscita. Un gateway NAT con lo stato di `Failed` è visibile nella console Amazon VPC per un breve periodo di tempo (in genere un'ora). Dopo un'ora, viene eliminato automaticamente.

Soluzione

Verifica le informazioni in Creazione gateway NAT non riuscita e prova a creare un nuovo gateway NAT.

Il gateway NAT non risponde a un comando ping

Problema

Quando cerchi di eseguire il ping dell'indirizzo IP elastico o indirizzo IP privato di un gateway NAT da Internet (ad esempio, dal computer di casa) o da qualsiasi istanza nel VPC, non ricevi una risposta.

Causa

Un gateway NAT passa solo traffico da un'istanza in una sottorete privata a Internet.

Soluzione

Per verificare se il gateway NAT funziona, consulta Test del gateway NAT pubblico.

Le istanze non possono accedere a Internet

Problema

Hai creato un gateway NAT e hai seguito i passaggi per testarlo, ma il comando `ping` non funziona o le istanze nella sottorete privata non riescono ad accedere a Internet.

Cause

La causa del problema può essere una delle seguenti:

- Il gateway NAT non è pronto a distribuire il traffico.
- Le tabelle di routing non sono configurate correttamente.
- I gruppi di sicurezza o le liste di controllo degli accessi di rete bloccano il traffico in entrata o in uscita.
- Utilizzi un protocollo non supportato.

Soluzione

Verifica le seguenti informazioni:

- Controlla che lo stato del gateway NAT sia `Available`. Nella console Amazon VPC, vai alla pagina NAT Gateways (Gateway NAT) e visualizza le informazioni sullo stato nel riquadro dei dettagli. Se il gateway NAT si trova nello stato di errore, è possibile che al momento della creazione si sia verificato un errore. Per ulteriori informazioni, consulta Creazione gateway NAT non riuscita.
- Controlla che le tabelle di routing siano state correttamente configurate:
  - Il gateway NAT deve trovarsi in una sottorete pubblica con una tabella di instradamento che instrada il traffico Internet a un Internet Gateway.
  - L'istanza deve trovarsi in una sottorete privata con una tabella di instradamento che instrada il traffico Internet al gateway NAT.
  - Controlla che non siano presenti voci della tabella di instradamento che instradano tutto o parte del traffico Internet a un altro dispositivo anziché al gateway NAT.
- Assicurati che le regole del gruppo di sicurezza per l'istanza privata consentano traffico Internet in uscita. Per poter utilizzare il comando `ping`, le regole devono anche consentire traffico ICMP in uscita.

  Il gateway NAT consente tutto il traffico in uscita e il traffico ricevuto in risposta a una richiesta in uscita (è pertanto stateful).
- Assicurati che le liste di controllo accessi di rete siano associate alla sottorete privata e che sottoreti pubbliche non dispongano di regole che bloccano il traffico Internet in entrata e in uscita. Per poter utilizzare il comando `ping`, le regole devono anche consentire traffico ICMP in entrata e in uscita.

  Puoi abilitare log di flusso per semplificare la diagnosi di connessioni interrotte a causa di regole della lista di controllo accessi di rete o del gruppo di sicurezza. Per ulteriori informazioni, consulta Registrazione del traffico IP utilizzando log di flusso VPC.
- Se utilizzi il comando `ping`, assicurati di eseguire il ping di host in cui ICMP è abilitato. Se ICMP non è abilitato, non riceverai pacchetti di risposta. Per completare il test, esegui lo stesso comando `ping` dal terminale a riga di comando sul computer.
- Controlla che l'istanza sia in grado di eseguire il ping di altre risorse, ad esempio, altre istanze nella sottorete privata (ipotizzando che sia consentito dalle regole del gruppo di sicurezza).
- Verifica che la connessione utilizzi solo un protocollo TCP, UDP o ICMP.

La connessione TCP a una destinazione non va a buon fine

Problema

Alcune delle connessioni TCP dalle istanze in una sottorete privata a una destinazione specifica tramite un gateway NAT vanno a buon fine, mentre altre sono inefficaci o scadute.

Cause

La causa del problema può essere una delle seguenti:

- L'endpoint di destinazione risponde con pacchetti TCP frammentati. I gateway NAT non supportano la frammentazione IP per TCP o ICMP. Per ulteriori informazioni, consulta Confronto delle istanze NAT e i gateway NAT.
- L'opzione `tcp_tw_recycle` è abilitata su un server remoto, noto per causare problemi quando ci sono più connessioni provenienti da un dispositivo NAT.

Soluzioni

Verifica se l'endpoint a cui provi a connetterti risponde con pacchetti TCP frammentati, nel seguente modo:

1. Utilizza un'istanza in una sottorete pubblica con un indirizzo IP pubblico per attivare una risposta sufficientemente grande da causare la frammentazione dall'endpoint specifico.
2. Utilizza l'utilità `tcpdump` per verificare che l'endpoint sta inviando pacchetti frammentati.

   > **Important**
   >
   > Per eseguire queste verifiche, devi utilizzare un'istanza in una sottorete pubblica. Non puoi utilizzare l'istanza da cui la connessione originale non riesce o un'istanza in una sottorete privata dietro un gateway NAT o un'istanza NAT.

   Strumenti di diagnostica che inviano o ricevono pacchetti ICMP di grandi dimensioni segnaleranno perdita di pacchetti. Ad esempio, il comando `ping -s 10000 example.com` non funziona dietro un gateway NAT.
3. Se l'endpoint invia pacchetti TCP frammentati, puoi utilizzare un'istanza NAT anziché un gateway NAT.

Se disponi dell'accesso al server remoto, puoi verificare se l'opzione `tcp_tw_recycle` è abilitata procedendo nel seguente modo:

1. Dal server, esegui questo comando:

   ```
   cat /proc/sys/net/ipv4/tcp_tw_recycle
   ```

   Se l'output è 1, l'opzione `tcp_tw_recycle` è abilitata.
2. Se `tcp_tw_recycle` è abilitata, ti consigliamo di disabilitarla. Se devi riutilizzare le connessioni, `tcp_tw_reuse` è un'opzione più sicura.

Se non disponi dell'accesso al server remoto, puoi eseguire il test disabilitando temporaneamente l'opzione `tcp_timestamps` su un'istanza nella sottorete privata. Quindi, effettua nuovamente la connessione al server remoto. Se la connessione va a buon fine, la causa del guasto precedente è probabilmente dovuta al fatto che `tcp_tw_recycle` è abilitata sul server remoto. Se possibile, contatta il proprietario del server remoto per verificare se l'opzione è abiitata e chiedine la disabilitazione.

L'output di tracciamento non visualizza l'indirizzo IP privato del gateway NAT

Problema

L'istanza può accedere a Internet, ma quando esegui il comando `traceroute`, l'output non visualizza l'indirizzo IP privato del gateway NAT.

Causa

L'istanza accede a Internet utilizzando un gateway diverso, ad esempio un Internet Gateway.

Soluzione

Nella tabella di instradamento della sottorete in cui si trova l'istanza, controlla le seguenti informazioni:

- Assicurati che Esista una route che invia traffico Internet al gateway NAT.
- Assicurati che non esista una route più specifica che invia traffico Internet ad altri dispositivi, ad esempio un gateway virtuale privato o un Internet Gateway.

Connessione Internet interrotta dopo 350 secondi

Problema

Le istanze possono accedere a Internet ma la connessione si interrompe dopo 350 secondi.

Causa

Se una connessione che utilizza un gateway NAT rimane inattiva per almeno 350 secondi, la connessione scade.

Quando si ha il timeout di una connessione, un gateway NAT restituisce un pacchetto RST a tutte le risorse dietro il gateway NAT che tentano di continuare la connessione (non invia un pacchetto FIN).

Soluzione

Per impedire l'interruzione della connessione, puoi avviare più traffico sulla connessione. In alternativa, puoi permettere a TCP di rimanere attivo sull'istanza con un valore inferiore ai 350 secondi.

Impossibile stabilire connessione IPsec

Problema

Non è possibile stabilire una connessione IPsec a una destinazione.

Causa

I gateway NAT al momento non supportano il protocollo IPsec.

Soluzione

Puoi utilizzare NAT-Trasversal (NAT-T) per incapsulare il traffico IPsec in UDP, un protocollo supportato per i gateway NAT. Assicurati di eseguire il test di NAT-T e della configurazione IPsec per verificare che il traffico IPsec non venga interrotto.

Impossibile avviare più connessioni

Problema

Disponi già di connessioni a una destinazione tramite un gateway NAT, ma non puoi stabilire più connessioni.

Causa

È possibile che sia stato raggiunto il limite di connessioni simultanee per un singolo gateway NAT.. Per ulteriori informazioni, consulta Nozioni di base sul gateway NAT. Se le istanze nella sottorete privata creano un numero elevato di connessioni, è possibile raggiungere questo limite.

Soluzione

Completa una delle seguenti operazioni:

- Crea un gateway NAT per zona di disponibilità e distribuisci i client su queste zone.
- Crea gateway NAT aggiuntivi nella sottorete pubblica e dividi i client in più sottoreti private, ciascuna con una route a un gateway NAT diverso.
- Limita il numero di connessioni alla destinazione che i client possono creare.
- Utilizza il parametro `IdleTimeoutCount` in CloudWatch per monitorare gli aumenti delle connessioni inattive. Per rilasciare la capacità, chiudi le connessioni inattive.
- Crea un gateway NAT con più indirizzi IP o aggiungi indirizzi IP secondari a un gateway NAT esistente. Ogni nuovo indirizzo IPv4 può supportare fino a 55.000 connessioni simultanee. Per ulteriori informazioni, consultare Creazione di un gateway NAT o Come modificare le associazioni di indirizzi IP secondari.

### Prezzi

Quando si effettua il provisioning di un gateway NAT, viene addebitata ogni ora in cui il gateway NAT è disponibile e ogni gigabyte di dati che elabora. Per ulteriori informazioni, consulta la pagina dei Prezzi di Amazon VPC.

Le seguenti strategie consentono di ridurre i costi di trasferimento dati per il gateway NAT:

- Se AWS le tue risorse inviano o ricevono un volume significativo di traffico tra le zone di disponibilità, assicurati che le risorse si trovino nella stessa zona di disponibilità del gateway NAT. In alternativa, crea un gateway NAT in ogni zona di disponibilità delle risorse.
- Se la maggior parte del traffico attraverso il gateway NAT è diretto a AWS servizi che supportano gli endpoint di interfaccia o gli endpoint gateway, valuta la possibilità di creare un endpoint di interfaccia o un endpoint gateway per questi servizi. Per ulteriori informazioni sui potenziali risparmi sui costi di utilizzo, consultare AWS PrivateLink Prezzi.

## Istanze NAT

Un'istanza NAT fornisce la Network Address Translation (NAT), ovvero la traduzione degli indirizzi di rete. È possibile utilizzare un'istanza NAT per consentire alle risorse di una sottorete privata di comunicare con destinazioni esterne al cloud privato virtuale (VPC), come Internet o una rete on-premise. Le risorse nella sottorete privata possono avviare il traffico IPv4 in uscita verso Internet, ma non possono ricevere il traffico in entrata avviato su Internet.

> **Important**
>
> L'AMI NAT è basato sull'ultima versione dell'AMI Amazon Linux, 2018.03, che ha raggiunto la fine del supporto standard il 31 dicembre 2020 e la fine del supporto di manutenzione il 31 dicembre 2023. Per ulteriori informazioni, consulta il seguente post sul blog: fine del supporto di Amazon Linux AMI.
>
> Se utilizzi un AMI NAT esistente, ti AWS consiglia di migrare a un gateway NAT. I gateway NAT offrono una migliore disponibilità, una larghezza di banda superiore e richiedono un numero minore di interventi amministrativi. Per ulteriori informazioni, consulta Confronto delle istanze NAT e i gateway NAT.
>
> Se le istanze NAT si adattano meglio al tuo caso d'uso rispetto ai gateway NAT, puoi creare la tua AMI NAT da una versione corrente di Amazon Linux come descritto in. the section called “Creazione di un'AMI NAT”

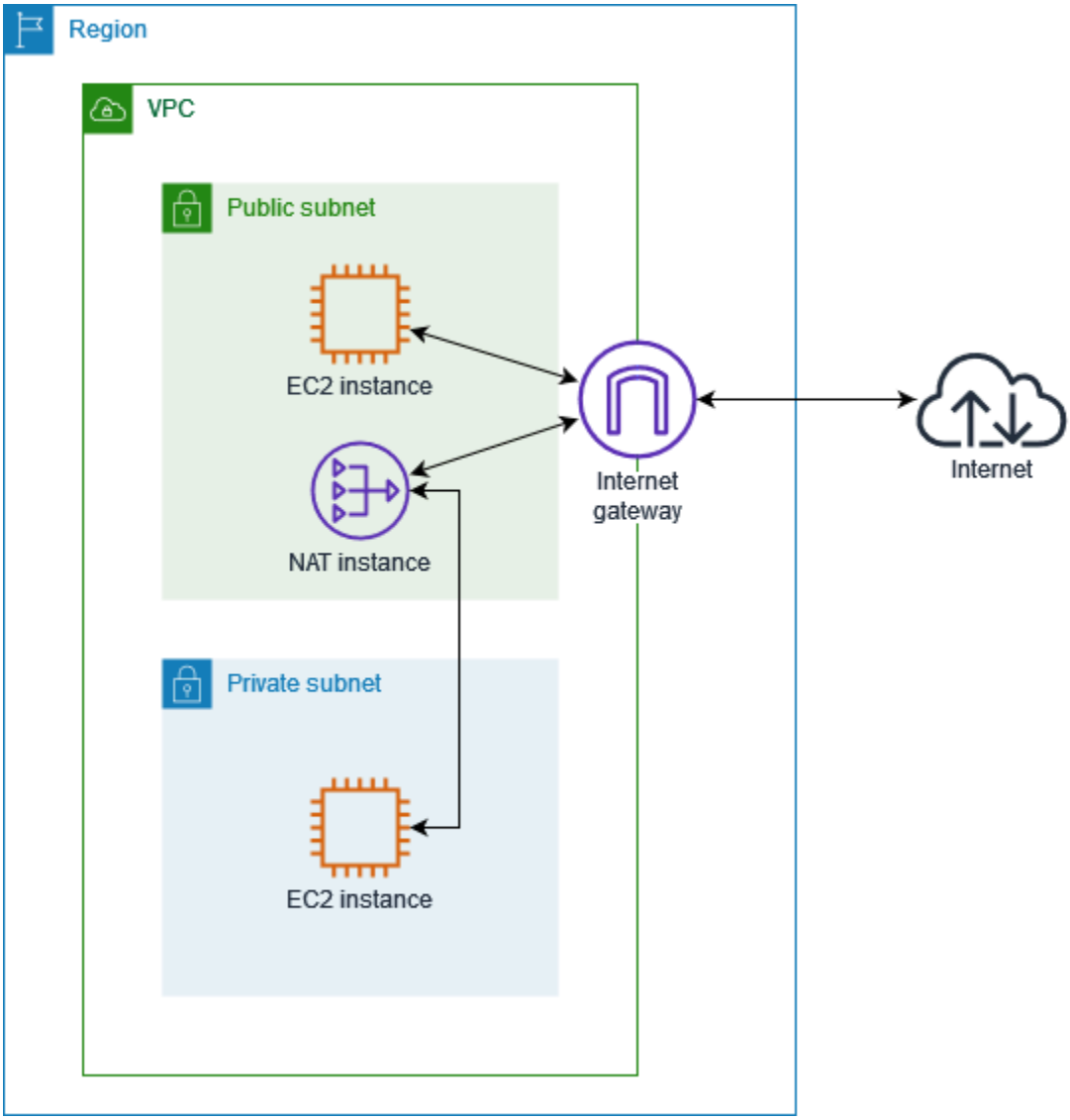
Indice



## Principi di base di un'istanza NAT

L'immagine seguente illustra i principi di base di un'istanza NAT. La tabella di routing associata alla sottorete privata invia il traffico Internet dalle istanze nella sottorete privata all'istanza NAT nella sottorete pubblica. L'istanza NAT invia quindi il traffico al gateway Internet. Il traffico è attribuito all'indirizzo IP pubblico dell'istanza NAT. L'istanza NAT specifica un numero di porta elevato per la risposta; se si riceve una risposta, l'istanza NAT la invia a un'istanza nella sottorete privata in base al numero di porta della risposta.

L'istanza NAT deve avere accesso a Internet pertanto deve trovarsi in una sottorete pubblica (una sottorete con una tabella di routing con un percorso verso il gateway Internet) e deve avere un indirizzo IP pubblico o un indirizzo IP elastico.




Per iniziare con le istanze NAT, crea un'AMI NAT, crea un gruppo di sicurezza per l'istanza NAT e avvia l'istanza NAT nel VPC.

La quota di istanze NAT dipende dalla quota di istanze per la regione. Per ulteriori informazioni, consulta Service Quotas di Amazon EC2 nella Riferimenti generali di AWS.

## Creazione di un VPC per l'istanza NAT

Utilizza la procedura seguente per creare un VPC con una sottorete pubblica e una sottorete privata.

Per creare il VPC

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Seleziona Crea VPC.
3. Per Resources to create (Risorse da creare), scegli VPC and more (VPC e altro).
4. Per Name tag auto-generation (Generazione automatica di tag nome), immetti un nome per il VPC.
5. Per configurare le sottoreti, procedi come segue:
   a. Per Number of Availability Zones (Numero di zone di disponibilità), scegli 1 o 2, a seconda delle tue esigenze.
   b. Per Number of public subnets (Numero di sottoreti pubbliche), assicurati di avere una sottorete pubblica per zona di disponibilità.
   c. Per Number of private subnets (Numero di sottoreti private), assicurati di avere una sottorete privata per ogni zona di disponibilità.
6. Seleziona Crea VPC.

## Creazione di un gruppo di sicurezza per l'istanza NAT

Crea un gruppo di sicurezza con le regole descritte nella tabella seguente. Queste regole consentono all'istanza NAT di ricevere traffico destinato a Internet dalle istanze nella sottorete privata nonché traffico SSH dalla propria rete. L'istanza NAT può anche inviare traffico a Internet, di modo che le istanze nella sottorete privata possano ottenere aggiornamenti software.

Di seguito sono riportate le regole consigliate.

In entrata

| Crea | Protocollo | Intervallo porte | Commenti |
| --- | --- | --- | --- |
| *CIDR della sottorete privata* | TCP | 80 | Consente il traffico HTTP in entrata dai server nella sottorete privata |

| Crea | Protocollo | Intervallo porte | Commenti |
| --- | --- | --- | --- |
| *CIDR della sottorete privata* | TCP | 443 | Consente il traffico HTTPS in entrata dai server nella sottorete privata |
| *Intervallo di indirizzi IP pubblici della rete* | TCP | 22 | Consente l'accesso SSH in entrata alle istanze NAT dalla rete (sul gateway Internet). |

In uscita

| Destinazione | Protocollo | Intervallo porte | Commenti |
| --- | --- | --- | --- |
| 0.0.0.0/0 | TCP | 80 | Consente l'accesso HTTP in uscita a Internet |
| 0.0.0.0/0 | TCP | 443 | Consente l'accesso HTTPS in uscita a Internet |

Creazione del gruppo di sicurezza

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegli Gruppi di sicurezza nel riquadro di navigazione.
3. Scegliere Create Security Group (Crea gruppo di sicurezza).
4. Immettere un nome e una descrizione per il gruppo di sicurezza.
5. Per VPC, seleziona l'ID del VPC per l'istanza NAT.
6. Aggiungi le regole per il traffico in entrata in Regole in entrata come riportato di seguito:
    a. Scegli Aggiungi regola. Scegli HTTP per Tipo e immetti l'intervallo di indirizzi IP della sottorete privata nel campo Origine.
    b. Scegli Aggiungi regola. Scegli HTTPS per Tipo e immetti l'intervallo di indirizzi IP della sottorete privata nel campo Origine.

c. Scegli Aggiungi regola. Scegli SSH per Tipo e inserisci l'intervallo di indirizzi IP della tua rete nel campo Origine.

7. Aggiungi le regole per il traffico in uscita in Regole in uscita come riportato di seguito:

   a. Scegli Aggiungi regola. Scegli HTTP per Tipo e immetti 0.0.0.0/0 nel campo Destinazione.
   b. Scegli Aggiungi regola. Scegli HTTPS per Tipo e immetti 0.0.0.0/0 nel campo Destinazione.

8. Scegliere Create Security Group (Crea gruppo di sicurezza).

Per ulteriori informazioni, consulta Gruppi di sicurezza.

## Creazione di un'AMI NAT

Un'AMI NAT è configurata per eseguire NAT su un'istanza EC2. È necessario creare un'AMI NAT e quindi avviare l'istanza NAT utilizzando l'AMI.

Se per l'AMI NAT prevedi di utilizzare un sistema operativo diverso da Amazon Linux, consulta la documentazione del sistema operativo per scoprire come configurare NAT. Assicurati di salvare queste impostazioni in modo che rimangano salvate anche dopo il riavvio dell'istanza.

Per creare un'AMI NAT per Amazon Linux

1. Avvia un'istanza EC2 con AL2023 o Amazon Linux 2 in esecuzione. Assicurati di specificare il gruppo di sicurezza che hai creato per l'istanza NAT.
2. Connettiti all'istanza ed esegui i comandi seguenti sull'istanza per abilitare iptables.

```
sudo yum install iptables-services -y
sudo systemctl enable iptables
sudo systemctl start iptables
```

3. Effettua le seguenti operazioni sull'istanza per abilitare l'inoltro IP in modo che persista dopo il riavvio:

   a. Usando un editor di testo, come nano o vim, crea il seguente file di configurazione: `/etc/sysctl.d/custom-ip-forwarding.conf`.
   b. Aggiungi la seguente riga al file di configurazione.

```
net.ipv4.ip_forward=1
```

   c. Salva il file di configurazione ed esci dall'editor di testo.

d. Esegui il seguente comando per applicare il file di configurazione.

```
sudo sysctl -p /etc/sysctl.d/custom-ip-forwarding.conf
```

4. Esegui il comando seguente sull'istanza e annota il nome dell'interfaccia di rete principale. Queste informazioni serviranno per la fase successiva.

```
netstat -i
```

Nel seguente output di esempio, `docker0` è un'interfaccia di rete creata da docker, `eth0` è l'interfaccia di rete principale e `lo` è l'interfaccia di loopback.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0   1500        0      0      0 0             0      0      0      0 BMU
eth0      9001  7276052      0      0 0       5364991      0      0      0 BMRU
lo       65536   538857      0      0 0        538857      0      0      0 LRU
```

Nell'output di esempio seguente, l'interfaccia di rete è `enX0`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enX0      9001     1076      0      0 0          1247      0      0      0 BMRU
lo       65536       24      0      0 0            24      0      0      0 LRU
```

Nell'output di esempio seguente, l'interfaccia di rete è `ens5`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens5      9001    14036      0      0 0          2116      0      0      0 BMRU
lo       65536       12      0      0 0            12      0      0      0 LRU
```

5. Esegui il comando riportato sull'istanza per configurare NAT. Se l'interfaccia di rete principale non è `eth0`, sostituire *`eth0`* con l'interfaccia di rete principale che hai annotato nel passaggio precedente.

```
sudo /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo /sbin/iptables -F FORWARD
sudo service iptables save
```

6. Crea un'AMI NAT dall'istanza EC2. Per ulteriori informazioni, consulta Creare un'AMI Linux da un'istanza nella Guida per l'utente di Amazon EC2.

## Avvio di un'istanza NAT

Utilizza la procedura seguente per avviare un'istanza NAT utilizzando il VPC, il gruppo di sicurezza e l'AMI NAT creata.

Avvio di un'istanza NAT

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di controllo scegliere Avvia istanza.
3. Nel campo Nome, inserisci un nome per l'istanza NAT.
4. Per Applicazioni e immagini del sistema operativo, seleziona l'AMI NAT (scegli Sfoglia altre AMI, Le mie AMI).
5. Per Tipo di istanza, seleziona un tipo di istanza che fornisce le risorse di calcolo, memoria e archiviazione di cui ha bisogno l'istanza NAT.
6. In Coppia di chiavi, scegli una coppia di chiavi esistente o Crea una nuova coppia di chiavi.
7. In Network settings (Impostazioni di rete) effettua le seguenti operazioni:
   a. Scegli Modifica.
   b. Per VPC scegli il VPC creato.
   c. Per Sottorete, scegli la sottorete pubblica creata per il VPC.
   d. Per Auto-assign Public IP (Assegna automaticamente IP pubblico), scegli Enable (Abilita). In alternativa, dopo aver avviato l'istanza NAT, alloca un indirizzo IP elastico e assegnalo all'istanza NAT.
   e. Per Firewall, scegli Seleziona gruppo di sicurezza esistente, quindi scegli il gruppo di sicurezza creato.
8. Scegliere Launch Instance (Avvia istanza). Scegli l'ID dell'istanza per aprire la relativa pagina dei dettagli. Attendi che lo stato dell'istanza passi a In esecuzione e che i controlli di stato abbiano esito positivo.
9. Disabilitazione dei controlli dell'origine/della destinazione per l'istanza NAT (consulta Disabilitazione dei controlli di origine/destinazione).
10. Aggiorna la tabella di routing per inviare il traffico all'istanza NAT (consulta Aggiornamento della tabella di routing).

## Disabilitazione dei controlli di origine/destinazione

Per impostazione predefinita, ogni istanza EC2 esegue controlli dell'origine/della destinazione. Ciò significa che l'istanza deve Essere l'origine o la destinazione di tutto il traffico che invia o riceve. Tuttavia, un'istanza NAT deve Essere in grado di inviare E ricevere traffico quando non è l'origine o la destinazione. Di conseguenza, devi disabilitare i controlli dell'origine/della destinazione sull'istanza NAT.

Disabilitazione dei controlli di origine/destinazione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Istanze.
3. Seleziona l'istanza NAT.
4. Seleziona Operazioni, Rete, Modifica il controllo dell'origine/della destinazione.
5. Per Controllo origine/destinazione, seleziona Arresta.
6. Selezionare Salva.
7. Se l'istanza NAT dispone di un'interfaccia di rete secondaria, selezionala da Interfacce di rete nella scheda Rete. Scegli l'ID interfaccia per accedere alla pagina delle interfacce di rete. Seleziona Operazioni, Modifica controllo di origine/destinazione, deseleziona l'opzione Abilita e scegli Salva.

## Aggiornamento della tabella di routing

La tabella di routing per la sottorete privata deve avere un percorso che invia traffico Internet all'istanza NAT.

Aggiornamento della tabella di routing

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Tabelle di routing.
3. Seleziona la tabella di routing per la sottorete privata.
4. Nella scheda Routing, scegli Modifica route e scegli Aggiungi instradamento.
5. Immetti 0,0.0.0/0 per Destinazione e l'ID dell'istanza NAT nel campo Destinazione.
6. Seleziona Salvataggio delle modifiche.

Per ulteriori informazioni, consulta Configurare le tabelle di routing.

## Testa l'istanza NAT

Dopo aver avviato un'istanza NAT e completato le fasi di configurazione descritte in precedenza, puoi eseguire un test per verificare se un'istanza nella sottorete privata può accedere a Internet tramite l'istanza NAT utilizzando quest'ultima come server host bastione.

Attività

- Fase 1: aggiornamento del gruppo di sicurezza dell'istanza NAT
- Fase 2. avvio di un'istanza di test nella sottorete privata
- Fase 3: esecuzione del ping di un sito Web abilitato per ICMP
- Fase 4: pulizia

### Fase 1: aggiornamento del gruppo di sicurezza dell'istanza NAT

Per consentire alle istanze della sottorete privata di inviare traffico ping all'istanza NAT, aggiungi una regola per permettere il traffico ICMP in entrata e in uscita. Per consentire all'istanza NAT di fungere da host bastione, aggiungi una regola per permettere il traffico SSH in uscita verso la sottorete privata.

Per aggiornare il gruppo di sicurezza dell'istanza NAT

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Gruppi di sicurezza.
3. Seleziona la casella di controllo relativa al gruppo di sicurezza associato all'istanza NAT.
4. Nella scheda Inbound rules (Regole in entrata), seleziona Edit inbound rules (Modifica regole in entrata).
5. Scegliere Add rule (Aggiungi regola). Scegli Tutti ICMP - IPv4 per Tipo.
   Scegli Personalizzato per Origine e specifica l'intervallo di indirizzi IP della sottorete privata.
   Scegliere Salva regole.
6. Dalla scheda Regole in uscita, seleziona Modifica regole in uscita.
7. Scegliere Add rule (Aggiungi regola). Seleziona SSH per Tipo.
   Seleziona Personalizzato per Destinazione e specifica l'intervallo di indirizzi IP della sottorete privata.
8. Scegliere Add rule (Aggiungi regola). Scegli Tutti ICMP - IPv4 per Tipo. Scegliere Ovunque - IPv4 per Destinazione. Scegliere Salva regole.

### Fase 2. avvio di un'istanza di test nella sottorete privata

Avviare un'istanza nella sottorete privata. È necessario consentire l'accesso SSH dall'istanza NAT e utilizzare la stessa coppia di chiavi utilizzata per l'istanza NAT.

Per avviare un'istanza di test nella sottorete privata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di controllo scegliere Avvia istanza.
3. Seleziona la sottorete privata.
4. Non assegnare un indirizzo IP pubblico all'istanza.
5. Assicurati che il gruppo di sicurezza di questa istanza consenta l'accesso SSH in entrata dall'istanza NAT o dall'intervallo di indirizzi IP della sottorete pubblica, e il traffico ICMP in uscita.
6. Seleziona la stessa coppia di chiavi utilizzata per l'istanza NAT.

### Fase 3: esecuzione del ping di un sito Web abilitato per ICMP

Per verificare che l'istanza di test nella sottorete privata possa utilizzare l'istanza NAT per comunicare con Internet, esegui il comando ping.

Test della connessione Internet dall'istanza privata

1. Dal computer locale, configura l'inoltro dell'agente SSH, in modo da poter utilizzare l'istanza NAT come host bastione.

   Linux and macOS

   ```
   ssh-add key.pem
   ```

   Windows

   Scarica e installa Pageant, se non è già installato.

   Converti la chiave privata in formato .ppk tramite PuTTYgen.

   Avvia Pageant, fai clic con il tasto destro del mouse sull'icona Pageant nella barra delle applicazioni (potrebbe essere nascosta), quindi seleziona Aggiungi chiave. Seleziona il file .ppk creato, immetti la passphrase se necessario e scegli Apri.
2. Dal computer locale connettiti all'istanza NAT.

Linux and macOS

```
ssh -A ec2-user@nat-instance-public-ip-address
```

Windows

Connettiti all'istanza NAT tramite PuTTY. In Autenticazione, devi selezionare Consenti inoltro agente e lascia vuoto il campo File della chiave privata per l'autenticazione.

3. Dall'istanza NAT, esegui il comando ping, che specifica un sito Web abilitato per ICMP.

```
[ec2-user@ip-10-0-4-184]$ ping ietf.org
```

Per confermare che l'istanza NAT abbia accesso a Internet, verifica di aver ricevuto un output simile al seguente, quindi premi Ctrl+C per annullare il comando ping. In caso contrario, verifica che l'istanza NAT si trovi in una sottorete pubblica (ossia che la relativa tabella di routing abbia una route verso un gateway Internet).

```
PING ietf.org (104.16.45.99) 56(84) bytes of data.
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=7.88 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.09 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=7.97 ms
...
```

4. Dall'istanza NAT, connettiti all'istanza nella sottorete privata utilizzando il relativo indirizzo IP privato.

```
[ec2-user@ip-10-0-4-184]$ ssh ec2-user@private-server-private-ip-address
```

5. Dall'istanza privata, verifica che sia possibile connettersi a Internet eseguendo il comando ping.

```
[ec2-user@ip-10-0-135-25]$ ping ietf.org
```

Per confermare che l'istanza privata abbia accesso a Internet tramite l'istanza NAT, verifica di aver ricevuto un output simile al seguente, quindi premi Ctrl+C per annullare il comando ping.

```
PING ietf.org (104.16.45.99) 56(84) bytes of data.
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=8.76 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.26 ms
```

```
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=8.27 ms
...
```

Risoluzione dei problemi

Se il comando ping non viene eseguito dal server nella sottorete privata, completa la seguente procedura per risolvere il problema:

- Verifica di aver eseguito il ping su un sito Web con ICMP abilitato. Altrimenti, il server non sarà in grado di ricevere pacchetti di risposta. Per completare il test, esegui lo stesso comando ping dal terminale a riga di comando sul computer.
- Verifica che il gruppo di sicurezza dell'istanza NAT consenta il traffico ICMP in entrata dalla sottorete privata. In caso contrario, l'istanza NAT non potrà ricevere il comando ping dall'istanza privata.
- Assicurati di aver disabilitato il controllo dell'origine/della destinazione per l'istanza NAT. Per ulteriori informazioni, consulta Disabilitazione dei controlli di origine/destinazione.
- Controlla che le tabelle di routing siano state correttamente configurate. Per ulteriori informazioni, consulta Aggiornamento della tabella di routing.

Fase 4: pulizia

Se non hai più bisogno del server di test nella sottorete privata, termina l'istanza in modo che non venga più fatturata. Per ulteriori informazioni, consulta la sezione relativa alla terminazione dell'istanza nella Guida per l'utente di Amazon EC2.

Se non hai più bisogno dell'istanza NAT, puoi interromperla o terminarla in modo che non venga più fatturata. Se hai creato un'AMI NAT, puoi creare una nuova istanza NAT ogni volta che è necessario.

## Confronto delle istanze NAT e i gateway NAT

Di seguito è riportato un riepilogo dettagliato delle differenze tra le istanze NAT e i gateway NAT. Si consiglia di utilizzare i gateway NAT perché offrono una maggiore disponibilità e larghezza di banda e richiedono meno sforzi di amministrazione per l'utente.

| Attributo | Gateway NAT | Istanza NAT |
| --- | --- | --- |
| Disponibilità | Alta disponibilità. I gateway NAT in ogni zona di disponibilità sono implementati in | Utilizza uno script per gestire failover tra le istanze. |

| Attributo | Gateway NAT | Istanza NAT |
| --- | --- | --- |
| | modo ridondante. Crea un gateway NAT in ogni zona di disponibilità affinché l'architettura sia indipendente dalle zone. | |
| Larghezza di banda | Aumentabile fino a 100 Gbps. | Dipende dalla larghezza di banda del tipo di istanza. |
| Manutenzione | Gestito da. AWS Non devi eseguire alcuna operazione di manutenzione. | Gestita da te, ad esempio, installando gli aggiornamenti software o le patch del sistema operativo sull'istanza. |
| Performance | Il software è ottimizzato per la gestione del traffico NAT. | Un'AMI generica configurata per eseguire NAT. |
| Costo | In base al numero di gateway NAT utilizzati, alla durata di utilizzo e alla quantità di dati inviati via i gateway NAT. | In base al numero di istanze NAT utilizzate, alla durata di utilizzo e al tipo e alla dimensione dell'istanza. |
| Tipo e dimensione | Offerta omogenea: non devi decidere il tipo o la dimensione. | Scegli il tipo e la dimensione appropriati in base al carico di lavoro previsto. |
| Indirizzi IP pubblici | Scegli l'indirizzo IP elastico da associare al gateway NAT in fase di creazione. | Utilizza un indirizzo IP elastico o un indirizzo IP pubblico con un'istanza NAT. Puoi modificare l'indirizzo IP pubblico in qualsiasi momento associando un nuovo indirizzo IP elastico all'istanza. |
| Indirizzi IP privati | Selezionati automaticamente dall'intervallo di indirizzi IP della sottorete quando crei il gateway. | Assegnazione di uno specifico indirizzo IP privato a partire dall'intervallo di indirizzi IP della sottorete quando avvii l'istanza. |
| Gruppi di sicurezza | Non puoi associare i gruppi di sicurezza ai gateway NAT. Puoi associarli alle tue risorse dietro il gateway NAT per controllare il traffico in entrata e in uscita. | Associati all'istanza NAT e alle risorse dietro l'istanza NAT per controllare il traffico in entrata e in uscita. |

| Attributo | Gateway NAT | Istanza NAT |
| --- | --- | --- |
| Liste di controllo accessi di rete | Utilizza una lista di controllo accessi di rete per controllare il traffico verso e dalla sottorete in cui si trova il gateway NAT. | Utilizza una lista di controllo accessi di rete per controllare il traffico verso e dalla sottorete in cui si trova l'istanza NAT. |
| Log di flusso | Utilizza log di flusso per acquisire il traffico. | Utilizza log di flusso per acquisire il traffico. |
| Inoltro alla porta | Non supportato. | Personalizza manualmente la configura zione per supportare l'inoltro alla porta. |
| Host bastioni | Non supportato. | Utilizza un host bastione. |
| Parametri di traffico | Visualizza i parametri CloudWatch per il gateway NAT. | Visualizza le CloudWatch metriche per l'istanza. |
| Comportamento del timeout | Quando si ha il timeout di una connessio ne, un gateway NAT restituisce un pacchetto RST a tutte le risorse dietro il gateway NAT che tentano di continuare la connessione (non invia un pacchetto FIN). | Quando si ha il timeout di una connessio ne, un'istanza NAT invia un pacchetto FIN alle risorse dietro l'istanza NAT per chiudere la connessione. |
| Frammentazione IP | Supporta l'inoltro di pacchetti frammentati IP per il protocollo UDP.<br><br>Non supporta la frammentazione per i protocolli TCP e ICMP. I pacchetti frammentati per questi protocolli saranno eliminati. | Supporta il riassemblaggio di pacchetti frammentati IP per i protocolli UDP, TCP e ICMP. |

### Migrazione da un'istanza NAT a un gateway NAT

Se si sta già utilizzando un'istanza NAT, consigliamo di sostituirla con un gateway NAT. È possibile creare un gateway NAT nella stessa sottorete dell'istanza NAT, quindi sostituire la route esistente nella tabella di instradamento che fa riferimento all'istanza NAT con una route che fa riferimento al gateway NAT. Per utilizzare lo stesso indirizzo IP elastico per il gateway NAT attualmente utilizzato per l'istanza NAT, è necessario innanzitutto dissociare l'indirizzo IP elastico dall'istanza NAT e associarlo al gateway NAT durante la creazione del gateway.

Modificando il routing da un'istanza NAT a un gateway NAT o annullando l'associazione dell'indirizzo IP elastico all'istanza NAT, le Eventuali connessioni correnti vengono rilasciate E devono essere nuovamente stabilite. Assicurati che non siano presenti attività critiche (o eventuali altre attività che funzionano attraverso l'istanza NAT) in esecuzione.

## Associare gli indirizzi IP elastici alle risorse nel VPC

Un indirizzo IP elastico è un indirizzo IPv4 pubblico, statico progettato per il cloud computing dinamico. Puoi associare un indirizzo IP elastico a qualsiasi istanza o interfaccia di rete in qualsiasi VPC nell'account. Con un indirizzo IP elastico puoi mascherare l'errore di un'istanza rimappando rapidamente l'indirizzo a un'altra istanza nel VPC.

### Concetti e regole degli indirizzi IP elastici

Per utilizzare un indirizzo IP elastico, occorre prima allocarlo per l'uso nel proprio account. Quindi, è possibile associarlo a un'istanza o interfaccia di rete nel VPC. Il tuo indirizzo IP elastico rimane assegnato al tuo AWS account fino a quando non lo rilasci esplicitamente.

Un indirizzo IP elastico appartiene a un'interfaccia di rete. È possibile associare un indirizzo IP elastico a un'istanza tramite l'aggiornamento dell'interfaccia di rete allegata all'istanza. Il vantaggio di associare l'indirizzo IP elastico all'interfaccia di rete anziché direttamente all'istanza è che puoi spostare tutti gli attributi dell'interfaccia di rete da un'istanza a un'altra in una singola fase. Per ulteriori informazioni, consulta Interfacce di rete elastiche nella Guida per l'utente di Amazon EC2.

Si applicano le regole seguenti:

- Un indirizzo IP elastico può essere associato a una singola istanza o interfaccia di rete alla volta.
- È possibile spostare un indirizzo IP elastico da un'istanza o interfaccia di rete a un'altra.
- Se si associa un indirizzo IP elastico all'interfaccia di rete Eth0 dell'istanza, il relativo indirizzo IPv4 pubblico corrente (se presente) viene rilasciato al pool di indirizzi IP pubblici EC2-VPC. Se

si annulla l'associazione dell'indirizzo IP elastico, l'interfaccia di rete Eth0 viene automaticamente assegnata a un nuovo indirizzo IPv4 pubblico entro pochi minuti. Ciò non vale se una seconda interfaccia di rete è stata collegata all'istanza.

- Il limite è di cinque indirizzi IP elastici. Per aiutare a conservarli, è possibile utilizzare un dispositivo NAT. Per ulteriori informazioni, consulta Eseguire la connessione a Internet o ad altri VPC utilizzando dispositivi NAT.
- Gli indirizzi IP elastici per IPv6 non sono supportati.
- Puoi contrassegnare un indirizzo IP elastico allocato per essere utilizzato in un VPC; tuttavia, i tag di allocazione dei costi non sono supportati. Se recuperi un indirizzo IP elastico, i tag non vengono recuperati.
- Puoi accedere a un indirizzo IP elastico da Internet quando il gruppo di sicurezza e la lista di controllo degli accessi di rete consentono il traffico dall'indirizzo IP di origine. Il traffico di risposta dall'interno del VPC a Internet richiede un gateway Internet. Per ulteriori informazioni, consulta Gruppi di sicurezza e Liste di controllo accessi (ACL) di rete.
- È possibile utilizzare una delle seguenti opzioni per gli indirizzi IP elastici:
  - Fare in modo che Amazon fornisca gli indirizzi IP elastici. Quando si seleziona questa opzione, è possibile associare gli indirizzi IP elastici a un gruppo di confine di rete. Questa è la posizione da cui pubblicizziamo il blocco CIDR. L'impostazione del gruppo di confine di rete limita il blocco CIDR a questo gruppo.
  - Utilizzo dei propri indirizzi IP Per informazioni su come portare i tuoi indirizzi IP, consulta Bring your own IP address (BYOIP) nella Amazon EC2 User Guide.

Gli indirizzi IP elastici sono legati alle regioni. Per ulteriori informazioni sull'utilizzo di Global Accelerator per il provisioning di indirizzi IP globali, consulta Utilizzo di indirizzi IP statici globali anziché indirizzi IP statici regionali nella Guida per gli sviluppatori di AWS Global Accelerator .

## Utilizzo degli indirizzi IP elastici

Le sezioni seguenti descrivono il funzionamento degli indirizzi IP elastici.

Attività

- Allocare un indirizzo IP elastico
- Associazione di un indirizzo IP elastico
- Visualizzazione degli indirizzi IP elastici
- Applicazione di tag a un indirizzo IP elastico

- Annullare l'associazione di un indirizzo IP elastico
- Trasferire indirizzi IP elastici
- Rilascio di un indirizzo IP elastico
- Recupero di un indirizzo IP elastico
- Panoramica sulle API e sui comandi

## Allocare un indirizzo IP elastico

Prima di utilizzare un IP elastico, è necessario allocarne uno per l'uso nel VPC.

Per allocare un indirizzo IP elastico

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elastic IPs (IP elastici).
3. Scegli Alloca indirizzo IP elastico.
4. (Facoltativo) Quando si assegna un indirizzo IP elastico (EIP), si sceglie il gruppo di confini di rete in cui allocare l'EIP. Un gruppo di confine di rete è una raccolta di Availability Zones (AZ), Local Zones o Wavelength Zones da AWS cui pubblicizza un indirizzo IP pubblico. Le Local Zones e Wavelength Zones possono avere gruppi di confini di rete diversi rispetto alle AZ di una regione per garantire una latenza o una distanza fisica minima tra AWS la rete e i clienti che accedono alle risorse in queste Zone.

   > **Important**
   >
   > È necessario allocare un EIP nello stesso gruppo di confini di rete della AWS risorsa che verrà associata all'EIP. Un EIP in un gruppo di confini di rete può essere pubblicizzato solo nelle zone di quel gruppo di confini di rete e non in altre zone rappresentate da altri gruppi di confini di rete.

   Se hai abilitato le zone locali o le zone Wavelength (per ulteriori informazioni, consulta Abilitazione di una zona locale o Abilitazione delle zone Wavelength), puoi scegliere un gruppo di confini di rete per AZ, zone locali o zone Wavelength. Scegliete con attenzione il gruppo di confini di rete poiché l'EIP e la AWS risorsa a cui è associato devono risiedere nello stesso gruppo di confini di rete. Puoi utilizzare la console EC2 per visualizzare il gruppo di confini di rete in cui si trovano le tue zone di disponibilità, zone locali o zone Wavelength (consulta Zone locali).

In genere, tutte le zone di disponibilità in una regione appartengono allo stesso gruppo di confini di rete, mentre le zone locali o le zone Wavelength Zone appartengono a gruppi di confini di rete separati.

Se non hai abilitato le zone locali o le zone Wavelength, quando allochi un EIP, il gruppo di confini di rete che rappresenta tutte le AZ della regione (ad esempio, `us-west-2`) è predefinito e non potrai modificarlo. Ciò significa che l'EIP assegnato a questo gruppo di confini di rete verrà pubblicizzato in tutte le AZ della regione in cui ti trovi.

5. Per Pool di indirizzi IPv4 pubblici scegliere una delle seguenti opzioni:

   - Amazon's pool of IP addresses (Pool di indirizzi IP di Amazon): se desideri che un indirizzo IPv4 venga allocato dal pool di indirizzi IP di Amazon.
   - Il mio pool di indirizzi IPv4 pubblici: se desideri allocare un indirizzo IPv4 da un pool di indirizzi IP che hai trasferito al tuo account. AWS Questa opzione è disattivata se non disponi di pool di indirizzi IP.
   - Pool di indirizzi IPv4 di proprietà del cliente: se si desidera allocare un indirizzo IPv4 da un pool creato dalla rete On-Premise da utilizzare con un Outpost. Questa opzione è disponibile solo ai possessori di un Outpost.

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

   [Aggiunta di un tag] Scegli Aggiungi nuovo tag e procedi come segue:

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

   [Rimuovi un tag] Scegli Rimuovi a destra della Chiave e del Valore del tag.

7. Selezionare Alloca.

## Associazione di un indirizzo IP elastico

È possibile associare un IP elastico a un'istanza o interfaccia di rete in esecuzione nel VPC.

Dopo aver associato un indirizzo IP elastico, l'istanza riceve un nome host DNS pubblico se i nomi host DNS sono abilitati. Per ulteriori informazioni, consulta Attributi DNS per il VPC.

Per associare un indirizzo IP elastico a un'istanza o un'interfaccia di rete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elastic IPs (IP elastici).
3. Selezionare un indirizzo IP elastico allocato per essere utilizzato con un VPC (la colonna Scope (Ambito) contiene un valore di `vpc`), quindi scegliere Actions (Operazioni), Associate Elastic IP address (Associa indirizzo IP elastico).
4. Selezionare Instance (Istanza) o Network interface (Interfaccia di rete), quindi selezionare l'ID dell'istanza o dell'interfaccia di rete. Selezionare l'indirizzo IP privato cui associare l'indirizzo IP elastico. Selezionare Associate (Associa).

## Visualizzazione degli indirizzi IP elastici

È possibile visualizzare gli indirizzi IP elastici allocati al proprio account.

Per visualizzare gli indirizzi IP elastici

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elastic IPs (IP elastici).
3. Per filtrare l'elenco visualizzato, iniziare a digitare parte dell'indirizzo IP elastico o uno dei relativi attributi nella casella di ricerca.

## Applicazione di tag a un indirizzo IP elastico

Puoi applicare tag all'indirizzo IP elastico per identificarlo o classificarlo più facilmente in base alle Esigenze dell'organizzazione.

Per applicare un tag a un indirizzo IP elastico

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico e scegliere Tags (Tag).
4. Selezionare Manage tags (Gestisci tag), immettere le chiavi e i valori dei tag e scegliere Save (Salva).

## Annullare l'associazione di un indirizzo IP elastico

Per modificare la risorsa a cui è associato l'indirizzo IP elastico, è innanzitutto necessario disassociarlo dalla risorsa attualmente associata.

Per annullare l'associazione di un indirizzo IP elastico

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico, quindi selezionare Actions (Operazioni), Disassociate Elastic IP address (Annulla associazione indirizzo IP elastico).
4. Quando richiesto, selezionare Disassociate (Annulla associazione).

## Trasferire indirizzi IP elastici

Questa sezione descrive come trasferire indirizzi IP elastici da un Account AWS a un altro. Il trasferimento di indirizzi IP elastici può risultare utile nelle seguenti situazioni:

- Ristrutturazione organizzativa: utilizza i trasferimenti di indirizzi IP elastici per spostare rapidamente i carichi di lavoro da uno all'altro. Account AWS Non è necessario attendere che i nuovi indirizzi IP elastici vengano inseriti nell'elenco consentito nei gruppi di sicurezza e nei NACL.
- Amministrazione centralizzata della sicurezza: utilizza un account di AWS sicurezza centralizzato per tracciare e trasferire indirizzi IP elastici che sono stati controllati per verificarne la conformità alla sicurezza.
- Ripristino di emergenza: utilizza i trasferimenti di indirizzi IP elastici per eseguire nuovamente la mappatura degli IP in modo rapido per i carichi di lavoro su Internet rivolti al pubblico durante gli eventi di emergenza.

Il trasferimento degli indirizzi IP elastici è gratuito.

Attività

- Abilitare il trasferimento di indirizzi IP elastici
- Disabilitare il trasferimento di indirizzi IP elastici
- Accettare un indirizzo IP elastico trasferito

## Abilitare il trasferimento di indirizzi IP elastici

Questa sezione descrive come accettare un indirizzo IP elastico trasferito. Prendi nota delle seguenti limitazioni relative all'abilitazione degli indirizzi IP elastici per il trasferimento:

- È possibile trasferire indirizzi IP elastici da qualsiasi Account AWS (account di origine) a qualsiasi altro AWS account nella stessa AWS regione (account di trasferimento).
- Quando si trasferisce un indirizzo IP elastico, viene eseguito un handshake in due passaggi tra gli Account AWS. Quando l'account di origine inizia il trasferimento, gli account di trasferimento hanno sette giorni per accettare il trasferimento dell'indirizzo IP elastico. Durante questi sette giorni, l'account di origine può visualizzare il trasferimento in sospeso (ad esempio nella AWS console o utilizzando il comando AWS CLI describe-address-transfers). Dopo sette giorni, il trasferimento scade e la proprietà dell'indirizzo IP elastico ritorna all'account di origine.
- I trasferimenti accettati sono visibili sull'account di origine (ad esempio nella AWS console o utilizzando il comando AWS CLI describe-address-transfers) per tre giorni dopo l'accettazione dei trasferimenti.
- AWS non notifica agli account di trasferimento le richieste di trasferimento di indirizzi IP elastici in sospeso. Il proprietario dell'account di origine deve notificare al proprietario dell'account di trasferimento che esiste una richiesta di trasferimento di indirizzo IP elastico che deve accettare.
- Tutti i tag che sono associati a un indirizzo IP elastico da trasferire vengono reimpostati al termine del trasferimento.
- Non è possibile trasferire indirizzi IP elastici allocati da pool di indirizzi IPv4 pubblici che vengono trasferiti ai propri pool di indirizzi, comunemente denominati pool di indirizzi Bring Your Own IP (BYOIP). Account AWS
- Se si tenta di trasferire un indirizzo IP elastico a cui è associato un record DNS inverso, è possibile iniziare il processo di trasferimento, ma l'account di trasferimento non sarà in grado di accettare il trasferimento finché il record DNS associato non verrà rimosso.
- Se hai abilitato e configurato AWS Outposts, potresti aver allocato indirizzi IP elastici da un pool di indirizzi IP (CoIP) di proprietà del cliente. Non è possibile trasferire indirizzi IP elastici allocati dai CoIP. Tuttavia, puoi utilizzarlo AWS RAM per condividere un CoIP con un altro account. Per ulteriori informazioni, consulta Indirizzi IP di proprietà del cliente nella Guida per l'utente di AWS Outposts .
- Puoi utilizzare Amazon VPC IPAM per monitorare il trasferimento di indirizzi IP elastici agli account di un'organizzazione da AWS Organizations. Per ulteriori informazioni, consulta Visualizza la cronologia degli indirizzi IP. Tuttavia, se un indirizzo IP elastico viene trasferito su un account

Account AWS esterno all'organizzazione la cronologia di controllo IPAM dell'indirizzo IP elastico andrà persa.

Questa sezione deve essere completata dall'account di origine.

Abilitare il trasferimento di indirizzi IP elastici

1. Assicurati di utilizzare l' AWS account di origine.
2. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Nel riquadro di navigazione, selezionare Elastic IPs (IP elastici).
4. Seleziona uno o più indirizzi IP elastici per abilitare il trasferimento e scegli Actions (Azioni), Enable transfer (Abilita trasferimento).
5. Se stai trasferendo più indirizzi IP elastici, vedrai l'opzione Transfwer type (Tipo di trasferimento). Selezionare una delle seguenti opzioni:
   - Scegli Account singolo se trasferisci gli indirizzi IP elastici su un unico AWS account.
   - Scegli Account multipli se trasferisci gli indirizzi IP elastici su più AWS account.
6. In Transfer account ID (ID degli account di trasferimento), inserisci gli ID degli account AWS a cui desideri trasferire gli indirizzi IP elastici.
7. Conferma il trasferimento inserendo **`enable`** nella casella di testo.
8. Scegli Invia.
9. Per accettare il trasferimento, consulta Accettare un indirizzo IP elastico trasferito. Per disabilitare il trasferimento, consulta Disabilitare il trasferimento di indirizzi IP elastici.

Disabilitare il trasferimento di indirizzi IP elastici

Questa sezione descrive come disabilitare un trasferimento di IP elastici dopo averlo abilitato.

Questi passaggi devono essere completati dall'account di origine che ha abilitato il trasferimento.

Disabilitazione del trasferimento di indirizzi IP elastici

1. Assicurati di utilizzare l' AWS account di origine.
2. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Nel riquadro di navigazione, selezionare Elastic IPs (IP elastici).

4. Nell'elenco delle risorse degli IP elastici, assicurati di avere abilitato la proprietà che mostra la colonna Transfer status (Stato del trasferimento).
5. Seleziona uno o più indirizzi IP elastici con Transfer status (Stato del trasferimento) impostato su Pending (In sospeso) e scegli Actions (Azioni), Disable transfer (Disabilita trasferimento).
6. Conferma inserendo **`disable`** nella casella di testo.
7. Scegli Invia.

### Accettare un indirizzo IP elastico trasferito

Questa sezione descrive come accettare un indirizzo IP elastico trasferito.

Quando si trasferisce un indirizzo IP elastico, viene eseguito un handshake in due passaggi tra gli Account AWS. Quando l'account di origine inizia il trasferimento, gli account di trasferimento hanno sette giorni per accettare il trasferimento dell'indirizzo IP elastico. Durante questi sette giorni, l'account di origine può visualizzare il trasferimento in sospeso (ad esempio nella AWS console o utilizzando il comando AWS CLI describe-address-transfers). Dopo sette giorni, il trasferimento scade e la proprietà dell'indirizzo IP elastico ritorna all'account di origine.

Quando si accettano i trasferimenti, è bene prendere nota delle seguenti eccezioni che potrebbero verificarsi e delle modalità di risoluzione:

- AddressLimitSuperata: se l'account di trasferimento ha superato la quota di indirizzi IP elastici, l'account di origine può abilitare il trasferimento di indirizzi IP elastici, ma questa eccezione si verifica quando l'account di trasferimento tenta di accettare il trasferimento. Per impostazione predefinita, tutti gli AWS account sono limitati a 5 indirizzi IP elastici per regione. Consulta il limite di indirizzi IP elastici nella Guida per l'utente di Amazon EC2 per istruzioni su come aumentare il limite.
- InvalidTransfer. AddressCustomPtrSet: Se tu o qualcuno della tua organizzazione avete configurato l'indirizzo IP elastico che state tentando di trasferire per utilizzare la ricerca DNS inversa, l'account di origine può abilitare il trasferimento per l'indirizzo IP elastico, ma questa eccezione si verifica quando l'account di trasferimento tenta di accettare il trasferimento. Per risolvere questo problema, l'account di origine deve rimuovere il record DNS per l'indirizzo IP elastico. Per ulteriori informazioni, consulta Rimuovere un record DNS inverso nella Guida per l'utente di Amazon EC2.
- InvalidTransfer. AddressAssociated: Se un indirizzo IP elastico è associato a un'istanza ENI o EC2, l'account di origine può abilitare il trasferimento per l'indirizzo IP elastico, ma questa eccezione si

verifica quando l'account di trasferimento tenta di accettare il trasferimento. Per risolvere questo problema, l'account di origine deve dissociare l'indirizzo IP elastico. Per ulteriori informazioni, consulta Dissociare un indirizzo IP elastico nella Amazon EC2 User Guide.

Per eventuali altre eccezioni, contatta il AWS Support.

Questa procedura deve essere completata dall'account di trasferimento.

Accettazione del trasferimento di un indirizzo IP elastico

1. Assicurati di utilizzare l'account di origine.
2. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Nel riquadro di navigazione, selezionare Elastic IPs (IP elastici).
4. Scegli Actions (Operazioni), Accept transfer (Accetta trasferimento).
5. Quando viene accettato il trasferimento, nessun tag associato all'indirizzo IP elastico da trasferire viene trasferito con l'indirizzo IP elastico. Se desideri definire un tag Name (Nome) per l'indirizzo IP elastico che stai accettando, seleziona Create a tag with a key of 'Name' and a value that you specify (Crea un tag con una chiave "Nome" e un valore da specificare).
6. Inserisci l'indirizzo IP elastico da trasferire.
7. Se stai accettando più indirizzi IP elastici trasferiti, scegli Add address (Aggiungi indirizzo) per inserire un indirizzo IP elastico aggiuntivo.
8. Scegli Invia.

## Rilascio di un indirizzo IP elastico

Se non hai più bisogno di un indirizzo IP Elastic, ti consigliamo di rilasciarlo. Ti verranno addebitati dei costi per ogni indirizzo IP elastico allocato per l'utilizzo su un VPC ma non associato ad alcuna istanza. L'indirizzo IP elastico non deve essere associato a un'istanza o un'interfaccia di rete.

per rilasciare un indirizzo IP elastico

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico e scegliere Actions (Operazioni), Release Elastic IP addresses (Rilascia indirizzi IP elastici).

4. Quando richiesto, selezionare Release (Rilascia).

## Recupero di un indirizzo IP elastico

Se rilasci l'indirizzo IP elastico ma cambi idea, dovresti riuscire a recuperarlo. Non puoi recuperare l'indirizzo IP elastico se è stato assegnato a un altro AWS account o se il ripristino comporta il superamento della quota di indirizzi IP elastici.

Puoi recuperare un indirizzo IP elastico soltanto utilizzando l'API di Amazon EC2 o lo strumento a riga di comando.

Per ripristinare un indirizzo IP elastico utilizzando il AWS CLI

Utilizzare il comando allocate-address e specificare l'indirizzo IP utilizzando il parametro `--address`.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

## Panoramica sulle API e sui comandi

Puoi eseguire le attività descritte in questa sezione tramite la riga di comando o un'API. Per ulteriori informazioni sulle interfacce a riga di comando e per un elenco delle operazioni API disponibili, consulta Uso di Amazon VPC.

Accettare il trasferimento di un indirizzo IP elastico

- accept-address-transfer (AWS CLI)
- Approve-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Allocare un indirizzo IP elastico

- allocate-address (AWS CLI)
- New-EC2Address (AWS Tools for Windows PowerShell)

Associazione di un indirizzo IP elastico a un'istanza o un'interfaccia di rete

- associate-address (AWS CLI)
- Register-EC2Address (AWS Tools for Windows PowerShell)

Descrivere i trasferimenti di indirizzi IP elastici

- describe-address-transfers (AWS CLI)
- Get-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Disabilitazione del trasferimento di indirizzi IP elastici

- disable-address-transfer (AWS CLI)
- Disable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Annullare l'associazione di un indirizzo IP elastico

- disassociate-address (AWS CLI)
- Unregister-EC2Address (AWS Tools for Windows PowerShell)

Abilitare il trasferimento di indirizzi IP elastici

- enable-address-transfer (AWS CLI)
- Enable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Rilascio di un indirizzo IP elastico

- release-address (AWS CLI)
- Remove-EC2Address (AWS Tools for Windows PowerShell)

Applicazione di tag a un indirizzo IP elastico

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Visualizzazione degli indirizzi IP elastici

- describe-addresses (AWS CLI)
- Get-EC2Address (AWS Tools for Windows PowerShell)

## Prezzi

Per garantire un uso efficiente degli indirizzi IP elastici, imponiamo una piccola tariffa oraria. Per ulteriori informazioni, consulta Indirizzo IPv4 pubblico nella pagina Prezzi di Amazon VPC.

# Collegare il VPC ad altri VPC e altre reti utilizzando un gateway di transito

Puoi collegare i cloud privati virtuali (VPC) e le reti locali utilizzando un gateway di transito, che funge da hub centrale, instradando il traffico tra VPC, connessioni VPN e connessioni AWS Direct Connect. Per ulteriori informazioni, consulta AWS Transit Gateway.

Nella tabella seguente vengono descritti alcuni casi d'uso comuni per i gateway di transito e sono presenti collegamenti a ulteriori informazioni in Amazon VPC Transit Gateway.

| Esempio | Utilizzo |
| --- | --- |
| Router centralizzato | Configurare il gateway di transito come un router centralizzato che collega tutte le connessioni di VPC, AWS Direct Connect e AWS Site-to-Site VPN. Per ulteriori informazioni, consulta Esempio: router centralizzato. |
| VPC isolati | Configurare il gateway di transito come più router isolati. Il caso d'uso è simile a quello dell'utilizzo di gateway di transito multipli, ma offre maggiore flessibilità nei casi in cui gli instradamenti e gli allegati siano soggetti a modifica. Per ulteriori informazioni, consulta Esempio: VPC isolati. |
| VPC isolati con servizi condivisi | Configurare il gateway di transito come più router isolati che utilizzano un servizio condiviso. Il caso d'uso è simile a quello dell'utilizzo di gateway di transito multipli, ma offre maggiore flessibilità nei casi in cui gli instradamenti e gli allegati siano soggetti a modifica. Per ulteriori informazioni, consulta Esempio: VPC isolati con servizi condivisi. |

# Connetti il tuo VPC a reti remote utilizzando AWS Virtual Private Network

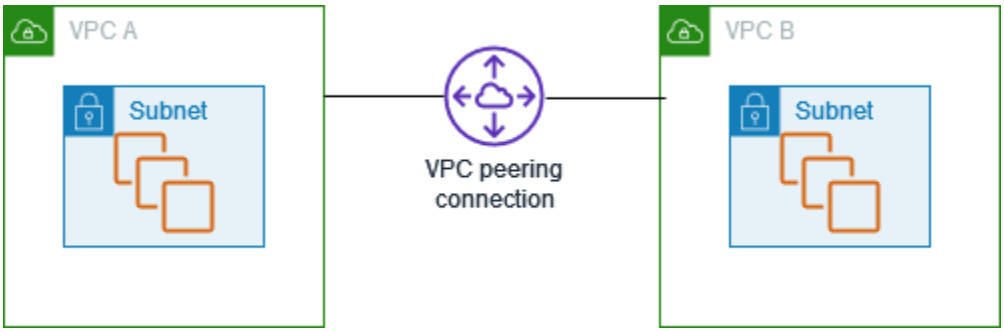
Puoi connettere il tuo VPC a reti e utenti remoti utilizzando le opzioni di connettività VPN seguenti.

| Opzione di connettività VPN | Descrizione |
| --- | --- |
| AWS Site-to-Site VPN | Puoi creare una connessione VPN IPsec tra il VPC e la rete remota. Sul lato AWS della connessione Site-to-Site VPN, un gateway virtuale privato o gateway di transito offre due endpoint VPN (tunnel) per il failover automatico. Configura il dispositivo gateway del cliente sul lato remoto della connessione Site-to-Site VPN. Per ulteriori informazioni, consulta laGuida per l'utente di AWS Site-to-Site VPN. |
| AWS Client VPN | AWS Client VPN è un servizio VPN gestito, basato su cloud, che consente di controllare in modo sicuro l'accesso alle risorse AWS nella tua rete locale. Con AWS Client VPN, configuri un endpoint al quale i tuoi utenti possono connettersi per stabilire una sessione VPN TLS protetta. In questo modo i client sono abilitati ad accedere alle risorse in AWS o On-Premise da qualsiasi postazione tramite un client VPN basato su OpenVPN. Per ulteriori informazioni, consulta la Guida per l'amministratore di AWS Client VPN. |
| AWS VPN CloudHub | Se sono disponibili più reti remote (ad esempio più filiali), puoi creare più connessioni AWS Site-to-Site VPN tramite il gateway privato virtuale per abilitare la comunicazione tra queste reti. Per ulteriori informazi oni, consulta Fornire una comunicazione sicura tra siti utilizzando VPN CloudHub nella Guida per l'utente di AWS Site-to-Site VPN. |
| Appliance software VPN di terze parti | È possibile creare una connessione VPN alla propria rete remota tramite un'istanza Amazon EC2 nel VPC che esegue un'appliance software VPN di terze parti. AWS non fornisce né gestisce appliance software VPN di terze parti, tuttavia è possibile scegliere tra diversi prodotti offerti da partner e community open source. Appliance software VPN di terze parti sono disponibili in Marketplace AWS Marketplace. |

Puoi anche utilizzare AWS Direct Connect per creare una connessione privata dedicata da una rete remota al VPC. Puoi combinare questa connessione con un AWS Site-to-Site VPN per creare una connessione crittografata IPsec. Per ulteriori informazioni, consulta Che cos'è AWS Direct Connect? nella Guida per l'utente AWS Direct Connect.

## Connettere i VPC utilizzando il peering VPC

Una connessione peering VPC è una connessione di rete tra due VPC che ti consente di instradare il traffico tra gli stessi in modo privato. Le risorse nei VPC in peering possono comunicare tra loro come se fossero nella stessa rete. Puoi creare una connessione peering VPC tra i VPC, con un VPC in un altro account Account AWS o con un VPC in una regione AWS diversa. Il traffico tra VPC in peering non attraversa la rete Internet pubblica.




AWS utilizza l'infrastruttura esistente di un VPC per creare una connessione peering VPC. Una connessione peering VPC non è un gateway o una connessione AWS Site-to-Site VPN e non dipende da un elemento hardware fisico separato. Non prevede alcun singolo punto di errore né colli di bottiglia.

Per ulteriori informazioni, consulta la Guida ad Amazon VPC Peering.

# Monitoraggio del VPC

È possibile utilizzare i seguenti strumenti per monitorare il traffico o l'accesso alla rete nel cloud privato virtuale (VPC).

Flussi di log VPC

I flussi di log VPC vengono utilizzati per acquisire informazioni sul traffico verso e dalle interfacce di rete nei VPC.

IP Address Manager (IPAM) di Amazon VPC

È possibile utilizzare IPAM per pianificare, tracciare e monitorare gli indirizzi IP per i carichi di lavoro. Per ulteriori informazioni, consulta IP Address Manager.

Mirroring del traffico

Puoi utilizzare questa caratteristica per copiare il traffico di rete da un'interfaccia di rete di un'istanza Amazon EC2 e quindi inviarlo a dispositivi di sicurezza e monitoraggio fuori banda per l'ispezione approfondita dei pacchetti. È possibile rilevare anomalie di rete e sicurezza, ottenere informazioni operative, implementare controlli di conformità e sicurezza e risolvere i problemi. Per ulteriori informazioni, consulta Mirroring del traffico.

Reachability Analyzer

È possibile utilizzare questo strumento per analizzare ed eseguire il debug della raggiungibilità della rete tra due risorse nel VPC. Dopo aver specificato le risorse di origine e di destinazione, Reachability Analyzer produce i dettagli hop-by-hop del percorso virtuale tra di loro quando sono raggiungibili e identifica il componente di blocco quando non sono raggiungibili. Per ulteriori informazioni, consulta Reachability Analyzer.

Network Access Analyzer

È possibile utilizzare Network Access Analyzer per comprendere l'accesso di rete alle risorse. In questo modo è possibile individuare miglioramenti alla posizione di sicurezza della rete e dimostrare che la rete soddisfa requisiti di conformità specifici. Per ulteriori informazioni, consulta Network Access Analyzer.

Log di CloudTrail

È possibile utilizzare AWS CloudTrail per acquisire informazioni dettagliate sulle chiamate effettuate all'API Amazon VPC. È possibile utilizzare i log di CloudTrail generati per determinare

quali chiamate sono state effettuate, l'indirizzo IP di origine da cui proveniva la chiamata, chi l'ha effettuata, quando e così via. Per maggiori informazioni, consulta Registrazione delle chiamate API Amazon EC2, Amazon EBS e Amazon VPC utilizzando AWS CloudTrail nella Documentazione di riferimento delle API Amazon EC2.

# Registrazione del traffico IP utilizzando log di flusso VPC

Log di flusso VPC è una funzione che consente di catturare le informazioni sul traffico IP da e per le interfacce di rete nel VPC. I dati dei log di flusso possono essere pubblicati nelle seguenti posizioni: Amazon CloudWatch Logs, Amazon S3 o Amazon Data Firehose. Dopo aver creato un log di flusso, è possibile recuperare e visualizzarne i record nel gruppo di log, nel bucket o nel flusso di consegna configurato.

I log di flusso possono essere utili per diverse attività, ad esempio:

- Diagnosi di regole del gruppo di sicurezza eccessivamente restrittive
- Monitoraggio del traffico che raggiunge l'istanza
- Identificazione della direzione del traffico da e verso le interfacce di rete

I dati di log del flusso vengono raccolti al di fuori del percorso del traffico di rete e pertanto non influiscono sulla velocità effettiva o sulla latenza della rete. È possibile creare o eliminare i log di flusso senza alcun rischio di impatto sulle prestazioni della rete.

> **Note**
>
> Questa sezione parla solo dei log di flusso per VPC. Per informazioni sui log di flusso per i gateway di transito introdotti nella versione 6, consulta Registrazione del traffico di rete utilizzando Transit Gateway Flow Logs nella Amazon VPC Transit Gateways User Guide.

Indice

- Prezzi
- Utilizzo dei log di flusso
- Pubblica i log di flusso su Logs CloudWatch
- Pubblicazione di log di flusso su Amazon S3
- Pubblica i log di flusso su Amazon Data Firehose
- Eseguire una query dei flussi di log tramite Amazon Athena
- Risoluzione dei problemi relativi ai log di flusso VPC

## Nozioni di base sui log di flusso

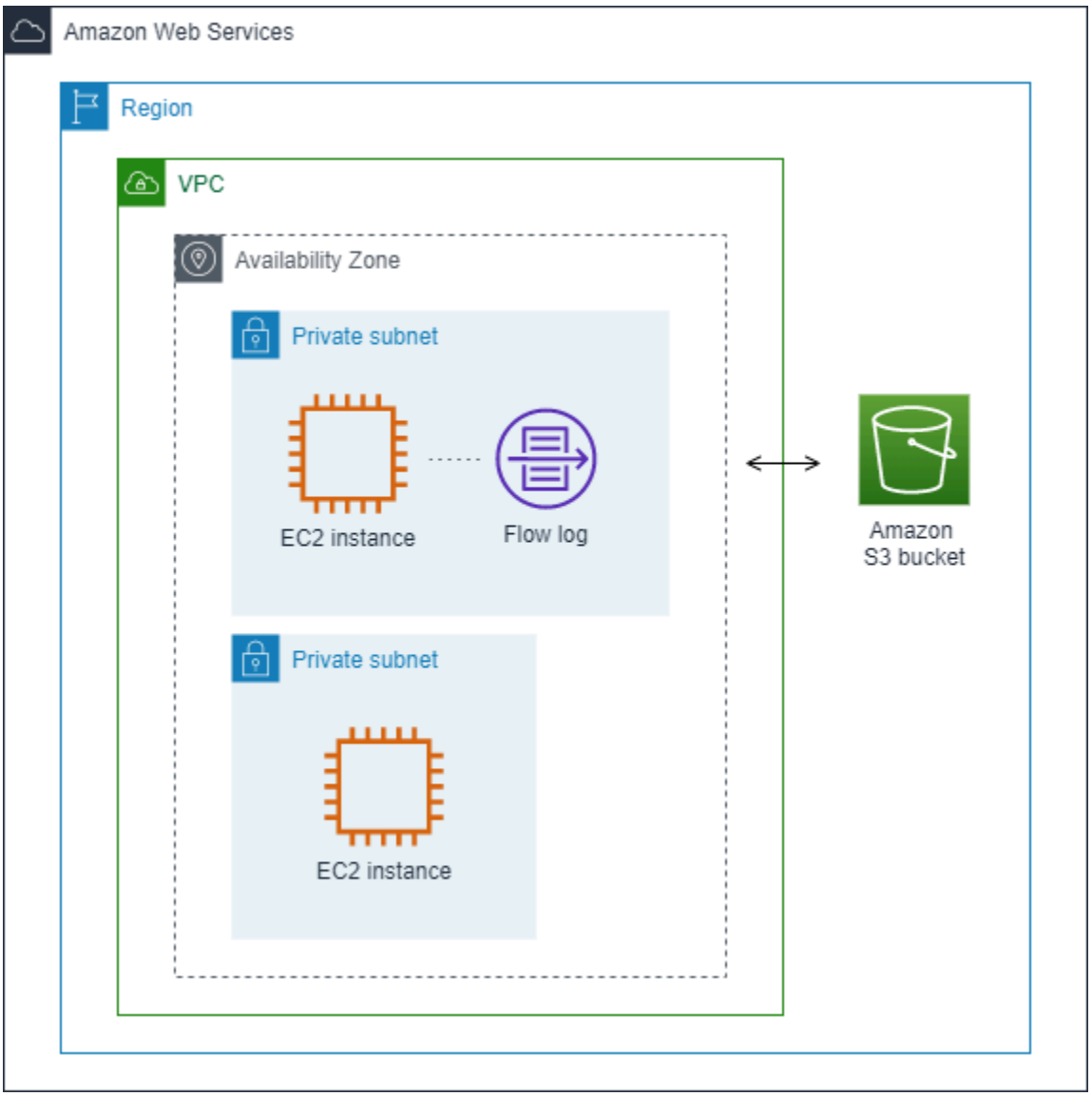
Puoi creare un log di flusso per un VPC, una sottorete o un'interfaccia di rete. Se crei un log di flusso per una sottorete o un VPC, viene monitorata ogni interfaccia di rete nella sottorete o nel VPC.

I dati del log di flusso per un'interfaccia di rete monitorata vengono registrati come record del log di flusso, che sono eventi di log costituiti da campi che descrivono il flusso di traffico. Per ulteriori informazioni, consulta Record di log di flusso.

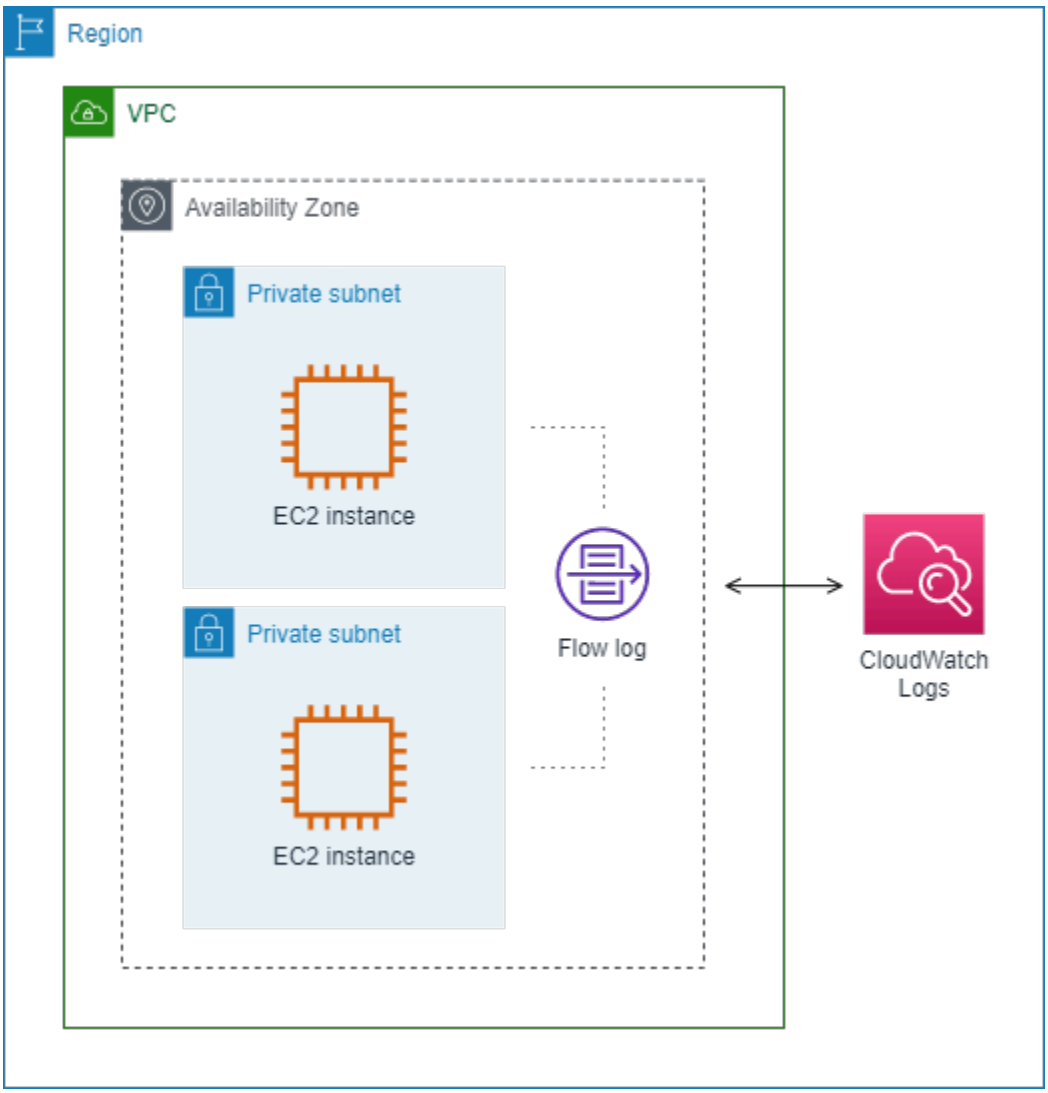
Per creare un log di flusso, occorre specificare:

- La risorsa per cui creare il log di flusso
- Il tipo di traffico da acquisire (traffico accettato, traffico rifiutato o tutto il traffico)
- Le destinazioni in cui pubblicare i dati del log di flusso

Nell'esempio seguente, viene creato un log di flusso che acquisisce il traffico accettato per l'interfaccia di rete per una delle istanze EC2 in una sottorete privata e pubblica i record del log di flusso in un bucket Amazon S3.




Nell'esempio seguente, un log di flusso acquisisce tutto il traffico per una sottorete e pubblica i record del log di flusso su Amazon Logs. CloudWatch Il log di flusso cattura il traffico per tutte le interfacce di rete nella sottorete.




Dopo aver creato un flusso di log, potrebbero essere necessari diversi minuti prima di iniziare a raccogliere dati e pubblicarli nelle destinazioni scelte. I log di flusso non acquisiscono flussi di log in tempo reale per le interfacce di rete. Per ulteriori informazioni, consulta Creazione di un log di flusso.

Se avvii un'istanza nella sottorete dopo aver creato un log di flusso per la sottorete o il VPC, creiamo un flusso di log (per CloudWatch Logs) o un oggetto file di log (per Amazon S3) per la nuova interfaccia di rete non appena c'è traffico di rete per l'interfaccia di rete.

È possibile creare log di flusso per interfacce di rete che vengono create da altri servizi AWS , ad esempio:

- Elastic Load Balancing
- Amazon RDS
- Amazon ElastiCache

- Amazon Redshift
- Amazon WorkSpaces
- Gateway NAT
- Gateway di transito

Indipendentemente dal tipo di interfaccia di rete, è necessario usare la console Amazon EC2 o l'API Amazon EC2 per creare un log di flusso per un'interfaccia di rete.

È possibile applicare tag ai log di flusso. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili. I tag consentono di organizzare i log di flusso, ad esempio per scopo o proprietario.

Se un log di flusso non è più necessario, puoi eliminarlo. L'eliminazione di un log di flusso disabilita il servizio del log di flusso per la risorsa in modo che nessun nuovo record del log di flusso viene creato o pubblicato. L'eliminazione di un log di flusso non elimina alcun dato del log di flusso esistente. Dopo aver eliminato un log di flusso, puoi eliminare i dati del log di flusso direttamente dalla destinazione quando hai finito di utilizzarla. Per ulteriori informazioni, consulta Eliminazione di un log di flusso.

## Record di log di flusso

Un record di log di flusso rappresenta un flusso di rete nel VPC. Per impostazione predefinita, ogni record acquisisce un flusso di traffico IP (Network Internet Protocol) (caratterizzato da 5 tuple in base all'interfaccia di rete) che si verifica all'interno di un intervallo di aggregazione, denominato anche finestra di acquisizione.

Ogni record è una stringa con campi separati da spazi. Un record include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

Quando crei un log di flusso, puoi utilizzare il formato predefinito oppure specificare un formato personalizzato.

Indice

## Intervallo di aggregazione

L'intervallo di aggregazione è il periodo di tempo durante il quale un particolare flusso viene acquisito e aggregato in un record di log di flusso. Per impostazione predefinita, l'intervallo di aggregazione massimo è di 10 minuti. Quando crei un log di flusso, puoi specificare facoltativamente un intervallo di aggregazione massimo di 1 minuto. I log di flusso con un intervallo di aggregazione massimo di 1 minuto producono un volume maggiore di record del log di flusso rispetto ai log di flusso con un intervallo di aggregazione massimo di 10 minuti.

Quando un'interfaccia di rete viene collegata a un'istanza basata su Nitro, l'intervallo di aggregazione è sempre pari o inferiore a 1 minuto, a prescindere dall'intervallo di aggregazione massimo specificato.

Dopo l'acquisizione dei dati entro un intervallo di aggregazione, è necessario più tempo per elaborare e pubblicare i dati su CloudWatch Logs o Amazon S3. Il servizio di log di flusso in genere consegna i CloudWatch log a Logs in circa 5 minuti e ad Amazon S3 in circa 10 minuti. Tuttavia, la consegna dei log avviene nel miglior modo possibile e i registri potrebbero essere ritardati oltre i tempi di consegna tipici.

## Formato predefinito

Con il formato predefinito, i record del log di flusso includono i campi versione 2, nell'ordine mostrato nella tabella campi disponibili . Non è possibile personalizzare o modificare il formato predefinito. Per acquisire i campi aggiuntivi o un diverso sottoinsieme di campi, specifica un formato personalizzato.

## Formato personalizzato

Con un formato personalizzato, è possibile specificare quali campi sono inclusi nei record del log di flusso e il relativo ordine. In questo modo è possibile creare log di flusso specifici per le proprie esigenze e omettere i campi non pertinenti. L'uso di un formato personalizzato può anche ridurre la necessità di processi separati per estrarre informazioni specifiche dai log di flusso pubblicati. Puoi specificare un numero qualsiasi di campi del log di flusso disponibili, ma devi specificarne almeno uno.

## Campi disponibili

Nella tabella seguente sono descritti tutti i campi disponibili per un record di log di flusso. La colonna Versione indica la versione dei log di flusso VPC in cui è stato introdotto il campo. Il formato predefinito include tutti i campi della versione 2 nello stesso ordine in cui sono riportati nella tabella.

Quando si pubblicano i dati del flusso di log su Amazon S3, il tipo di dati per i campi dipende dal formato del flusso di log. Se il formato è di testo normale, tutti i campi sono di tipo STRING. Se il formato è Parquet, vedere la tabella per i tipi di dati di campo.

Se un campo non è applicabile o non può essere calcolato per un record specifico, il record visualizza un simbolo "-" per tale voce. I campi dei metadati che non provengono direttamente dall'intestazione del pacchetto sono approssimazioni ottimali e i loro valori potrebbero essere mancanti o imprecisi.

| Campo | Descrizione | Version |
| --- | --- | --- |
| version | La versione dei log di flusso del VPC. Se usi il formato predefinito, la versione è 2. Se usi un formato personalizzato, la versione è quella più alta tra i campi specificati. Ad esempio, se specifichi solo i campi della versione 2, la versione sarà 2. Se specifichi una combinazione di campi dalle versioni 2, 3 e 4, la versione sarà 4.<br><br>Tipo di dati parquet: INT_32 | 2 |
| account-id | L'ID dell' AWS account del proprietario dell'interfaccia di rete di origine per la quale viene registrato il traffico. Se l'interfaccia di rete viene creata da un AWS servizio, ad esempio quando si crea un endpoint VPC o un Network Load Balancer, il record potrebbe essere unknown visualizzato per questo campo.<br><br>Tipo di dati Parquet: STRING | 2 |
| interface-id | L'ID dell'interfaccia di rete per la quale il traffico viene registrato.<br><br>Tipo di dati parquet: STRING | 2 |
| srcaddr | L'indirizzo di origine per il traffico in entrata oppure l'indirizzo IPv4 o IPv6 dell'interfaccia rete per il traffico in uscita sull'interfaccia di rete. L'indirizzo IPv4 dell'interfaccia di rete è sempre il suo indirizzo IPv4 privato. Consulta anche pkt-srcaddr.<br><br>Tipo di dati parquet: STRING | 2 |
| dstaddr | L'indirizzo di destinazione per il traffico in uscita oppure l'indirizzo IPv4 o IPv6 dell'interfaccia rete per il traffico in entrata sull'inte | 2 |

| Campo | Descrizione | Version |
| --- | --- | --- |
| | rfaccia di rete. L'indirizzo IPv4 dell'interfaccia di rete è sempre il suo indirizzo IPv4 privato. Consulta anche pkt-dstaddr.<br><br>Tipo di dati parquet: STRING | |
| srcport | La porta di origine del traffico.<br><br>Tipo di dati parquet: INT_32 | 2 |
| dstport | La porta di destinazione del traffico.<br><br>Tipo di dati Parquet: INT_32 | 2 |
| protocol | Il numero di protocollo IANA del traffico. Per ulteriori informazioni, consulta la sezione relativa ai numeri di protocollo Internet assegnati.<br><br>Tipo di dati parquet: INT_32 | 2 |
| packets | Il numero di pacchetti trasferiti durante il flusso.<br><br>Tipo di dati parquet: INT_64 | 2 |
| bytes | Il numero di byte trasferiti durante il flusso.<br><br>Tipo di dati Parquet: INT_64 | 2 |
| start | L'ora, in secondi Unix, di ricezione del primo pacchetto del flusso all'interno dell'intervallo di aggregazione. Potrebbe essere fino a 60 secondi dopo che il pacchetto è stato trasmesso o ricevuto sull'interfaccia di rete.<br><br>Tipo di dati parquet: INT_64 | 2 |

| Campo | Descrizione | Version |
| --- | --- | --- |
| end | L'ora, in secondi Unix, in cui l'ultimo pacchetto del flusso è stato ricevuto entro l'intervallo di aggregazione. Potrebbe essere fino a 60 secondi dopo che il pacchetto è stato trasmesso o ricevuto sull'interfaccia di rete.<br><br>Tipo di dati parquet: INT_64 | 2 |
| action | L'operazione associata al traffico:<br><br>• ACCEPT - Il traffico è stato accettato.<br>• REJECT - Il traffico è stato respinto. Ad esempio, il traffico non era consentito dai gruppi di sicurezza o dalle ACL di rete oppure i pacchetti sono arrivati dopo la chiusura della connessione.<br><br>Tipo di dati Parquet: STRING | 2 |
| log-status | Lo stato di registrazione del log di flusso:<br><br>• OK: i dati vengono registrati normalmente nelle destinazioni scelte.<br>• NODATA: non vi è alcun traffico di rete da o per l'interfaccia di rete durante l'intervallo di aggregazione.<br>• SKIPDATA: alcuni record del log di flusso sono stati ignorati durante l'intervallo di aggregazione. Ciò può essere causato da un vincolo di capacità interna o da un errore interno.<br><br>Tipo di dati Parquet: STRING | 2 |
| vpc-id | L'ID del VPC che contiene l'interfaccia di rete per cui viene registrato il traffico.<br><br>Tipo di dati parquet: STRING | 3 |

| Campo | Descrizione | Version |
| --- | --- | --- |
| subnet-id | L'ID della subnet che contiene l'interfaccia di rete per cui viene registrato il traffico.<br><br>Tipo di dati parquet: STRING | 3 |
| instance-id | L'ID dell'istanza associata all'interfaccia di rete per cui viene registrato il traffico, se l'istanza appartiene a te. Restituisce un simbolo '-' per un'interfaccia di rete gestita dal richiedente, ad esempio l'interfaccia di rete per un gateway NAT.<br><br>Tipo di dati parquet: STRING | 3 |

| Campo | Descrizione | Version |
| --- | --- | --- |
| tcp-flags | Il valore bitmask per i seguenti flag TCP:<br>• FIN - 1<br>• SYN - 2<br>• RST - 4<br>• SYN-ACK - 18<br><br>Se non viene registrato alcun flag supportato, il valore del flag TCP è 0. Ad esempio, siccome tcp-flags non supporta la registrazione di log dei flag ACK o PSH, i record per il traffico con questi flag non supportati restituiranno un valore tcp-flags 0. Tuttavia, se un flag non supportato è accompagnato da un flag supportato, riportere mo il valore del flag supportato. Ad esempio, se ACK fa parte di SYN-ACK, riporta 18. Inoltre, se esiste un record come SYN+ECE, siccome SYN è un flag supportato ed ECE no, il valore del flag TCP è 2. Se per qualche motivo la combinazione di flag non è valida e il valore non può essere calcolato, il valore è '-'. Se non viene inviato alcun flag, il valore del flag TCP è 0.<br><br>I flag TCP sono introdotti da un operatore OR durante l'intervallo di aggregazione. Per le connessioni brevi, i flag possono essere impostati sulla stessa riga nel record del log di flusso, ad esempio 19 per SYN-ACK e FIN e 3 per SYN e FIN. Per un esempio, consulta Sequenza di flag TCP.<br><br>Per informazioni generali sui flag TCP (come il significato di flag come FIN, SYN e ACK), consulta Struttura del segmento TCP su Wikipedia.<br><br>Tipo di dati parquet: INT_32 | 3 |
| type | Il tipo di traffico. I valori possibili sono: IPv4 \| IPv6 \| EFA. Per ulteriori informazioni, consulta Elastic Fabric Adapter (EFA).<br><br>Tipo di dati parquet: STRING | 3 |

| Campo | Descrizione | Version |
| --- | --- | --- |
| pkt-srcaddr | L'indirizzo IP di origine a livello di pacchetto (originale) del traffico. Usa questo campo con il campo srcaddr per distinguere l'indiriz zo IP di un livello intermedio su cui fluisce il traffico e l'indirizzo IP di origine originale del traffico. Ad esempio, quando il traffico passa attraverso un'interfaccia di rete per un gateway NAT o quando l'indirizzo IP di un pod in Amazon EKS è diverso dall'indi rizzo IP dell'interfaccia di rete del nodo dell'istanza in cui il pod è in esecuzione (per la comunicazione all'interno di un VPC).<br><br>Tipo di dati parquet: STRING | 3 |
| pkt-dstaddr | L'indirizzo IP di destinazione a livello di pacchetto (originale) per il traffico. Usa questo campo con il campo dstaddr per distingue re l'indirizzo IP di un livello intermedio su cui fluisce il traffico e l'indirizzo IP di destinazione finale del traffico. Ad esempio, quando il traffico passa attraverso un'interfaccia di rete per un gateway NAT o quando l'indirizzo IP di un pod in Amazon EKS è diverso dall'indi rizzo IP dell'interfaccia di rete del nodo dell'istanza in cui il pod è in esecuzione (per la comunicazione all'interno di un VPC).<br><br>Tipo di dati parquet: STRING | 3 |
| region | Regione che contiene l'interfaccia di rete per la quale viene registrat o il traffico.<br><br>Tipo di dati parquet: STRING | 4 |
| az-id | ID della zona di disponibilità che contiene l'interfaccia di rete per la quale viene registrato il traffico. Se il traffico proviene da una posizione secondaria, il record visualizza un simbolo '-' per questo campo.<br><br>Tipo di dati parquet: STRING | 4 |

| Campo | Descrizione | Version |
| --- | --- | --- |
| sublocation-type | Il tipo di posizione secondaria restituito nel campo sublocation-id. I valori possibili sono: wavelength \| outpost \| localzone. Se il traffico non proviene da una posizione secondaria, il record visualizza un simbolo '-' per questo campo.<br><br>Tipo di dati parquet: STRING | 4 |
| sublocation-id | L'ID della sottorete che contiene l'interfaccia di rete per cui viene registrato il traffico. Se il traffico non proviene da una posizione secondaria, il record visualizza un simbolo '-' per questo campo.<br><br>Tipo di dati parquet: STRING | 4 |
| pkt-src-aws-service | Il nome del sottoinsieme di intervalli di indirizzi IP per il pkt-srcaddr campo, se l'indirizzo IP di origine è per un servizio. AWS Se pkt-srcaddr appartiene a un intervallo sovrapposto, pkt-src-aws-service mostrerà solo uno dei codici di servizio. AWS I valori possibili sono: AMAZON \| AMAZON_APPFLOW \| AMAZON_CONNECT \| API_GATEWAY \| CHIME_MEETINGS \| CHIME_VOICECONNECTOR \| CLOUD9 \| CLOUDFRONT \| CODEBUILD \| DYNAMODB \| EBS \| EC2 \| EC2_INSTANCE_CONNECT \| GLOBALACCELERATOR \| KINESIS_VIDEO_STREAMS \| ROUTE53 \| ROUTE53_HEALTHCHECKS \| ROUTE53_HEALTHCHECKS_PUBLISHING \| ROUTE53_RESOLVER \| S3 \| WORKSPACES_GATEWAYS.<br><br>Tipo di dati parquet: STRING | 5 |
| pkt-dst-aws-service | Il nome del sottoinsieme di intervalli di indirizzi IP per il pkt-dstaddr campo, se l'indirizzo IP di destinazione è per un servizio. AWS Per un elenco di possibili valori, consulta il campo pkt-src-aws-service.<br><br>Tipo di dati parquet: STRING | 5 |
| flow-direction | La direzione del flusso rispetto all'interfaccia in cui viene catturato il traffico. I valori possibili sono: ingress \| egress.<br><br>Tipo di dati parquet: STRING | 5 |

| Campo | Descrizione | Version |
| --- | --- | --- |
| traffic-path | Il percorso che porta il traffico in uscita verso la destinazione. Per determinare se il traffico è in uscita, controlla il campo flow-dire ction. I valori possibili sono quelli riportati di seguito. Se nessuno dei valori viene applicato, il campo è impostato su -.<br>• 1 - Tramite un'altra risorsa nello stesso VPC, comprese le risorse che creano un'interfaccia di rete nel VPC<br>• 2 - Tramite un gateway Internet o un endpoint VPC gateway<br>• 3 - Tramite un gateway privato virtuale<br>• 4 - Tramite una connessione di peering VPC all'interno della regione<br>• 5 - Tramite una connessione di peering VPC tra regioni<br>• 6 - Tramite un gateway locale<br>• 7 — Tramite un endpoint VPC del gateway (solo istanze basate su Nitro)<br>• 8 — Tramite un gateway Internet (solo istanze basate su Nitro)<br><br>Tipo di dati parquet: INT_32 | 5 |
| ecs-cluster-arn | AWS Nome risorsa (ARN) del cluster ECS se il traffico proviene da un'attività ECS in esecuzione. Per includere questo campo nel tuo abbonamento, devi essere autorizzato a chiamare ecs:. ListClusters<br>Tipo di dati Parquet: STRING | 7 |
| ecs-cluster-name | Nome del cluster ECS se il traffico proviene da un'attività ECS in esecuzione. Per includere questo campo nel tuo abbonamento, hai bisogno del permesso di chiamare ecs:. ListClusters<br>Tipo di dati Parquet: STRING | 7 |

| Campo | Descrizione | Version |
| --- | --- | --- |
| ecs-container-instance-arn | ARN dell'istanza del contenitore ECS se il traffico proviene da un'attività ECS in esecuzione su un'istanza EC2. Se il fornitore di capacità è AWS Fargate, questo campo sarà '-'. Per includere questo campo nell'abbonamento, è necessaria l'autorizzazione a chiamare ecs: ListClusters ed ecs: Instances. ListContainer<br>Tipo di dati Parquet: STRING | 7 |
| ecs-container-instance-id | ID dell'istanza del contenitore ECS se il traffico proviene da un'attività ECS in esecuzione su un'istanza EC2. Se il fornitore di capacità è AWS Fargate, questo campo sarà '-'. Per includere questo campo nell'abbonamento, è necessaria l'autorizzazione a chiamare ecs: ListClusters ed ecs: Instances. ListContainer<br>Tipo di dati Parquet: STRING | 7 |
| ecs-container-id | ID di runtime Docker del contenitore se il traffico proviene da un'attività ECS in esecuzione. Se ci sono uno o più contenitori nell'attività ECS, questo sarà l'ID di runtime docker del primo contenitore. Per includere questo campo nel tuo abbonamento, hai bisogno del permesso di chiamare ecs:. ListClusters<br>Tipo di dati Parquet: STRING | 7 |
| ecs-second-container-id | ID di runtime Docker del contenitore se il traffico proviene da un'attività ECS in esecuzione. Se nell'attività ECS sono presenti più contenitori, questo sarà l'ID di runtime Docker del secondo contenitore. Per includere questo campo nel tuo abbonamento, devi essere autorizzato a chiamare ecs:. ListClusters<br>Tipo di dati Parquet: STRING | 7 |
| nome-servizio ecs | Nome del servizio ECS se il traffico proviene da un'attività ECS in esecuzione e l'attività ECS viene avviata da un servizio ECS. Se l'attività ECS non viene avviata da un servizio ECS, questo campo sarà '-'. Per includere questo campo nel tuo abbonamento, devi essere autorizzato a chiamare ecs: ed ecs:. ListClusters ListServices<br>Tipo di dati Parquet: STRING | 7 |

| Campo | Descrizione | Version |
| --- | --- | --- |
| ecs-task-definitio n-arn | ARN della definizione dell'attività ECS se il traffico proviene da un'attività ECS in esecuzione. Per includere questo campo nel tuo abbonamento, devi essere autorizzato a chiamare ecs: ed ecs: ListClusters ListTaskDefinitions<br>Tipo di dati Parquet: STRING | 7 |
| ecs-task-arn | ARN dell'attività ECS se il traffico proviene da un'attività ECS in esecuzione. Per includere questo campo nel tuo abbonamento, devi essere autorizzato a chiamare ecs: ed ecs:ListClusters . ListTasks<br>Tipo di dati Parquet: STRING | 7 |
| ecs-task-id | ID dell'attività ECS se il traffico proviene da un'attività ECS in esecuzione. Per includere questo campo nel tuo abbonamento, devi essere autorizzato a chiamare ecs: ListClusters ed ecs:. ListTasks<br>Tipo di dati Parquet: STRING | 7 |

## Esempi di record di log di flusso

Di seguito sono riportati alcuni esempi di record di log di flusso che acquisiscono specifici flussi di traffico.

Per informazioni sul formato dei record di log di flusso, vedere Record di log di flusso. Per informazioni sulla creazione di log di flusso, consulta Utilizzo dei log di flusso.

Indice

## Traffico accettato e rifiutato

Di seguito sono riportati esempi di record di log di flusso predefiniti.

In questo esempio, il traffico SSH (porta di destinazione 22, protocollo TCP) dall'indirizzo IP 172.31.16.139 all'interfaccia di rete con indirizzo IP privato è 172.31.16.21 e l'ID eni-1235b8ca123456789 nell'account 123456789010 era consentito.

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249
 1418530010 1418530070 ACCEPT OK
```

In questo esempio, il traffico RDP (porta di destinazione 3389, protocollo TCP) all'interfaccia di rete eni-1235b8ca123456789 nell'account 123456789010 è stato rifiutato.

```
2 123456789010 eni-1235b8ca123456789 172.31.9.69 172.31.9.12 49761 3389 6 20 4249
 1418530010 1418530070 REJECT OK
```

## Nessun dato e record ignorati

Di seguito sono riportati esempi di record di log di flusso predefiniti.

In questo esempio non è stato registrato alcun dato durante l'intervallo di aggregazione.

```
2 123456789010 eni-1235b8ca123456789 - - - - - - - 1431280876 1431280934 - NODATA
```

In questo esempio, i record sono stati ignorati durante l'intervallo di aggregazione. VPC Flow Logs salta i record quando non è in grado di acquisire i dati del flusso di log durante un intervallo di aggregazione perché supera la capacità interna. Un singolo registro ignorato può rappresentare flussi multipli che non sono stati acquisiti per l'interfaccia di rete durante l'intervallo di aggregazione.

```
2 123456789010 eni-11111111aaaaaaaaa - - - - - - - 1431280876 1431280934 - SKIPDATA
```

## Regole del gruppo di sicurezza e della lista di controllo accessi di rete

Se stai utilizzando log di flusso per diagnosticare regole del gruppo di sicurezza o della lista di controllo accessi di rete troppo restrittive o permissive, considera che le risorse sono stateless. I gruppi di sicurezza sono stateful: ovvero le risposte a traffico consentito sono consentite, anche se le regole nel gruppo di sicurezza non lo permettono. Viceversa, le liste di controllo accessi di rete sono stateless, pertanto le risposte al traffico consentito sono soggette alle regole della lista di controllo accessi di rete.

Ad esempio, il comando ping viene utilizzato dal computer di casa (con indirizzo IP 203.0.113.12) all'istanza (con indirizzo IP privato dell'interfaccia di rete 172.31.16.139). Il traffico ICMP è consentito dalle regole in ingresso del gruppo di sicurezza, ma non dalle regole in uscita. Dato che i gruppi di sicurezza sono stateful, il ping di risposta dall'istanza è consentito. La lista di controllo accessi di rete permette traffico ICMP in entrata ma non traffico ICMP in uscita. Poiché le liste di controllo degli accessi di rete sono stateless, il ping di risposta viene interrotto e non raggiunge il computer di casa. In un log di flusso predefinito, questo viene visualizzato come due record di log di flusso:

- Un record ACCEPT per il ping originario è stato consentito dalla lista di controllo accessi di rete E dal gruppo di sicurezza, pertanto può raggiungere l'istanza.
- Un record REJECT per il ping di risposta rifiutato dalla lista di controllo accessi di rete.

```
2 123456789010 eni-1235b8ca123456789 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027
 1432917142 ACCEPT OK
```

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094
 1432917142 REJECT OK
```

Se la lista di controllo accessi di rete permette traffico ICMP in uscita, il log di flusso visualizza due record ACCEPT (uno per il ping originario e uno per il ping di risposta). Se il gruppo di sicurezza nega il traffico ICMP in entrata, il log di flusso visualizza un singolo record REJECT, perché il traffico non può raggiungere l'istanza.

## Traffico IPv6

Di seguito è riportato un esempio di record del log di flusso predefinito. Nell'esempio, è stato consentito il traffico SSH (porta 22) dall'indirizzo IPv6 2001:db8:1234:a100:8d6e:3477:df66:f105 all'interfaccia di rete eni-1235b8ca123456789 nell'account 123456789010.

```
2 123456789010 eni-1235b8ca123456789 2001:db8:1234:a100:8d6e:3477:df66:f105
 2001:db8:1234:a102:3304:8879:34cf:4071 34892 22 6 54 8855 1477913708 1477913820 ACCEPT
 OK
```

## Sequenza di flag TCP

Questa sezione contiene esempi di log di flusso personalizzati che acquisiscono i campi seguenti nell'ordine riportato di seguito.

```
version vpc-id subnet-id instance-id interface-id account-id type srcaddr dstaddr
 srcport dstport pkt-srcaddr pkt-dstaddr protocol bytes packets start end action tcp-
flags log-status
```

Il campo negli esempi di tcp-flags questa sezione è rappresentato dal valore nel log di flusso. second-to-last I flag TCP possono essere utili per identificare la direzione del traffico, ad esempio per sapere quale server ha inizializzato la connessione.

> **Note**
>
> Per ulteriori informazioni sull'opzione tcp-flags e per la spiegazione di ciascuno dei flag TCP, consulta Campi disponibili.

Nei record seguenti (avvio alle 7:47:55 PM e fine alle 7:48:53 PM), sono state avviate due connessioni da un client a un server in esecuzione sulla porta 5001. Il server ha ricevuto due flag SYN (2) dal client da diverse porte di origine sul client (43416 e 43418). Per ogni SYN, è stato inviato un SYN-ACK dal server al client (18) sulla porta corrispondente.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43416 5001
 52.213.180.42 10.0.0.62 6 568 8 1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43416 10.0.0.62
 52.213.180.42 6 376 7 1566848875 1566848933 ACCEPT 18 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 100701 70 1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 632 12 1566848875 1566848933 ACCEPT 18 OK
```

Nel secondo intervallo di aggregazione, una delle connessioni stabilite nel flusso precedente viene chiusa. Il client ha inviato un flag FIN (1) al server per la connessione sulla porta 43418. Il server ha inviato un FIN al client sulla porta 43418.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 63388 1219 1566848933 1566849113 ACCEPT 1 OK
```

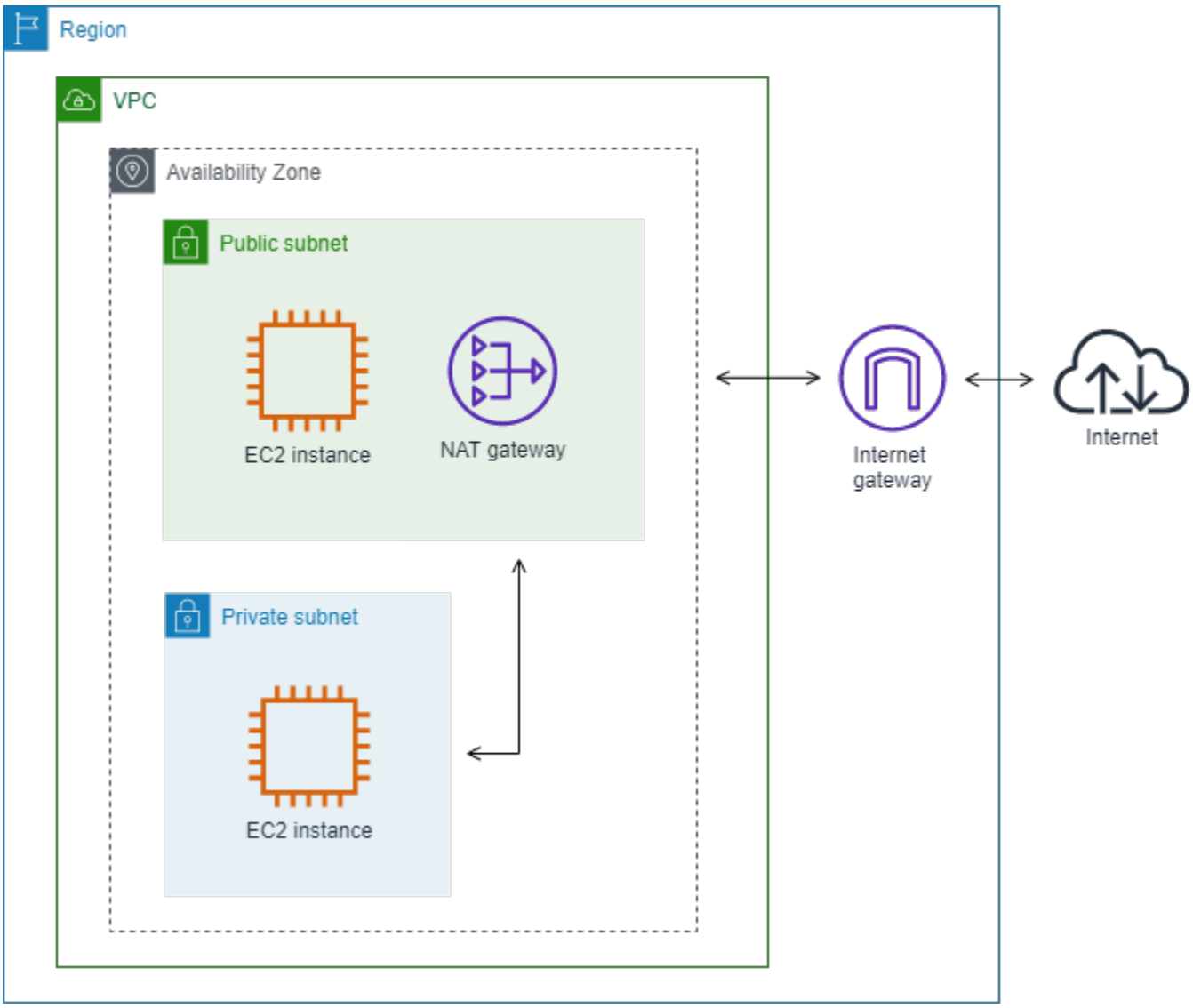
```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 23294588 15774 1566848933 1566849113 ACCEPT 1 OK
```

Per le connessioni brevi (ad esempio di alcuni secondi) che vengono aperte e chiuse entro un unico intervallo di aggregazione, i flag potrebbero essere impostati sulla stessa riga nel record di log di flusso per il flusso di traffico nella stessa direzione. Nell'esempio seguente, la connessione viene stabilita e terminata all'interno dello stesso intervallo di aggregazione. Nella prima riga, il valore del flag TCP è 3, che indica la presenza di un SYN e di un messaggio FIN inviato dal client al server. Nella seconda riga, il valore del flag TCP è 19, che indica la presenza di un SYN-ACK e di un messaggio FIN inviato dal server al client.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43638 5001
 52.213.180.42 10.0.0.62 6 1260 17 1566933133 1566933193 ACCEPT 3 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43638  10.0.0.62
 52.213.180.42 6 967 14 1566933133 1566933193 ACCEPT 19 OK
```

## Traffico tramite un gateway NAT

In questo esempio, un'istanza in una sottorete privata accede a Internet tramite un gateway NAT situato in una sottorete pubblica.




Il seguente log di flusso personalizzato per l'interfaccia di rete del gateway NAT acquisisce i campi seguenti nell'ordine seguente.

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

Il log di flusso mostra il flusso di traffico dall'indirizzo IP dell'istanza (10.0.1.5) tramite l'interfaccia di rete del gateway NAT fino a un host su Internet (203.0.113.5). L'interfaccia di rete del gateway NAT è un'interfaccia di rete gestita dal richiedente, per cui il record del log di flusso visualizza un simbolo '-' per il campo instance-id. La riga seguente mostra il traffico dall'istanza di origine all'interfaccia di rete del gateway NAT. I valori per i campi dstaddr e pkt-dstaddr sono diversi. Il campo dstaddr visualizza l'indirizzo IP privato dell'interfaccia di rete del gateway NAT e il campo pkt-dstaddr visualizza l'indirizzo IP di destinazione finale dell'host su Internet.

```
- eni-1235b8ca123456789 10.0.1.5 10.0.0.220 10.0.1.5 203.0.113.5
```

Le due righe successive mostrano il traffico dall'interfaccia di rete del gateway NAT all'host target su Internet e il traffico di risposta dall'host all'interfaccia di rete del gateway NAT.

```
- eni-1235b8ca123456789 10.0.0.220 203.0.113.5 10.0.0.220 203.0.113.5
- eni-1235b8ca123456789 203.0.113.5 10.0.0.220 203.0.113.5 10.0.0.220
```

La riga seguente mostra il traffico di risposta dall'interfaccia di rete del gateway NAT all'istanza di origine. I valori per i campi srcaddr e pkt-srcaddr sono diversi. Il campo srcaddr visualizza l'indirizzo IP privato dell'interfaccia di rete del gateway NAT e il campo pkt-srcaddr visualizza l'indirizzo IP dell'host su Internet.

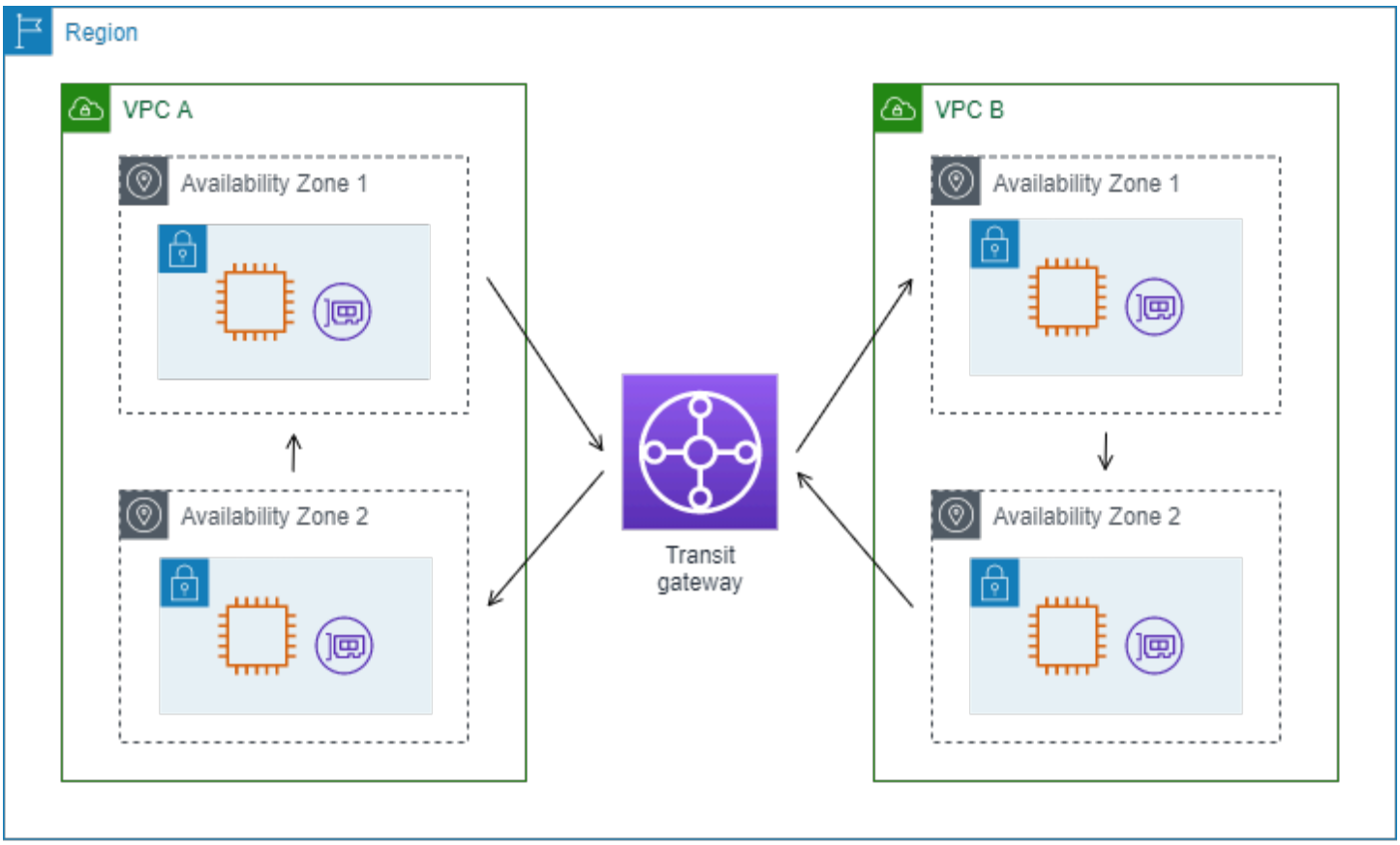
```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

Per creare un altro log di flusso personalizzato, puoi usare lo stesso set di campi riportato sopra. Puoi creare il log di flusso per l'interfaccia di rete per l'istanza nella sottorete privata. In questo caso, il campo instance-id restituisce l'ID dell'istanza associata all'interfaccia di rete e non c'è differenza tra i campi dstaddr e pkt-dstaddr e i campi srcaddr e pkt-srcaddr. A differenza dell'interfaccia di rete per il gateway NAT, questa non è un'interfaccia di rete intermedia per il traffico.

```
i-01234567890123456 eni-1111aaaa2222bbbb3 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
 #Traffic from the source instance to host on the internet
i-01234567890123456 eni-1111aaaa2222bbbb3 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
 #Response traffic from host on the internet to the source instance
```

## Traffico tramite un gateway di transito

In questo esempio, un client in VPC A si connette a un server Web in VPC B tramite un gateway di transito. Il client e il server sono in diverse zone di disponibilità. Il traffico arriva al server nel VPC B utilizzando un ID dell'interfaccia di rete elastica (in questo esempio, supponiamo che l'ID sia eni-1111111111111111) e lascia il VPC B usandone un altro (ad esempio, eni-22222222222222222).




Puoi creare un log di flusso personalizzato per VPC B con il formato seguente.

```
version interface-id account-id vpc-id subnet-id instance-id srcaddr dstaddr srcport
 dstport protocol tcp-flags type pkt-srcaddr pkt-dstaddr action log-status
```

Le seguenti righe dei record di file di log dimostrano il flusso del traffico sull'interfaccia di rete per il server Web. La prima riga è il traffico di richiesta dal client e l'ultima riga è il traffico di risposta dal server Web.

```
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.20.33.164 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164
 10.40.2.236 ACCEPT OK
...
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.40.2.236 10.20.33.164 80 39812 6 19 IPv4 10.40.2.236
 10.20.33.164 ACCEPT OK
```

La riga seguente è il traffico di richiesta su eni-11111111111111111, un'interfaccia di rete gestita dal richiedente per il gateway di transito nella sottorete subnet-11111111aaaaaaaaa. Nel record del

log di flusso, pertanto, è presente un simbolo '-' per il campo instance-id. Il campo srcaddr visualizza l'indirizzo IP privato dell'interfaccia di rete del gateway di transito e il campo pkt-srcaddr visualizza l'indirizzo IP di origine del client nel VPC A.

```
3 eni-11111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaaa -
 10.40.1.175 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164 10.40.2.236 ACCEPT OK
```

La riga seguente è il traffico di risposta su eni-22222222222222222, un'interfaccia di rete gestita dal richiedente per il gateway di transito nella sottorete subnet-22222222bbbbbbbbb. Il campo dstaddr visualizza l'indirizzo IP privato dell'interfaccia di rete dell'interfaccia di rete del gateway di transito e il campo pkt-dstaddr visualizza l'indirizzo IP del client nel VPC A.

```
3 eni-22222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb -
 10.40.2.236 10.40.2.31 80 39812 6 19 IPv4 10.40.2.236 10.20.33.164 ACCEPT OK
```

## Nome del servizio, percorso di traffico e direzione del flusso

Di seguito è riportato un esempio dei campi per un record di log di flusso personalizzato.

```
version srcaddr dstaddr srcport dstport protocol start end type packets bytes account-
id vpc-id subnet-id instance-id interface-id region az-id sublocation-type sublocation-
id action tcp-flags pkt-srcaddr pkt-dstaddr pkt-src-aws-service pkt-dst-aws-service
 traffic-path flow-direction log-status
```

Nell'esempio seguente, la versione è 5 perché i record includono campi della versione 5. Un'istanza EC2 chiama il servizio Amazon S3. I log di flusso vengono acquisiti sull'interfaccia di rete per l'istanza. Il primo record ha una direzione di flusso pari a ingress mentre il secondo record ha una direzione di flusso pari a egress. Per il record egress, traffic-path è 8 e indica che il traffico passa attraverso un gateway Internet. Il campo traffic-path non è supportato per il traffico ingress. Quando pkt-srcaddr o pkt-dstaddr è un indirizzo IP pubblico, viene visualizzato il nome del servizio.

```
5 52.95.128.179 10.0.0.71 80 34210 6 1616729292 1616729349 IPv4 14 15044
 123456789012 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b
 eni-1235b8ca123456789 ap-southeast-2 apse2-az3 - - ACCEPT 19 52.95.128.179 10.0.0.71
 S3 - - ingress OK
5 10.0.0.71 52.95.128.179 34210 80 6 1616729292 1616729349 IPv4 7 471 123456789012 vpc-
abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b eni-1235b8ca123456789
 ap-southeast-2 apse2-az3 - - ACCEPT 3 10.0.0.71 52.95.128.179 - S3 8 egress OK
```

# Limitazioni del log di flusso

Per utilizzare i log di flusso, occorre considerare le seguenti limitazioni:

- Non è possibile abilitare log di flusso per VPC che sono collegati in peering al VPC a meno che il VPC di peering non si trovi nel proprio account.
- Dopo avere creato un log di flusso, non è possibile modificarne la configurazione o cambiare il formato del registro di log di flusso. Ad esempio, non è possibile associare un ruolo IAM diverso al log di flusso o aggiungere o rimuovere campi nel record del log di flusso. Invece, è possibile eliminare il log di flusso e crearne uno nuovo con la configurazione richiesta.
- Se l'interfaccia di rete dispone di più indirizzi IPv4 e il traffico viene inviato a un indirizzo IPv4 privato secondario, il log di flusso visualizza l'indirizzo IPv4 privato principale nel campo `dstaddr`. Per acquisire l'indirizzo IP di destinazione originale, crea un log di flusso con il campo `pkt-dstaddr`.
- Se il traffico viene inviato a un'interfaccia di rete e la destinazione non è uno degli indirizzi IP dell'interfaccia di rete, il log di flusso visualizza l'indirizzo IPv4 privato principale nel campo `dstaddr`. Per acquisire l'indirizzo IP di destinazione originale, crea un log di flusso con il campo `pkt-dstaddr`.
- Se il traffico proviene da un'interfaccia di rete e l'origine non è uno degli indirizzi IP dell'interfaccia di rete, il log di flusso visualizza l'indirizzo IPv4 privato principale nel campo `srcaddr`. Per acquisire l'indirizzo IP di origine originale, crea un log di flusso con il campo `pkt-srcaddr`.
- Se il traffico viene inviato a/da un'interfaccia di rete, i campi `srcaddr` e `dstaddr` nel log di flusso visualizzano sempre l'indirizzo IPv4 privato principale, indipendentemente dall'origine o dalla destinazione del pacchetto. Per acquisire l'origine o la destinazione del pacchetto, crea un log di flusso con i campi `pkt-srcaddr` e `pkt-dstaddr`.
- Quando l'interfaccia di rete viene collegata a un'istanza basata su Nitro, l'intervallo di aggregazione è sempre pari o inferiore a 1 minuto, a prescindere dall'intervallo di aggregazione massimo specificato.

I log di flusso non acquisiscono tutto il traffico IP. I seguenti tipi di traffico non vengono registrati:

- Traffico generato da istanze quando contattano il server Amazon DNS. Se si utilizza il proprio server DNS, tutto il traffico al server DNS viene registrato.
- Traffico generato da un'istanza Windows per attivazione licenza Windows Amazon.
- Traffico da e per `169.254.169.254` per metadati istanza.

- Traffico da e per `169.254.169.123` per Amazon Time Sync Service.
- Traffico DHCP.
- Traffico con mirroring.
- Traffico all'indirizzo IP riservato per il router VPC predefinito.
- Traffico tra un'interfaccia di rete endpoint e un'interfaccia di rete Network Load Balancer.

Limitazioni specifiche dei campi ECS disponibili nella versione 7:

- Per creare sottoscrizioni ai log di flusso con campi ECS, l'account deve contenere almeno un cluster ECS.
- I campi ECS non vengono calcolati se le attività ECS sottostanti non sono di proprietà del proprietario dell'abbonamento al log di flusso. Ad esempio, se condividi una subnet (`SubnetA`) con un altro account (`AccountB`) e poi crei un abbonamento al log di flusso per`SubnetA`, se `AccountB` avvia attività ECS nella sottorete condivisa, l'abbonamento riceverà i registri del traffico dalle attività ECS avviate da, `AccountB` ma i campi ECS per questi log non verranno calcolati a causa di problemi di sicurezza.
- Se crei abbonamenti ai log di flusso con campi ECS a livello di risorsa VPC/Subnet, tutto il traffico generato per le interfacce di rete non ECS verrà distribuito anche per i tuoi abbonamenti. I valori per i campi ECS saranno '-' per il traffico IP non ECS. Ad esempio, hai una subnet (`subnet-000000`) e crei un abbonamento al log di flusso per questa sottorete con ECS fields (). `fl-00000000` In`subnet-000000`, avvii un'istanza EC2 (`i-0000000`) connessa a Internet e che genera attivamente traffico IP. Puoi anche avviare un'attività ECS (`ECS-Task-1`) in esecuzione nella stessa sottorete. Poiché entrambe `i-0000000` `ECS-Task-1` generano traffico IP, l'abbonamento al log di flusso `fl-00000000` fornirà i registri di traffico per entrambe le entità. Tuttavia, `ECS-Task-1` disporrà solo dei metadati ECS effettivi per i campi ECS che hai incluso nel tuo LogFormat. Per il traffico `i-0000000` correlato, questi campi avranno il valore '-'.
- `ecs-container-ide` `ecs-second-container-id` vengono ordinati quando il servizio VPC Flow Logs li riceve dal flusso di eventi ECS. Non è garantito che siano nello stesso ordine in cui vengono visualizzati sulla console ECS o nella chiamata API. DescribeTask Se un contenitore entra nello stato STOPED mentre l'attività è ancora in esecuzione, potrebbe continuare a comparire nel registro.
- I metadati ECS e i registri del traffico IP provengono da due fonti diverse. Iniziamo a calcolare il traffico ECS non appena otteniamo tutte le informazioni richieste dalle dipendenze upstream. Dopo aver iniziato una nuova attività, iniziamo a calcolare i campi ECS 1) quando riceviamo il traffico IP per l'interfaccia di rete sottostante e 2) quando riceviamo l'evento ECS che contiene i metadati

dell'attività ECS per indicare che l'attività è ora in esecuzione. Dopo aver interrotto un'attività, interrompiamo il calcolo dei campi ECS 1) quando non riceviamo più traffico IP per l'interfaccia di rete sottostante o riceviamo traffico IP che viene ritardato per più di un giorno e 2) quando riceviamo l'evento ECS che contiene i metadati per l'attività ECS per indicare che l'attività non è più in esecuzione.

- Sono supportate solo le attività ECS avviate in modalità rete. `awsvpc`

## Prezzi

Gli addebiti per l'importazione dei dati e l'archiviazione per i log distribuiti vengono applicati quando si pubblicano i log di flusso. Per ulteriori informazioni sui prezzi per la pubblicazione dei registri di vendita, apri Amazon CloudWatch Pricing, seleziona Log e trova Vended Logs.

Per tenere traccia degli addebiti derivanti dalla pubblicazione dei log di flusso, puoi applicare tag di allocazione dei costi alla risorsa di destinazione. Successivamente, il rapporto sull'allocazione AWS dei costi include l'utilizzo e i costi aggregati in base a questi tag. Puoi applicare i tag che rappresentano categorie di business (come centri di costo, nomi di applicazioni o proprietari) per organizzare i costi. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Uso dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .
- Contrassegna i gruppi di log in Amazon CloudWatch Logs nella Amazon CloudWatch Logs User Guide
- Utilizzo dei tag dei bucket S3 per l'allocazione dei costi nella Guida per l'utente di Amazon Simple Storage Service
- Taggare i flussi di distribuzione nella Amazon Data Firehose Developer Guide

## Utilizzo dei log di flusso

Puoi lavorare con i log di flusso utilizzando le console di Amazon EC2 e Amazon VPC.

Attività

- Controllo dell'utilizzo dei log di flusso
- Creazione di un log di flusso
- Visualizzazione di un log di flusso
- Tagging di un log di flusso

- Eliminazione di un log di flusso
- Panoramica su API e CLI

## Controllo dell'utilizzo dei log di flusso

Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per utilizzare log di flusso. Puoi creare un ruolo IAM con una policy collegata che concede agli utenti le autorizzazioni per creare, descrivere ed eliminare log di flusso.

Di seguito è riportata una policy di esempio che concede agli utenti autorizzazioni complete per creare, descrivere ed eliminare log di flusso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

Per ulteriori informazioni, consulta the section called “Come funziona Amazon VPC con IAM”.

## Creazione di un log di flusso

È possibile creare log di flusso per VPC, sottoreti o interfacce di rete. Quando si crea un log di flusso, è necessario specificare una destinazione per il log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- the section called “Crea un log di flusso da pubblicare su Logs CloudWatch ”
- the section called “Creazione di un log di flusso che pubblica in Amazon S3”
- the section called “Crea un log di flusso da pubblicare su Amazon Data Firehose”

## Visualizzazione di un log di flusso

È possibile visualizzare le informazioni sui log di flusso per una risorsa, ad esempio un'interfaccia di rete. Le informazioni visualizzate includono l'ID del log di flusso, la configurazione del log di flusso e le informazioni relative allo stato del log di flusso.

Visualizzazione delle informazioni sui log di flusso

1. Esegui una di queste operazioni:
   - Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete). Seleziona la casella di controllo relativa all'interfaccia di rete.
   - Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC). Selezionare la casella di controllo relativa al VPC.
   - Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel riquadro di navigazione, scegliere Subnets (Sottoreti). Seleziona la casella di controllo della sottorete.
2. Scegli Flow Logs (Log di flusso).
3. (Facoltativo) Per visualizzare i dati del log di flusso, apri la destinazione del log.

## Tagging di un log di flusso

Puoi aggiungere o rimuovere tag per un log di flusso in qualsiasi momento.

Gestione dei tag per un log di flusso

1. Esegui una di queste operazioni:
   - Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete). Seleziona la casella di controllo relativa all'interfaccia di rete.
   - Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC). Selezionare la casella di controllo relativa al VPC.

- Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel riquadro di navigazione, scegliere Subnets (Sottoreti). Seleziona la casella di controllo della sottorete.

2. Scegli Flow Logs (Log di flusso).
3. Scegliere Actions (Operazioni), Manage tags (Gestisci tag).
4. Per aggiungere un nuovo tag, scegli Add new tag (Aggiungi nuovo tag), quindi specifica la chiave e il valore. Per rimuovere un tag, scegli Remove (Rimuovi).
5. Al termine dell'aggiunta o della rimozione dei tag, scegli Save (Salva).

## Eliminazione di un log di flusso

Puoi eliminare un log di flusso in qualsiasi momento. Dopo aver eliminato un log di flusso, potrebbero essere necessari diversi minuti per interrompere la raccolta dei dati.

L'eliminazione di un log di flusso non comporta l'eliminazione dei dati del log dalla destinazione né modifica la risorsa di destinazione. È necessario eliminare i dati del log di flusso esistenti direttamente dalla destinazione e pulire la risorsa di destinazione, utilizzando la console per il servizio di destinazione.

Eliminazione di un log di flusso

1. Esegui una di queste operazioni:
   - Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete). Seleziona la casella di controllo relativa all'interfaccia di rete.
   - Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC). Selezionare la casella di controllo relativa al VPC.
   - Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel riquadro di navigazione, scegliere Subnets (Sottoreti). Seleziona la casella di controllo della sottorete.
2. Scegli Flow Logs (Log di flusso).
3. Scegli Actions (Operazioni), Delete flow logs (Elimina log di flusso).
4. Quando viene richiesta la conferma, digitare **`delete`** e quindi scegliere Delete (Elimina).

### Panoramica su API e CLI

Puoi eseguire le attività descritte in questa pagina tramite la riga di comando o l'API. Per ulteriori informazioni sulle interfacce a riga di comando e per un elenco delle operazioni API disponibili, consulta Uso di Amazon VPC.

Creazione di un log di flusso

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)
- CreateFlowRegistri (API di interrogazione Amazon EC2)

Descrizione di un log di flusso

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)
- DescribeFlowRegistri (API di interrogazione Amazon EC2)

Tagging di un log di flusso

- create-tags e delete-tags (AWS CLI)
- New-EC2Tage Remove-EC2Tag()AWS Tools for Windows PowerShell
- CreateTagse DeleteTags(API di interrogazione Amazon EC2)

Eliminazione di un log di flusso

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlowRegistri (API di interrogazione Amazon EC2)

## Pubblica i log di flusso su Logs CloudWatch

I log di flusso possono pubblicare i dati dei log di flusso direttamente su Amazon CloudWatch.

Quando vengono pubblicati su CloudWatch Logs, i dati del log di flusso vengono pubblicati in un gruppo di log e ogni interfaccia di rete ha un flusso di log unico nel gruppo di log. I flussi di log

contengono record del log di flusso. Puoi creare più log di flusso che pubblicano dati nello stesso gruppo di log. Se la stessa interfaccia di rete è presente in uno o più log di flusso nello stesso gruppo di log, dispone di un flusso di log combinato. Se è stato specificato che un log di flusso deve acquisire traffico rifiutato e l'altro log di flusso deve acquisire traffico accettato, il flusso di log combinato acquisisce tutto il traffico.

In CloudWatch Logs, il campo timestamp corrisponde all'ora di inizio acquisita nel record del log di flusso. Il campo IngestionTime indica la data e l'ora in cui il record del log di flusso è stato ricevuto da Logs. CloudWatch Questo timestamp è successivo all'ora di fine acquisita nel record di log di flusso.

Per ulteriori informazioni sui CloudWatch log, consulta Logs sent to Logs nella Amazon CloudWatch CloudWatch Logs User Guide.

Prezzi

I costi di ingestione e archiviazione dei dati per i log venduti si applicano quando pubblichi i log di flusso su Logs. CloudWatch Per ulteriori informazioni, apri Amazon CloudWatch Pricing, seleziona Logs e trova Vending Logs.

Indice



## Ruolo IAM per la pubblicazione dei log di flusso su Logs CloudWatch

Il ruolo IAM associato al log di flusso deve disporre di autorizzazioni sufficienti per pubblicare i log di flusso nel gruppo di log specificato in Logs. CloudWatch Il ruolo IAM deve appartenere al tuo account. AWS

La policy IAM collegata al ruolo IAM deve includere almeno le autorizzazioni seguenti:

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

Verificare che il ruolo abbia la seguente policy di attendibilità che consente al servizio dei log di flusso di assumere il ruolo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Si consiglia di utilizzare il le chiavi di condizione `aws:SourceAccount` e `aws:SourceArn` per proteggersi dal problema del "confused deputy". Ad esempio, è possibile aggiungere il seguente blocco di condizione alla policy di attendibilità precedente. L'account di origine è il proprietario del flusso di log e l'ARN di origine è l'ARN del flusso di log. Se non si conosce l'ID del flusso di log, è possibile sostituire quella parte dell'ARN con un carattere jolly (*) e quindi aggiornare la policy dopo aver creato il flusso di log.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
```

```
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

Creazione di un ruolo IAM per i log di flusso

È possibile aggiornare un ruolo esistente come descritto in precedenza. In alternativa, puoi utilizzare la seguente procedura per creare un nuovo ruolo per l'utilizzo con log di flusso. Questo ruolo dovrà essere specificato quando crei il log del flusso.

Per creare un ruolo IAM per i log di flusso

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, selezionare Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Nella pagina Create policy (Crea policy), eseguire le operazioni seguenti:
   a. Scegli JSON.
   b. Sostituisci il contenuto di questa finestra con la policy delle autorizzazioni all'inizio di questa sezione.
   c. Seleziona Successivo.
   d. Inserisci un nome per la policy e una descrizione e dei tag opzionali, quindi scegli Crea policy.
5. Nel pannello di navigazione, seleziona Roles (Ruoli).
6. Selezionare Create role (Crea ruolo).
7. Per Trusted entity type (Tipo di entità attendibile), scegli Custom trust policy (Policy di attendibilità personalizzata). Per Custom trust policy (Policy di attendibilità personalizzata), sostituisci `"Principal": {},` con quanto segue, quindi seleziona Next (Successivo).

   ```
   "Principal": {
      "Service": "vpc-flow-logs.amazonaws.com"
   },
   ```

8. Sulla pagina Add permissions (Aggiungi autorizzazioni), seleziona la casella di controllo relativa alla policy creata in precedenza in questa procedura, quindi scegli Next (Successivo).
9. Immetti un nome per il ruolo e fornisci una descrizione facoltativa.

10. Seleziona Create role (Crea ruolo).

## Autorizzazioni per i principali IAM che pubblicano i log di flusso su Logs CloudWatch

Verifica che il principale IAM che stai utilizzando per effettuare la richiesta disponga delle autorizzazioni per avviare l'azione. `iam:PassRole`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

## Crea un log di flusso da pubblicare su Logs CloudWatch

È possibile creare log di flusso per VPC, sottoreti o interfacce di rete. Se esegui questa procedura come utente che utilizza un particolare ruolo IAM, assicurati che il ruolo disponga delle autorizzazioni per utilizzare l'operazione `iam:PassRole`. Per ulteriori informazioni, consulta Autorizzazioni per i principali IAM che pubblicano i log di flusso su Logs CloudWatch .

Prerequisito

- Crea un ruolo IAM, come descritto in the section called “Ruolo IAM per la pubblicazione dei log di flusso su Logs CloudWatch ”.

Creazione di un flusso di log tramite la console

1. Esegui una di queste operazioni:
   - Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete). Seleziona la casella di controllo relativa all'interfaccia di rete.
   - Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC). Selezionare la casella di controllo relativa al VPC.

- Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel riquadro di navigazione, scegliere Subnets (Sottoreti). Seleziona la casella di controllo della sottorete.

2. Scegli Actions (Operazioni), Create flow log (Crea flusso di log).
3. Per Filtra, specifica il tipo di traffico di cui eseguire il log. Seleziona All (Tutti) per registrare il traffico accettato e rifiutato, Reject (Rifiutato) per eseguire il log solo del traffico rifiutato oppure Accept (Accettato) per eseguirlo solo sul traffico accettato.
4. Per Maximum aggregation interval (Intervallo di aggregazione massimo), scegliere il periodo di tempo massimo durante il quale un flusso viene acquisito e aggregato in un record di log di flusso.
5. Per Destinazione, scegli Invia ai registri. CloudWatch
6. Per Gruppo di log di destinazione, scegli il nome di un gruppo di log esistente o inserisci il nome di un nuovo gruppo di log che verrà creato quando crei questo log di flusso.
7. Per il ruolo IAM, specifica il nome del ruolo che dispone delle autorizzazioni per pubblicare i log in Logs. CloudWatch
8. Per Formato record di log, seleziona il formato per il record del log di flusso.
   - Per utilizzare il formato del record di log di flusso predefinito, seleziona Formato predefinito AWS .
   - Per utilizzare un formato personalizzato, scegli Formato personalizzato, quindi seleziona i campi da Formato di log .
9. Per Metadati aggiuntivi, seleziona se desideri includere i metadati di Amazon ECS nel formato di registro.
10. (Facoltativo) Seleziona Aggiungi tag per applicare i tag al log di flusso.
11. Selezionare Create flow log (Crea log di flusso).

Per creare un log di flusso utilizzando la riga di comando

Utilizzare uno dei seguenti comandi.

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)

L' AWS CLI esempio seguente crea un log di flusso che acquisisce tutto il traffico accettato per la sottorete specificata. I log di flusso vengono consegnati al gruppo di log specificato. Il `--deliver-logs-permission-arn` parametro specifica il ruolo IAM richiesto per la pubblicazione su Logs. CloudWatch

```
aws ec2 create-flow-logs --resource-type Subnet --resource-ids subnet-1a2b3c4d --
traffic-type ACCEPT --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

## Visualizzazione dei record dei log di flusso

È possibile visualizzare i record del log di flusso utilizzando la console CloudWatch Logs. Dopo che il flusso di log è stato creato, potrebbero essere necessari alcuni minuti prima che sia visibile nella console.

Per visualizzare i record del log di flusso pubblicati su CloudWatch Logs utilizzando la console

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione a sinistra, scegli Log, Gruppi di log.
3. Seleziona il nome del gruppo di log contenente i log di flusso per aprirne la pagina dei dettagli.
4. Seleziona il nome del flusso di log contenente i record del log di flusso. Per ulteriori informazioni, consulta Record di log di flusso.

Per visualizzare i record dei log di flusso pubblicati su CloudWatch Logs utilizzando la riga di comando

- get-log-events (AWS CLI)
- LogEventGet-CWL ()AWS Tools for Windows PowerShell

## Ricerca dei record dei log di flusso

È possibile cercare i record del log di flusso pubblicati su CloudWatch Logs utilizzando la console Logs. CloudWatch È possibile utilizzare filtri metrici per filtrare i record del log di flusso. I record del log di flusso sono delimitati da spazio.

Per cercare i record del log di flusso utilizzando la CloudWatch console Logs

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.

2. Nel pannello di navigazione a sinistra, scegli Log, Gruppi di log.
3. Seleziona il gruppo di log contenente il log di flusso, quindi seleziona il flusso di log, se conosci l'interfaccia di rete che stai cercando. In alternativa, scegli Search log group (Cerca nel gruppo di log). Questo potrebbe richiedere del tempo se nel gruppo di log sono presenti molte interfacce di rete o in base all'intervallo di tempo selezionato.
4. In Filtra eventi, inserisci la stringa seguente. Ciò presuppone che il record del log di flusso utilizzi il formato predefinito.

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport, protocol,
 packets, bytes, start, end, action, logstatus]
```

5. Modificare il filtro in base alle esigenze specificando i valori per i campi. Negli esempi seguenti il filtro viene applicato in base a specifici indirizzi IP di origine.

```
[version, accountid, interfaceid, srcaddr = 10.0.0.1, dstaddr, srcport, dstport,
 protocol, packets, bytes, start, end, action, logstatus]
[version, accountid, interfaceid, srcaddr = 10.0.2.*, dstaddr, srcport, dstport,
 protocol, packets, bytes, start, end, action, logstatus]
```

Negli esempi seguenti il filtro viene applicato in base alla porta di destinazione, al numero di byte e all'eventuale rifiuto del traffico.

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
 dstport = 8080, protocol, packets, bytes, start, end, action, logstatus]
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
 dstport = 8080, protocol, packets, bytes >= 400, start, end, action = REJECT,
 logstatus]
```

## Elabora i record del registro del flusso in CloudWatch Logs

È possibile utilizzare i record del log di flusso come si farebbe con qualsiasi altro evento di registro raccolto da CloudWatch Logs. Per ulteriori informazioni sul monitoraggio dei dati di log e sui filtri delle metriche, consulta Searching and Filtering Log Data nella Amazon CloudWatch User Guide.

Esempio: crea un filtro CloudWatch metrico e un allarme per un log di flusso

In questo esempio, si dispone di un log di flusso per `eni-1a2b3c4d`. Si desidera creare un allarme che avvisa se si sono verificati almeno 10 tentativi di connessione all'istanza sulla porta TCP 22

(SSH) entro un periodo di tempo di 1 ora. Innanzitutto, crea un filtro parametri che corrisponde al modello di traffico per il quale creare l'allarme. Quindi, puoi creare un allarme per il filtro parametri.

Per creare il filtro parametri per traffico SSH rifiutato e creare un allarme per il filtro

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione a sinistra, scegli Logs (Registri), Log groups (Gruppi di registri).
3. Seleziona la casella di controllo per il gruppo di log e scegli Actions (Operazioni), poi Create metric filter (Crea filtri parametri).
4. Per Filter pattern (Modello di filtro), immetti la seguente stringa.

```
[version, account, eni, source, destination, srcport, destport="22", protocol="6",
 packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]
```

5. Per Select Log Data to Test (Seleziona i dati di log per il test), seleziona il flusso di log per l'interfaccia di rete. (Facoltativo) Per visualizzare le righe di dati di log che corrispondono al modello di filtro, scegli Test Pattern (Modello di test).
6. Al termine, scegli Next (Successivo).
7. Inserisci un nome per il filtro, uno spazio dei nomi dei parametri e il nome del parametro. Imposta il valore del parametro su 1. Al termine, scegli Next (Successivo) e in seguito Create metric filter (Crea filtri parametri).
8. Nel pannello di navigazione, seleziona Alarms (Allarmi), All alarms (Tutti gli allarmi).
9. Scegli Crea allarme.
10. Seleziona il nome della metrica che hai creato, quindi scegli Seleziona metrica.
11. Configura l'allarme come segue, quindi scegli Next (Successivo):
    - Per Statistic (Statistica), scegliere Sum (Somma). Ciò ti garantisce di acquisire il numero totale di punti di dati per il periodo di tempo specificato.
    - Per Period (Periodo), scegli 1 Hour (1 ora).
    - Per Whenever is TimeSinceLastActive ... , scegli Maggiore/Uguale e inserisci 10 per la soglia.
    - In Additional configuration (Configurazione aggiuntiva), Datapoints to alarm (Punti dati ad allarme) lascia il valore di default 1.
12. Seleziona Successivo.
13. Per Notification (Notifica) scegli un argomento SNS esistente oppure Create new topic (Crea nuovo argomento), per crearne uno nuovo. Seleziona Successivo.

14. Inserisci un nome e una descrizione per l'allarme, quindi scegli Next (Successivo).
15. Quando hai finito di visualizzare l'anteprima dell'avviso, scegli Crea allarme.

## Pubblicazione di log di flusso su Amazon S3

I log di flusso possono pubblicare dati di log di flusso in Amazon S3.

Durante la pubblicazione in Amazon S3, i dati del log di flusso vengono pubblicati in un bucket Amazon S3 esistente specificato. I record di log di flusso per tutte le interfacce di rete monitorate vengono pubblicati in una serie di oggetti file di log che sono archiviati nel bucket. Se il log di flusso acquisisce dati per un VPC, pubblica i record di log di flusso per tutte le interfacce di rete nel VPC selezionato.

Per creare un bucket Amazon S3 da utilizzare con i flussi di log, consulta Creazione di un bucket nella Guida per l'utente di Amazon Simple Storage Service.

Per ulteriori informazioni sulla registrazione di più account, consulta Registrazione centrale nella libreria di soluzioni di AWS .

Per ulteriori informazioni sui CloudWatch log, consulta Logs sent to Amazon S3 nella Amazon Logs User Guide CloudWatch .

Prezzi

Gli addebiti per l'inserimento e l'archiviazione dei dati per i log forniti vengono applicati quando si pubblicano i log di flusso in Amazon S3. Per ulteriori informazioni, apri Amazon CloudWatch Pricing, seleziona Logs e trova Vending Logs.

Indice

- Elaborazione di record del log di flusso in Amazon S3

## File di log di flusso

VPC Flow Logs raccoglie i dati sul traffico IP in entrata e in uscita dal tuo VPC in record di registro, aggrega tali record in file di registro e quindi pubblica i file di registro nel bucket Amazon S3 a intervalli di 5 minuti. È possibile pubblicare più file e ogni file di registro può contenere alcuni o tutti i record del log di flusso per il traffico IP registrato nei 5 minuti precedenti.

In Amazon S3, il campo Last modified (Ultima modifica) per il file di log di flusso indica la data e l'ora in cui il file è stato caricato nel bucket Amazon S3. Questa è successiva al timestamp nel nome del file e differisce per il tempo impiegato per caricare il file nel bucket Amazon S3.

### Formato dei file di log

Per i file di log, puoi specificare uno dei seguenti formati. Ciascun file viene compresso in un singolo file Gzip.

- Text: Testo normale. Questo è il formato predefinito.
- Parquet: Apache Parquet è un formato dati colonnare. Le query sui dati in formato Parquet sono da 10 a 100 volte più veloci, rispetto alle query sui dati in testo normale. I dati in formato Parquet con compressione Gzip occupano il 20% di spazio di archiviazione in meno, rispetto al testo normale con compressione Gzip.

> **Note**
>
> Se i dati in formato Parquet con compressione Gzip sono inferiori a 100 KB per periodo di aggregazione, l'archiviazione dei dati in formato Parquet può occupare più spazio rispetto al testo normale con compressione Gzip a causa dei requisiti di memoria dei file Parquet.

### Opzioni di file di log

È inoltre possibile specificare le seguenti opzioni.

- Hive-compatible S3 prefixes (Prefissi S3 compatibili con Hive): Abilita i prefissi compatibili con Hive invece di importare partizioni negli strumenti compatibili. Prima di eseguire query, utilizza il comando MSCK REPAIR TABLE.

- Hourly partitions (Partizioni orarie): se disponi di un grande volume di registri e di solito indirizzi le query a un'ora specifica, partizionando i log su base oraria puoi ottenere risultati più rapidi e risparmiare sui costi delle query.

### Struttura del bucket S3 dei file di log

I file di log vengono salvati nel bucket Amazon S3; utilizzando una struttura di cartelle determinata dall'ID del flusso di log, dalla Regione e dalla loro data di creazione.

Per impostazione predefinita, i file vengono recapitati alla seguente posizione.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Se abiliti i prefissi S3 compatibili con Hive, i file vengono recapitati nella seguente posizione.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/
```

Se abiliti le partizioni orarie, i file vengono recapitati nella seguente posizione.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

Se abiliti le partizioni compatibili con Hive e partizioni il flusso di log per ora, i file vengono recapitati nella posizione seguente.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/hour=hour/
```

### Nome del file di log

Il nome di un file di log si basa sull'ID del flusso di log, sulla Regione e sulla data e ora di creazione. I nomi file utilizzano il formato seguente.

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

Ad esempio, di seguito viene mostrata la struttura di cartelle e il nome di un file di log per un flusso di log creato dall'account AWS 123456789012, per una risorsa nella Regione us-east-1 su June 20, 2018 in 16:20 UTC. Il file contiene i registri dei flussi di log con un'ora di fine tra 16:20:00 e 16:24:59.

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

## Autorizzazioni per i principali IAM che pubblicano i log di flusso in Amazon S3

Il principale IAM che crea il log di flusso deve utilizzare un ruolo IAM con le seguenti autorizzazioni, necessarie per pubblicare log di flusso nel bucket Amazon S3 di destinazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource": "*"
    }
  ]
}
```

## Autorizzazioni dei bucket Amazon S3 per log di flusso

Per impostazione predefinita, i bucket Amazon S3 e gli oggetti che contengono sono privati. Solo il proprietario del bucket può accedere al bucket e agli oggetti in esso archiviati. Il proprietario del bucket, tuttavia, può concedere l'accesso ad altre risorse e ad altri utenti scrivendo una policy di accesso.

Se l'utente che crea il flusso di log è il proprietario del bucket e ha le autorizzazioni `PutBucketPolicy` e `GetBucketPolicy` per il bucket, verrà automaticamente allegata la seguente policy al bucket. Questa policy sovrascrive qualsiasi policy esistente collegata al bucket.

In caso contrario, il proprietario del bucket deve aggiungere tale policy al bucket, specificando l'ID dell'account AWS del creatore del flusso di log o la creazione del flusso di log fallirà. Per maggiori informazioni, consulta Utilizzo delle policy di bucket nella Guida per l'utente di Amazon Simple Storage Service.

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

```
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "my-s3-arn/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id,
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketAcl",
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        }
    ]
}
```

L'ARN per cui si specifica *my-s3-arn* dipende dal fatto che si utilizzino prefissi S3 compatibili con Hive.

- Prefissi di default

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- Prefissi S3 compatibili con Hive

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

È consigliabile concedere queste autorizzazioni al responsabile del servizio di consegna dei log anziché ai singoli Account AWS ARN. Una best practice è anche usare le chiavi di condizione `aws:SourceAccount` e `aws:SourceArn` per proteggersi dal problema del "confused deputy". L'account di origine è il proprietario del flusso di log e l'ARN di origine è l'ARN jolly (*) del servizio log.

## Policy di chiave richiesta per l'uso con SSE-KMS

Puoi proteggere i dati nel tuo bucket Amazon S3 abilitando la crittografia lato server con Amazon S3 Managed Keys (SSE-S3) o la crittografia lato server con chiavi archiviate in KMS (SSE-KMS) sul tuo bucket S3. Per ulteriori informazioni, consulta Protezione dei dati con la crittografia lato server nella Guida per l'utente di Amazon S3.

Se si sceglie SSE-S3, non è richiesta alcuna configurazione aggiuntiva. Amazon S3 gestisce la chiave di crittografia.

Se scegli SSE-KMS, devi utilizzare l'ARN di una chiave gestita dal cliente. Se utilizzi un ID chiave, è possibile che si verifichi un errore LogDestination non consegnabile durante la creazione di un log di flusso. Inoltre, devi aggiornare la policy della chiave gestita dal cliente in modo che l'account di distribuzione dei log possa scrivere nel bucket S3. Per ulteriori informazioni sulla politica delle chiavi richiesta per l'uso con SSE-KMS, consulta la crittografia lato server con bucket Amazon S3 nella Amazon Logs User Guide. CloudWatch

## Autorizzazioni del file di log Amazon S3

In aggiunta alle policy dei bucket obbligatorie, Amazon S3 utilizza liste di controllo accessi per gestire l'accesso ai file di log creati da un log di flusso. Per impostazione predefinita, il proprietario del bucket dispone di autorizzazioni `FULL_CONTROL` su ogni file di log. Il proprietario della distribuzione dei log, se diverso dal proprietario del bucket, non dispone di autorizzazioni. L'account di distribuzione dei log dispone delle autorizzazioni `READ` e `WRITE`. Per ulteriori informazioni, consulta Panoramica della lista di controllo accessi nella Guida per l'utente di Amazon Simple Storage Service.

## Creazione di un log di flusso che pubblica in Amazon S3

Dopo aver creato e configurato il bucket Amazon S3, è possibile creare flussi di log per interfacce di rete, sottoreti e VPC.

Creazione di un flusso di log tramite la console

1. Esegui una di queste operazioni:
   - Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete). Seleziona la casella di controllo relativa all'interfaccia di rete.
   - Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC). Selezionare la casella di controllo relativa al VPC.
   - Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel riquadro di navigazione, scegliere Subnets (Sottoreti). Seleziona la casella di controllo della sottorete.
2. Scegli Actions (Operazioni), Create flow log (Crea flusso di log).
3. Per Filter (Filtro), specificare il tipo di dati di traffico IP di cui eseguire il log.
   - Accetta: registra solo il traffico accettato.
   - Rifiuta: registra solo il traffico rifiutato.
   - All (Tutto): esegui il log sia del traffico accettato che di quello rifiutato.
4. Per Maximum aggregation interval (Intervallo di aggregazione massimo), scegliere il periodo di tempo massimo durante il quale un flusso viene acquisito e aggregato in un record di log di flusso.
5. Per Destinazione, scegli Invia a un bucket Amazon S3.
6. Per S3 bucket ARN (ARN bucket S3), specificare l'Amazon Resource Name (ARN) di un bucket Amazon S3 esistente. Puoi anche includere una sottocartella. Ad esempio, per specificare una sottocartella denominata `my-logs` in un bucket denominato `my-bucket`, utilizzare il seguente ARN:

   ```
   arn:aws:s3:::my-bucket/my-logs/
   ```

   Il bucket non può utilizzare `AWSLogs` come nome di sottocartella, in quanto si tratta di un termine riservato.

Se si è il proprietario del bucket, noi creiamo automaticamente una policy delle risorse e la colleghiamo al bucket. Per ulteriori informazioni, consulta Autorizzazioni dei bucket Amazon S3 per log di flusso.

7. Per Log record format (Formato registro di log), seleziona il formato per il registro del flusso di log.
   - Per utilizzare il formato di record di log di flusso predefinito, seleziona Formato predefinito AWS .
   - Per creare un formato personalizzato, scegliere Custom format (Formato personalizzato). Per Log format (Formato log), scegliere i campi da includere nel record di log di flusso.
8. Per Metadati aggiuntivi, seleziona se desideri includere i metadati di Amazon ECS nel formato di registro.
9. Per Log file format (Formato dei file di log), specifica il formato per il file di log.
   - Text: Testo normale. Questo è il formato predefinito.
   - Parquet: Apache Parquet è un formato dati colonnare. Le query sui dati in formato Parquet sono da 10 a 100 volte più veloci, rispetto alle query sui dati in testo normale. I dati in formato Parquet con compressione Gzip occupano il 20% di spazio di archiviazione in meno, rispetto al testo normale con compressione Gzip.
10. (Facoltativo) Per utilizzare prefissi S3 compatibili con Hive, scegli Hive-compatible S3 prefix (Prefisso S3 compatibile con Hive),Enable (Abilita).
11. (Facoltativo) Per partizionare i flussi di log per ora, scegli Every 1 hour (60 mins) Ogni ora (60 minuti).
12. (Facoltativo) Per aggiungere un tag al flusso di log, scegli Add new tag (Aggiungi nuovo tag) e specifica la chiave e il valore del tag.
13. Selezionare Create flow log (Crea log di flusso).

Per creare un log di flusso che pubblica in Amazon S3 utilizzando uno strumento a riga di comando

Utilizzare uno dei seguenti comandi:

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)

L' AWS CLI esempio seguente crea un log di flusso che acquisisce tutto il traffico per il VPC specificato e consegna i log di flusso al bucket Amazon S3 specificato. Il parametro `--log-format` specifica un formato personalizzato per i record di log di flusso.

```
aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-00112233344556677 --
traffic-type ALL --log-destination-type s3 --log-destination arn:aws:s3:::flow-log-
bucket/custom-flow-logs/ --log-format '${version} ${vpc-id} ${subnet-id} ${instance-
id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${tcp-flags} ${type} ${pkt-
srcaddr} ${pkt-dstaddr}'
```

### Visualizzazione dei record dei log di flusso

È possibile visualizzare i record del log di flusso utilizzando la console Amazon S3. Dopo che il flusso di log è stato creato, potrebbero essere necessari alcuni minuti prima che sia visibile nella console.

Per visualizzare i record del log di flusso pubblicati in Amazon S3

1. Apri la console Amazon S3 su https://console.aws.amazon.com/s3/.
2. Seleziona il nome del bucket per aprirne la pagina dei dettagli.
3. Passa alla cartella con i file di log. *Ad esempio, prefix/account_id AWSLogs / vpcflowlogs/ region/year/month/day /.*
4. Seleziona la casella di controllo accanto al nome del file, quindi scegli Download (Scarica).

### Elaborazione di record del log di flusso in Amazon S3

I file di log sono compressi. Se si aprono i file di log utilizzando la console Amazon S3, vengono decompressi e i record del log di flusso visualizzati. Se i file vengono scaricati, devono essere decompressi per visualizzare i record del log di flusso.

Puoi anche eseguire query sui record del log di flusso nei file di log utilizzando Amazon Athena. Amazon Athena è un servizio di query interattivo che semplifica l'analisi dei dati in Amazon S3 con SQL standard. Per ulteriori informazioni, consulta la sezione relativa all'Esecuzione di query su log di flusso Amazon VPC nella Guida per l'utente di Amazon Athena.

## Pubblica i log di flusso su Amazon Data Firehose

I log di flusso possono pubblicare i dati dei log di flusso direttamente su Amazon Data Firehose.

Quando si pubblica su Amazon Data Firehose, i dati del log di flusso vengono pubblicati in un flusso di distribuzione di Amazon Data Firehose, in formato testo semplice.

Prezzi

Si applicano le spese standard di acquisizione e consegna. Per ulteriori informazioni, apri Amazon CloudWatch Pricing, seleziona Logs e trova Vending Logs.

Indice



## Ruoli IAM per la consegna tra account

Quando pubblichi su Amazon Data Firehose, puoi scegliere un flusso di distribuzione nello stesso account della risorsa da monitorare (l'account di origine) o in un altro account (l'account di destinazione). Per consentire la consegna dei log di flusso su più account ad Amazon Data Firehose, devi creare un ruolo IAM nell'account di origine e un ruolo IAM nell'account di destinazione.

Roles



### Ruolo dell'account di origine

Nell'account di origine, crea un ruolo che conceda le seguenti autorizzazioni. In questo esempio, il nome del ruolo è `mySourceRole` ma è possibile scegliere un nome diverso. L'ultima istruzione consente al ruolo nell'account di destinazione di assumere questo ruolo. Le istruzioni sulle condizioni assicurano che questo ruolo venga passato solo al servizio di consegna dei log e solo durante il monitoraggio della risorsa specificata. Quando si crea la propria policy, specifica i VPC, le interfacce di rete o le sottoreti che si stanno monitorando con la chiave di condizione `iam:AssociatedResourceARN`.

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

```
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
          "StringEquals": {
              "iam:PassedToService": "delivery.logs.amazonaws.com"
          },
          "StringLike": {
              "iam:AssociatedResourceARN": [
                  "arn:aws:ec2:region:source-account:vpc/vpc-00112233344556677"
              ]
          }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
          "logs:CreateLogDelivery",
          "logs:DeleteLogDelivery",
          "logs:ListLogDeliveries",
          "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}
```

Verifica che questo ruolo abbia la seguente policy di attendibilità che consente al servizio di consegna dei log di assumere il ruolo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
```

```
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Dall'account di origine, utilizza la seguente procedura per creare il ruolo.

Creazione del ruolo dell'account di origine

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, selezionare Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Nella pagina Create policy (Crea policy), eseguire le operazioni seguenti:
   a. Scegli JSON.
   b. Sostituisci il contenuto di questa finestra con la policy delle autorizzazioni all'inizio di questa sezione.
   c. Seleziona Successivo.
   d. Inserisci un nome per la tua policy e una descrizione e tag opzionali, quindi scegli Crea policy.
5. Nel pannello di navigazione, seleziona Roles (Ruoli).
6. Selezionare Create role (Crea ruolo).
7. Per Trusted entity type (Tipo di entità attendibile), scegli Custom trust policy (Policy di attendibilità personalizzata). Per Custom trust policy (Policy di attendibilità personalizzata), sostituisci `"Principal": {},` con quanto segue, che specifica il servizio di consegna dei log. Seleziona Successivo.

   ```
   "Principal": {
      "Service": "delivery.logs.amazonaws.com"
   },
   ```

8. Sulla pagina Add permissions (Aggiungi autorizzazioni), seleziona la casella di controllo relativa alla policy creata in precedenza in questa procedura, quindi scegli Next (Successivo).
9. Immetti un nome per il ruolo e fornisci una descrizione facoltativa.
10. Seleziona Create role (Crea ruolo).

Ruolo dell'account di destinazione

Nell'account di destinazione, crea un ruolo con un nome che inizia con AWSLogDeliveryFirehoseCrossAccountRole. Questo ruolo deve concedere le autorizzazioni riportate di seguito.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

Assicurarsi che questo ruolo abbia la seguente policy di attendibilità, che consenta al ruolo creato nell'account di origine di assumere questo ruolo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Dall'account di destinazione, utilizza la seguente procedura per creare il ruolo.

Creazione del ruolo dell'account di destinazione

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, selezionare Policies (Policy).

3. Scegli Create Policy (Crea policy).
4. Nella pagina Create policy (Crea policy), eseguire le operazioni seguenti:
   a. Scegli JSON.
   b. Sostituisci il contenuto di questa finestra con la policy delle autorizzazioni all'inizio di questa sezione.
   c. Seleziona Successivo.
   d. Inserisci un nome per la tua politica che inizia con AWSLogDeliveryFirehoseCrossAccountRole, quindi scegli Crea politica.
5. Nel pannello di navigazione, seleziona Roles (Ruoli).
6. Selezionare Create role (Crea ruolo).
7. Per Trusted entity type (Tipo di entità attendibile), scegli Custom trust policy (Policy di attendibilità personalizzata). Per Custom trust policy (Policy di attendibilità personalizzata), sostituisci `"Principal": {},` con quanto segue, che specifica il ruolo dell'account di origine. Seleziona Successivo.

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. Sulla pagina Add permissions (Aggiungi autorizzazioni), seleziona la casella di controllo relativa alla policy creata in precedenza in questa procedura, quindi scegli Next (Successivo).
9. Immetti un nome per il ruolo e fornisci una descrizione facoltativa.
10. Seleziona Create role (Crea ruolo).

## Crea un log di flusso da pubblicare su Amazon Data Firehose

È possibile creare log di flusso per VPC, sottoreti o interfacce di rete.

Prerequisiti

- Crea il flusso di distribuzione Amazon Data Firehose di destinazione. Utilizza Direct Put (PUT diretto) come origine. Per ulteriori informazioni, consulta Creazione di un flusso di distribuzione Amazon Data Firehose.
- Se stai pubblicando i log del flusso su un account diverso, crea i ruoli IAM richiesti come descritto in the section called “Ruoli IAM per la consegna tra account”.

Per creare un log di flusso da pubblicare su Amazon Data Firehose

1. Esegui una di queste operazioni:
   - Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete). Seleziona la casella di controllo relativa all'interfaccia di rete.
   - Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC). Selezionare la casella di controllo relativa al VPC.
   - Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel riquadro di navigazione, scegliere Subnets (Sottoreti). Seleziona la casella di controllo della sottorete.
2. Scegli Actions (Operazioni), Create flow log (Crea flusso di log).
3. Per Filtra, specifica il tipo di traffico di cui eseguire il log.
   - Accept (Accetta): esegui il log solo del traffico accettato.
   - Reject (Rifiuta): esegui il log solo del traffico rifiutato.
   - All (Tutto): esegui il log sia del traffico accettato che di quello rifiutato.
4. Per Maximum aggregation interval (Intervallo di aggregazione massimo), scegliere il periodo di tempo massimo durante il quale un flusso viene acquisito e aggregato in un record di log di flusso.
5. In Destination (Destinazione) scegli una delle seguenti opzioni:
   - Invia ad Amazon Data Firehose con lo stesso account: il flusso di distribuzione e la risorsa da monitorare si trovano nello stesso account.
   - Invia ad Amazon Data Firehose con un account diverso: il flusso di distribuzione e la risorsa da monitorare si trovano in account diversi.
6. Per il nome dello stream Amazon Data Firehose, scegli il flusso di distribuzione che hai creato.
7. [Solo consegna tra account] Per IAM roles (Ruoli IAM), specifica i ruoli richiesti (consulta the section called “Ruoli IAM per la consegna tra account”).
8. Per Log record format (Formato registro di log), seleziona il formato per il registro del flusso di log.
   - Per utilizzare il formato di record di log di flusso predefinito, seleziona Formato predefinito AWS .

- Per creare un formato personalizzato, scegliere Custom format (Formato personalizzato). Per Log format (Formato log), scegliere i campi da includere nel record di log di flusso.

9. Per Metadati aggiuntivi, seleziona se desideri includere i metadati di Amazon ECS nel formato di registro.
10. (Facoltativo) Scegli Aggiungi tag per applicare i tag al log di flusso.
11. Selezionare Create flow log (Crea log di flusso).

Per creare un log di flusso da pubblicare su Amazon Data Firehose utilizzando uno strumento da riga di comando

Utilizzare uno dei seguenti comandi:

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)

L' AWS CLI esempio seguente crea un log di flusso che acquisisce tutto il traffico per il VPC specificato e invia i log di flusso al flusso di distribuzione Amazon Data Firehose specificato nello stesso account.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream
```

L' AWS CLI esempio seguente crea un log di flusso che acquisisce tutto il traffico per il VPC specificato e invia i log di flusso al flusso di distribuzione Amazon Data Firehose specificato in un account diverso.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
```

```
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

### Record di log del flusso di processo in Amazon Data Firehose

È possibile ottenere i dati del log del flusso dalla destinazione configurata per il flusso di consegna.

## Eseguire una query dei flussi di log tramite Amazon Athena

Amazon Athena è un servizio di query interattivo che consente di analizzare i dati in Amazon S3, come i log di flusso, utilizzando SQL standard. È possibile utilizzare Athena con i log di flusso del VPC in modo da ottenere rapidamente informazioni utili sul traffico che scorre attraverso il VPC. Ad esempio, è possibile identificare quali risorse nei cloud privati virtuali (VPC) sono i principali talker o identificare gli indirizzi IP con le connessioni TCP più rifiutate.

Opzioni

- Puoi semplificare e automatizzare l'integrazione dei log di flusso VPC con Athena generando un CloudFormation modello che crea AWS le risorse necessarie e le query predefinite che puoi eseguire per ottenere informazioni sul traffico che scorre attraverso il tuo VPC.
- Se si desidera, si possono creare query utilizzando Athena. Per ulteriori informazioni, consulta la sezione relativa all'Esecuzione di query su flussi di log utilizzando Amazon Athena nella Guida per l'utente di Amazon Athena.

Prezzi

Si applicano i costi standard di Amazon Athena per l'esecuzione di query. Si applicano i costi standard di AWS Lambda per la funzione Lambda che carica nuove partizioni con una pianificazione ricorrente (quando si specifica una frequenza di caricamento della partizione ma non si specifica una data di inizio e di fine).

Per utilizzare le query predefinite

- Genera il modello utilizzando la console CloudFormation
- Genera il CloudFormation modello utilizzando il AWS CLI
- Esecuzione di una query predefinita

## Genera il modello utilizzando la console CloudFormation

Dopo aver inviato i primi log di flusso al tuo bucket S3, puoi integrarti con Athena generando un CloudFormation modello e utilizzandolo per creare uno stack.

Requisiti

- La regione selezionata deve supportare Amazon Athena AWS Lambda e Amazon Athena.
- I bucket Amazon S3 devono trovarsi nella regione selezionata.
- Il formato del record del log per il log di flusso deve includere i campi utilizzati dalle query predefinite specifiche che desideri eseguire.

Per generare il modello utilizzando la console

1. Scegliere una delle seguenti operazioni:
   - Aprire la console Amazon VPC. Nel riquadro di navigazione, selezionare I tuoi VPC, quindi selezionare il VPC.
   - Aprire la console Amazon VPC. Nel riquadro di navigazione, scegliere Sottoreti e selezionare la sottorete desiderata.
   - Apri la console di Amazon EC2. Nel riquadro di navigazione, scegliere Interfacce di rete e selezionare quindi l'interfaccia di rete.
2. Nella scheda Log di flusso, selezionare un log di flusso che viene pubblicato su Amazon S3, quindi scegliere Azioni, Genera integrazione Athena.
3. Specificare la frequenza di caricamento della partizione. Se si sceglie Nessuna, sarà necessario specificare la data di inizio e di fine della partizione utilizzando date del passato. Se si sceglie Giornaliero, Settimanaleo Mensile, le date di inizio e di fine della partizione sono facoltative. Se non si specificano le date di inizio e fine, il CloudFormation modello crea una funzione Lambda che carica nuove partizioni in base a una pianificazione ricorrente.
4. Selezionare o creare un bucket S3 per il modello generato e un bucket S3 per i risultati della query.
5. Scegliere Genera integrazione Athena.
6. (Facoltativo) Nel messaggio di successo, scegliete il link per accedere al bucket specificato per il modello e personalizzate il CloudFormation modello.
7. Nel messaggio di successo, scegli Crea CloudFormation stack per aprire la procedura guidata Create Stack nella console. AWS CloudFormation L'URL per il CloudFormation modello generato

è specificato nella sezione Modello. Completare la procedura guidata per creare le risorse specificate nel modello.

Risorse create dal CloudFormation modello

- Un database di Athena. Il nome del database è vpcflowlogsathenadatabase<ID-sottoscrizione-log-flusso>.
- Un gruppo di lavoro Athena. Il nome del gruppo di lavoro è <flow-log-subscription-id><partition-load-frequency><start-date><end-date>workgroup
- Una tabella Athena partizionata che corrisponde ai record del log di flusso. Il nome della tabella è <flow-log-subscription-id><partition-load-frequency><start-date><end-date>.
- Un insieme di query denominate Athena. Per ulteriori informazioni, consulta Query predefinite.
- Una funzione Lambda che carica nuove partizioni nella tabella in base alla pianificazione specificata (giornaliera, settimanale o mensile).
- Un ruolo IAM che concede l'autorizzazione per eseguire le funzioni Lambda.

## Genera il CloudFormation modello utilizzando il AWS CLI

Dopo aver inviato i primi log di flusso al tuo bucket S3, puoi generare e utilizzare un CloudFormation modello per l'integrazione con Athena.

Utilizza il seguente comando get-flow-logs-integration-template per generare il modello. CloudFormation

```
aws ec2 get-flow-logs-integration-template --cli-input-json file://config.json
```

Di seguito è riportato un esempio del file `config.json`.

```
{
    "FlowLogId": "fl-12345678901234567",
    "ConfigDeliveryS3DestinationArn": "arn:aws:s3:::my-flow-logs-athena-integration/
templates/",
    "IntegrateServices": {
        "AthenaIntegrations": [
            {
                "IntegrationResultS3DestinationArn": "arn:aws:s3:::my-flow-logs-
analysis/athena-query-results/",
```

```
                "PartitionLoadFrequency": "monthly",
                "PartitionStartDate": "2021-01-01T00:00:00",
                "PartitionEndDate": "2021-12-31T00:00:00"
            }
        ]
    }
}
```

Utilizzate il seguente comando create-stack per creare uno stack utilizzando il modello generato. CloudFormation

```
aws cloudformation create-stack --stack-name my-vpc-flow-logs --template-body file://
my-cloudformation-template.json
```

## Esecuzione di una query predefinita

Il CloudFormation modello generato fornisce una serie di query predefinite che è possibile eseguire per ottenere rapidamente informazioni significative sul traffico della rete. AWS Dopo aver creato lo stack e verificato che tutte le risorse siano state create correttamente, sarà possibile eseguire una delle query predefinite.

Per eseguire una query predefinita utilizzando la console

1. Aprire la console Athena.
2. Nel riquadro di navigazione, scegli Query editor (Editor della query). In Gruppo di lavoro, seleziona il gruppo di lavoro creato dal modello. CloudFormation
3. Seleziona Saved queries (Query salvate), modifica i parametri come necessario ed esegui la query. Per un elenco delle query predefinite disponibili, consulta Query predefinite.
4. In Query results (Risultati della query), visualizza i risultati della query.

### Query predefinite

Di seguito è riportato l'elenco completo delle query denominate Athena. Le query predefinite fornite quando si genera il modello dipendono dai campi che fanno parte del formato record del log per il log di flusso. Pertanto, il modello potrebbe non contenere tutte queste query predefinite.

- VpcFlowLogsAcceptedTraffico: le connessioni TCP consentite in base ai gruppi di sicurezza e agli ACL di rete.

- VpcFlowLogsAdminPortTraffic— I primi 10 indirizzi IP con il maggior traffico, registrati dalle applicazioni che soddisfano le richieste sulle porte amministrative.
- VpcFlowLogsIPv4Traffic: i byte totali del traffico IPv4 registrati.
- VpcFlowLogIPv6Traffic: i byte totali del traffico IPv6 registrati.
- VpcFlowLogsRejectedTCPTraffic: le connessioni TCP che sono state rifiutate in base ai gruppi di sicurezza o agli ACL di rete.
- VpcFlowLogsRejectedTraffico: il traffico che è stato rifiutato in base ai gruppi di sicurezza o agli ACL di rete.
- VpcFlowLogsSshRdpTraffic— Il traffico SSH e RDP.
- VpcFlowLogsTopTalker: i 50 indirizzi IP con il maggior traffico registrato.
- VpcFlowLogsTopTalkersPacketLivello: i 50 indirizzi IP a livello di pacchetto con il maggior traffico registrato.
- VpcFlowLogsTopTalkingInstances— Gli ID delle 50 istanze con il maggior traffico registrato.
- VpcFlowLogsTopTalkingSubnets— Gli ID delle 50 sottoreti con il maggior traffico registrato.
- VpcFlowLogsTopTCPTraffic: tutto il traffico TCP registrato per un indirizzo IP di origine.
- VpcFlowLogsTotalBytesTransferred— Le 50 coppie di indirizzi IP di origine e destinazione con il maggior numero di byte registrati.
- VpcFlowLogsTotalBytesTransferredPacketLevel— Le 50 coppie di indirizzi IP di origine e destinazione a livello di pacchetto con il maggior numero di byte registrati.
- VpcFlowLogsTrafficFrmSrcAddr: il traffico registrato per uno specifico indirizzo IP di origine.
- VpcFlowLogsTrafficToDstAddr: il traffico registrato per uno specifico indirizzo IP di destinazione.

## Risoluzione dei problemi relativi ai log di flusso VPC

Di seguito sono elencati i problemi che si potrebbero riscontrare durante l'utilizzo di log di flusso.

Problemi

- Record del log di flusso incompleti
- Log di flusso attivo, ma nessun record di log di flusso o gruppo di log
- Errore «LogDestinationNotFoundEccezione» o «Accesso negato per» LogDestination
- Superamento del limite di policy del bucket Amazon S3
- LogDestination non consegnabile

## Record del log di flusso incompleti

### Problema

I record dei log di flusso sono incompleti o non vengono più pubblicati.

### Causa

Potrebbe esserci un problema nel recapitare i log di flusso al gruppo CloudWatch Logs log.

### Soluzione

Nella console Amazon EC2 o Amazon VPC, selezionare la scheda Flow Logs (Log di flusso) per la risorsa pertinente. Per ulteriori informazioni, consulta Visualizzazione di un log di flusso. La tabella dei log di flusso contiene gli eventuali errori nella colonna State (Stato). In alternativa, utilizza il comando describe-flow-logs e verifica il valore restituito nel campo `DeliverLogsErrorMessage`. Potrebbe essere visualizzato uno degli errori seguenti:

- `Rate limited`: Questo errore può verificarsi se è stata applicata la limitazione dei CloudWatch log, ovvero quando il numero di record del log di flusso per un'interfaccia di rete è superiore al numero massimo di record che possono essere pubblicati entro un periodo di tempo specifico. Questo errore può verificarsi anche se è stata raggiunta la quota per il numero di gruppi di log dei CloudWatch log che è possibile creare. Per ulteriori informazioni, consulta CloudWatchService Quotas nella Amazon CloudWatch User Guide.
- `Access error`: questo errore può verificarsi per uno dei seguenti motivi:
  - Il ruolo IAM per il log di flusso non dispone di autorizzazioni sufficienti per pubblicare i record del log di flusso nel CloudWatch gruppo di log
  - Il ruolo IAM non ha una relazione di trust con il servizio dei log di flusso.
  - La relazione di trust non specifica il servizio di log di flusso come entità principale.

  Per ulteriori informazioni, consulta Ruolo IAM per la pubblicazione dei log di flusso su Logs CloudWatch .
- `Unknown error`: si è verificato un errore interno nel servizio log di flusso.

## Log di flusso attivo, ma nessun record di log di flusso o gruppo di log

### Problema

Hai creato un flusso di log e la console Amazon VPC o Amazon EC2; visualizza il log di flusso come `Active`. Tuttavia, non è possibile visualizzare alcun flusso di log in CloudWatch Logs o file di log nel bucket Amazon S3.

Possibili cause

- Il flusso di log è ancora in corso di creazione. In alcuni casi, dopo che il flusso di log è stato creato possono essere richiesti fino a 10 minuti o più per creare il gruppo di log e per visualizzare i dati.
- Non è ancora stato registrato alcun traffico per le interfacce di rete. Il gruppo di log in CloudWatch Logs viene creato solo quando viene registrato il traffico.

Soluzione

Attendi alcuni minuti per la creazione del gruppo di log o per la registrazione del traffico.

## Errore «LogDestinationNotFoundEccezione» o «Accesso negato per» LogDestination

Problema

Viene visualizzato un errore `Access Denied for LogDestination` o `LogDestinationNotFoundException` quando si tenta di creare un flusso di log.

Possibili cause

- Quando si crea un flusso di log che pubblica i dati in un bucket Amazon S3, questo errore indica che non è stato possibile trovare il bucket S3 specificato o che la policy del bucket non permette di inviare i log al bucket.
- Quando si crea un log di flusso che pubblica dati su Amazon CloudWatch Logs, questo errore indica che il ruolo IAM non consente la consegna dei log al gruppo di log.

Soluzione

- Quando si pubblica in Amazon S3, verifica di aver specificato l'ARN di un bucket S3 esistente e che l'ARN sia nel formato corretto. Se non si possiede il bucket S3, verifica che la policy del bucket disponga delle autorizzazioni richieste e utilizzi l'ID account e il nome del bucket corretti nell'ARN.
- Durante la pubblicazione su CloudWatch Logs, verifica che il ruolo IAM disponga delle autorizzazioni richieste.

## Superamento del limite di policy del bucket Amazon S3

### Problema

Ricevi il seguente errore quando provi a creare un log di fluss: `LogDestinationPermissionIssueException`.

### Possibili cause

Le dimensioni delle policy dei bucket Amazon S3 sono limitate a 20 KB.

Ogni volta che viene creato un log di flusso che pubblica in un bucket Amazon S3, l'ARN del bucket specificato, che include il percorso della cartella, viene aggiunto automaticamente all'elemento `Resource` nella policy di bucket.

Creare log di flusso multipli che pubblicano nello stesso bucket potrebbe causare il superamento dei limiti della policy di bucket.

### Soluzione

- Ripulisci la policy del bucket rimuovendo le voci del flusso di log non più necessarie.
- Concedere autorizzazioni all'intero bucket sostituendo le singole voci del log di flusso con quanto segue.

  ```
  arn:aws:s3:::bucket_name/*
  ```

  Se si concedono autorizzazioni all'intero bucket, nuove sottoscrizioni al log di flusso non aggiungono nuove autorizzazioni alla policy di bucket.

## LogDestination non consegnabile

### Problema

Ricevi il seguente errore quando provi a creare un log di fluss: `LogDestination <bucket name> is undeliverable`.

### Possibili cause

Il bucket Amazon S3 di destinazione è crittografato utilizzando la crittografia lato server con AWS KMS (SSE-KMS) e la crittografia predefinita del bucket è un ID chiave KMS.

### Soluzione

Il valore deve essere l'ARN di una chiave KMS. Cambia il tipo di crittografia S3 predefinita dall'ID chiave KMS ad ARN della chiave KMS. Per ulteriori informazioni, consulta Configurazione della crittografia predefinita nella Guida per l'utente di Amazon Simple Storage Service.

# Parametri di CloudWatch per i VPC

Amazon VPC pubblica i dati sui tuoi VPC su Amazon CloudWatch. Puoi recuperare le statistiche sui VPC come set ordinato di dati di serie temporali, noti anche come parametri. Pensa a un parametro come a una variabile da monitorare e ai dati come ai valori di questa variabile nel tempo. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon CloudWatch.

Indice



## Parametri e dimensioni di NAU

Network Address Usage (NAU) (NAU) è un parametro applicato alle risorse sulla rete virtuale che consentono di pianificare e monitorare le dimensioni del VPC. Il monitoraggio del NAU è gratuito. Il monitoraggio del NAU è utile perché se si esauriscono le quote NAU o NAU con peering per il VPC, non è possibile avviare nuove istanze EC2 né eseguire il provisioning di nuove risorse, come Network Load Balancer, endpoint VPC, funzioni Lambda, collegamenti del gateway di transito alla VPN e gateway NAT.

Se hai abilitato il monitoraggio del NAU per un VPC, Amazon VPC invia i parametri relativi a NAU ad Amazon CloudWatch. La dimensione di un VPC viene misurata dal numero di unità NAU (Network Address Usage) contenute nel VPC.

È possibile utilizzare questi parametri per comprendere il tasso di crescita del VPC, prevedere quando il VPC raggiungerà il limite di dimensione o creare allarmi quando le soglie di dimensione vengono superate.

Lo spazio dei nomi `AWS/EC2` include i parametri descritti di seguito per il monitoraggio del NAU.

| Parametro | Descrizione |
| --- | --- |
| `NetworkAddressUsage` | Il numero di NAU per VPC. |

| Parametro | Descrizione |
| --- | --- |
| | Criteri per la creazione di report<br>• Ogni 24 ore.<br><br>Dimensioni<br>• Nome: `Per-VPC Metrics`, valore: l'ID VPC. |
| `NetworkAddressUsagePeered` | I NAU rientrano nel conteggio per il VPC e tutti i VPC con cui è stato effettuato il peering.<br><br>Criteri per la creazione di report<br>• Ogni 24 ore.<br><br>Dimensioni<br>• Nome: `Per-VPC Metrics`, valore: l'ID VPC. |

Lo spazio dei nomi `AWS/Usage` include i parametri descritti di seguito per il monitoraggio del NAU.

| Parametro | Descrizione |
| --- | --- |
| `ResourceCount` | Il numero di NAU per VPC.<br><br>Criteri per la creazione di report<br>• Ogni 24 ore.<br><br>Dimensioni<br>• Nome: `Service`, valore: `EC2`<br>• Nome: `Type`, valore: `Resource`<br>• Nome: `Resource`, valore: l'ID VPC. |

| Parametro | Descrizione |
| --- | --- |
| | • Nome: `Class`, valore: `NetworkAddressUsage` |
| `ResourceCount` | I NAU rientrano nel conteggio per il VPC e tutti i VPC con cui è stato effettuato il peering.<br><br>Criteri per la creazione di report<br><br>• Ogni 24 ore.<br><br>Dimensioni<br><br>• Nome: `Service`, valore: `EC2`<br>• Nome: `Type`, valore: `Resource`<br>• Nome: `Resource`, valore: l'ID VPC.<br>• Nome: `Class`, valore: `NetworkAddressUsagePeered` |
| `ResourceCount` | Una vista combinata dell'utilizzo NAU tra i VPC.<br><br>Criteri per la creazione di report<br><br>• Ogni 24 ore.<br><br>Dimensioni<br><br>• Nome: `Service`, valore: `EC2`<br>• Nome: `Type`, valore: `Resource`<br>• Nome: `Resource`, valore: `VPC`<br>• Nome: `Class`, valore: `NetworkAddressUsage` |

| Parametro | Descrizione |
| --- | --- |
| `ResourceCount` | Una vista combinata dell'utilizzo NAU tra i VPC con peering.<br><br>Criteri per la creazione di report<br><br>• Ogni 24 ore.<br><br>Dimensioni<br><br>• Nome: `Service`, valore: `EC2`<br>• Nome: `Type`, valore: `Resource`<br>• Nome: `Resource`, valore: `VPC`<br>• Nome: `Class`, valore: `NetworkAddressUsagePeered` |

## Abilita o disabilita il monitoraggio del NAU

Per visualizzare i parametri NAU in CloudWatch, devi prima abilitare il monitoraggio su ogni VPC da monitorare.

Abilitazione o disabilitazione del monitoraggio del NAU

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
3. Seleziona la casella di controllo per il VPC.
4. Seleziona Actions (Operazioni), Edit VPC settings (Modifica impostazioni del VPC).
5. Completa una delle seguenti operazioni:

   - Per abilitare il monitoraggio, seleziona Network mapping units metrics settings (Impostazioni parametri delle unità di mappatura), Enable network address usage metrics (Abilita i parametri di Network Address Usage).
   - Per disabilitare il monitoraggio, deseleziona Network mapping units metrics settings (Impostazioni parametri delle unità di mappatura), Enable network address usage metrics (Abilita i parametri di Network Address Usage).

Abilitazione o disabilitazione del monitoraggio tramite la riga di comando

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

## Esempio di allarme CloudWatch per NAU

È possibile utilizzare il seguente comando della AWS CLI e l'esempio `.json` per creare un allarme Amazon CloudWatch e una notifica SNS che monitori l'utilizzo del NAU del VPC con soglia di 50.000 NAU. Questo esempio richiede la creazione preventiva di un argomento Amazon SNS. Per ulteriori informazioni, consulta Nozioni di base su Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

```
aws cloudwatch put-metric-alarm --cli-input-json file://nau-alarm.json
```

Di seguito è riportato un esempio di `nau-alarm.json`.

```
{
    "Namespace": "AWS/EC2",
    "MetricName": "NetworkAddressUsage",
    "Dimensions": [{
        "Name": "Per-VPC Metrics",
        "Value": "vpc-0123456798"
    }],
    "AlarmActions": ["arn:aws:sns:us-west-1:123456789012:my_sns_topic"],
    "ComparisonOperator": "GreaterThanThreshold",
    "Period": 86400,
    "EvaluationPeriods": 1,
    "Threshold": 50000,
    "AlarmDescription": "Tracks NAU utilization of the VPC with 50k NAUs as the
 threshold",
    "AlarmName": "VPC NAU Utilization",
    "Statistic": "Maximum"
}
```

# Sicurezza in Amazon Virtual Private Cloud

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per informazioni sui programmi di conformità che si applicano ad Amazon Virtual Private Cloud, consulta AWS Services in Scope by Compliance Program AWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio 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 aiuta a comprendere come applicare il modello di responsabilità condivisa quando si utilizza Amazon VPC. Gli argomenti seguenti illustrano come configurare Amazon VPC per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Amazon VPC.

Indice

# Protezione dei dati in Amazon Virtual Private Cloud

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in Amazon Virtual Private Cloud. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. 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 .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or 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.
- Usa 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 soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno 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 hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite 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. Ciò include quando lavori con Amazon VPC o altro Servizi AWS utilizzando la console, l'API o AWS gli AWS CLI SDK. 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.

## Riservatezza del traffico Internet in Amazon VPC

Amazon Virtual Private Cloud fornisce caratteristiche che puoi utilizzare per aumentare e monitorare la sicurezza del tuo virtual private cloud (VPC):

- Gruppi di sicurezza: i gruppi di sicurezza consentono traffico specifico in entrata e in uscita a livello di risorsa (ad esempio un'istanza EC2). Quando avvii un'istanza, puoi associare tale istanza a uno o più gruppi di sicurezza. Ogni istanza nel VPC può appartenere a un set differente di gruppi di sicurezza. Se non specifichi un gruppo di sicurezza quando avvii un'istanza, questa viene automaticamente associata al gruppo di sicurezza predefinito per il VPC. Per ulteriori informazioni, consulta Gruppi di sicurezza.
- Lista di controllo degli accessi (ACL): le liste di controllo degli accessi di rete permettono o negano traffico in entrata e in uscita specifico a livello di sottorete. Per ulteriori informazioni, consulta Come controllare il traffico verso le sottoreti utilizzando le liste di controllo degli accessi di rete.
- Log di flusso: i log di flusso VPC acquisiscono informazioni sul traffico IP da e verso le interfacce di rete nel VPC. È possibile creare un log di flusso per un VPC, una sottorete o un'interfaccia di rete singola. I dati dei log di flusso vengono pubblicati su CloudWatch Logs o Amazon S3 e possono aiutarti a diagnosticare regole ACL di rete e gruppi di sicurezza eccessivamente restrittive o eccessivamente permissive. Per ulteriori informazioni, consulta Registrazione del traffico IP utilizzando log di flusso VPC.
- Mirroring del traffico: puoi copiare il traffico di rete da un'interfaccia di rete elastica di un'istanza Amazon EC2. È quindi possibile inviare il traffico ai dispositivi di sicurezza e monitoraggio. out-of-band Per ulteriori informazioni, vedere la Guida al mirroring del traffico.

# Identity and Access Management per Amazon VPC

AWS Identity and Access Management (IAM) è un programma Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) a utilizzare risorse Amazon VPC. IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Indice

- Come funziona Amazon VPC con IAM
- Esempi delle policy di Amazon VPC
- Risoluzione dei problemi relativi all'identità e all'accesso di Amazon VPC
- AWS politiche gestite per Amazon Virtual Private Cloud

## Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon VPC.

Utente del servizio - Se utilizzi il servizio Amazon VPC per eseguire il tuo lavoro, l'amministratore fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di caratteristiche Amazon VPC utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità in Amazon VPC, consulta Risoluzione dei problemi relativi all'identità e all'accesso di Amazon VPC.

Amministratore del servizio - Se sei il responsabile delle risorse Amazon VPC presso la tua azienda, probabilmente disponi dell'accesso completo ai servizi che utilizzi. Il tuo compito è determinare le caratteristiche e le risorse Amazon VPC a cui i dipendenti devono accedere. Devi quindi inviare richieste all'amministratore IAM per la modifica delle 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 Amazon VPC, consulta Come funziona Amazon VPC con IAM.

Amministratore IAM: gli amministratori IAM potrebbero essere interessati a ottenere informazioni dettagliate su come scrivere policy per gestire l'accesso ad Amazon VPC. Per visualizzare le policy di esempio, consulta Esempi delle policy di Amazon VPC.

## Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se

accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo 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 AWSnella Guida per l'utente IAM.

### Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso 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. Conserva le credenziali dell'utente root e utilizzale 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 IAM.

### Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che 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 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 IAMAdmins 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 IAM.

## Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente 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 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 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, con alcuni Servizi AWS, è possibile allegare 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 IAM.

- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di 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.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un preside. 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 chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. 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 che un servizio assume per eseguire azioni 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 AWSnella Guida per l'utente 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'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e 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: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di 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 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 degli accessi tramite le policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come 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 IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. 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. L'amministratore può quindi 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 dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

### 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 azioni 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 IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. 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 IAM.

## Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare 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 utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata 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 puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle 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 su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF 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 tipi di policy aggiuntivi e 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 funzionalità 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 IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account

AWS 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. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. 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 IAM.

### Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

## Come funziona Amazon VPC con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon VPC, è necessario comprendere quali funzioni IAM sono disponibili per l'uso con Amazon VPC. Per avere una visione di alto livello di come Amazon VPC e AWS altri servizi funzionano con IAM, AWS consulta i servizi che funzionano con IAM nella IAM User Guide.

Indice



Con le policy basate sull'identità IAM, è possibile specificare azioni consentite o negate. Per alcune azioni, è possibile specificare le risorse e le condizioni in cui le azioni sono consentite o negate.

Amazon VPC supporta specifiche operazioni, risorse e chiavi di condizione. 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 chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. 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.

L'operazione viene utilizzata in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Amazon VPC condivide il suo spazio dei nomi API con Amazon EC2. Le operazioni delle policy in Amazon VPC utilizzano il seguente prefisso prima dell'operazione: `ec2:`. Ad esempio, per concedere a un utente l'autorizzazione a creare un VPC utilizzando l'operazione API `CreateVpc`, concedi l'accesso all'operazione `ec2:CreateVpc`. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`.

Per specificare più operazioni in una singola istruzione, separarle con virgole, come illustrato nell'esempio seguente.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

Puoi specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `Describe`, includi la seguente operazione.

```
"Action": "ec2:Describe*"
```

Per visualizzare un elenco di operazioni di Amazon EC2, consulta Operazioni definite da Amazon EC2 nella Guida di riferimento per l'autorizzazione al servizio.

## Risorse

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. 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": "*"
```

La risorsa VPC ha l'ARN mostrato nell'esempio seguente.

```
arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}
```

Ad esempio, per specificare il VPC `vpc-1234567890abcdef0` nell'istruzione, utilizzare l'ARN mostrato nell'esempio seguente.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-1234567890abcdef0"
```

Per specificare tutti i VPC di una regione specifica che appartengono a un account specifico, utilizza il carattere jolly (*).

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
```

Alcune operazioni Amazon VPC, 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": "*"
```

Molte operazioni API di Amazon EC2 coinvolgono più risorse. Per specificare più risorse in una singola istruzione, separa gli ARN con le virgole.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Per visualizzare un elenco di tipi di risorse Amazon VPC e i relativi ARN, consulta Tipi di risorse definiti da Amazon EC2 nella Guida di riferimento per l'autorizzazione al servizio.

## Chiavi di condizione

Gli amministratori possono utilizzare le policy AWS JSON 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 si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` 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 del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Tutte le operazioni Amazon EC2 supportano le chiavi di condizione `aws:RequestedRegion` e `ec2:Region`. Per ulteriori informazioni, consulta Esempio: limitazione dell'accesso a una regione specifica.

Amazon VPC definisce il proprio set di chiavi di condizione e supporta anche l'uso di alcune chiavi di condizione globali. Per visualizzare un elenco di chiavi di condizione Amazon VPC, consulta nella

Chiavi di condizione per Amazon EC2 nella Guida di riferimento per l'autorizzazione al servizio. Per scoprire con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Operazioni definite da Amazon EC2.

### Policy basate sulle risorse di Amazon VPC

Le policy basate su risorse sono documenti di policy JSON che specificano le operazioni che possono essere eseguite da un'entità principale specificata sulla risorsa Amazon VPC e in base a quali condizioni.

Per consentire l'accesso a più account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata su risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa si trovano in AWS account diversi, è inoltre necessario concedere all'entità principale l'autorizzazione ad accedere alla risorsa. Concedi l'autorizzazione collegando una policy basata sull'identità all'entità. Tuttavia, se una policy basata su risorse concede l'accesso a un'entità 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.

### Autorizzazione basata su tag

Puoi collegare i tag alle risorse Amazon VPC o passarli in una richiesta. Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione. Per ulteriori informazioni, consulta Applicazione di tag durante la creazione e Controllo dell'accesso alle risorse EC2 mediante tag di risorse nella Guida per l'utente di Amazon EC2.

Per visualizzare un esempio di policy basata su identità per limitare l'accesso a una risorsa in base ai tag di tale risorsa, consulta Avvio di istanze in un VPC specifico.

### Ruoli IAM

Un ruolo IAM è un'entità all'interno dell'utente Account AWS che dispone di autorizzazioni specifiche.

#### Utilizzo di credenziali temporanee

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. Puoi ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come AssumeRoleo GetFederation Token.

Amazon VPC supporta l'uso di credenziali temporanee.

Ruoli collegati ai servizi

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

I gateway di transito supportano i ruoli collegati al servizio.

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore IAM può modificare le autorizzazioni per questo ruolo. Tuttavia, questo potrebbe pregiudicare la funzionalità del servizio.

Amazon VPC supporta i ruoli di servizio per i log di flusso. Quando si crea un log di flusso, è necessario scegliere un ruolo che consenta al servizio di log di flusso di accedere a Logs. CloudWatch Per ulteriori informazioni, consulta the section called “Ruolo IAM per la pubblicazione dei log di flusso su Logs CloudWatch ”.

## Esempi delle policy di Amazon VPC

Per impostazione predefinita, i ruoli IAM non dispongono dell'autorizzazione per creare o modificare risorse del VPC. Inoltre, non possono eseguire attività utilizzando l'API AWS Management Console AWS CLI, o AWS . Un amministratore IAM deve creare policy IAM che concedono ai ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi collegare queste policy ai ruoli IAM che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente di IAM.

Indice

- Creare un VPC con una sottorete pubblica
- Modifica ed eliminazione delle risorse VPC
- Gestione dei gruppi di sicurezza
- Gestione delle regole del gruppo di sicurezza
- Avvio di istanze in una sottorete specifica
- Avvio di istanze in un VPC specifico
- Esempi aggiuntivi di policy di Amazon VPC

## Best practice per le policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon VPC nell'account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: 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 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 anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio 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 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 alla sintassi 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 IAM.

- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'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 IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

## Utilizzo della console Amazon VPC

Per accedere alla console Amazon VPC, è necessario disporre di un set di autorizzazioni minimo. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Amazon VPC nel AWS tuo account. Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (ruoli IAM) associate a tale policy.

La seguente policy concede ai ruoli l'autorizzazione per elencare le risorse nella console VPC, ma non per crearle, aggiornarle o eliminarle.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeMovingAddresses",
```

```
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeStaleSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTrafficMirrorFilters",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetManagedPrefixListAssociations",
                "ec2:GetManagedPrefixListEntries"
            ],
            "Resource": "*"
        }
    ]
}
```

Non è necessario consentire autorizzazioni minime da console per i ruoli che effettuano chiamate solo verso AWS CLI o l'API. AWS Al contrario, concedi l'accesso solo alle operazioni che soddisfano l'operazione API che il ruolo deve eseguire.

## Creare un VPC con una sottorete pubblica

L'esempio seguente consente ai ruoli di creare VPC, sottoreti, tabelle di instradamento e gateway Internet. Gli utenti possono anche collegare un gateway Internet a un VPC e creare route nelle tabelle di instradamento. L'operazione `ec2:ModifyVpcAttribute` consente ai ruoli di abilitare i nomi host DNS per il VPC in modo che ogni istanza lanciata in un VPC riceva un nome host DNS.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateInternetGateway",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource": "*"
    }
   ]
}
```

La policy precedente consente inoltre ai ruoli di creare un VPC nella console Amazon VPC.

## Modifica ed eliminazione delle risorse VPC

È possibile che sia necessario controllare le risorse VPC che i ruoli possono modificare o eliminare. Ad esempio, la seguente policy consente ai ruoli di utilizzare ed eliminare le tabelle di instradamento che hanno il tag `Purpose=Test`. La policy specifica inoltre che i ruoli possono eliminare solo i gateway Internet che hanno il tag `Purpose=Test`. I ruoli non possono utilizzare tabelle di instradamento o gateway Internet che non hanno questo tag.

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

```
            "Action": "ec2:DeleteInternetGateway",
            "Resource": "arn:aws:ec2:*:*:internet-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRouteTable",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:route-table/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        }
    ]
}
```

## Gestione dei gruppi di sicurezza

La policy seguente consente ai ruoli di gestire i gruppi di sicurezza. La prima istruzione consente ai ruoli di eliminare qualsiasi gruppo di sicurezza con il tag `Stack=test` e gestire le regole in entrata e in uscita per tutti i gruppi di sicurezza con il tag `Stack=test`. La seconda istruzione richiede ai ruoli di taggare tutti i gruppi di sicurezza creati con il tag `Stack=Test`. La terza istruzione consente ai ruoli di creare tag durante la creazione di un gruppo di sicurezza. La quarta istruzione consente ai ruoli di visualizzare qualsiasi gruppo di sicurezza e regola del gruppo di sicurezza. La quinta istruzione consente ai ruoli di creare un gruppo di sicurezza in un VPC.

> **Note**
>
> Questa politica non può essere utilizzata dal AWS CloudFormation servizio per creare un gruppo di sicurezza con tag obbligatori. Se rimuovi la condizione sull'azione `ec2:CreateSecurityGroup` che richiede il tag, la policy funzionerà.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:ModifySecurityGroupRules",
                "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Stack": "test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Stack": "test"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "Stack"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeVpcs",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        }
    ]
}
```

Per permettere ai ruoli di modificare il gruppo di sicurezza associato a un'istanza, aggiungi l'operazione `ec2:ModifyInstanceAttribute` alla policy.

Per permettere ai ruoli di modificare i gruppi di sicurezza per un'interfaccia di rete, aggiungi l'operazione `ec2:ModifyNetworkInterfaceAttribute` alla policy.

## Gestione delle regole del gruppo di sicurezza

La seguente policy concede ai ruoli l'autorizzazione per visualizzare tutti i gruppi di sicurezza e le regole del gruppo di sicurezza, per aggiungere e rimuovere le regole in entrata e in uscita per i gruppi di sicurezza per un VPC specifico e per modificare le descrizioni delle regole per il VPC specificato. La prima istruzione utilizza la chiave di condizione `ec2:Vpc` per determinare l'ambito delle autorizzazioni di un VPC specifico.

La seconda istruzione concede ai ruoli l'autorizzazione per descrivere tutti i gruppi di sicurezza, le regole dei gruppi di sicurezza e i tag. In questo modo i ruoli possono visualizzare le regole dei gruppi di sicurezza per modificarle.

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

```
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupEgress",
       "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
       "ec2:ModifySecurityGroupRules"
    ],
     "Resource": "arn:aws:ec2:region:account-id:security-group/*",
      "Condition": {
        "ArnEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:DescribeSecurityGroups",
          "ec2:DescribeSecurityGroupRules",
          "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:ModifySecurityGroupRules"
      ],
      "Resource": "arn:aws:ec2:region:account-id:security-group-rule/*"
    }
  ]
}
```

## Avvio di istanze in una sottorete specifica

La seguente policy concede ai ruoli le autorizzazioni per avviare le istanze in una sottorete specifica e utilizzare un gruppo di sicurezza specifico nella richiesta. La policy esegue questa operazione specificando l'ARN per la sottorete e l'ARN per il gruppo di sicurezza. Se gli utenti provano ad avviare un'istanza in una sottorete diversa o utilizzando un gruppo di sicurezza diverso, la richiesta non va a buon fine (a meno che un'altra policy o istruzione non conceda ai ruoli l'autorizzazione appropriata).

La policy concede anche l'autorizzazione per utilizzare la risorsa dell'interfaccia di rete. Quando viene avviata in una sottorete, la richiesta `RunInstances` crea un'interfaccia di rete principale per impostazione predefinita, pertanto il ruolo necessita dell'autorizzazione per creare questa risorsa quando avvia l'istanza.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-*",
        "arn:aws:ec2:region:account:instance/*",
        "arn:aws:ec2:region:account:subnet/subnet-id",
        "arn:aws:ec2:region:account:network-interface/*",
        "arn:aws:ec2:region:account:volume/*",
        "arn:aws:ec2:region:account:key-pair/*",
        "arn:aws:ec2:region:account:security-group/sg-id"
      ]
    }
   ]
}
```

## Avvio di istanze in un VPC specifico

La seguente policy concede ai ruoli l'autorizzazione per avviare istanze in qualsiasi sottorete all'interno di un VPC specifico. La policy fa questo applicando una chiave di condizione (`ec2:Vpc`) alla risorsa di sottorete.

La policy concede inoltre ai ruoli l'autorizzazione per avviare le istanze utilizzando solo le AMI con il tag "`department=dev`".

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account-id:subnet/*",
        "Condition": {
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
         }
```

```
        }
    },
    {
        "Effect": "Allow",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:region::image/ami-*",
        "Condition": {
            "StringEquals": {
                "ec2:ResourceTag/department": "dev"
                }
        }
    },
    {
        "Effect": "Allow",
        "Action": "ec2:RunInstances",
        "Resource": [
            "arn:aws:ec2:region:account:instance/*",
            "arn:aws:ec2:region:account:volume/*",
            "arn:aws:ec2:region:account:network-interface/*",
            "arn:aws:ec2:region:account:key-pair/*",
            "arn:aws:ec2:region:account:security-group/*"
            ]
        }
    ]
}
```

## Esempi aggiuntivi di policy di Amazon VPC

Puoi trovare ulteriori esempi di policy IAM relative ad Amazon VPC nella seguente documentazione:

- Elenchi di prefissi gestiti
- Mirroring del traffico
- Gateway di transito
- Endpoint VPC e servizi endpoint VPC
- Policy di endpoint VPC
- Peering VPC
- AWS Wavelength

# Risoluzione dei problemi relativi all'identità e all'accesso di Amazon VPC

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Amazon VPC e IAM.

Problemi



## Non sono autorizzato a eseguire un'operazione in Amazon VPC

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

Il seguente errore di esempio si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una sottorete ma appartiene a un ruolo IAM che non dispone delle autorizzazioni `ec2:DescribeSubnets`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeSubnets on resource: subnet-id
```

In questo caso, Mateo richiede al suo amministratore di aggiornare le sue policy per poter accedere alla sottorete.

## Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, per poter passare un ruolo ad Amazon VPC dovrai aggiornare le policy.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. 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` cerca di utilizzare la console per eseguire un'operazione in Amazon VPC. 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`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse Amazon VPC

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 degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon VPC supporta queste caratteristiche, consulta Come funziona Amazon VPC con IAM.
- Per scoprire come fornire l'accesso alle tue risorse su Account AWS risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti 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 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.

# AWS politiche gestite per Amazon Virtual Private Cloud

Una politica AWS gestita è una politica autonoma creata e amministrata da. AWS AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti 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 politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

## AWS politica gestita: AmazonVPC FullAccess

Puoi collegare la policy `AmazonVPCFullAccess` alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso completo ad Amazon VPC.

Per visualizzare le autorizzazioni relative a questa politica, consulta FullAccessAmazonVPC nel Managed Policy Reference.AWS

## AWS politica gestita: AmazonVPC Access ReadOnly

Puoi collegare la policy `AmazonVPCReadOnlyAccess` alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso in sola lettura ad Amazon VPC.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonVPC ReadOnly Access nel Managed Policy Reference.AWS

## AWS politica gestita: AmazonVPC Operations CrossAccount NetworkInterface

È possibile allegare la policy `AmazonVPCCrossAccountNetworkInterfaceOperations`alle identità IAM. Questa policy concede autorizzazioni che consentono all'identità di creare interfacce di rete e di collegarle alle risorse tra account.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonVPC CrossAccount NetworkInterface Operations nel Managed Policy Reference.AWS

## Amazon VPC si aggiorna alle AWS policy gestite

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per Amazon VPC da quando questo servizio ha iniziato a tracciare queste modifiche a marzo 2021.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| the section called “Amazon VPC FullAccess”: aggiornamento a una policy esistente | È stata aggiunta l'GetSecurityGroupsForVpcazione, che ti consente di ottenere gruppi di sicurezza utilizzabili nel tuo VPC. | 8 febbraio 2024 |
| the section called “Accesso ad ReadOnly Amazon VPC”: aggiornamento a una policy esistente | È stata aggiunta l'GetSecurityGroupsForVpcazione, che ti consente di ottenere gruppi di sicurezza utilizzabili nel tuo VPC. | 8 febbraio 2024 |
| the section called “Operazioni Amazon VPC CrossAccount NetworkInterface”: aggiornamento a una policy esistente | Sono state aggiunte le azioni AssignIpv6Addresses e UnassignIpv6Addresses, che consentono di gestire gli indirizzi IPv6 associati alle interfacce di rete. | 25 settembre 2023 |
| the section called “Accesso ad ReadOnly Amazon VPC”: aggiornamento a una policy esistente | Aggiunta l'azione DescribeSecurityGroupRules, che consente di visualizzare le regole del gruppo di sicurezza. | 2 agosto 2021 |
| the section called “Amazon VPC FullAccess”: aggiornamento a una policy esistente | Aggiunte le azioni DescribeSecurityGroupRules e ModifySecurityGroupRules, che | 2 agosto 2021 |

| Modifica | Descrizione | Data |
| --- | --- | --- |
| | consentono di visualizz are le regole del gruppo di sicurezza. | |
| the section called “Amazon VPC FullAccess”: aggiornam ento a una policy esistente | Sono state aggiunte azioni per gateway carrier, pool IPv6, gateway locali e tabelle di routing del gateway locale. | 23 giugno 2021 |
| the section called “Accesso ad ReadOnly Amazon VPC”: aggiornamento a una policy esistente | Sono state aggiunte azioni per gateway carrier, pool IPv6, gateway locali e tabelle di routing del gateway locale. | 23 giugno 2021 |

# Sicurezza dell'infrastruttura in Amazon VPC

In quanto servizio gestito, Amazon Virtual Private Cloud è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere ad Amazon VPC attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), 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. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

## Isolamento della rete

Un cloud privato virtuale (VPC) è una rete virtuale nella propria area logicamente isolata nel cloud. AWS Utilizza VPC separati per isolare l'infrastruttura in base a carico di lavoro o entità dell'organizzazione.

Una sottorete è un intervallo di indirizzi IP in un VPC. Quando avvii un'istanza, questa operazione viene eseguita in una sottorete nel VPC. Utilizza sottoreti per isolare i livelli dell'applicazione (ad esempio, web, applicazione e database) all'interno di un singolo VPC. Utilizza sottoreti private per le istanze se non devono essere accessibili direttamente da Internet.

Puoi utilizzarlo AWS PrivateLinkper abilitare la connessione alle risorse del tuo VPC Servizi AWS utilizzando indirizzi IP privati, come se tali servizi fossero ospitati direttamente nel tuo VPC. Pertanto, non è necessario utilizzare un gateway Internet o un dispositivo NAT per accedere. Servizi AWS

## Controllo del traffico di rete

Valuta le opzioni seguenti per il controllo del traffico di rete verso le risorse nel VPC, come le istanze EC2:

- Sfrutta i gruppi di sicurezza come meccanismo principale per controllare l'accesso della rete ai VPC. Se necessario, utilizza le liste di controllo degli accessi alla rete (ACL di rete) per fornire un controllo di rete stateless non granulare. I gruppi di sicurezza sono più versatili delle ACL di rete grazie alla loro capacità di eseguire il filtro dei pacchetti stateful e di creare regole che fanno riferimento ad altri gruppi di sicurezza. Le ACL di rete possono essere efficaci come controllo secondario (ad esempio, per rifiutare un sottoinsieme specifico di traffico) o per fornire alla sottorete una protezione di alto livello. Inoltre, poiché gli ACL di rete si applicano a un'intera sottorete, possono essere utilizzati come defense-in-depth nel caso in cui un'istanza venga avviata senza il gruppo di sicurezza corretto.
- Utilizza sottoreti private per le istanze se non devono essere accessibili direttamente da Internet. Utilizza un host bastione o gateway NAT per l'accesso a Internet dalle istanze nelle sottoreti private.
- Configura le tabelle di instradamento della sottorete con i percorsi di rete minimi per supportare i tuoi requisiti di connettività.
- Prendi in considerazione l'utilizzo di gruppi di sicurezza aggiuntivi per controllare e verificare il traffico di gestione delle istanze Amazon EC2 separatamente dal normale traffico delle applicazioni. Pertanto, puoi implementare policy IAM speciali per il controllo delle modifiche, semplificando l'audit delle modifiche apportate alle regole dei gruppi di sicurezza o agli script di verifica

automatica delle regole. Più interfacce di rete forniscono inoltre opzioni aggiuntive per il controllo del traffico di rete, inclusa la possibilità di creare policy di instradamento basate su host o sfruttare diverse regole di instradamento delle sottoreti VPC basate sulle interfacce di rete assegnate a una sottorete.

- Utilizza AWS Virtual Private Network o AWS Direct Connect per stabilire connessioni private dalle tue reti remote ai tuoi VPC. Per ulteriori informazioni, consulta Opzioni di connettività tra rete e Amazon VPC.
- Utilizza Log di flusso VPC per monitorare il traffico che raggiunge le istanze.
- Utilizza AWS Security Hub per verificare accessibilità di rete indesiderata dalle istanze.
- Utilizza AWS Network Firewall per proteggere le sottoreti del VPC dalle minacce di rete comuni.

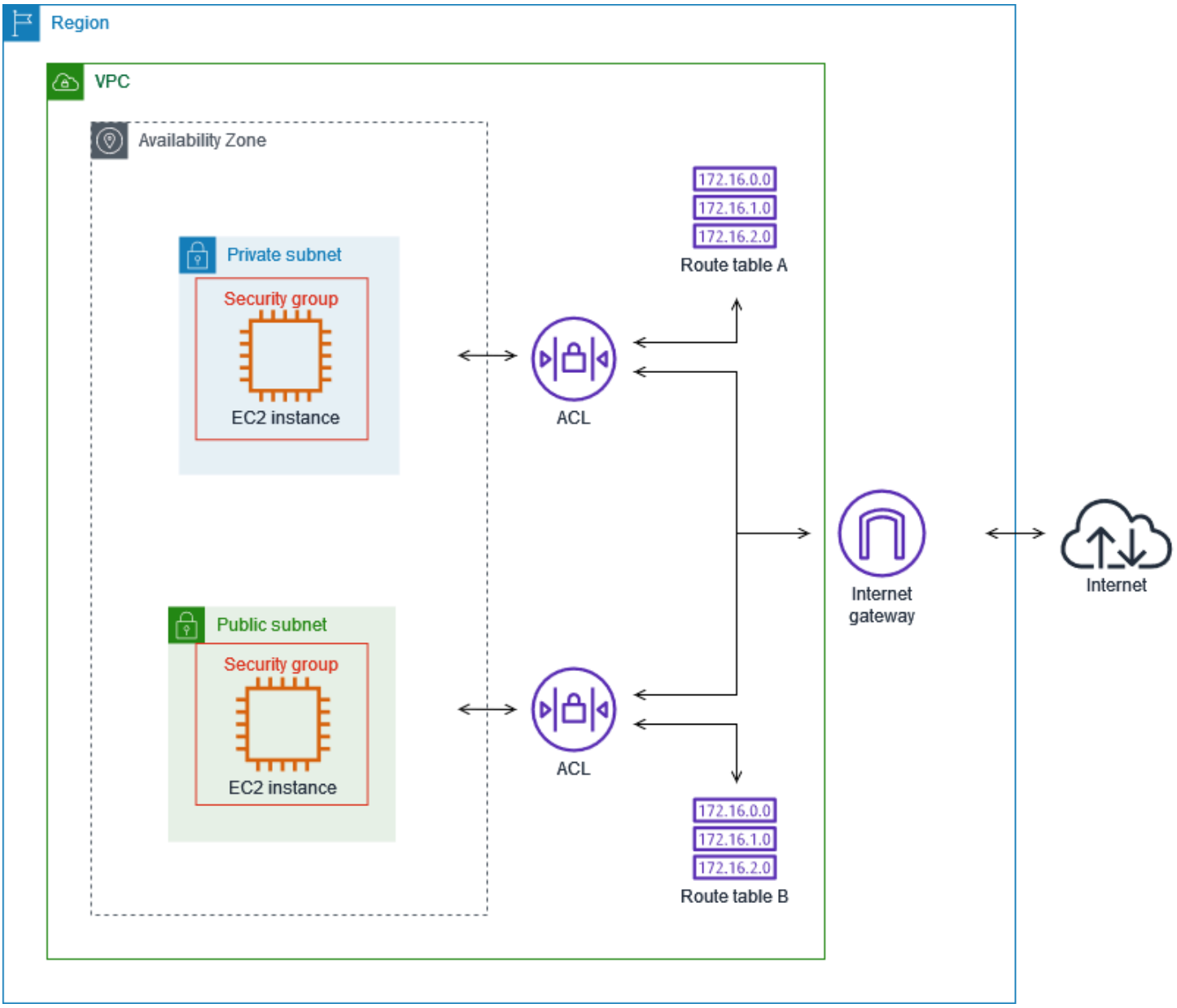
## Confronto dei gruppi di sicurezza e delle liste di controllo accessi di rete

Nella tabella seguente vengono riepilogate le differenze basilari tra i gruppi di sicurezza e le liste di controllo accessi di rete.

| Gruppo di sicurezza | Lista di controllo degli accessi di rete |
|---|---|
| Opera a livello di istanza. | Opera a livello di sottorete. |
| Si applica a un'istanza solo se è associata all'istanza | Si applica a tutte le istanze distribuite nella sottorete associata (fornendo un livello di difesa supplementare se le regole del gruppo di sicurezza sono troppo permissive) |
| Supporta solo le regole Consenti. | Supporta le regole Consenti e Nega. |
| Valuta tutte le regole prima di decidere se consentire il traffico. | Quando decidiamo se consentire il traffico, valutiamo le regole in un certo ordine, a partire dalla regola numerata più bassa. |
| Stateful: il traffico di ritorno è consentito, a prescindere dalle regole | Stateless: il traffico di ritorno deve essere consentito esplicitamente dalle regole. |

Nel diagramma seguente sono illustrati i livelli di sicurezza forniti dai gruppi di sicurezza e dalle liste di controllo accessi di rete. Ad esempio, il traffico da un Internet Gateway viene instradato

alla sottorete appropriata utilizzando le route nella tabella di instradamento. Le regole delle liste di controllo accessi di rete associate alla sottorete determinano quale traffico è consentito alla sottorete. Le regole del gruppo di sicurezza associato a un'istanza determinano quale traffico è consentito all'istanza.



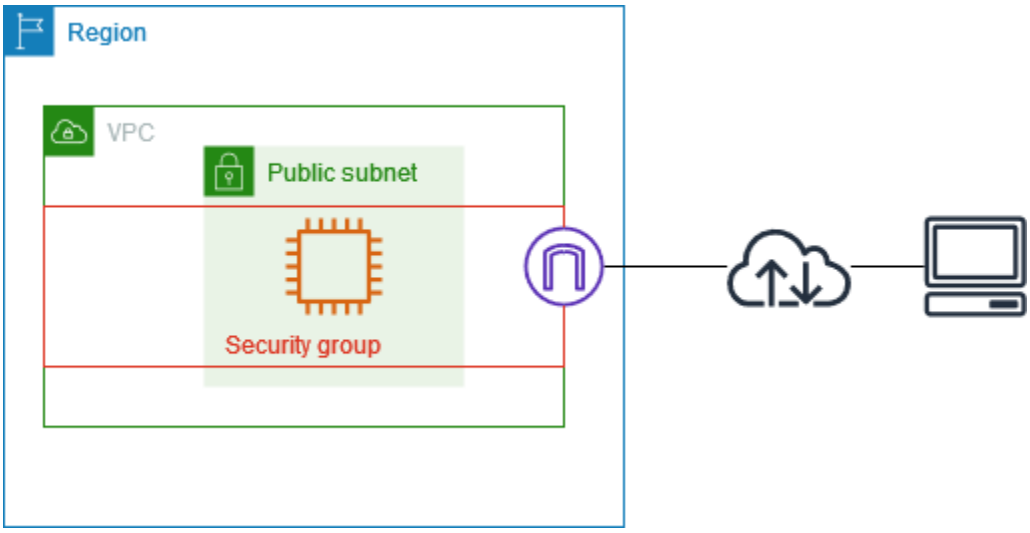

È possibile proteggere le istanze utilizzando solo gruppi di sicurezza. Tuttavia, è possibile aggiungere le liste di controllo degli accessi di rete come ulteriore livello di difesa. Per ulteriori informazioni, consulta Esempio: controllo dell'accesso alle istanze in una sottorete.

# Controlla il traffico verso le tue AWS risorse utilizzando i gruppi di sicurezza

Un gruppo di sicurezza controlla il traffico consentito per raggiungere e lasciare le risorse a cui è associato. Ad esempio, dopo aver associato un gruppo di sicurezza a un'istanza EC2, controlla il traffico in entrata e in uscita per l'istanza.

Al momento della creazione di un VPC, questo include un gruppo di sicurezza di default. È possibile creare gruppi di sicurezza aggiuntivi per un VPC, ciascuno con le proprie regole in entrata e in uscita. È possibile specificare l'origine, l'intervallo di porte e il protocollo per ogni regola in entrata. È possibile specificare la destinazione, l'intervallo di porte e il protocollo per ogni regola in uscita.

Il diagramma seguente mostra un VPC con una sottorete, un gateway Internet e un gruppo di sicurezza. La sottorete contiene un'istanza EC2. Il gruppo di sicurezza del viene assegnato all'istanza. Il gruppo di sicurezza funziona da firewall virtuale. L'unico traffico che raggiunge l'istanza è quello consentito dalle regole del gruppo di sicurezza. Ad esempio, se il gruppo di sicurezza contiene una regola che consente il traffico ICMP verso l'istanza dalla rete, è possibile eseguire il ping dell'istanza dal computer. Se il gruppo di sicurezza non contiene una regola che consenta il traffico SSH, non potrai connetterti all'istanza tramite SSH.




Indice

- Utilizzo dei gruppi di sicurezza

Prezzi

L'utilizzo di gruppi di sicurezza non comporta costi supplementari.

## Nozioni di base sui gruppi di sicurezza

- È possibile assegnare un gruppo di sicurezza solo alle risorse create nello stesso VPC del gruppo di sicurezza. Puoi assegnare più gruppi di sicurezza a una risorsa.
- Quando crei un gruppo di sicurezza, devi indicarne il nome e la descrizione. Si applicano le regole seguenti:
  - Il nome di un gruppo di sicurezza deve Essere univoco all'interno del VPC.
  - I nomi e le descrizioni possono avere una lunghezza massima di 255 caratteri.
  - I nomi e le descrizioni possono contenere solo i seguenti caratteri: a-z, A-Z, 0-9, spazi e ._-:/ ()#,@[]+=&;{}!$*.
  - Quando il nome contiene spazi finali, questi vengono eliminati. Ad esempio, se inserisci “Test Security Group ". per il nome, lo memorizziamo come “Test Security Group”.
  - Il nome di un gruppo di sicurezza non può iniziare per `sg-`.
- I gruppi di sicurezza sono stateful. Ad esempio, inviando una richiesta da un'istanza, il traffico in risposta alla richiesta è autorizzato a raggiungerla, indipendentemente dalle regole in entrata del gruppo di sicurezza. Le risposte al traffico in entrata autorizzato possono lasciare l'istanza indipendentemente dalle regole in uscita.
- I gruppi di sicurezza non filtrano il traffico destinato a e da i seguenti:
  - Amazon Domain Name Services (DNS)
  - Amazon Dynamic Host Configuration Protocol (DHCP)
  - Metadati delle istanze Amazon EC2.
  - Endpoint di metadati dei processi Amazon ECS
  - Attivazione della licenza per le istanze Windows
  - Servizio di sincronizzazione oraria di Amazon
  - Indirizzi IP riservati utilizzati dal router VPC predefinito
- Esistono delle quote per il numero di gruppi di sicurezza che si possono creare per ogni VPC, al numero di regole che si possono aggiungere a ciascun gruppo di sicurezza e al numero di gruppi

di sicurezza che si possono associare a un'interfaccia di rete. Per ulteriori informazioni, consulta Quote Amazon VPC.

Best practice

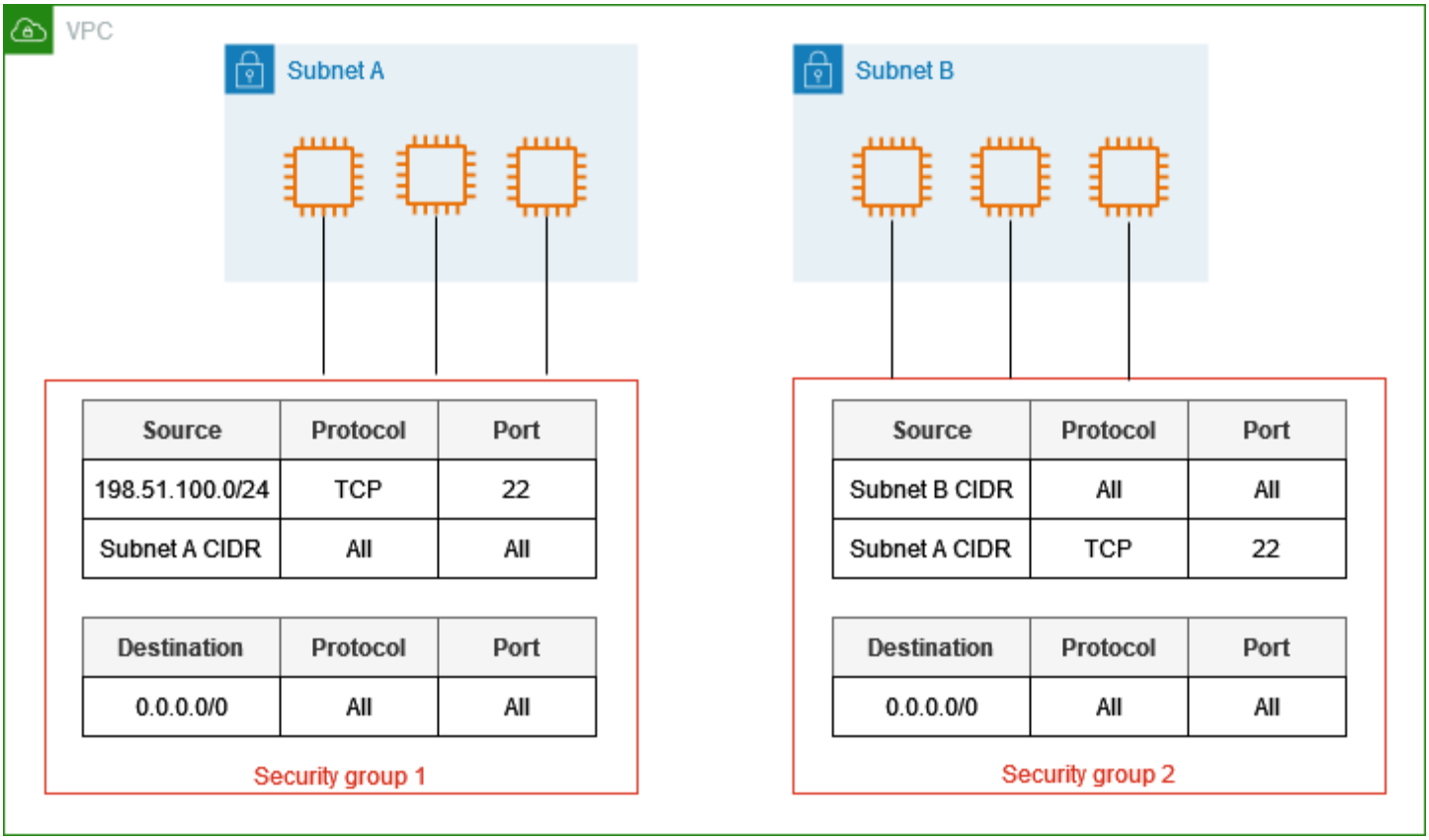
- Autorizza solo specifici principali IAM a creare e modificare gruppi di sicurezza.
- Crea il numero minimo di gruppi di sicurezza di cui hai bisogno per ridurre il rischio di errore. Utilizza ogni gruppo di sicurezza per gestire l'accesso a risorse con funzioni e requisiti di sicurezza simili.
- Quando aggiungi regole per le porte 22 (SSH) o 3389 (RDP) in modo da poter accedere alle istanze EC2, autorizza solo intervalli di indirizzi IP specifici. Se specifichi 0.0.0.0/0 (IPv4) e ::/ (IPv6), ciò consente a chiunque di accedere alle istanze da qualsiasi indirizzo IP utilizzando il protocollo specificato.
- Non aprire grandi intervalli di porte. Assicurati che l'accesso tramite ciascuna porta sia limitato alle origini o alle destinazioni che lo richiedono.
- Considera la creazione delle ACL di rete con regole simili a quelle dei gruppi di sicurezza, in modo tale da aggiungere un ulteriore livello di sicurezza al VPC. Per ulteriori informazioni sulle differenze tra gruppi di sicurezza e liste di controllo accessi di rete, consulta Confronto dei gruppi di sicurezza e delle liste di controllo accessi di rete.

## Esempio di gruppo di sicurezza

Il seguente diagramma mostra un VPC con due gruppi di sicurezza e due sottoreti. Le istanze nella sottorete A hanno gli stessi requisiti di connettività, quindi sono associate al gruppo di sicurezza 1. Le istanze nella sottorete B hanno gli stessi requisiti di connettività, quindi sono associate al gruppo di sicurezza 2. Le regole del gruppo di sicurezza consentono il traffico nel modo seguente:

- La prima regola in entrata nel gruppo di sicurezza 1 consente il traffico SSH verso le istanze nella sottorete A dall'intervallo di indirizzi specificato (ad esempio, un intervallo nella propria rete).
- La seconda regola in entrata nel gruppo di sicurezza 1 consente alle istanze della sottorete A di comunicare tra loro utilizzando qualsiasi protocollo e porta.
- La seconda regola in entrata nel gruppo di sicurezza 2 consente alle istanze della sottorete B di comunicare tra loro utilizzando qualsiasi protocollo e porta.
- La seconda regola in entrata nel gruppo di sicurezza 2 consente alle istanze della sottorete A di comunicare con le istanze nella sottorete B utilizzando SSH.

- Entrambi i gruppi di sicurezza usano la regola in uscita predefinita che consente tutto il traffico.




## Regole del gruppo di sicurezza

Le regole di un gruppo di sicurezza controllano il traffico in entrata autorizzato a raggiungere le risorse associate al gruppo di sicurezza. e il traffico in uscita autorizzato a lasciarle.

Puoi aggiungere o rimuovere le regole di un gruppo di sicurezza (autorizzazione o revoca dell'accesso in entrata o in uscita). Una regola si applica al traffico in entrata (ingresso) o al traffico in uscita (uscita). Puoi concedere l'accesso a un'origine o a una destinazione specifica.

Indice

- Utilizzo delle regole dei gruppi di sicurezza
- Regole di esempio
- Risolvere i problemi di raggiungibilità

## Nozioni di base sulle regole dei gruppi di sicurezza

- Puoi specificare regole che autorizzano, non regole che negano.
- Al momento della sua creazione, un gruppo di sicurezza è privo di regole in entrata. Di conseguenza, non è consentito alcun traffico in entrata fino a quando al gruppo di sicurezza non vengono aggiunte regole in entrata.
- Quando si crea per la prima volta un gruppo di sicurezza, questo include una regola in uscita che consente tutto il traffico in uscita dalla risorsa. Puoi rimuovere la regola e aggiungere regole in uscita che autorizzano l'uscita solo di un determinato tipo di traffico. Se un gruppo di sicurezza è privo di regole in uscita, non viene autorizzato alcun traffico in uscita.
- Se si associano a una risorsa molteplici gruppi di sicurezza, le regole di ciascun gruppo di sicurezza vengono aggregate efficacemente per creare un unico set di regole utilizzate per determinare se consentire l'accesso o meno.
- Quando si aggiunge, aggiorna o rimuove delle regole, queste si applicano automaticamente a tutte le risorse associate al gruppo di sicurezza. Gli effetti di alcune modifiche delle regole possono dipendere dalle modalità di monitoraggio del traffico. Per ulteriori informazioni, consulta Tracciamento delle connessioni nella Guida per l'utente di Amazon EC2.
- Quando crei una regola del gruppo di sicurezza, AWS assegna un ID univoco alla regola. È possibile utilizzare l'ID di una regola quando si utilizza l'API o la CLI per modificare o eliminare la regola.

### Limitazione

I gruppi di sicurezza non possono bloccare le richieste DNS da o verso il Route 53 Resolver, a volte indicato come «indirizzo IP VPC+2» (vedi Amazon Route 53 Resolvernella Amazon Route 53 Developer Guide) o come DNS. AmazonProvided Per filtrare le richieste DNS attraverso il risolutore Route 53, utilizza DNS Firewall per il risolutore Route 53.

## Componenti di una regola di un gruppo di sicurezza

- Protocollo: il protocollo da autorizzare. I protocolli più comuni sono 6 (TCP) 17 (UDP) e 1 (ICMP).

- Intervallo di porte: per un protocollo personalizzato o per TCP e UDP, l'intervallo di porte da autorizzare. Puoi specificare un solo numero di porta (ad esempio 22) o un intervallo dei numeri di porta (ad esempio `7000-8000`).
- Tipo e codice ICMP: per ICMP, il tipo e il codice ICMP. Ad esempio, utilizza il tipo 8 per la richiesta Echo ICMP o il tipo 128 per la richiesta Echo ICMPv6.
- Origine o destinazione: l'origine (regole in entrata) o la destinazione (regole in uscita) del traffico da consentire. Specifica una delle seguenti proprietà:
  - Un singolo indirizzo IPv4. Devi utilizzare la lunghezza del prefisso `/32`. Ad esempio, `203.0.113.1/32`.
  - Un singolo indirizzo IPv6. Devi utilizzare la lunghezza del prefisso `/128`. Ad esempio, `2001:db8:1234:1a00::123/128`.
  - Un intervallo di indirizzi IPv4 in notazione a blocco CIDR. Ad esempio, `203.0.113.0/24`.
  - Un intervallo di indirizzi IPv6 in notazione a blocco CIDR. Ad esempio, `2001:db8:1234:1a00::/64`.
  - L'ID di un elenco di prefissi. Ad esempio, `pl-1234abc1234abc123`. Per ulteriori informazioni, consulta the section called “Elenchi di prefissi gestiti”.
  - L'ID di un gruppo di sicurezza. Ad esempio, `sg-1234567890abcdef0`. Per ulteriori informazioni, consulta the section called “Riferimenti dei gruppi di sicurezza”.
- (Opzionale) Descrizione: puoi aggiungere una descrizione della regola, per semplificarne l'identificazione in un secondo momento. Una descrizione può essere lunga fino a 255 caratteri. I caratteri consentiti sono a-z, A-Z, 0-9, spazi e ._-:/()#,@[]+=;{}!$*.

## Riferimenti dei gruppi di sicurezza

Quando specifichi un gruppo di sicurezza come origine o destinazione di una regola, la regola interessa tutte le istanze associate ai gruppi di sicurezza. Le istanze possono comunicare nella direzione specificata utilizzando gli indirizzi IP privati delle istanze tramite il protocollo e la porta specificati.

Ad esempio, la tabella seguente rappresenta una regola in entrata per un gruppo di sicurezza che si riferisce al gruppo di sicurezza sg-0abcdef1234567890. Questa regola consente il traffico SSH in entrata dalle istanze associate a sg-0abcdef1234567890.

| Crea | Protocollo | Intervallo porte |
| --- | --- | --- |
| *sg-0abcdef1234567890* | TCP | 22 |

Quando fai riferimento a un gruppo di sicurezza in una regola di un gruppo di sicurezza, tieni presente quanto segue:

- Entrambi i gruppi di sicurezza devono appartenere allo stesso VPC o ai VPC in peering.
- Nessuna regola del gruppo di sicurezza di riferimento viene aggiunta al gruppo di sicurezza che vi fa riferimento.
- Per le regole in entrata, le istanze EC2 associate al gruppo di sicurezza possono ricevere traffico in entrata dagli indirizzi IP privati delle istanze EC2 associate al gruppo di sicurezza di riferimento.
- Per le regole in uscita, le istanze EC2 associate al gruppo di sicurezza possono inviare traffico in uscita agli indirizzi IP privati delle istanze EC2 associate al gruppo di sicurezza di riferimento.

Limitazione

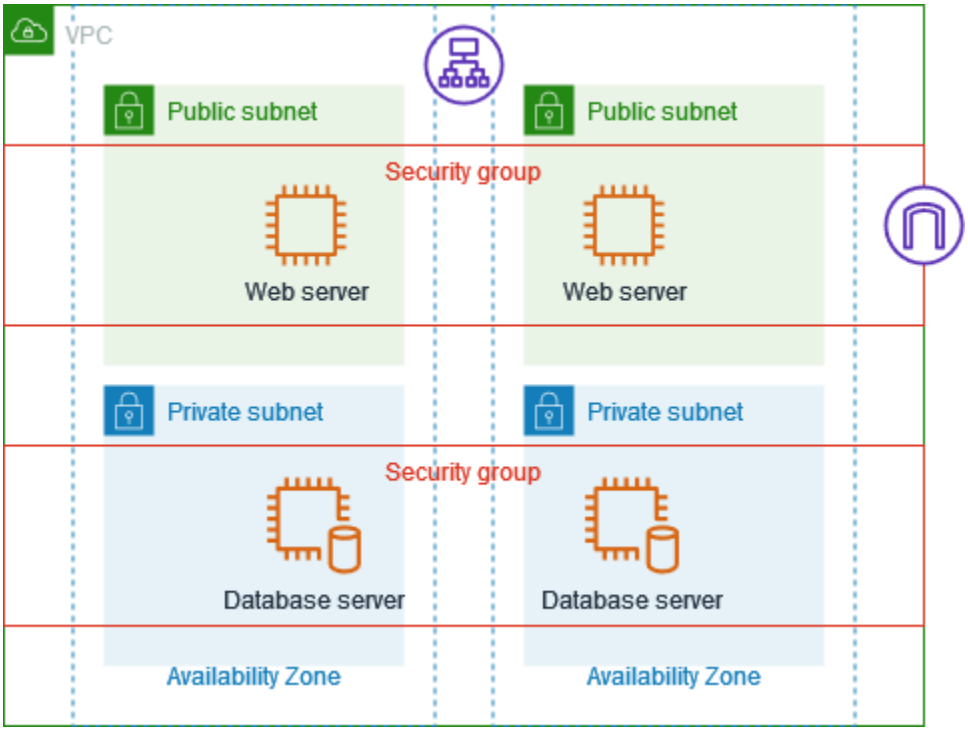
Se le route vengono configurate per inoltrare il traffico tra due istanze in sottoreti diverse attraverso un'appliance middlebox, è necessario assicurarsi che i gruppi di sicurezza per entrambe le istanze consentano il flusso del traffico tra le istanze. Il gruppo di sicurezza per ogni istanza deve fare riferimento all'indirizzo IP privato dell'altra istanza o all'intervallo CIDR della sottorete che contiene l'altra istanza come origine. Se si fa riferimento al gruppo di sicurezza dell'altra istanza come origine, allora il flusso del traffico tra le istanze non sarà consentito.

Esempio

Il seguente diagramma mostra un VPC con sottoreti in due zone di disponibilità, un gateway Internet e un Application Load Balancer. Ogni zona di disponibilità ha una sottorete pubblica per i server web e una sottorete privata per i server di database. Esistono gruppi di sicurezza separati per il sistema di bilanciamento del carico, i server web e i server di database. Crea le seguenti regole del gruppo di sicurezza per consentire il traffico.

- Aggiungi regole al gruppo di sicurezza del sistema di bilanciamento del carico per consentire il traffico HTTP e HTTPS da Internet. Il codice sorgente è 0.0.0.0/0.

- Aggiungi regole al gruppo di sicurezza dei server Web per consentire il traffico HTTP e HTTPS solo dal sistema di bilanciamento del carico. L'origine è il gruppo di sicurezza per il sistema di bilanciamento del carico.
- Aggiungi regole al gruppo di sicurezza dei server di database per consentire le richieste dei database dai server Web. L'origine è il gruppo di sicurezza dei server Web.




## Dimensioni dei gruppi di sicurezza

Il tipo di origine o destinazione determina la modalità con cui ogni regola viene conteggiata ai fini del numero massimo di regole che è possibile avere per ogni gruppo di sicurezza.

- Una regola che fa riferimento a un blocco CIDR viene conteggiata come regola singola.
- Una regola che fa riferimento a un altro gruppo di sicurezza viene conteggiata come regola singola, indipendentemente dalle dimensioni del gruppo di sicurezza di riferimento.
- Una regola che fa riferimento a un elenco di prefissi gestito dal cliente viene conteggiata in base alla dimensione massima dell'elenco di prefissi. Ad esempio, se la dimensione massima dell'elenco di prefissi è 20, una regola che fa riferimento a questo elenco di prefissi viene conteggiata come 20 regole.
- Una regola che fa riferimento a un elenco di prefissi AWS-managed conta come peso dell'elenco di prefissi. Ad esempio, se il peso dell'elenco di prefissi è 10, una regola che fa riferimento a tale

elenco di prefissi viene conteggiata come 10 regole. Per ulteriori informazioni, consulta the section called “Elenchi di AWS prefissi gestiti disponibili”.

## Regole obsolete del gruppo di sicurezza

Se il VPC ha una connessione peering VPC con un altro VPC, o se utilizza un VPC condiviso da un altro account, una regola del gruppo di sicurezza potrebbe fare riferimento all'altro gruppo di sicurezza nel VPC simile o condiviso. Ciò consente alle risorse associate al gruppo di sicurezza e a quelle associate al gruppo di protezione di riferimento di comunicare tra loro.

Se il gruppo di sicurezza nel VPC condiviso viene eliminato o se la connessione peering VPC viene eliminata, la regola del gruppo di sicurezza viene contrassegnata come obsoleta. Le regole obsolete possono essere Eliminate nello stesso modo delle altre regole del gruppo di sicurezza. Per ulteriori informazioni, consulta Lavora con le regole dei gruppi di sicurezza obsolete nella Amazon VPC Peering Guide.

## Utilizzo delle regole dei gruppi di sicurezza

Le attività seguenti illustrano come utilizzare le regole dei gruppi di sicurezza.

Autorizzazioni richieste

- Gestione delle regole del gruppo di sicurezza

Attività

- Aggiunta di regole a un gruppo di sicurezza
- Aggiornamento delle regole del gruppo di sicurezza
- Tag delle regole del gruppo di sicurezza
- Eliminazione delle regole di un gruppo di sicurezza

### Aggiunta di regole a un gruppo di sicurezza

Quando si aggiunge una regola a un gruppo di sicurezza, la nuova regola viene applicata automaticamente a tutte le risorse associate al gruppo di sicurezza.

Se disponi di una connessione peering VPC, puoi fare riferimento ai gruppi di sicurezza del VPC in peering come origine o destinazione delle regole del gruppo di sicurezza. Per ulteriori informazioni,

consulta la sezione relativa all'Aggiornamento dei gruppi di sicurezza ai gruppi di sicurezza del VPC in peering di riferimento nella Guida Amazon VPC Peering.

Per informazioni sulle autorizzazioni richieste per gestire le regole del gruppo di sicurezza, consulta Gestione delle regole del gruppo di sicurezza.

> **Warning**
>
> Se scegli Anywhere-IPv4, consenti il traffico da tutti gli indirizzi IPv4. Se scegli Anywhere-IPv6, consenti il traffico da tutti gli indirizzi IPv6. Quando aggiungi regole per le porte 22 (SSH) o 3389 (RDP), autorizzi l'accesso alle istanze soltanto da parte di un intervallo di indirizzi IP specifico.

Per aggiungere una regola tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegli Gruppi di sicurezza nel riquadro di navigazione.
3. Selezionare il gruppo di sicurezza.
4. Scegliere Actions (Operazioni), Edit inbound rules (Modifica regole in entrata) o Actions (Operazioni), Edit outbound rules (Modifica regole in uscita).
5. Per ogni regola, seleziona Aggiungi regola e completa le attività riportate di seguito.

    a. Per Type (Tipo), scegliere il tipo di protocollo consentito.

    - Per TCP o UDP, è necessario immettere l'intervallo di porte consentito.
    - Se si sceglie un protocollo ICMP personalizzato, occorre scegliere il nome del tipo ICMP da Protocollo e, se applicabile, il nome del codice da Intervallo di porte.
    - Se si sceglie qualsiasi altro tipo, il protocollo e l'intervallo di porte vengono configurati automaticamente.

    b. Per Source type (Tipo di origine) (regole in entrata) o Destination type (Tipo di destinazione (regole in uscita), effettua una delle seguenti operazioni per consentire il traffico:

    - Scegli Personalizzato, quindi immetti un indirizzo IP in notazione CIDR, un blocco CIDR, un altro gruppo di sicurezza o un elenco di prefissi.
    - Scegli Anywhere-IPv4 (Ovunque-IPv4) per consentire il traffico proveniente da qualsiasi indirizzo IPv4 (regole in entrata) o per consentire al traffico di raggiungere tutti gli indirizzi

IPv4 (regole in uscita). Ciò aggiunge automaticamente una regola per il blocco CIDR IPv4 0.0.0.0/0.

- Scegli Anywhere-IPv6 (Ovunque-IPv6) per consentire il traffico proveniente da qualsiasi indirizzo IPv6 (regole in entrata) o per consentire al traffico di raggiungere tutti gli indirizzi IPv6 (regole in uscita). Ciò aggiunge automaticamente una regola per il blocco CIDR IPv6 ::/0.
- Seleziona Il mio IP per permettere il traffico solo da (regole in entrata) o verso (regole in uscita) l'indirizzo IPv4 pubblico del computer locale.

c. (Facoltativo) Per Descrizione, specifica una breve descrizione della regola.

6. Scegliere Salva regole.

Per aggiungere una regola a un gruppo di sicurezza utilizzando il AWS CLI

Utilizzare i comandi authorize-security-group-ingress e authorize-security-group-egress.

Aggiornamento delle regole del gruppo di sicurezza

Quando si aggiorna una regola, la regola aggiornata viene applicata automaticamente a tutte le risorse associate al gruppo di sicurezza.

Per informazioni sulle autorizzazioni richieste per gestire le regole del gruppo di sicurezza, consulta Gestione delle regole del gruppo di sicurezza.

Per aggiornare una regola utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegli Gruppi di sicurezza nel riquadro di navigazione.
3. Selezionare il gruppo di sicurezza.
4. Scegliere Actions (Operazioni), Edit inbound rules (Modifica regole in entrata) o Actions (Operazioni), Edit outbound rules (Modifica regole in uscita).
5. Aggiornare la regola come richiesto.
6. Scegliere Save rules (Salva regole).

Per aggiornare una regola del gruppo di sicurezza utilizzando il AWS CLI

Usa i comandi modify-security-group-rulesupdate-security-group-rule-descriptions-ingress e update-security-group-rule-descriptions-egress.

### Tag delle regole del gruppo di sicurezza

Aggiungi tag alle risorse per aiutarti a organizzarle e identificarle, differenziandole ad esempio per scopo, proprietario o ambiente. Puoi aggiungere i tag anche alle regole di un gruppo di sicurezza. Le chiavi dei tag devono essere univoche per ogni regola del gruppo di sicurezza. Se aggiungi un tag con una chiave già associata al gruppo target, il valore del tag viene aggiornato.

#### Come aggiungere un tag a una regola tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegli Gruppi di sicurezza nel riquadro di navigazione.
3. Selezionare il gruppo di sicurezza.
4. In Regole in entrata o Regole in uscita, seleziona la casella di controllo della regola e quindi scegli Gestisci tag.
5. La pagina Gestisci tag visualizza tutti i tag assegnati alla regola. Per aggiungere un tag, selezionare Add tag (Aggiungi tag), quindi specifica la chiave del tag e il suo valore. Per eliminare un tag, scegliere Remove (Rimuovi) accanto al tag che desideri eliminare.
6. Selezionare Save changes (Salva modifiche).

#### Per etichettare una regola utilizzando il AWS CLI

Utilizzare il comando crea tag.

### Eliminazione delle regole di un gruppo di sicurezza

Quando elimini una regola da un gruppo di sicurezza, la modifica viene applicata automaticamente a tutte le istanze associate al gruppo di sicurezza.

#### Per eliminare una regola di un gruppo di sicurezza tramite console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegli Gruppi di sicurezza nel riquadro di navigazione.
3. Selezionare il gruppo di sicurezza.
4. Seleziona Operazioni, quindi Modifica regole in entrata per rimuovere una regola in entrata o Modifica regole in uscita per rimuovere una regola in uscita.
5. Seleziona il pulsante Elimina accanto alla regola da eliminare.

6. Scegliere Save rules (Salva regole). In alternativa, scegli Anteprima modifiche, rivedi le modifiche e scegli Conferma.

Per eliminare una regola del gruppo di sicurezza utilizzando il AWS CLI

Usa i comandi revoke-security-group-ingress e revoke-security-group-egress

## Regole di esempio

Server Web

Le seguenti sono regole di esempio per un gruppo di sicurezza per i server Web. I server Web possono ricevere traffico HTTP e HTTPS da tutti gli indirizzi IPv4 e IPv6 e possono inviare traffico SQL o MySQL ai server di database.

> **Warning**
>
> Quando si aggiungono regole per le porte 22 (SSH) o 3389 (RDP) in modo da poter accedere alle istanze EC2, consigliamo di autorizzare solo intervalli di indirizzi IP specifici. Se specifichi 0.0.0.0/0 (IPv4) e ::/ (IPv6), ciò consente a chiunque di accedere alle istanze da qualsiasi indirizzo IP utilizzando il protocollo specificato.

In entrata

| Crea | Protocollo | Intervallo porte | Descrizione |
|---|---|---|---|
| 0.0.0.0/0 | TCP | 80 | Permette l'accesso HTTP in entrata da tutti gli indirizzi IPv4 |
| ::/0 | TCP | 80 | Consente l'accesso HTTP in entrata da tutti gli indirizzi IPv6 |
| 0.0.0.0/0 | TCP | 443 | Autorizza l'accesso HTTPS in entrata da tutti gli indirizzi IPv4 |

| Crea | Protocollo | Intervallo porte | Descrizione |
| --- | --- | --- | --- |
| ::/0 | TCP | 443 | Consente l'accesso HTTPS in entrata da tutti gli indirizzi IPv6 |
| *Intervallo di indirizzi IPv4 pubblici della rete* | TCP | 22 | (Facoltativo) Autorizza l'accesso SSH in entrata dagli indirizzi IP IPv4 nella rete |
| *Intervallo di indirizzi IPv6 della rete* | TCP | 22 | (Facoltativo) Autorizza l'accesso SSH in entrata dagli indirizzi IP IPv6 nella rete |
| *Intervallo di indirizzi IPv4 pubblici della rete* | TCP | 3389 | (Facoltativo) Autorizza l'accesso RDP in entrata dagli indirizzi IP IPv4 nella rete |
| *Intervallo di indirizzi IPv6 della rete* | TCP | 3389 | (Facoltativo) Autorizza l'accesso RDP in entrata dagli indirizzi IP IPv6 nella rete |
| *ID di questo gruppo di sicurezza* | Tutti | Tutti | (Facoltativo) Autorizza il traffico in entrata dagli altri server associati a questo gruppo di sicurezza |

In uscita

| Destinazione | Protocollo | Intervallo porte | Descrizione |
| --- | --- | --- | --- |
| *ID del gruppo di sicurezza per le* | TCP | 1433 | |

| Destinazione | Protocollo | Intervallo porte | Descrizione |
| --- | --- | --- | --- |
| *istanze che eseguono Microsoft SQL Server* | | | Autorizza l'accesso Microsoft SQL Server in uscita |
| *ID del gruppo di sicurezza per le istanze che eseguono MySQL* | TCP | 3306 | Autorizza l'accesso MySQL in uscita |

Server di database

I server di database richiedono regole che autorizzino protocolli specifici in entrata, come MySQL o Microsoft SQL Server. Per degli esempi, consulta la sezione Regole del server di database nella Guida per l'utente di Amazon EC2. Per maggiori informazioni sui gruppi di sicurezza per le istanze di Amazon RDS DB, consulta Controllo dell'accesso con i gruppi di sicurezza nella Guida dell'utente di Amazon RDS.

### Risolvere i problemi di raggiungibilità

Reachability Analyzer è uno strumento di analisi statica della configurazione. Usa Reachability Analyzer per analizzare ed eseguire il debug della raggiungibilità della rete tra due risorse nel tuo VPC. Reachability Analyzer hop-by-hop produce dettagli del percorso virtuale tra queste risorse quando sono raggiungibili e identifica il componente di blocco in caso contrario. Ad esempio, può identificare le regole del gruppo di sicurezza mancanti o non configurate correttamente.

Per ulteriori informazioni, consulta la Guida di Reachability Analyzer.

## Gruppi di sicurezza di default per VPC

I VPC predefiniti e tutti i VPC creati includono un gruppo di sicurezza di default. Il nome del gruppo di sicurezza predefinito è "default".

Ti consigliamo di creare gruppi di sicurezza per risorse o gruppi di risorse specifici invece di utilizzare il gruppo di sicurezza predefinito. Tuttavia, per alcune risorse, se non si associa un gruppo di sicurezza quando vengono create, queste vengono associate al gruppo di sicurezza predefinito. Ad esempio, se non specifichi un gruppo di sicurezza all'avvio di un'istanza EC2, l'istanza sarà associata al gruppo di sicurezza predefinito per il relativo VPC.

## Nozioni di base sui gruppi di sicurezza predefiniti

- È possibile modificare le regole di un gruppo di sicurezza di default.
- Non è possibile eliminare un gruppo di sicurezza predefinito. Se provi a eliminare un gruppo di sicurezza predefinito, sarà restituito il seguente codice di errore: `Client.CannotDelete`.

## Regole predefinite

Le tabelle seguenti descrivono le regole predefinite di un gruppo di sicurezza predefinito.

In entrata

| Crea | Protocollo | Intervallo porte | Descrizione |
|---|---|---|---|
| *sg-1234567890abcdef0* | Tutti | Tutti | Consente il traffico in entrata da tutte le risorse assegnate a questo gruppo di sicurezza. L'origine è l'ID di questo gruppo di sicurezza. |

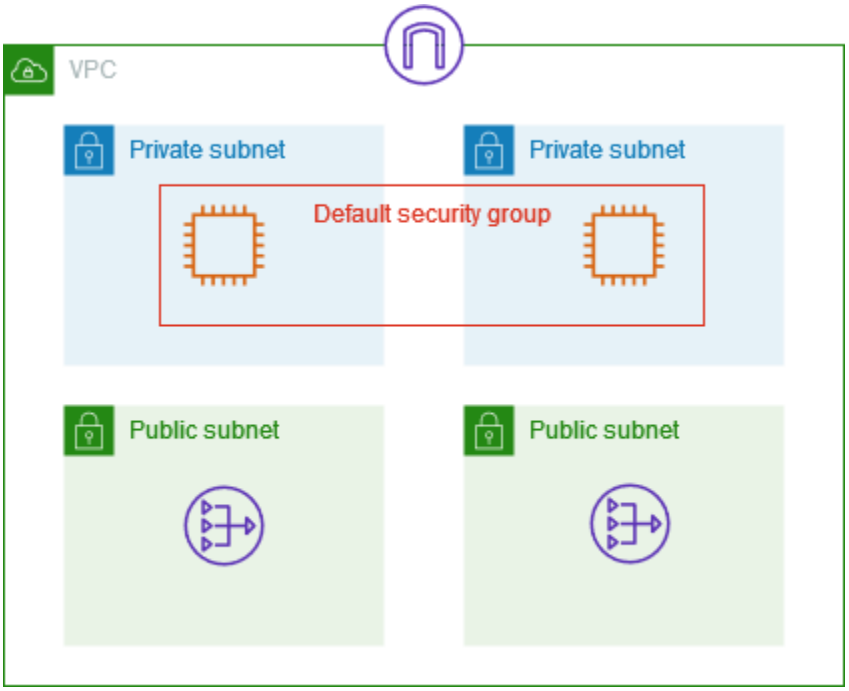
In uscita

| Destinazione | Protocollo | Intervallo porte | Descrizione |
|---|---|---|---|
| 0.0.0.0/0 | Tutti | Tutti | Autorizza tutto il traffico IPv4 in uscita. |
| ::/0 | Tutti | Tutti | Autorizza tutto il traffico IPv6 in uscita. Questa regola viene aggiunta solo se il VPC ha un blocco CIDR IPv6 associato. |

## Esempio

Il diagramma seguente mostra un VPC con un gruppo di sicurezza predefinito, un gateway Internet e un gateway NAT. Il gruppo di sicurezza predefinito contiene solo le regole predefinite ed è associato

a due istanze EC2 in esecuzione nel cloud VPC. In questo scenario, ogni istanza può ricevere traffico in entrata da un'altra istanza su tutte le porte e i protocolli. Le regole predefinite non consentono alle istanze di ricevere traffico dal gateway Internet o dal gateway NAT. Se le istanze devono ricevere traffico aggiuntivo, è consigliabile creare un gruppo di sicurezza con le regole richieste e associare il nuovo gruppo di sicurezza alle istanze anziché il gruppo di sicurezza predefinito.




## Utilizzo dei gruppi di sicurezza

Le attività seguenti illustrano come utilizzare i gruppi di sicurezza.

Attività

- Creazione di un gruppo di sicurezza
- Visualizzazione dei gruppi di sicurezza
- Tag dei gruppi di sicurezza
- Eliminare un gruppo di sicurezza
- Gestione dei gruppi di sicurezza con Firewall Manager

Autorizzazioni richieste

Prima di iniziare, assicurati di disporre delle autorizzazioni richieste.

- Gestione dei gruppi di sicurezza

- Gestione delle regole del gruppo di sicurezza

Le regole di un gruppo di sicurezza controllano il traffico in entrata autorizzato a raggiungere le risorse associate al gruppo di sicurezza. Per ulteriori informazioni sulle regole del gruppo di sicurezza, consultare Regole del gruppo di sicurezza.

## Creazione di un gruppo di sicurezza

Di default, i nuovi gruppi di sicurezza hanno solo una regola in uscita che autorizza tutto il traffico a lasciare la risorsa. Devi aggiungere le regole per autorizzare qualsiasi tipo di traffico in entrata o per limitare quello in uscita.

Per creare un gruppo di sicurezza tramite console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegli Gruppi di sicurezza nel riquadro di navigazione.
3. Scegliere Create Security Group (Crea gruppo di sicurezza).
4. Immettere un nome e una descrizione per il gruppo di sicurezza. Non è possibile modificare il nome e la descrizione di un gruppo di sicurezza dopo averlo creato.
5. Da VPC, seleziona un VPC. Il gruppo di sicurezza può essere utilizzato solo nel VPC per cui viene creato.
6. È possibile aggiungere le regole del gruppo di sicurezza a questo punto oppure in un secondo momento. Per ulteriori informazioni, consulta Aggiunta di regole a un gruppo di sicurezza.
7. È possibile aggiungere tag a questo punto oppure in un secondo momento. Per aggiungere un tag, sceglie Aggiungi tag, quindi specifica la chiave e il valore del tag.
8. Scegliere Create Security Group (Crea gruppo di sicurezza).

Dopo aver creato un gruppo di sicurezza, puoi effettuare una delle seguenti operazioni:

- Assegnare il gruppo di sicurezza a un'istanza EC2 quando avvii l'istanza o quando modifichi il gruppo di sicurezza assegnato attualmente a un'istanza. Per ulteriori informazioni, consulta Launch an Instance or Change security group nella Amazon EC2 User Guide.
- Aggiungere regole del gruppo di sicurezza. Le regole di un gruppo di sicurezza controllano il traffico in entrata autorizzato a raggiungere le risorse associate al gruppo di sicurezza. Per ulteriori informazioni sulle regole del gruppo di sicurezza, consultare Utilizzo delle regole dei gruppi di sicurezza.

Per creare un gruppo di sicurezza utilizzando il AWS CLI

Utilizza il comando create-security-group.

## Visualizzazione dei gruppi di sicurezza

È possibile visualizzare informazioni dettagliate sui gruppi di sicurezza come riportato di seguito.

Come visualizzare i gruppi di sicurezza utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegli Gruppi di sicurezza nel riquadro di navigazione.
3. I gruppi di sicurezza vengono elencati. Per visualizzare i dettagli di un gruppo di sicurezza specifico, incluse le regole in entrata e in uscita, seleziona il gruppo di sicurezza. Per ulteriori informazioni sull'aggiornamento delle regole del gruppo di sicurezza, consulta Aggiornamento delle regole del gruppo di sicurezza.

Come visualizzare tutti i gruppi di sicurezza tra regioni

Aprire la console Amazon EC2 Global View all'indirizzo https://console.aws.amazon.com/ec2globalview/home. Per ulteriori informazioni, consulta Elencare e filtrare le risorse utilizzando Amazon EC2 Global View nella Amazon EC2 User Guide.

Per visualizzare i tuoi gruppi di sicurezza utilizzando il AWS CLI

Usa i comandi describe-security-groups e describe-security-group-rules

## Tag dei gruppi di sicurezza

Aggiungi tag alle risorse per aiutarti a organizzarle e identificarle, differenziandole ad esempio per scopo, proprietario o ambiente. Puoi aggiungere i tag anche ai gruppi di sicurezza. Le chiavi dei tag devono essere univoche per ogni gruppo di sicurezza. Se aggiungi un tag con una chiave già associata alla regola, il valore del tag viene aggiornato.

Come aggiungere un tag a un gruppo di sicurezza tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegli Gruppi di sicurezza nel riquadro di navigazione.
3. Selezionare la casella accanto al gruppo di sicurezza.

4. Scegliere Actions (Operazioni), Manage tags (Gestisci tag). Nella sezione Gestisci tag vengono visualizzati tutti i tag assegnati al gruppo di sicurezza.
5. Per aggiungere un tag, scegli Aggiungi nuovo tag, quindi specifica la chiave e il valore del tag. Per eliminare un tag, scegliere Remove (Rimuovi) accanto al tag da eliminare.
6. Seleziona Salva modifiche.

Per etichettare un gruppo di sicurezza utilizzando il AWS CLI

Utilizzare il comando crea tag.

## Eliminare un gruppo di sicurezza

È possibile eliminare un gruppo di sicurezza solo se non è associato a una risorsa. Non è possibile eliminare un gruppo di sicurezza predefinito.

Se utilizzi la console, puoi eliminare più di un gruppo di sicurezza alla volta. Se utilizzi la riga di comando o l'API, puoi eliminare solo un gruppo di sicurezza alla volta.

Per eliminare un gruppo di sicurezza tramite console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Gruppi di sicurezza.
3. Seleziona il gruppo di sicurezza e scegli Operazioni, Elimina gruppi di sicurezza.
4. Quando viene richiesta la conferma, seleziona Delete (Elimina).

Per eliminare un gruppo di sicurezza utilizzando il AWS CLI

Usa il comando delete-security-group.

## Gestione dei gruppi di sicurezza con Firewall Manager

AWS Firewall Manager semplifica le attività di amministrazione e manutenzione dei gruppi di sicurezza su più account e risorse. Con Firewall Manager puoi configurare e controllare i gruppi di sicurezza per l'organizzazione da un unico account amministratore centrale. Firewall Manager applica automaticamente le regole e le protezioni su tutti gli account e le risorse, anche quando vengono aggiunte nuove risorse. Firewall Manager è particolarmente utile quando si desidera proteggere l'intera organizzazione o se si aggiungono spesso nuove risorse che si desidera proteggere da un account amministratore centrale.

È possibile utilizzare Firewall Manager per gestire centralmente i gruppi di sicurezza nei seguenti modi:

- Configurazione dei gruppi di sicurezza di base comuni nell'organizzazione: è possibile utilizzare una policy di gruppo di sicurezza comune per fornire un'associazione controllata centralmente di gruppi di sicurezza agli account e alle risorse dell'organizzazione. Specificare dove e come applicare le policy nell'organizzazione.
- Controllo dei gruppi di sicurezza esistenti nell'organizzazione: è possibile utilizzare una policy di gruppo di sicurezza di controllo per controllare le regole esistenti in uso nei gruppi di sicurezza dell'organizzazione. È possibile definire l'ambito della policy per controllare tutti gli account, gli account specifici o le risorse contrassegnate all'interno dell'organizzazione. Firewall Manager rileva automaticamente nuovi account e risorse e li controlla. È possibile creare regole di controllo per impostare i guardrail per quali regole dei gruppi di sicurezza consentire o non consentire all'interno dell'organizzazione e per verificare la presenza di gruppi di sicurezza inutilizzati o ridondanti.
- Ottenimento di report sulle risorse non conformi e correggerle: è possibile ottenere report e avvisi per le risorse non conformi per le policy di base e di controllo. È inoltre possibile impostare flussi di lavoro di correzione automatica per correggere eventuali risorse non conformi rilevate da Firewall Manager.

Per ulteriori informazioni sull'utilizzo di Firewall Manager per gestire i gruppi di sicurezza, consulta le seguenti risorse nella guida per AWS Firewall Manager sviluppatori:

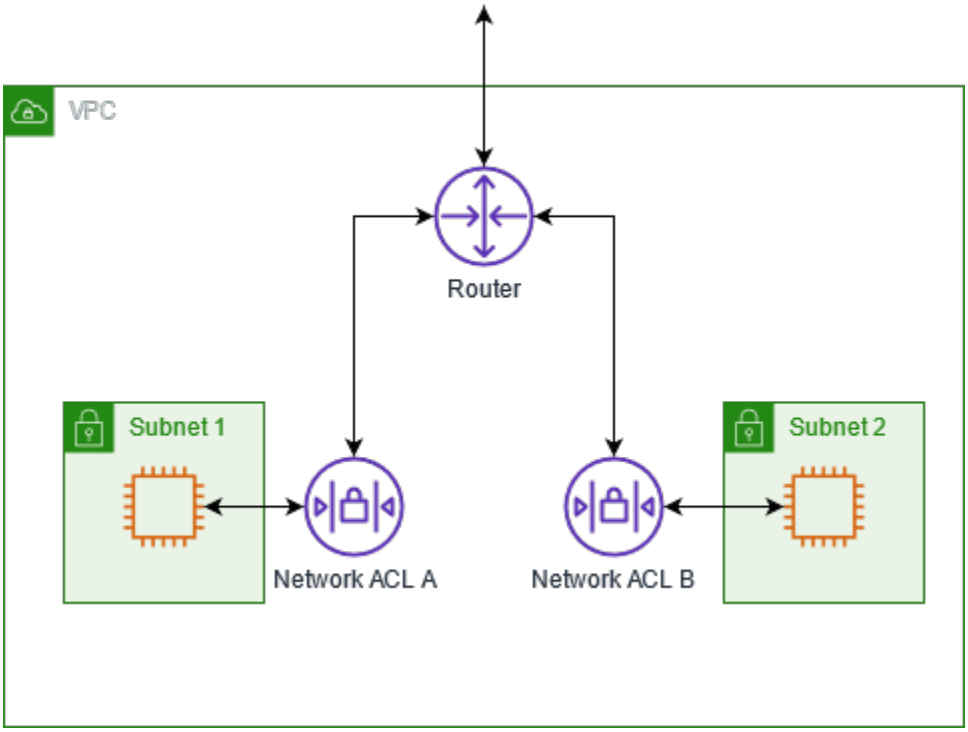
- AWS Firewall Manager prerequisiti
- Guida introduttiva alle policy dei gruppi di sicurezza di AWS Firewall Manager Amazon VPC
- Come funzionano le policy dei gruppi di sicurezza AWS Firewall Manager
- Casi d'uso delle policy di gruppo di sicurezza

## Come controllare il traffico verso le sottoreti utilizzando le liste di controllo degli accessi di rete

Una lista di controllo degli accessi (ACL) di rete consente o nega traffico specifico in entrata o in uscita a livello di sottorete. Si possono utilizzare liste di controllo accessi di rete predefinite per il VPC oppure creare liste di controllo accessi di rete personalizzate per il VPC con regole simili a quelle del gruppo di sicurezza, in modo tale da aggiungere un ulteriore livello di sicurezza al VPC.

L'utilizzo di liste di controllo degli accessi di rete non comporta costi supplementari.

Il seguente diagramma mostra un VPC con due sottoreti. Ogni sottorete ha un'ACL di rete. Quando il traffico entra nel VPC (ad esempio, da un VPC in peering, da una connessione VPN o da Internet), il router invia il traffico a destinazione. L'ACL di rete A determina quale traffico destinato alla sottorete 1 può entrare nella sottorete 1 e quale traffico destinato a una posizione esterna alla sottorete 1 può uscire dalla sottorete 1. Analogamente, l'ACL B della rete determina quale traffico può entrare e uscire dalla sottorete 2.




Per informazioni sulle differenze tra i gruppi di sicurezza e le liste di controllo degli accessi di rete, consulta Confronto dei gruppi di sicurezza e delle liste di controllo accessi di rete.

Indice

- Utilizzo di ACL di rete
- Esempio: controllo dell'accesso alle istanze in una sottorete
- Risolvi i problemi di raggiungibilità

## Informazioni di base sulla lista di controllo accessi di rete

Di seguito sono riportate le nozioni di base che occorre sapere sulle liste di controllo accessi di rete:

- Il VPC viene fornito automaticamente con una lista di controllo accessi di rete modificabile. Per impostazione predefinita, consente tutto il traffico IPv4 in entrata e in uscita e, se applicabile, il traffico IPv6.
- Puoi creare una lista personalizzata di controllo degli accessi di rete e associarla a una sottorete per consentire o negare traffico specifico in entrata o in uscita al livello di sottorete.
- Ogni sottorete nel VPC deve Essere associata a una lista di controllo accessi di rete. Se non associ in maniera esplicita una sottorete a una lista di controllo accessi di rete, la sottorete viene associata automaticamente alla lista di controllo accessi di rete predefinita.
- Puoi associare una lista di controllo accessi di rete a più sottoreti. Tuttavia, una sottorete può essere associata a una sola lista di controllo accessi di rete alla volta. Quando associ una lista di controllo accessi di rete a una sottorete, l'associazione precedente viene rimossa.
- Un'ACL di rete ha regole in entrata e regole in uscita. Ogni regola può consentire o negare il traffico. Ogni regola ha un numero compreso tra 1 e 32766. Quando decidiamo se consentire o rifiutare il traffico, valutiamo le regole in ordine, a partire dalla regola numerata più bassa. Se il traffico corrisponde a una regola, la regola viene applicata e non ne viene valutata nessun'altra. Ti consigliamo di iniziare creando regole in incrementi (ad esempio, incrementi di 10 o 100) in modo da poter inserire nuove regole se richiesto in seguito.
- Valutiamo le regole ACL di rete quando il traffico entra ed esce dalla sottorete, non quando viene instradato all'interno di una sottorete.
- I NAC sono stateless, quindi le informazioni sul traffico inviato o ricevuto in precedenza non vengono salvate. Se, ad esempio, si crea una regola NACL per consentire un traffico in entrata specifico verso una sottorete, le risposte a tale traffico non vengono consentite automaticamente. Ciò è in contrasto con il funzionamento dei gruppi di sicurezza. I NAC sono stateful, quindi le informazioni sul traffico inviato o ricevuto in precedenza vengono salvate. Se, ad esempio, un gruppo di sicurezza consente il traffico in entrata verso un'istanza EC2, le risposte vengono automaticamente consentite, indipendentemente dalle regole del gruppo di sicurezza in uscita.

- Gli ACL di rete non possono bloccare le richieste DNS da o verso il Route 53 Resolver (noto anche come indirizzo IP VPC+2 o DNS). AmazonProvided Per filtrare le richieste DNS tramite il risolutore Route 53, puoi abilitare il firewall DNS per il risolutore Route 53; consulta il relativo argomento nella Guida per gli sviluppatori di Amazon Route 53.
- Le ACL di rete non possono bloccare il traffico verso il servizio Instance Metadata Service (IMDS). Per gestire l'accesso a IMDS, consulta la pagina Configurazione delle opzioni dei metadati dell'istanza nella Guida per l'utente di Amazon EC2.
- Le ACL di rete non filtrano il traffico destinato a e da i seguenti:
  - Amazon Domain Name Services (DNS)
  - Amazon Dynamic Host Configuration Protocol (DHCP)
  - Metadati delle istanze Amazon EC2.
  - Endpoint di metadati dei processi Amazon ECS
  - Attivazione della licenza per le istanze Windows
  - Servizio di sincronizzazione oraria di Amazon
  - Indirizzi IP riservati utilizzati dal router VPC predefinito
- Esistono quote (note anche come limiti) per le ACL di rete per VPC e per il numero di regole per ACL di rete. Per ulteriori informazioni, consulta Quote Amazon VPC.

## Regole di liste di controllo accessi di rete

Puoi aggiungere o rimuovere regole dalla lista di controllo accessi di rete predefinita o creare liste di controllo accessi di rete aggiuntive per il VPC. Quando aggiungi o rimuovi regole da una lista di controllo accessi di rete, le modifiche vengono applicate automaticamente alle sottoreti cui è associata.

Di seguito sono riportate le parti di una regola della lista di controllo accessi di rete:

- Numero regola. Le regole sono valutate a partire da quella con numerazione più bassa. Non appena una regola corrisponde al traffico, viene applicata a prescindere da qualsiasi altra regola con numerazione più alta che potrebbe contraddirla.
- Tipo. Il tipo di traffico; ad esempio, SSH. Puoi anche specificare tutto il traffico o un intervallo personalizzato.
- Protocol (Protocollo. Puoi specificare qualsiasi protocollo che dispone di un numero di protocollo standard. Per ulteriori informazioni, consulta la sezione relativa ai numeri di protocollo. Se specifichi ICMP come protocollo, puoi specificare qualcuno o tutti dei tipi e dei codici ICMP.

- Intervallo porte. La porta di ascolto o l'intervallo di porte per il traffico. Ad esempio, 80 per il traffico HTTP.
- Source (Origine. [Solo regole in entrata] L'origine del traffico (intervallo CIDR).
- Destination (Destinazione. [Solo regole in uscita] La destinazione per il traffico (intervallo CIDR).
- Consenti/Nega. Scelta tra le opzioni allow o deny per il traffico specificato.

Se si aggiunge una regola utilizzando uno strumento a riga di comando o l'API Amazon EC2, l'intervallo CIDR viene modificato automaticamente nel suo formato canonico. Ad esempio, se si specifica `100.68.0.18/18` per l'intervallo CIDR, verrà creata una regola con un intervallo CIDR `100.68.0.0/18`.

## lista di controllo accessi di rete predefinita

La lista di controllo degli accessi di rete predefinita viene configurata per consentire tutto il traffico in entrata e in uscita dalle sottoreti cui è associata. Ogni ACL di rete include anche una regola il cui numero regola è un asterisco (*). Questa regola garantisce che se un pacchetto non corrisponde a nessuna delle altre regole numerate, viene rifiutato. Non puoi modificare né rimuovere questa regola.

Di seguito è riportato un esempio di lista di controllo accessi di rete predefinita per un VPC che supporta solo IPv4.

In entrata

| Rule # | Tipo | Protocollo | Intervallo porte | Crea | Consenti/Nega |
|---|---|---|---|---|---|
| 100 | Tutto il traffico IPv4 | Tutti | Tutti | 0.0.0.0/0 | PERMETTI |
| * | Tutto il traffico IPv4 | Tutti | Tutti | 0.0.0.0/0 | DENY |

In uscita

| Rule # | Tipo | Protocollo | Intervallo porte | Destinazione | Consenti/ Nega |
|---|---|---|---|---|---|
| 100 | Tutto il traffico IPv4 | Tutti | Tutti | 0.0.0.0/0 | PERMETTI |
| * | Tutto il traffico IPv4 | Tutti | Tutti | 0.0.0.0/0 | DENY |

Se crei un VPC con un blocco CIDR IPv6 o se associ un blocco CIDR IPv6 a un VPC esistente, aggiungiamo automaticamente regole che consentono il flusso di tutto il traffico IPv6 in entrata e in uscita dalla sottorete. Aggiungiamo anche regole i cui numeri regola sono un asterisco che garantisce che un pacchetto viene rifiutato se non corrisponde ad alcuna delle altre regole numerate. Non puoi modificare né rimuovere queste regole. Di seguito è riportato un esempio di lista di controllo accessi di rete predefinita per un VPC che supporta IPv4 e IPv6.

> **Note**
>
> Se hai modificato le regole in entrata della ACL di rete predefinita, non aggiungiamo automaticamente una regola `ALLOW` per il traffico IPv6 in entrata quando associ un blocco IPv6 al VPC. Analogamente, se hai modificato le regole in uscita, non aggiungiamo automaticamente una regola `ALLOW` per il traffico IPv6 in uscita.

In entrata

| Rule # | Tipo | Protocollo | Intervallo porte | Crea | Consenti/ Nega |
|---|---|---|---|---|---|
| 100 | Tutto il traffico IPv4 | Tutti | Tutti | 0.0.0.0/0 | PERMETTI |
| 101 | Tutto il traffico IPv6 | Tutti | Tutti | ::/0 | ALLOW |

| Rule # | Tipo | Protocollo | Intervallo porte | Crea | Consenti/ Nega |
|---|---|---|---|---|---|
| * | Tutto il traffico | Tutti | Tutti | 0.0.0.0/0 | DENY |
| * | Tutto il traffico IPv6 | Tutti | Tutti | ::/0 | RIFIUTA |

In uscita

| Rule # | Tipo | Protocollo | Intervallo porte | Destinazione | Consenti/ Nega |
|---|---|---|---|---|---|
| 100 | Tutto il traffico | Tutti | Tutti | 0.0.0.0/0 | PERMETTI |
| 101 | Tutto il traffico IPv6 | Tutti | Tutti | ::/0 | ALLOW |
| * | Tutto il traffico | Tutti | Tutti | 0.0.0.0/0 | DENY |
| * | Tutto il traffico IPv6 | Tutti | Tutti | ::/0 | RIFIUTA |

## lista di controllo accessi di rete personalizzata

Nell'esempio seguente viene mostrata una ACL di rete personalizzata per un VPC che supporta solo IPv4. Include regole in entrata che consentono il traffico HTTP e HTTPS (100 e 110). Esiste una regola in uscita corrispondente che abilita le risposte a tale traffico in entrata (140), che copre le porte temporanee 32768-65535. Per ulteriori informazioni su come selezionare l'intervallo di porte temporanee appropriato, consulta Porte Effimere.

La lista di controllo accessi di rete include anche regole in entrata che consentono traffico SSH e RDP nella sottorete. La regola in uscita 120 consente le risposte in uscita dalla sottorete.

La lista di controllo accessi di rete dispone di regole in uscita (100 e 110) che consentono traffico HTTP e HTTPS in uscita dalla sottorete. Esiste una regola in entrata corrispondente che abilita le risposte a tale traffico in uscita (140), che copre le porte temporanee 32768-65535.

Ogni lista di controllo accessi di rete include una regola predefinita il cui numero regola è un asterisco. Questa regola garantisce che se un pacchetto non corrisponde a nessuna delle altre regole, viene rifiutato. Non puoi modificare né rimuovere questa regola.

In entrata

| Rule # | Tipo | Protocollo | Intervallo porte | Crea | Consenti/Nega | Commenti |
|---|---|---|---|---|---|---|
| 100 | HTTP | TCP | 80 | 0.0.0.0/0 | PERMETTI | Consente traffico HTTP in entrata da qualunque indirizzo IPv4. |
| 110 | HTTPS | TCP | 443 | 0.0.0.0/0 | PERMETTI | Consente traffico HTTPS in entrata da qualsiasi indirizzo IPv4. |
| 120 | SSH | TCP | 22 | 192.0.2.0/24 | PERMETTI | Consente traffico SSH in entrata dall'intervallo di indirizzi IPv4 pubblici della rete privata (su Internet gateway). |
| 130 | RDP | TCP | 3389 | 192.0.2.0/24 | PERMETTI | Consente traffico RDP in entrata ai server Web dall'intervallo di indirizzi IPv4 pubblici della rete privata (su Internet gateway). |

| Rule # | Tipo | Protocollo | Intervallo porte | Crea | Consenti/Nega | Commenti |
|---|---|---|---|---|---|---|
| 140 | TCP personalizzato | TCP | 32768-65535 | 0.0.0.0/0 | PERMETTI | Consente traffico IPv4 di ritorno in entrata da Internet (ovvero, per richieste che originano nella sottorete).<br><br>Questo intervallo è solo un esempio. |
| * | Tutto il traffico | Tutti | Tutti | 0.0.0.0/0 | RIFIUTA | Rifiuta tutto il traffico IPv4 in entrata che non è già gestito da una regola precedente (non modificabile). |

In uscita

| Rule # | Tipo | Protocollo | Intervallo porte | Destinazione | Consenti/Nega | Commenti |
|---|---|---|---|---|---|---|
| 100 | HTTP | TCP | 80 | 0.0.0.0/0 | PERMETTI | Permette traffico HTTP IPv4 in uscita dalla sottorete a Internet. |
| 110 | HTTPS | TCP | 443 | 0.0.0.0/0 | PERMETTI | Permette traffico HTTPS IPv4 in uscita dalla sottorete a Internet. |
| 120 | SSH | TCP | 1024-65535 | 192.0.2.0/24 | PERMETTI | Consente il traffico SSH di ritorno in uscita verso l'intervallo di indirizzi IPv4 |

| Rule # | Tipo | Protocollo | Intervallo porte | Destinazione | Consenti/Nega | Commenti |
|---|---|---|---|---|---|---|
| | | | | | | pubblico della rete domestica (tramite il gateway Internet). |
| 140 | TCP personalizzato | TCP | 32768-65535 | 0.0.0.0/0 | PERMETTI | Permette risposte IPv4 in uscita a client su Internet (ad esempio, distribuzione di pagine Web a persone che visitano i server Web nella sottorete).<br><br>Questo intervallo è solo un esempio. |
| * | Tutto il traffico | Tutti | Tutti | 0.0.0.0/0 | DENY | Rifiuta tutto il traffico IPv4 in uscita che non è già gestito da una regola precedente (non modificabile). |

Non appena un pacchetto arriva nella sottorete, lo valutiamo rispetto alle regole in ingresso della lista di controllo accessi cui è associata la sottorete (partendo dall'inizio dell'elenco di regole e spostandoci verso la fine). Di seguito viene descritta la valutazione se il pacchetto è destinato alla porta HTTPS (443). Il pacchetto non corrisponde alla prima regola valutata (regola 100). Non corrisponde alla seconda regola (110), che consente il pacchetto nella sottorete. Se il pacchetto era destinato alla porta 139 (NetBIOS), non corrisponde a nessuna delle regole E la regola * rifiuta alla fine il pacchetto.

Potrebbe essere necessario aggiungere una regola deny in una situazione in cui hai legittimamente la necessità di aprire un ampio intervallo di porte, ma alcune di esse sono incluse nell'intervallo di porte che desideri rifiutare. Devi accertarti di posizionare la regola deny il prima possibile nella tabella rispetto alla regola che consente l'ampio intervallo di traffico porta.

Le regole allow vengono aggiunte a seconda del caso d'uso. Ad esempio, è possibile aggiungere una regola che consente l'accesso TCP e UDP in uscita sulla porta 53 per la risoluzione DNS. Per ogni regola aggiunta, verificare che vi sia una regola in entrata e in uscita corrispondente che abiliti il traffico di risposta.

Nell'esempio seguente viene mostrata una ACL di rete personalizzata per un VPC cui è associato un blocco CIDR IPv6. Questa lista di controllo accessi di rete include tutto il traffico HTTP e HTTPS IPv6. In questo caso, sono state inserite nuove regole tra le regole esistenti per il traffico IPv4. È inoltre possibile aggiungere le regole come regole con numeri più alti dopo le regole IPv4. Il traffico IPv4 è separato dal traffico IPv6 e, pertanto, nessuna delle regole per il traffico IPv4 si applica al traffico IPv6.

In entrata

| Rule # | Tipo | Protocollo | Intervallo porte | Crea | Consenti/Nega | Commenti |
|---|---|---|---|---|---|---|
| 100 | HTTP | TCP | 80 | 0.0.0.0/0 | PERMETTI | Consente traffico HTTP in entrata da qualunque indirizzo IPv4. |
| 105 | HTTP | TCP | 80 | ::/0 | PERMETTI | Permette traffico HTTP in entrata da qualunque indirizzo IPv6. |
| 110 | HTTPS | TCP | 443 | 0.0.0.0/0 | PERMETTI | Consente traffico HTTPS in entrata da qualsiasi indirizzo IPv4. |
| 115 | HTTPS | TCP | 443 | ::/0 | PERMETTI | Permette traffico HTTPS in entrata da qualsiasi indirizzo IPv6. |
| 120 | SSH | TCP | 22 | 192.0.2.0/24 | PERMETTI | Consente traffico SSH in entrata dall'inte |

| Rule # | Tipo | Protocollo | Intervallo porte | Crea | Consenti/Nega | Commenti |
|---|---|---|---|---|---|---|
| | | | | | | rvallo di indirizzi IPv4 pubblici della rete privata (su Internet gateway). |
| 130 | RDP | TCP | 3389 | 192.0.2.0/24 | PERMETTI | Consente traffico RDP in entrata ai server Web dall'intervallo di indirizzi IPv4 pubblici della rete privata (su Internet gateway). |
| 140 | TCP personalizzato | TCP | 32768-65535 | 0.0.0.0/0 | PERMETTI | Consente traffico IPv4 di ritorno in entrata da Internet (ovvero, per richieste che originano nella sottorete).<br><br>Questo intervallo è solo un esempio. |
| 145 | TCP personalizzato | TCP | 32768-65535 | ::/0 | ALLOW | Permette traffico IPv6 di ritorno in entrata da Internet (ovvero, per richieste che originano nella sottorete).<br><br>Questo intervallo è solo un esempio. |

| Rule # | Tipo | Protocollo | Intervallo porte | Crea | Consenti/Nega | Commenti |
|---|---|---|---|---|---|---|
| * | Tutto il traffico | Tutti | Tutti | 0.0.0.0/0 | RIFIUTA | Rifiuta tutto il traffico IPv4 in entrata che non è già gestito da una regola precedente (non modificabile). |
| * | Tutto il traffico | Tutti | Tutti | ::/0 | RIFIUTA | Rifiuta tutto il traffico IPv6 in entrata che non è già gestito da una regola precedente (non modificabile). |

In uscita

| Rule # | Tipo | Protocollo | Intervallo porte | Destinazione | Consenti/Nega | Commenti |
|---|---|---|---|---|---|---|
| 100 | HTTP | TCP | 80 | 0.0.0.0/0 | PERMETTI | Permette traffico HTTP IPv4 in uscita dalla sottorete a Internet. |
| 105 | HTTP | TCP | 80 | ::/0 | PERMETTI | Permette traffico HTTP IPv6 in uscita dalla sottorete a Internet. |
| 110 | HTTPS | TCP | 443 | 0.0.0.0/0 | PERMETTI | Permette traffico HTTPS IPv4 in uscita dalla sottorete a Internet. |
| 115 | HTTPS | TCP | 443 | ::/0 | PERMETTI | Permette traffico HTTPS IPv6 in uscita |

| Rule # | Tipo | Protocollo | Intervallo porte | Destinazione | Consenti/Nega | Commenti |
|---|---|---|---|---|---|---|
| | | | | | | dalla sottorete a Internet. |
| 140 | TCP personalizzato | TCP | 32768-65535 | 0.0.0.0/0 | PERMETTI | Permette risposte IPv4 in uscita a client su Internet (ad esempio, distribuzione di pagine Web a persone che visitano i server Web nella sottorete).<br><br>Questo intervallo è solo un esempio. |
| 145 | TCP personalizzato | TCP | 32768-65535 | ::/0 | PERMETTI | Permette risposte IPv6 in uscita a client su Internet (ad esempio, distribuzione di pagine Web a persone che visitano i server Web nella sottorete).<br><br>Questo intervallo è solo un esempio. |
| * | Tutto il traffico | Tutti | Tutti | 0.0.0.0/0 | DENY | Rifiuta tutto il traffico IPv4 in uscita che non è già gestito da una regola precedente (non modificabile). |

| Rule # | Tipo | Protocollo | Intervallo porte | Destinazione | Consenti/Nega | Commenti |
|---|---|---|---|---|---|---|
| * | Tutto il traffico | Tutti | Tutti | ::/0 | RIFIUTA | Rifiuta tutto il traffico IPv6 in uscita che non è già gestito da una regola precedente (non modificabile). |

## ACL di rete personalizzati e altri servizi AWS

Se crei un ACL di rete personalizzato, tieni presente in che modo ciò potrebbe influire sulle risorse create utilizzando altri AWS servizi.

Con Elastic Load Balancing, se la sottorete per le istanze di back-end dispone di una lista di controllo accessi di rete in cui è stata aggiunta una regola deny per tutto il traffico con un'origine di `0.0.0.0/0` o il CIDR della sottorete, il load balancer non può eseguire controlli di stato sulle istanze. Per ulteriori informazioni sulle regole della lista di controllo accessi di rete consigliate per i load balancer e le istanze di back-end, consulta Liste di controllo degli accessi di rete per sistemi di bilanciamento del carico in un VPC nella Guida per l'utente di Classic Load Balancers.

## Porte Effimere

La lista di controllo accessi di rete di esempio nella sezione precedente utilizza un intervallo di porte Effimere di 32768-65535. Tuttavia, potrebbe Essere necessario utilizzare un intervallo diverso per le liste di controllo accessi di rete a seconda del tipo di client in uso o con cui si comunica.

Il client che avvia la richiesta sceglie l'intervallo di porte Effimere. L'intervallo varia a seconda del sistema operativo del client.

- Molti kernel Linux (incluso il kernel Amazon Linux) usano le porte 32768-61000.
- Le richieste provenienti da Elastic Load Balancing utilizzano le porte 1024-65535.
- I sistemi operativi Windows tramite Windows Server 2003 utilizzano porte 1025-5000.
- Windows Server 2008 e versioni successive utilizzano porte 49152-65535.
- Un gateway NAT utilizza le porte 1024-65535.
- AWS Lambda le funzioni utilizzano le porte 1024-65535.

Ad esempio, se una richiesta arriva in un server Web nel VPC da un client Windows 10 su Internet, la lista di controllo degli accessi di rete deve disporre di una regola in uscita per abilitare il traffico destinato alle porte 49152-65535.

Se un'istanza nel VPC è il client che avvia una richiesta, la lista di controllo accessi di rete deve disporre di una regola in entrata per abilitare il traffico destinato alle porte temporanee specifiche per il tipo di istanza (Amazon Linux, Windows Server 2008 e così via).

In pratica, per coprire i diversi tipi di client che possono avviare il traffico su istanze rivolte al pubblico nel VPC, puoi aprire porte Effimere 1024-65535. Tuttavia, puoi anche aggiungere regole alla lista di controllo accessi per rifiutare il traffico su porte dannose all'interno di tale intervallo. Accertati di posizionare le regole deny il prima possibile nella tabella rispetto alle regole allow che aprono l'ampio intervallo di porte temporanee.

## Rilevamento della MTU del percorso

Il rilevamento della MTU del percorso è utilizzato per determinare la MTU del percorso tra due dispositivi. La MTU del percorso è la dimensione massima del pacchetto che è supportata nel percorso tra l'host di origine e quello ricevente.

Per IPv4, se un host invia un pacchetto più grande della MTU dell'host ricevente o della MTU di un dispositivo lungo il percorso, l'host o il dispositivo ricevente rifiuta il pacchetto e restituisce il seguente messaggio ICMP: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipo 3, Codice 4). Questo indica all'host trasmittente di dividere il payload in più pacchetti più piccoli e quindi di trasmetterli di nuovo.

Il protocollo IPv6 non supporta la frammentazione nella rete. Se un host invia un pacchetto più grande della MTU dell'host ricevente o della MTU di un dispositivo lungo il percorso, l'host o il dispositivo ricevente elimina il pacchetto e restituisce il seguente messaggio ICMP: `ICMPv6 Packet Too Big (PTB)` (Tipo 2). Questo indica all'host trasmittente di dividere il carico in più pacchetti più piccoli e quindi di trasmetterli di nuovo.

Se l'unità di trasmissione massima (MTU) tra gli host nelle sottoreti è diversa o se le istanze comunicano con peer su Internet, devi aggiungere la regola della lista di controllo degli accessi (ACL) seguente, sia in entrata sia in uscita. Ciò garantisce il corretto funzionamento del rilevamento della MTU del percorso e previene la perdita di pacchetti. Seleziona Custom ICMP Rule (Regola ICMP personalizzata) per il tipo e Destination Unreachable, fragmentation required, and DF flag set (Destinazione irraggiungibile: richiesta frammentazione e flag DF attivo) per l'intervallo di porte (tipo 3, codice 4). Se si utilizza traceroute, aggiungere anche la seguente regola: selezionare Custom

ICMP Rule (Regola ICMP personalizzata) per il tipo e Time Exceeded (Orario superato), TTL expired transit (Transito TTL scaduto) per l'intervallo porte (tipo 11, codice 0). Per ulteriori informazioni, consulta Network maximum transmission unit (MTU) per la tua istanza EC2 nella Amazon EC2 User Guide.

## Utilizzo di ACL di rete

Le attività seguenti mostrano come utilizzare liste di controllo accessi di rete tramite la console Amazon VPC.

Attività

- Determinazione delle associazioni della lista di controllo accessi di rete
- Creazione di una lista di controllo degli accessi di rete
- Aggiunta ed eliminazione di regole
- Associazione di una sottorete a una lista di controllo accessi di rete
- Annullamento dell'associazione di una lista di controllo accessi di rete a una sottorete
- Modifica dell'ACL di rete di una sottorete
- Eliminazione di una lista di controllo accessi di rete
- Panoramica sulle API e sui comandi
- Gestire gli ACL di rete utilizzando Firewall Manager

### Determinazione delle associazioni della lista di controllo accessi di rete

Puoi utilizzare la console Amazon VPC per determinare la lista di controllo accessi di rete che è associata a una sottorete. Le liste di controllo accessi di rete possono essere associate a più sottoreti, pertanto puoi anche determinare quali sottoreti sono associate a una lista di controllo accessi di rete.

Per determinare quale lista di controllo accessi di rete è associata a una sottorete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti) e selezionare la sottorete.

   La lista di controllo accessi di rete associata alla sottorete è inclusa nella scheda Network ACL (lista di controllo accessi di rete), insieme alle regole della lista di controllo accessi di rete.

Per determinare quale sottoreti sono associate a una lista di controllo accessi di rete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Network ACL (lista di controllo accessi di rete). Nella colonna Associated With (Associato con) è indicato il numero di sottoreti associate per ogni lista di controllo accessi di rete.
3. Selezionare una lista di controllo accessi di rete.
4. Nel riquadro dei dettagli, scegliere Subnet Associations (Associazioni sottorete) per visualizzare le sottoreti che sono associate alla lista di controllo accessi di rete.

## Creazione di una lista di controllo degli accessi di rete

Puoi creare una lista di controllo accessi di rete personalizzata dal VPC. Per impostazione predefinita, una lista di controllo accessi di rete creata dall'utente blocca tutto il traffico in entrata e in uscita finché non si aggiungono regole E non è associata a una sottorete finché una non viene associata in maniera esplicita.

Per creare una lista di controllo accessi di rete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Network ACL (lista di controllo accessi di rete).
3. Selezionare Create Network ACL (Crea lista di controllo accessi di rete).
4. Nella finestra di dialogo Create Network ACL (Crea lista di controllo accessi di rete), assegnare facoltativamente un nome alla lista di controllo accessi di rete e selezionare l'ID del VPC dall'elenco VPC. Quindi selezionare Yes, Create (Sì, crea).

## Aggiunta ed eliminazione di regole

Quando aggiungi o elimini una regola da una lista di controllo accessi, le eventuali sottoreti associate alla lista di controllo accessi sono influenzate dalla modifica. Non occorre terminare e avviare nuovamente le istanze nella sottorete. Le modifiche diventano effettive dopo un breve periodo di tempo.

> **Important**
>
> È necessario prestare molta attenzione se si aggiungono ed eliminano regole contemporaneamente. Le regole della lista di controllo degli accessi di rete definiscono

quali tipi di traffico di rete possono entrare o uscire dai VPC. Se si eliminano regole in entrata o in uscita e quindi si aggiungono nuove voci rispetto a quelle consentite in Quote Amazon VPC, le voci selezionate per l'eliminazione verranno rimosse e le nuove voci non verranno aggiunte. Ciò potrebbe causare problemi di connettività imprevisti e impedire involontariamente l'accesso da e verso i VPC.

Se stai utilizzando l'API Amazon EC2 o uno strumento a riga di comando, non puoi modificare le regole. Puoi solo aggiungere ed eliminare regole. Se stai utilizzando la console Amazon VPC, puoi modificare le voci relative alle regole esistenti. La console rimuove la regola esistente e aggiunge una nuova regola automaticamente. Se occorre modificare l'ordine di una regola nella lista di controllo accessi, devi aggiungere una nuova regola con il nuovo numero regola , quindi eliminare la regola originale.

Per aggiungere regole a una lista di controllo accessi di rete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Network ACL (lista di controllo accessi di rete).
3. Nel riquadro dei dettagli, scegliere la scheda Inbound Rules (Regole in entrata) o Outbound Rules (Regole in uscita), in base al tipo di regola che occorre aggiungere, quindi selezionare Edit (Modifica).
4. In Rule # (N. regola), immettere un numero regola (ad esempio, 100). Il numero regola non deve già essere in uso nella lista di controllo accessi di rete. Elaboriamo le regole nell'ordine, partendo da quella con il numero più basso.

   Ti consigliamo di lasciare degli spazi vuoti tra i numeri regola (ad esempio 100, 200, 300), anziché utilizzare numeri in sequenziali (101, 102, 103). Questo semplifica l'aggiunta di una nuova regola senza la necessità di numerare le regole Esistenti.
5. Selezionare una regola dall'elenco Type (Tipo). Ad esempio, per aggiungere una regola per HTTP, scegliere HTTP. Per aggiungere una regola per consentire tutto il traffico TCP, scegliere All TCP (Tutto TCP). Per alcune di queste opzioni (ad esempio, HTTP), la porta viene compilata automaticamente. Per utilizzare un protocollo non elencato, scegliere Custom Protocol Rule (Regola protocollo personalizzata).
6. (Facoltativo) Se si sta creando una regola protocollo personalizzata, selezionare il numero e il nome del protocollo dall'elenco Protocol (Protocollo). Per ulteriori informazioni, consulta la sezione relativa all'elenco IANA di numeri di protocollo.

7. (Facoltativo) Se il protocollo selezionato richiede un numero di porta, immettere il numero di porta o l'intervallo di porte separato da un trattino (ad esempio, 49152-65535).
8. Nel campo Source (Origine) o Destination (Destinazione) (a seconda che si tratti di una regola in entrata o in uscita), immettere l'intervallo CIDR cui si applica la regola.
9. Dall'elenco Allow/Deny (Consenti/Rifiuta), selezionare ALLOW per consentire il traffico specificato o DENY per rifiutare il traffico specificato.
10. (Facoltativo) Per aggiungere un'altra regola, selezionare Add another rule (Aggiungi un'altra regola) e ripetere le fasi da 4 a 9 come richiesto.
11. Al termine, scegliere Save (Salva).

Per eliminare una regola da una lista di controllo accessi di rete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Network ACLs (liste di controllo accessi di rete), quindi selezionare la lista di controllo accessi di rete.
3. Nel riquadro dei dettagli, selezionare la scheda Inbound Rules (Regole in entrata) o Outbound Rules (Regole in uscita), quindi selezionare Edit (Modifica). Selezionare Remove (Rimuovi) per la regola da eliminare, quindi selezionare Save (Salva).

## Associazione di una sottorete a una lista di controllo accessi di rete

Per applicare le regole di una lista di controllo accessi di rete a una particolare sottorete, occorre associare la sottorete alla lista di controllo accessi di rete. Puoi associare una lista di controllo accessi di rete a più sottoreti. Tuttavia, una sottorete può essere associata a una sola lista di controllo accessi di rete. Eventuali sottoreti non associate a una particolare lista di controllo accessi vengono associate per impostazione predefinita alla lista di controllo accessi di rete predefinita.

Per associare una sottorete a una lista di controllo accessi di rete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Network ACLs (liste di controllo accessi di rete), quindi selezionare la lista di controllo accessi di rete.
3. Nel riquadro dei dettagli, nella scheda Subnet Associations (Associazioni sottorete) scegliere Edit (Modifica). Selezionare la casella di controllo Associate (Associa) per la sottorete da associare alla lista di controllo accessi di rete, quindi selezionare Save (Salva).

## Annullamento dell'associazione di una lista di controllo accessi di rete a una sottorete

È possibile annullare l'associazione di una lista di controllo accessi di rete personalizzata da una sottorete. Quando viene annullata l'associazione della sottorete dalla lista di controllo accessi di rete personalizzata, la sottorete viene quindi associata automaticamente alla lista di controllo accessi di rete predefinita.

Per annullare l'associazione di una sottorete a una lista di controllo accessi di rete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Network ACLs (liste di controllo accessi di rete), quindi selezionare la lista di controllo accessi di rete.
3. Nel riquadro dei dettagli, selezionare la scheda Subnet Associations (Associazioni sottorete).
4. Selezionare Edit (Modifica), quindi deselezionare la casella di controllo Associate (Associa) per la sottorete. Selezionare Salva.

## Modifica dell'ACL di rete di una sottorete

Puoi modificare la lista di controllo accessi di rete associata a una sottorete. Ad esempio, al momento della creazione, una sottorete viene inizialmente associata alla lista di controllo accessi di rete predefinita. Potrebbe invece Essere necessario associarla a una lista di controllo accessi di rete personalizzata creata.

Dopo aver modificato la lista di controllo accessi di rete di una sottorete, non è necessario terminare e riavviare le istanze nella sottorete. Le modifiche diventano effettive dopo un breve periodo di tempo.

Per modificare l'associazione della lista di controllo accessi di rete di una sottorete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Subnets (Sottoreti) e selezionare la sottorete.
3. Seleziona la scheda Network ACL (lista di controllo accessi di rete), quindi selezionare Edit (Modifica).
4. Selezionare la lista di controllo accessi di rete cui associare la sottorete dall'elenco Change in (Modifica in), quindi selezionare Save (Salva).

## Eliminazione di una lista di controllo accessi di rete

Puoi eliminare una lista di controllo accessi di rete solo se a essa non sono associate sottoreti. Non puoi eliminare la lista di controllo accessi di rete predefinita.

Per eliminare una lista di controllo accessi di rete

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Network ACL (lista di controllo accessi di rete).
3. Selezionare la lista di controllo accessi di rete, quindi selezionare Delete (Elimina).
4. Nella finestra di dialogo di conferma, scegliere Yes, Delete (Sì, elimina).

## Panoramica sulle API e sui comandi

Puoi eseguire le attività descritte in questa pagina tramite la riga di comando o un'API. Per ulteriori informazioni sulle interfacce a riga di comando e per un elenco delle API disponibili, consulta Uso di Amazon VPC.

Creazione di una lista di controllo accessi di rete per il VPC

- create-network-acl (AWS CLI)
- New-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Descrizione di una o più liste di controllo accessi di rete

- describe-network-acls (AWS CLI)
- Get-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Aggiunta di una regola a una lista di controllo accessi di rete

- create-network-acl-entry (AWS CLI)
- New-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Eliminazione di una regola da una lista di controllo accessi di rete

- delete-network-acl-entry (AWS CLI)
- Remove-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Sostituzione di una regola esistente in una lista di controllo accessi di rete

- replace-network-acl-entry (AWS CLI)
- Set-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Sostituzione di un'associazione della lista di controllo accessi di rete

- replace-network-acl-association (AWS CLI)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Eliminazione di una lista di controllo accessi di rete

- delete-network-acl (AWS CLI)
- Remove-EC2NetworkAcl (AWS Tools for Windows PowerShell)

## Gestire gli ACL di rete utilizzando Firewall Manager

AWS Firewall Manager semplifica le attività di amministrazione e manutenzione degli ACL di rete su più account e sottoreti. È possibile utilizzare Firewall Manager per monitorare account e sottoreti all'interno dell'organizzazione e applicare automaticamente le configurazioni ACL di rete definite. Firewall Manager è particolarmente utile quando si desidera proteggere l'intera organizzazione o se si aggiungono frequentemente nuove sottoreti che si desidera proteggere automaticamente da un account di amministratore centrale.

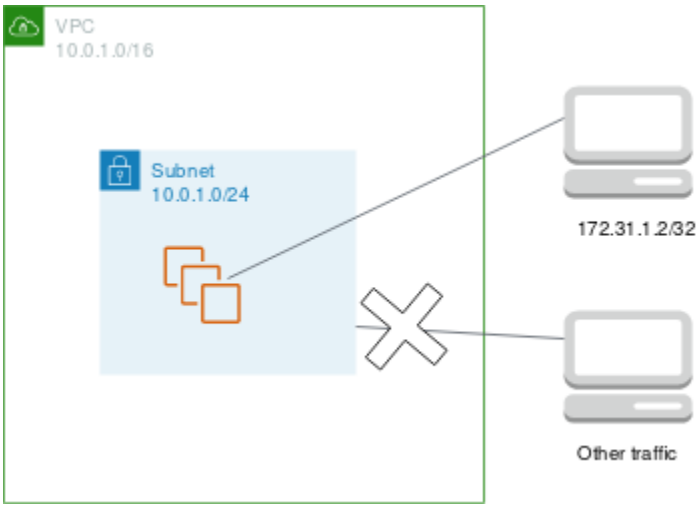
Con una politica ACL di rete Firewall Manager, utilizzando un unico account amministratore, è possibile configurare, monitorare e gestire i set di regole minimi che si desidera siano definiti negli ACL di rete utilizzati nell'organizzazione. È possibile specificare quali account e sottoreti dell'organizzazione rientrano nell'ambito della politica di Firewall Manager. Firewall Manager segnala lo stato di conformità degli ACL di rete per le sottoreti relative all'ambito ed è possibile configurare Firewall Manager per correggere automaticamente gli ACL di rete non conformi e renderli conformi.

Per ulteriori informazioni sull'utilizzo di Firewall Manager per gestire gli ACL di rete, consulta le seguenti risorse nella guida per gli AWS Firewall Manager sviluppatori:

- AWS Firewall Manager prerequisiti
- Guida introduttiva alle AWS Firewall Manager policy ACL della rete Amazon VPC
- Policy della lista di controllo degli accessi alla rete (ACL) di Amazon Virtual Private Cloud

# Esempio: controllo dell'accesso alle istanze in una sottorete

In questo esempio, le istanze nella sottorete possono comunicare tra loro e sono accessibili da un computer remoto affidabile. Il computer remoto potrebbe essere un computer della rete locale o un'istanza in una sottorete o in un VPC diversi. Viene usato per connettersi alle istanze in modo da eseguire attività amministrative. Le regole del gruppo di sicurezza e le regole della lista di controllo accessi di rete consentono l'accesso dall'indirizzo IP del computer remoto (172.31.1.2/32). Tutto il traffico restante da Internet o altre reti viene rifiutato. Questo scenario offre la flessibilità per modificare i gruppi di sicurezza o le regole dei gruppi di sicurezza per le istanze. La lista di controllo accessi di rete funziona come livello di difesa di backup.




Di seguito è riportato un esempio di gruppo di sicurezza da associare alle istanze. I gruppi di sicurezza sono stateful. Pertanto non è necessaria una regola che consenta le risposte al traffico in entrata.

In entrata

| Tipo di protocollo | Protocollo | Intervallo porte | Crea | Commenti |
|---|---|---|---|---|
| Tutto il traffico | Tutti | Tutti | sg-1234567890abcdef0 | Tutte le istanze associate a questo gruppo di sicurezza possono comunicare tra loro. |

| Tipo di protocollo | Protocollo | Intervallo porte | Crea | Commenti |
|---|---|---|---|---|
| SSH | TCP | 22 | 172.31.1.2/32 | Permette l'accesso SSH in entrata dal computer remoto. |

In uscita

| Tipo di protocollo | Protocollo | Intervallo porte | Destinazione | Commenti |
|---|---|---|---|---|
| Tutto il traffico | Tutti | Tutti | sg-123456 7890abcdef0 | Tutte le istanze associate a questo gruppo di sicurezza possono comunicare tra loro. |

Di seguito è riportato un esempio di ACL di rete da associare alle sottoreti per le istanze. Le regole delle liste di controllo accessi di rete si applicano a tutte le istanze nella sottorete. Le liste di controllo accessi di rete sono stateless. Pertanto, è necessaria una regola che consenta le risposte al traffico in entrata.

In entrata

| Rule # | Tipo | Protocollo | Intervallo porte | Crea | Consenti/ Nega | Commenti |
|---|---|---|---|---|---|---|
| 100 | SSH | TCP | 22 | 172.31.1. 2/32 | PERMETTI | Permette il traffico SSH in entrata dal computer remoto. |

| Rule # | Tipo | Protocollo | Intervallo porte | Crea | Consenti/ Nega | Commenti |
|---|---|---|---|---|---|---|
| * | Tutto il traffico | Tutti | Tutti | 0.0.0.0/0 | RIFIUTA | Nega tutto il traffico in entrata. |

In uscita

| Rule # | Tipo | Protocollo | Intervallo porte | Destinazione | Consenti/ Nega | Commenti |
|---|---|---|---|---|---|---|
| 100 | TCP personalizzato | TCP | 1024-65535 | 172.31.1.2/32 | PERMETTI | Permette risposte in uscita al computer remoto. |
| * | Tutto il traffico | Tutti | Tutti | 0.0.0.0/0 | RIFIUTA | Nega tutto il traffico in uscita. |

Se per errore le regole del gruppo di sicurezza vengono rese troppo permissive, le regole della lista di controllo accessi di rete in questo esempio continuano a consentire l'accesso solo dall'indirizzo IP specificato. Ad esempio, il seguente gruppo di sicurezza contiene una regola che consente l'accesso SSH in ingresso da qualsiasi indirizzo IP. Tuttavia, se si associa questo gruppo di sicurezza a un'istanza in una sottorete che utilizza l'ACL di rete, solo altre istanze all'interno della sottorete e del computer remoto possono accedere all'istanza, poiché le regole ACL di rete negano altro traffico in ingresso alla sottorete.

In entrata

| Type | Protocollo | Intervallo porte | Crea | Commenti |
|---|---|---|---|---|
| Tutto il traffico | Tutti | Tutti | sg-1234567890abcdef0 | Tutte le istanze associate a questo gruppo |

| Type | Protocollo | Intervallo porte | Crea | Commenti |
|---|---|---|---|---|
| | | | | di sicurezza possono comunicare tra loro. |
| SSH | TCP | 22 | 0.0.0.0/0 | Permette l'accesso SSH da qualsiasi indirizzo IP. |

In uscita

| Type | Protocollo | Intervallo porte | Destinazione | Commenti |
|---|---|---|---|---|
| Tutto il traffico | Tutti | Tutti | 0.0.0.0/0 | Autorizza tutto il traffico in uscita. |

## Risolvi i problemi di raggiungibilità

Reachability Analyzer è uno strumento di analisi statica della configurazione. Usa Reachability Analyzer per analizzare ed eseguire il debug della raggiungibilità della rete tra due risorse nel tuo VPC. Reachability Analyzer hop-by-hop produce dettagli del percorso virtuale tra queste risorse quando sono raggiungibili e identifica il componente di blocco in caso contrario. Ad esempio, è in grado di identificare le regole ACL di rete mancanti o non configurate correttamente.

Per ulteriori informazioni, consulta la Guida di Reachability Analyzer.

# Resilienza in Amazon Virtual Private Cloud

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate tramite reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover 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 tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Puoi configurare i VPC per soddisfare i requisiti di resilienza dei carichi di lavoro. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Comprendi i modelli e i compromessi di resilienza (Architecture Blog)AWS
- Pianifica la tua topologia di rete (AWS Well-Architected Framework)
- Opzioni di connettività Amazon Virtual Private Cloud (AWS white paper)

## Convalida della conformità per Amazon Virtual Private Cloud

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)).
- Evaluating Resources with Rules nella AWS Config Developer Guide: 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.

## Best practice per la sicurezza per il VPC

Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

- Quando aggiungi sottoreti al tuo VPC per ospitare l'applicazione, creale in più zone di disponibilità. Una zona di disponibilità è uno o più data center discreti con alimentazione, rete e connettività ridondanti in una regione. AWS Le zone di disponibilità consentono di rendere le applicazioni di produzione altamente disponibili, tolleranti ai guasti e scalabili. Per ulteriori informazioni, consulta la pagina Amazon VPC su AWS.
- Utilizza i gruppi di sicurezza per controllare il traffico verso le istanze EC2 nelle sottoreti. Per ulteriori informazioni, consulta Gruppi di sicurezza.

- Utilizza le ACL di rete per controllare il traffico in entrata e in uscita a livello di sottorete. Per ulteriori informazioni, consulta Come controllare il traffico verso le sottoreti utilizzando le liste di controllo degli accessi di rete.
- Gestisci l'accesso alle AWS risorse nel tuo VPC utilizzando la federazione delle identità AWS Identity and Access Management (IAM), gli utenti e i ruoli. Per ulteriori informazioni, consulta Identity and Access Management per Amazon VPC.
- Utilizza i log di flusso VPC per monitorare il traffico IP verso e da un'interfaccia di VPC, sottorete o rete. Per ulteriori informazioni, consulta Log di flusso VPC.
- Utilizza lo Strumento di analisi degli accessi alla rete per identificare un accesso di rete involontario alle risorse nei nostri VPC. Per ulteriori informazioni, consulta la Guida di Strumento di analisi degli accessi alla rete.
- Utilizzalo AWS Network Firewall per monitorare e proteggere il tuo VPC filtrando il traffico in entrata e in uscita. Per ulteriori informazioni, consulta la Guida per AWS Network Firewall.
- Usa Amazon GuardDuty per rilevare potenziali minacce ai tuoi account, contenitori, carichi di lavoro e dati all'interno del tuo AWS ambiente. Il rilevamento fondamentale delle minacce include il monitoraggio dei log di flusso VPC associati alle istanze Amazon EC2. Per ulteriori informazioni, consulta VPC Flow Logs nella Amazon GuardDuty  User Guide.

Per ottenere le risposte alle domande frequenti relative alla sicurezza del VPC, consulta Filtraggio e sicurezza in Domande frequenti su Amazon VPC.

# Usa Amazon VPC con altri Servizi AWS

Puoi utilizzare Amazon VPC con altri Servizi AWS per creare soluzioni che soddisfino le tue esigenze.

Indice



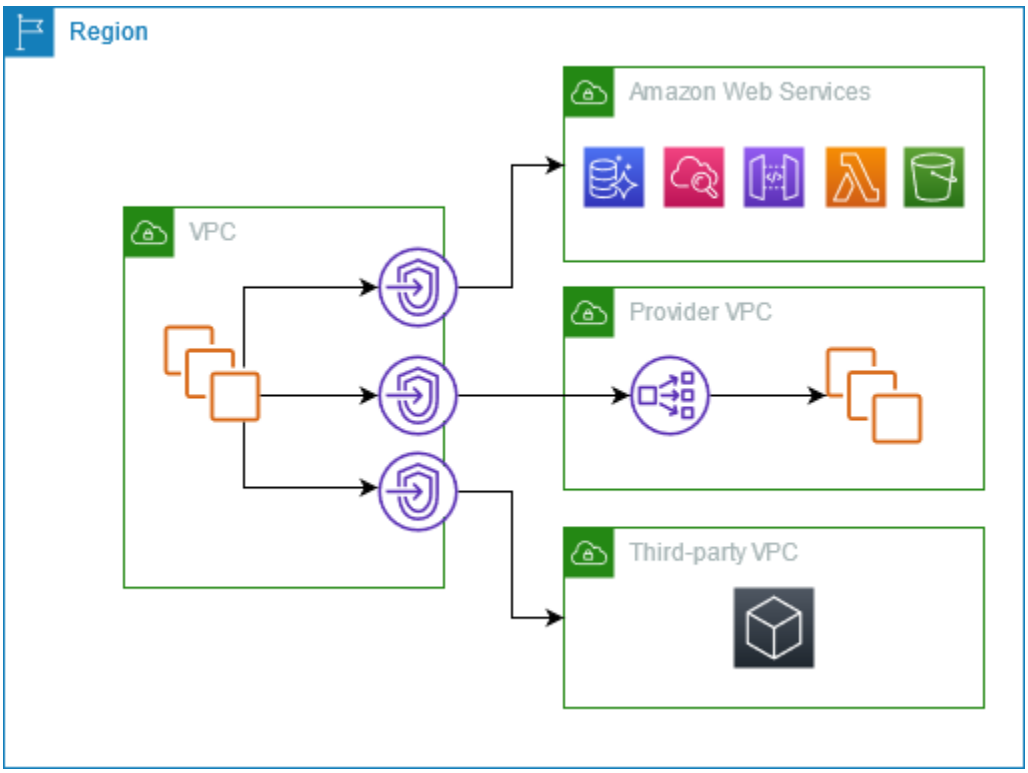
## Connetti il tuo VPC ai servizi utilizzando AWS PrivateLink

AWS PrivateLink stabilisce una connettività privata tra cloud privati virtuali (VPC) e Servizi AWS supportati, servizi ospitati da altri Account AWS e servizi Marketplace AWS supportati. Per comunicare con il servizio non sono necessari gateway Internet, dispositivi NAT, connessione AWS Direct Connect o connessione AWS Site-to-Site VPN.

Per utilizzare AWS PrivateLink, crea un endpoint VPC nel VPC specificando il nome del servizio e una sottorete. In questo modo, nella sottorete si crea un'interfaccia di rete Elastica che funge da punto di ingresso per traffico destinato al servizio.

Puoi creare il tuo servizio endpoint VPC, basato su AWS PrivateLink, e consentire ad altri clienti AWS di accedere al servizio.

Il seguente diagramma mostra i casi d'uso comuni per AWS PrivateLink. Il VPC a sinistra ha diverse istanze EC2 in una sottorete privata e tre endpoint VPC di interfaccia. L'endpoint VPC superiore si connette a un Servizio AWS. L'endpoint VPC centrale si connette a un servizio ospitato da un altro Account AWS (un servizio endpoint VPC). L'endpoint VPC inferiore si collega a un servizio partner Marketplace AWS.




Per ulteriori informazioni, consulta AWS PrivateLink.

## Filtrare il traffico di rete utilizzando AWS Network Firewall

Puoi filtrare il traffico di rete sul perimetro del VPC utilizzando AWS Network Firewall. Network Firewall è un firewall di rete con servizio di prevenzione e rilevamento delle intrusioni gestito di tipo stateful. Per ulteriori informazioni, consulta la Guida per sviluppatori di AWS Network Firewall.

Puoi implementare Network Firewall con le risorse AWS riportate di seguito.

| Risorsa di Network Firewall | Descrizione |
| --- | --- |
| Firewall | Un firewall collega il comportamento di filtraggio del traffico di rete della policy di un firewall al VPC che si desidera proteggere. La configura zione del firewall include specifiche per le zone di disponibilità e le sottoreti in cui sono collocati gli endpoint del firewall. Definisce inoltre impostazioni di alto livello come la configurazione della registrazione firewall e il tagging sulla risorsa firewall AWS. |

| Risorsa di Network Firewall | Descrizione |
| --- | --- |
| | Per ulteriori informazioni, consulta Firewall in AWS Network Firewall. |
| Policy firewall | Una policy firewall definisce il comportamento di monitoraggio e protezione per un firewall. I dettagli del comportamento vengono definiti nei gruppi di regole aggiunti alle policy e in alcune impostazioni predefinite. Per utilizzare una policy firewall, è necessario associarla a uno o più firewall.<br><br>Per ulteriori informazioni, consulta Policy del firewall in AWS Network Firewall. |
| Gruppo di regole | Un gruppo di regole è un insieme di criteri riutilizzabili per l'ispezione e la gestione del traffico di rete. Puoi aggiungere uno o più gruppi di regole a una policy firewall come parte della configurazione della policy. Puoi definire gruppi di regole stateless per ispezionare ogni pacchetto di rete in isolamento. I gruppi di regole stateless sono simili nel comportamento e nell'utilizzo degli elenchi di controllo degli accessi (ACL) di rete di Amazon VPC. Puoi inoltre definire gruppi di regole stateful per ispezionare i pacchetti nel contesto del flusso di traffico. I gruppi di regole stateful sono simili nel comportamento e nell'utilizzo dei gruppi di sicurezza di Amazon VPC.<br><br>Per ulteriori informazioni, consulta Gruppi di regole in AWS Network Firewall. |

Puoi inoltre utilizzare AWS Firewall Manager per configurare e gestire centralmente le risorse di Network Firewall tra gli account e le applicazioni in AWS Organizations. I firewall possono essere gestiti per più account utilizzando un unico account in Firewall Manager. Per ulteriori informazioni, consulta AWS Firewall Manager nella Guida per gli sviluppatori di AWS WAF, AWS Firewall Manager e AWS Shield Advanced.

## Filtrare il traffico DNS utilizzando Route 53 Resolver DNS Firewall

Con DNS Firewall puoi definire le regole di filtro dei nomi di dominio nei gruppi di regole associati ai VPC. Puoi specificare elenchi di nomi di dominio da consentire o bloccare ed è possibile

personalizzare le risposte per le query DNS bloccate. Per ulteriori informazioni, consulta la documentazione di DNS Firewall per Route 53 Resolver.

Puoi implementare DNS Firewall con le seguenti risorse AWS.

| Risorsa DNS Firewall | Descrizione |
| --- | --- |
| Gruppo di regole DNS Firewall | Un gruppo di regole DNS Firewall è un insieme denominato e riutilizzabile di regole di DNS Firewall per filtrare le query DNS. Compila il gruppo di regole con le regole di filtro, quindi associa il gruppo di regole a uno o più VPC di Amazon VPC. Quando associ un gruppo di regole a un VPC, si abilita il filtro DNS Firewall per il VPC. Quindi, quando Resolver riceve una query DNS per un VPC che ha un gruppo di regole associato, Resolver passa la query a DNS Firewall per il filtro.<br><br>Ogni regola all'interno del gruppo di regole specifica un elenco di domini e un'azione da eseguire sulle query DNS i cui domini corrispondono alle specifiche del dominio nell'elenco. Puoi consentire, bloccare o avvisare le query corrispondenti. Puoi inoltre definire risposte personalizzate per le query bloccate.<br><br>Per ulteriori informazioni, consulta Gruppi di regole e regole in DNS Firewall per Route 53 Resolver. |
| Elenco dei domini | Un elenco di domini è un insieme riutilizzabile di specifiche di dominio utilizzate in una regola DNS Firewall all'interno di un gruppo di regole.<br><br>Per maggiori informazioni, consulta Elenchi di dominio in DNS Firewall per Route 53 Resolver. |

Puoi inoltre utilizzare AWS Firewall Manager per configurare e gestire centralmente le risorse di DNS Firewall tra gli account e le organizzazioni in AWS Organizations. I firewall possono essere gestiti per più account utilizzando un unico account in Firewall Manager. Per ulteriori informazioni, consulta AWS Firewall Manager nella Guida per gli sviluppatori di AWS WAF, AWS Firewall Manager e AWS Shield Advanced.

# Risolvi i problemi di raggiungibilità utilizzando Reachability Analyzer

Reachability Analyzer è uno strumento di analisi statica della configurazione. Usa Reachability Analyzer per analizzare ed eseguire il debug della raggiungibilità della rete tra due risorse nel tuo VPC. Reachability Analyzer hop-by-hop produce dettagli del percorso virtuale tra queste risorse quando sono raggiungibili e identifica il componente di blocco in caso contrario.

È possibile utilizzare Reachability Analyzer per analizzare la raggiungibilità tra le seguenti risorse:

- Istanze
- Gateway Internet
- Interfacce di rete
- Gateway di transito
- Collegamenti del gateway di transito
- Servizi endpoint VPC
- Endpoint VPC
- Connessioni in peering di VPC
- Gateway VPN

Per ulteriori informazioni, consulta la Guida di Reachability Analyzer.

# Esempi di VPC

Le seguenti sono configurazioni di esempio per i cloud privati virtuali (VPC).

Esempi

- Esempio: VPC per un ambiente di test
- Esempio: VPC per server Web e di database
- Esempio: VPC con server in sottoreti private e NAT

Esempi correlati

- Per connettere i tuoi VPC tra loro, consulta la pagina Configurazioni di peering VPC nella Guida alle connessioni peering di Amazon VPC.
- Per connettere i tuoi VPC alla tua rete, consulta la pagina Architetture VPN Site-to-Site nella Guida per l'utente di AWS Site-to-Site VPN.
- Per connettere i tuoi VPC tra loro e alla tua rete, consulta la pagina Esempi di gateway di transito in Gateway di transito Amazon VPC.

Risorse aggiuntive

- Apprendi i modelli e i compromessi di resilienza (Blog di architettura di AWS)
- Pianifica la tua topologia di rete (Canone di architettura di AWS)
- Opzioni di connettività di Amazon Virtual Private Cloud (Whitepaper di AWS)

# Esempio: VPC per un ambiente di test

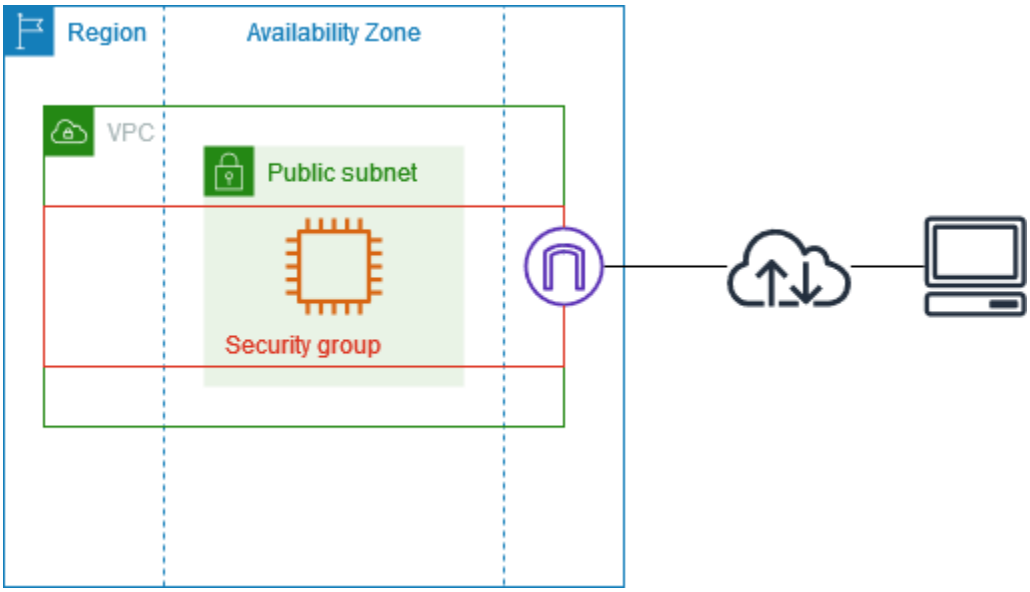
Questo esempio illustra come creare un VPC da utilizzare come ambiente di sviluppo o test. Poiché questo VPC non è destinato all'uso in produzione, non è necessario distribuire i server in più zone di disponibilità. Per contenere i costi e la complessità, è possibile distribuire i server in un'unica zona di disponibilità.

Indice

- Distribuzione dell'applicazione
- Test della configurazione
- Elimina

## Panoramica

Nel diagramma seguente viene fornita una panoramica delle risorse incluse in questo esempio. Il VPC ha una sottorete pubblica in un'unica zona di disponibilità e un gateway Internet. Il server è un'istanza EC2 che viene eseguita nella sottorete pubblica. Il gruppo di sicurezza dell'istanza consente il traffico SSH dal tuo computer, oltre a qualsiasi altro traffico specificamente richiesto per le tue attività di sviluppo o test.




### Routing

Quando crei questo VPC utilizzando la console Amazon VPC, creiamo una tabella di routing per la sottorete pubblica con percorsi locali e percorsi verso il gateway Internet. Di seguito è riportato un esempio di tabella di instradamento con percorsi per IPv4 e IPv6. Se crei una sottorete solo IPv4 anziché una sottorete a doppio stack, la tabella di instradamento contiene solo i percorsi IPv4.

| Destinazione | Target |
| --- | --- |
| *10.0.0.0/16* | locale |
| *2001:db8:1234:1a00::/56* | locale |

| Destinazione | Target |
| --- | --- |
| 0.0.0.0/0 | *igw-id* |
| ::/0 | *igw-id* |

## Sicurezza

Per questa configurazione di esempio, è necessario creare un gruppo di sicurezza per l'istanza che consenta il traffico di cui l'applicazione ha bisogno. Ad esempio, potrebbe essere necessario aggiungere una regola che consenta il traffico SSH dal computer o il traffico HTTP dalla rete.

Di seguito sono riportati esempi di regole in entrata per un gruppo di sicurezza, con regole sia per IPv4 sia per IPv6. Se crei sottoreti solo IPv4 anziché sottoreti a doppio stack, hai bisogno soltanto delle regole per IPv4.

In entrata

| Crea | Protocollo | Intervallo porte | Descrizione |
| --- | --- | --- | --- |
| 0.0.0.0/0 | TCP | 80 | Permette l'accesso HTTP in entrata da tutti gli indirizzi IPv4 |
| ::/0 | TCP | 80 | Consente l'accesso HTTP in entrata da tutti gli indirizzi IPv6 |
| 0.0.0.0/0 | TCP | 443 | Autorizza l'accesso HTTPS in entrata da tutti gli indirizzi IPv4 |
| ::/0 | TCP | 443 | Consente l'accesso HTTPS in entrata da tutti gli indirizzi IPv6 |
| *Intervallo di indirizzi IPv4 pubblici della rete* | TCP | 22 | (Facoltativo) Autorizza l'accesso SSH in entrata dagli indirizzi IP IPv4 nella rete |

| Crea | Protocollo | Intervallo porte | Descrizione |
|---|---|---|---|
| *Intervallo di indirizzi IPv6 della rete* | TCP | 22 | (Facoltativo) Autorizza l'accesso SSH in entrata dagli indirizzi IP IPv6 nella rete |
| *Intervallo di indirizzi IPv4 pubblici della rete* | TCP | 3389 | (Facoltativo) Autorizza l'accesso RDP in entrata dagli indirizzi IP IPv4 nella rete |
| *Intervallo di indirizzi IPv6 della rete* | TCP | 3389 | (Facoltativo) Autorizza l'accesso RDP in entrata dagli indirizzi IP IPv6 nella rete |

## Creazione del VPC

Utilizza la procedura seguente per creare un VPC con una sottorete pubblica in una zona di disponibilità. Questa configurazione è adatta per un ambiente di sviluppo o test.

Per creare il VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di controllo, scegli Crea VPC.
3. Per Resources to create (Risorse da creare), scegli VPC and more (VPC e altro).
4. Configurazione del VPC
    a. Per Name tag auto-generation (Generazione automatica di tag nome), immetti un nome per il VPC.
    b. Per Blocco CIDR IPv4, mantieni il suggerimento predefinito o, in alternativa, inserisci il blocco CIDR richiesto dall'applicazione o dalla rete. Per ulteriori informazioni, consulta the section called “Blocchi CIDR del VPC”.
    c. (Facoltativo) Se l'applicazione comunica utilizzando indirizzi IPv6, scegli Blocco CIDR IPv6, Blocco CIDR IPv6 fornito da Amazon.
5. Configurazione delle sottoreti

a. Per Numero di zone di disponibilità, scegli 1. Puoi mantenere la zona di disponibilità (AZ) predefinita o, in alternativa, puoi espandere Personalizza AZ e selezionare una zona di disponibilità.
b. Per Number of public subnets (Numero di sottoreti pubbliche), scegli 1.
c. Per Number of private subnets (Numero di sottoreti private), scegli 0.
d. Puoi mantenere il blocco CIDR predefinito per la sottorete pubblica o, in alternativa, espandere Personalizza blocchi CIDR della sottorete e inserire un blocco CIDR. Per ulteriori informazioni, consulta the section called “Blocchi CIDR di sottorete”.

6. Per Gateway NAT, mantieni il valore predefinito, Nessuno.
7. Per VPC endpoints (Endpoint VPC), scegli None (Nessuno). Un endpoint VPC del gateway per S3 viene utilizzato solo per accedere ad Amazon S3 da sottoreti private.
8. Mantieni selezionate entrambe le opzioni in Opzioni DNS. Di conseguenza, l'istanza riceverà un nome host DNS pubblico che corrisponde al suo indirizzo IP pubblico.
9. Seleziona Create VPC (Crea VPC).

## Distribuzione dell'applicazione

È possibile implementare le istanze EC2 in diversi modi. Ad esempio:

- Procedura guidata di avvio dell'istanza Amazon EC2
- Amazon EC2 Auto Scaling
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Dopo aver implementato un'istanza EC2, puoi connetterti all'istanza, installare il software necessario per l'applicazione e quindi creare un'immagine per l'uso futuro. Per ulteriori informazioni, consulta la pagina Creazione di un'AMI Linux o Creazione di un'AMI Windows nella documentazione di Amazon EC2. In alternativa, puoi usare EC2 Image Builder per creare e gestire l'Amazon Machine Image (AMI).

## Test della configurazione

Dopo aver completato l'implementazione dell'applicazione, potrai testarla. Se non riesci a connetterti all'istanza EC2 o se l'applicazione non è in grado di inviare o ricevere il traffico previsto, puoi

utilizzare Sistema di analisi della reperibilità per risolvere i problemi. Ad esempio, Sistema di analisi della reperibilità può identificare i problemi di configurazione relativi alle tabelle di instradamento o ai gruppi di sicurezza. Per ulteriori informazioni, consulta la Guida di Reachability Analyzer.

### Elimina

Quando la configurazione non è più necessaria, è possibile eliminarla. Prima di eliminare il VPC, è necessario terminare l'istanza. Per ulteriori informazioni, consulta the section called “Eliminazione del VPC”.

## Esempio: VPC per server Web e di database

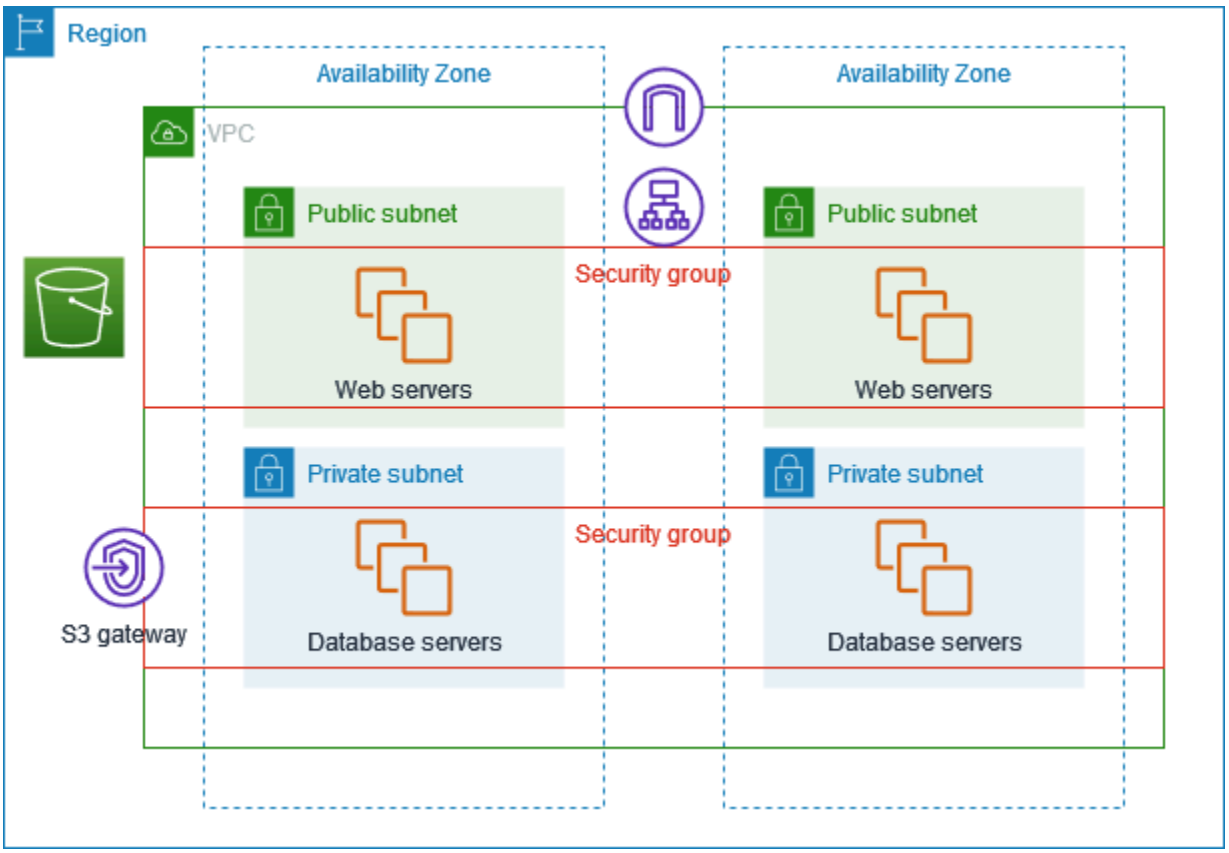
Questo esempio spiega come creare un VPC da utilizzare per un'architettura a due livelli in un ambiente di produzione. Per migliorare la resilienza, implementerai i server in due zone di disponibilità.

Indice



### Panoramica

Nel diagramma seguente viene fornita una panoramica delle risorse incluse in questo esempio. Il VPC dispone di sottoreti pubbliche e private in due zone di disponibilità. I server Web vengono eseguiti nelle sottoreti pubbliche e ricevono traffico dai client tramite un sistema di bilanciamento del carico. Il gruppo di sicurezza dei server Web consente il traffico dal sistema di bilanciamento del carico. I server di database vengono eseguiti nelle sottoreti private e ricevono traffico dai server Web. Il gruppo di sicurezza dei server Web consente il traffico dai server Web. I server di database possono connettersi ad Amazon S3 utilizzando un endpoint VPC gateway.




## Routing

Quando crei questo VPC utilizzando la console Amazon VPC, creiamo una tabella di routing per le sottoreti pubbliche con percorsi locali e percorsi verso il gateway Internet, nonché una tabella di routing per ogni sottorete privata con percorsi locali e un percorso verso l'endpoint VPC del gateway.

Di seguito è riportato un esempio di tabella di routing per le sottoreti pubbliche, con percorsi sia per IPv4 sia per IPv6. Se crei sottoreti solo IPv4 anziché sottoreti a doppio stack, la tabella di routing include solo i percorsi IPv4.

| Destinazione | Target |
| --- | --- |
| *10,0,0/16* | locale |
| *2001:db8:1234:1a00::/56* | locale |
| 0.0.0.0/0 | *igw-id* |
| ::/0 | *igw-id* |

Di seguito è riportato un esempio di tabella di routing per le sottoreti private, con percorsi sia per IPv4 sia per IPv6. Se hai creato sottoreti solo IPv4, la tabella di instradamento include solo il percorso IPv4. L'ultimo percorso invia il traffico destinato ad Amazon S3 all'endpoint VPC del gateway.

| Destinazione | Target |
| --- | --- |
| *10,0,0/16* | locale |
| *2001:db8:1234:1a00::/56* | local |
| *s3-prefix-list-id* | *s3-gateway-id* |

## Sicurezza

Per questa configurazione di esempio, crei un gruppo di sicurezza per il sistema di bilanciamento del carico, un gruppo di sicurezza per i server Web e uno per i server di database.

Sistema di bilanciamento del carico (load balancer)

Il gruppo di sicurezza dell'Application Load Balancer o Network Load Balancer deve consentire il traffico in entrata dai client sulla porta ascoltatore del sistema di bilanciamento del carico. Per accettare traffico da qualunque punto di Internet, specifica 0.0.0.0/0 come origine. Il gruppo di sicurezza del sistema di bilanciamento del carico deve inoltre permettere il traffico in entrata dal sistema di bilanciamento del carico alle istanze di destinazione sulla porta dell'ascoltatore dell'istanza e sulla porta di controllo dell'integrità.

Server Web

Le seguenti regole per il gruppo di sicurezza consentono ai server Web di ricevere traffico HTTP e HTTPS dal sistema di bilanciamento del carico. Facoltativamente, puoi consentire ai server Web di ricevere traffico SSH o RDP dalla tua rete. I server Web possono inviare traffico SQL o MySQL ai server di database.

In entrata

| Crea | Protocollo | Intervallo porte | Descrizione |
| --- | --- | --- | --- |
| *L'ID del gruppo di sicurezza per il sistema di* | TCP | 80 | Consente l'accesso HTTP in entrata dal sistema di bilanciam ento del carico |

| Crea | Protocollo | Intervallo porte | Descrizione |
| --- | --- | --- | --- |
| *bilanciamento del carico* | | | |
| *L'ID del gruppo di sicurezza per il sistema di bilanciamento del carico* | TCP | 443 | Consente l'accesso HTTP in entrata dal sistema di bilanciamento del carico |
| *Intervallo di indirizzi IPv4 pubblici della rete* | TCP | 22 | (Facoltativo) Autorizza l'accesso SSH in entrata dagli indirizzi IP IPv4 nella rete |
| *Intervallo di indirizzi IPv6 della rete* | TCP | 22 | (Facoltativo) Autorizza l'accesso SSH in entrata dagli indirizzi IP IPv6 nella rete |
| *Intervallo di indirizzi IPv4 pubblici della rete* | TCP | 3389 | (Facoltativo) Autorizza l'accesso RDP in entrata dagli indirizzi IP IPv4 nella rete |
| *Intervallo di indirizzi IPv6 della rete* | TCP | 3389 | (Facoltativo) Autorizza l'accesso RDP in entrata dagli indirizzi IP IPv6 nella rete |

In uscita

| Destinazione | Protocollo | Intervallo porte | Descrizione |
| --- | --- | --- | --- |
| *ID del gruppo di sicurezza per le istanze che eseguono Microsoft SQL Server* | TCP | 1433 | Consente l'accesso Microsoft SQL Server in uscita ai server di database |

| Destinazione | Protocollo | Intervallo porte | Descrizione |
| --- | --- | --- | --- |
| *ID del gruppo di sicurezza per le istanze che eseguono MySQL* | TCP | 3306 | Consente l'accesso a MySQL in uscita ai server di database |

Server di database

Le regole del gruppo di sicurezza seguente consentono ai server di database di ricevere richieste di lettura e scrittura dai server Web.

In entrata

| Crea | Protocollo | Intervallo porte | Commenti |
| --- | --- | --- | --- |
| *ID del gruppo di sicurezza del server Web* | TCP | 1433 | Consente l'accesso Microsoft SQL Server in entrata dai server Web |
| *ID del gruppo di sicurezza del server Web* | TCP | 3306 | Consente l'accesso MySQL Server in entrata dai server Web |

In uscita

| Destinazione | Protocollo | Intervallo porte | Commenti |
| --- | --- | --- | --- |
| 0.0.0.0/0 | TCP | 80 | Consente l'accesso HTTP in uscita a Internet su IPv4 |
| 0.0.0.0/0 | TCP | 443 | Consente l'accesso HTTPS in uscita a Internet su IPv4 |

Per maggiori informazioni sui gruppi di sicurezza per le istanze di Amazon RDS DB, consulta Controllo dell'accesso con i gruppi di sicurezza nella Guida dell'utente di Amazon RDS.

# Creazione del VPC

Utilizza la procedura seguente per creare un VPC con una sottorete pubblica e una sottorete privata in due zone di disponibilità.

Per creare il VPC

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di controllo, scegli Crea VPC.
3. Per Risorse da creare, scegli VPC e altro.
4. Configura il VPC:
    a. Mantieni selezionata la generazione automatica dei tag Nome per creare i tag Nome per le risorse VPC o deselezionala per fornire i tuoi tag Nome per le risorse VPC.
    b. Per Blocco CIDR IPv4, mantieni il suggerimento predefinito o, in alternativa, inserisci il blocco CIDR richiesto dall'applicazione o dalla rete. Per ulteriori informazioni, consulta the section called “Blocchi CIDR del VPC”.
    c. (Facoltativo) Se l'applicazione comunica utilizzando indirizzi IPv6, scegli Blocco CIDR IPv6, Blocco CIDR IPv6 fornito da Amazon.
    d. Scegli un'opzione di tenancy. Questa opzione definisce se le istanze EC2 avviate nel VPC verranno eseguite su hardware condiviso con altri Account AWS o su hardware dedicato esclusivamente all'uso personale. Se scegli la tenancy del VPC, le istanze EC2 `Default` avviate in questo VPC utilizzeranno l'attributo di tenancy specificato all'avvio dell'istanza. Per ulteriori informazioni, consulta Launch an instance using defined parameters nella Amazon EC2 User Guide. Se scegli che la tenancy del VPC sia `Dedicated`, le istanze verranno sempre eseguite come Istanze dedicate su un hardware dedicato per il tuo utilizzo.
5. Configura le sottoreti:
    a. Per Numero di zone di disponibilità, scegli 2, in modo da poter avviare le istanze in due zone di disponibilità per migliorare la resilienza.
    b. Per Number of public subnets (Numero di sottoreti pubbliche), scegli 2.
    c. Per Number of private subnets (Numero di sottoreti private), scegli 2.
    d. È possibile mantenere i blocchi CIDR predefiniti per le sottoreti o, in alternativa, espandere i blocchi CIDR di Customize subnet e inserire un blocco CIDR. Per ulteriori informazioni, consulta the section called “Blocchi CIDR di sottorete”.
6. Per Gateway NAT, mantieni il valore predefinito, Nessuno.

7. Per Endpoint VPC, mantieni il valore predefinito, Gateway S3. Sebbene non vi sia alcun effetto a meno che non si acceda a un bucket S3, l'attivazione di questo endpoint VPC non comporta alcun costo.
8. Mantieni selezionate entrambe le opzioni in Opzioni DNS. Di conseguenza, i server Web riceveranno nomi host DNS pubblici che corrispondono ai loro indirizzi IP pubblici.
9. Seleziona Crea VPC.

## Distribuzione dell'applicazione

Idealmente, hai già testato i server Web e i server di database in un ambiente di sviluppo o test e hai creato gli script o le immagini che utilizzerai per implementare l'applicazione in produzione.

Puoi utilizzare le istanze EC2 per i tuoi server web. È possibile implementare le istanze EC2 in diversi modi. Per esempio:

- Procedura guidata di avvio dell'istanza Amazon EC2
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Per migliorare la disponibilità, puoi utilizzare Dimensionamento automatico Amazon EC2 per implementare server in più zone di disponibilità e mantenere la capacità minima del server che è richiesta dalla tua applicazione.

Puoi utilizzare Elastic Load Balancing per distribuire il traffico in modo uniforme tra i tuoi server. Puoi collegare un sistema di bilanciamento del carico al gruppo con scalabilità automatica.

Puoi utilizzare le istanze EC2 per i tuoi server di database o uno dei nostri tipi di database dedicati. Per ulteriori informazioni, consulta Databases on: How to choose. AWS

## Test della configurazione

Dopo aver completato l'implementazione dell'applicazione, potrai testarla. Se l'applicazione non è in grado di inviare o ricevere il traffico previsto, puoi utilizzare Sistema di analisi della reperibilità per risolvere i problemi. Ad esempio, Sistema di analisi della reperibilità può identificare i problemi di configurazione relativi alle tabelle di instradamento o ai gruppi di sicurezza. Per ulteriori informazioni, consulta la Guida di Reachability Analyzer.

## Eliminazione

Quando la configurazione non è più necessaria, è possibile eliminarla. Prima di eliminare il VPC, è necessario terminare le istanze ed eliminare il sistema di bilanciamento del carico. Per ulteriori informazioni, consulta the section called “Eliminazione del VPC”.

# Esempio: VPC con server in sottoreti private e NAT

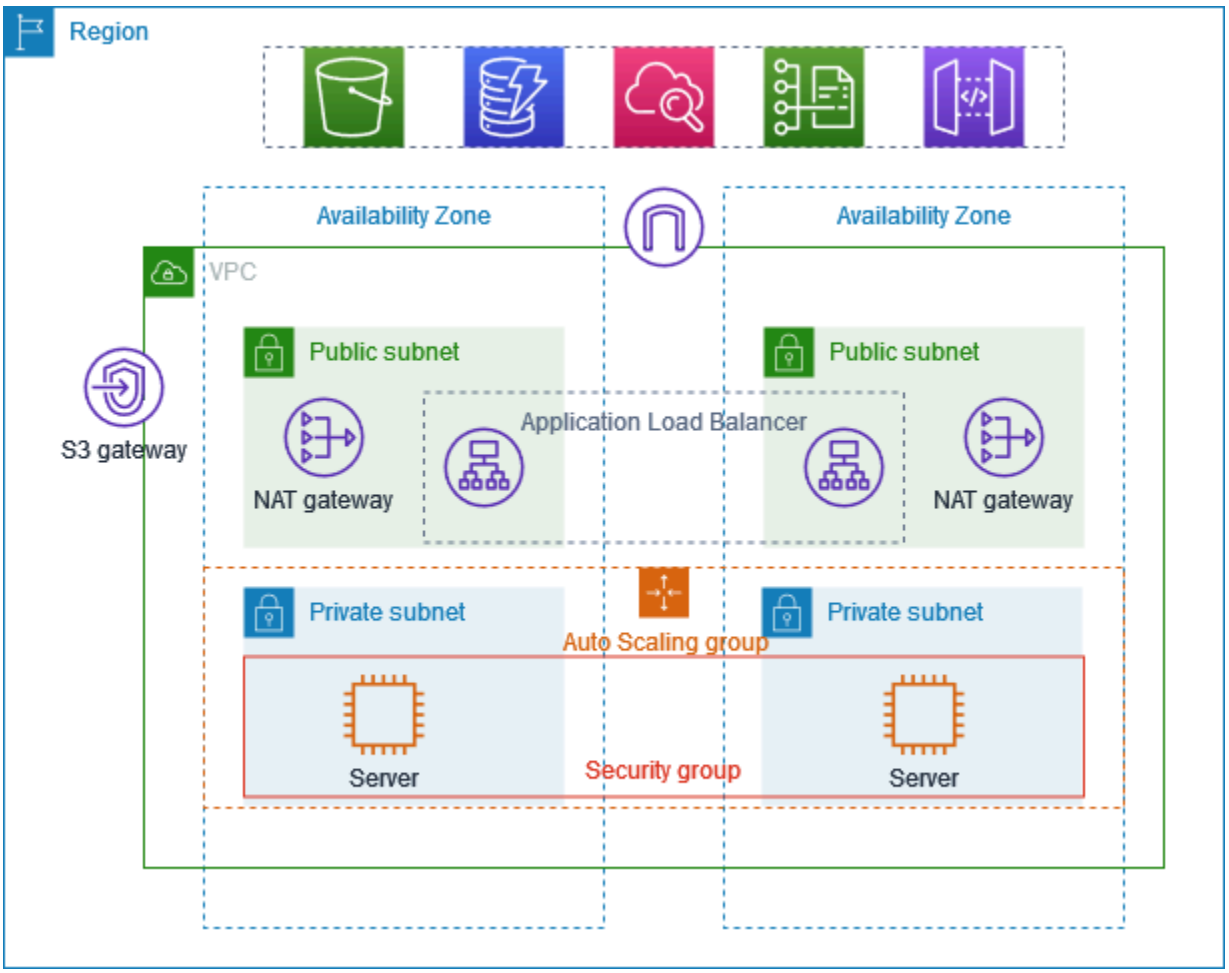
Questo esempio spiega come creare un VPC da utilizzare per i server in un ambiente di produzione. Per migliorare la resilienza, implementerai i server in due zone di disponibilità, utilizzando un gruppo con scalabilità automatica e un Application Load Balancer. Per una maggiore sicurezza, implementerai i server in sottoreti private. I server ricevono le richieste tramite il sistema di bilanciamento del carico. I server possono connettersi a Internet utilizzando un gateway NAT. Per migliorare la resilienza, implementerai il gateway NAT in entrambe le zone di disponibilità.

Indice



## Panoramica

Nel diagramma seguente viene fornita una panoramica delle risorse incluse in questo esempio. Il VPC dispone di sottoreti pubbliche e private in due zone di disponibilità. Ogni sottorete pubblica contiene un gateway NAT e un nodo del sistema di bilanciamento del carico. I server vengono eseguiti nelle sottoreti private, vengono avviati e terminati utilizzando un gruppo con scalabilità automatica e ricevono traffico dal sistema di bilanciamento del carico. I server possono connettersi a Internet utilizzando il gateway NAT. I server possono connettersi ad Amazon S3 utilizzando un endpoint VPC gateway.




## Routing

Quando crei questo VPC utilizzando la console Amazon VPC, creiamo una tabella di routing per le sottoreti pubbliche con percorsi locali e percorsi verso il gateway Internet. Creiamo anche una tabella di instradamento per le sottoreti private con percorsi locali e percorsi verso il gateway NAT, il gateway Internet solo in uscita e l'endpoint VPC del gateway.

Di seguito è riportato un esempio di tabella di instradamento per le sottoreti pubbliche, con percorsi sia per IPv4 sia per IPv6. Se crei sottoreti solo IPv4 anziché sottoreti a doppio stack, la tabella di instradamento include solo i percorsi IPv4.

| Destinazione | Target |
| --- | --- |
| *10.0.0.0/16* | locale |
| *2001:db8:1234:1a00::/56* | locale |

| Destinazione | Target |
| --- | --- |
| 0.0.0.0/0 | *igw-id* |
| ::/0 | *igw-id* |

Di seguito è riportato un esempio di tabella di instradamento per le sottoreti private, con percorsi sia per IPv4 sia per IPv6. Se hai creato sottoreti solo IPv4, la tabella di instradamento include solo i percorsi IPv4. L'ultimo percorso invia il traffico destinato ad Amazon S3 all'endpoint VPC del gateway.

| Destinazione | Target |
| --- | --- |
| *10.0.0.0/16* | locale |
| *2001:db8:1234:1a00::/56* | locale |
| 0.0.0.0/0 | *nat-gateway-id* |
| ::/0 | *eigw-id* |
| *s3-prefix-list-id* | *s3-gateway-id* |

## Sicurezza

Di seguito è riportato un esempio delle regole che è possibile creare per il gruppo di sicurezza che si associa ai server. Il gruppo di sicurezza deve consentire il traffico dal sistema di bilanciamento del carico al protocollo e alla porta dell'ascoltatore. Deve inoltre consentire il controllo dell'integrità del traffico.

In entrata

| Crea | Protocollo | Intervallo porte | Commenti |
| --- | --- | --- | --- |
| *ID del gruppo di sicurezza del sistema di bilanciamento del carico* | *protocollo dell'ascoltatore* | *porta dell'ascoltatore* | Consente il traffico in entrata dal sistema di bilanciamento del carico sulla porta dell'ascoltatore |

| Crea | Protocollo | Intervallo porte | Commenti |
| --- | --- | --- | --- |
| *ID del gruppo di sicurezza del sistema di bilanciamento del carico* | *protocollo di controllo dell'integrità* | *porta di controllo dell'integrità* | Autorizza il traffico del controllo dell'integrità dal sistema di bilanciamento del carico |

## Creazione del VPC

Utilizza la procedura seguente per creare un VPC con una sottorete pubblica e una sottorete privata in due zone di disponibilità e un gateway NAT in ciascuna zona di disponibilità.

Per creare il VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di controllo, scegli Crea VPC.
3. Per Resources to create (Risorse da creare), scegli VPC and more (VPC e altro).
4. Configurazione del VPC
   a. Per Name tag auto-generation (Generazione automatica di tag nome), immetti un nome per il VPC.
   b. Per Blocco CIDR IPv4, mantieni il suggerimento predefinito o, in alternativa, inserisci il blocco CIDR richiesto dall'applicazione o dalla rete.
   c. Se l'applicazione comunica utilizzando indirizzi IPv6, scegli Blocco CIDR IPv6, Blocco CIDR IPv6 fornito da Amazon.
5. Configurazione delle sottoreti
   a. Per Numero di zone di disponibilità, scegli 2, in modo da poter avviare le istanze in più zone di disponibilità per migliorare la resilienza.
   b. Per Number of public subnets (Numero di sottoreti pubbliche), scegli 2.
   c. Per Number of private subnets (Numero di sottoreti private), scegli 2.
   d. Puoi mantenere il blocco CIDR predefinito per la sottorete pubblica o, in alternativa, espandere Personalizza blocchi CIDR della sottorete e inserire un blocco CIDR. Per ulteriori informazioni, consulta the section called “Blocchi CIDR di sottorete”.

6. Per Gateway NAT, scegli 1 per AZ per migliorare la resilienza.
7. Se l'applicazione comunica utilizzando indirizzi IPv6, per Gateway Internet egress-only, scegli Sì.
8. Per Endpoint VPC, se le istanze devono accedere a un bucket S3, mantieni il Gateway S3 predefinito. Altrimenti, le istanze nella tua sottorete privata non possono accedere ad Amazon S3. Questa opzione è gratuita, quindi puoi mantenere l'impostazione predefinita se in futuro prevedi di utilizzare un bucket S3. Se scegli Nessuno, puoi sempre aggiungere un endpoint VPC gateway in un secondo momento.
9. Per Opzioni DNS, deseleziona Abilita i nomi host DNS.
10. Seleziona Create VPC (Crea VPC).

## Distribuzione dell'applicazione

Idealmente, hai finito di testare i tuoi server in un ambiente di sviluppo o test e creato gli script o le immagini che utilizzerai per implementare l'applicazione in produzione.

Puoi utilizzare Dimensionamento automatico Amazon EC2 per distribuire server in più zone di disponibilità e mantenere la capacità minima del server richiesta dalla tua applicazione.

Avvio di istanze utilizzando un gruppo con scalabilità automatica

1. Crea un modello di avvio per specificare le informazioni di configurazione necessarie per avviare le istanze EC2 utilizzando Dimensionamento automatico Amazon EC2. Per ulteriori informazioni, consulta la pagina Creazione di un modello di avvio per un gruppo con scalabilità automatica nella Guida per l'utente di Dimensionamento automatico Amazon EC2.
2. Crea un gruppo con scalabilità automatica, ossia una raccolta di istanze EC2 con una dimensione minima, massima e desiderata. Per istruzioni dettagliate, consulta la pagina Creazione di un gruppo con scalabilità automatica utilizzando un modello di avvio nella Guida per l'utente di Dimensionamento automatico Amazon EC2.
3. Crea un sistema di bilanciamento del carico, che distribuisce il traffico in modo uniforme nel gruppo con scalabilità automatica, e collega il sistema di bilanciamento del carico al gruppo con scalabilità automatica. Per ulteriori informazioni, consulta la Guida per l'utente di Elastic Load Balancing e Utilizzo di Elastic Load Balancing nella Guida per l'utente di Dimensionamento automatico Amazon EC2.

## Test della configurazione

Dopo aver completato l'implementazione dell'applicazione, potrai testarla. Se l'applicazione non è in grado di inviare o ricevere il traffico previsto, puoi utilizzare Sistema di analisi della reperibilità per risolvere i problemi. Ad esempio, Sistema di analisi della reperibilità può identificare i problemi di configurazione relativi alle tabelle di instradamento o ai gruppi di sicurezza. Per ulteriori informazioni, consulta la Guida di Reachability Analyzer.

## Elimina

Quando la configurazione non è più necessaria, è possibile eliminarla. Prima di poter eliminare il VPC, è necessario eliminare il gruppo con scalabilità automatica, terminare le istanze, eliminare i gateway NAT ed eliminare il sistema di bilanciamento del carico. Per ulteriori informazioni, consulta the section called “Eliminazione del VPC”.

# Quote Amazon VPC

Le tabelle seguenti elencano le quote, precedentemente denominate limiti, per le risorse Amazon VPC per il tuo account. AWS Salvo diversa indicazione, le quote sono calcolate per regione.

Se richiedi di aumentare una quota applicabile per risorsa, viene aumentata la quota per tutte le risorse nella regione.

## VPC e sottoreti

| Nome | Predefinita | Adattabile | Commenti |
|---|---|---|---|
| VPC per regione | 5 | Sì | L'aumento di questa quota comporta di pari passo l'aumento della quota relativa agli Internet gateway per Regione.<br><br>Puoi aumentare questo limite in modo da avere centinaia di VPC per ogni regione. |
| Sottoreti per VPC | 200 | Sì | |
| Blocchi CIDR IPv4 per VPC | 5 | Sì<br><br>(fino a 50) | Questo blocco CIDR principale e tutti i blocchi CIDR secondari vengono conteggiati ai fini di questa quota. |
| Blocchi CIDR IPv6 per VPC | 5 | Sì<br><br>(fino a 50) | Il numero di CIDR che puoi allocare a un singolo VPC. |

## DNS

Ciascuna istanza EC2 può inviare 1024 pacchetti al secondo per interfaccia di rete a Route 53 Resolver (in particolare l'indirizzo .2, come 10.0.0.2, e 169.254.169.253). Questa quota non può essere aumentata. Il numero di query DNS al secondo supportate da Route 53 Resolver varia in

base al tipo di query, alla dimensione della risposta e al protocollo in uso. Per ulteriori informazioni e suggerimenti sulle architetture DNS scalabili, consulta la guida tecnica DNS ibrido AWS con Active Directory.

## Indirizzi IP elastici

| Nome | Predefinita | Adattabile | Commenti |
|---|---|---|---|
| Indirizzi IP elastici per regione | 5 | Sì | Questa quota si applica ai VPC individuali e ai Account AWS VPC condivisi. |
| Indirizzi IP elastici per ogni gateway NAT pubblico | 2 | Sì | Puoi richiedere un aumento della quota fino a 8. |

## Gateway

| Nome | Predefinita | Adattabile | Commenti |
|---|---|---|---|
| Internet gateway egress-only per Regione | 5 | Sì | Per aumentare questa quota, aumenta la quota dei VPC per ogni regione.<br><br>È possibile collegare un solo Internet gateway egress-only alla volta a un VPC. |
| Internet gateway per regione | 5 | Sì | Per aumentare questa quota, aumenta la quota dei VPC per ogni regione.<br><br>È possibile allegare un solo gateway Internet a un VPC alla volta. |
| Gateway NAT per zona di disponibilità | 5 | Sì | I gateway NAT vengono conteggiati ai fini delle quote negli stati `pending`, `active` e `deleting`. |

| Nome | Predefinita | Adattabile | Commenti |
|---|---|---|---|
| Quota di indirizzi IP privati per gateway NAT | 8 | No | |
| Gateway carrier per VPC | 1 | No | |

## Elenchi di prefissi gestiti dal cliente

Sebbene le quote predefinite per gli elenchi di prefissi gestiti dal cliente siano regolabili, non è possibile richiedere un aumento utilizzando la console Service Quotas. È necessario aprire un caso di aumento del limite di servizio utilizzando il AWS Support Center Console.

| Nome | Predefinita | Adattabile | Commenti |
|---|---|---|---|
| Elenchi di prefissi per regione | 100 | Sì | |
| Versioni per elenco di prefissi | 1.000 | Sì | Se un elenco di prefissi dispone di 1.000 versioni archiviate e si aggiunge una nuova versione, la versione meno recente viene eliminata per poter aggiungere la nuova versione. |
| Numero massimo di voci per elenco di prefissi | 1.000 | Sì | È possibile ridimensionare un elenco di prefissi gestito dal cliente fino a 1.000. Per ulteriori informazioni, consulta Ridimensionamento di un elenco di prefissi. Quando fai riferimento a un elenco di prefissi in una risorsa, il numero massimo di voci per gli elenchi di prefissi viene conteggiato rispetto alla quota del numero di voci per la risorsa. Ad esempio, se crei un elenco di prefissi con 20 voci e fai riferimento a tale elenco in |

| Nome | Predefinita | Adattabile | Commenti |
| --- | --- | --- | --- |
| | | | una regola di gruppo di sicurezza, questo valore viene conteggiato come 20 regole per il gruppo di sicurezza. |
| Riferimenti a un elenco di prefissi per tipo di risorsa | 5.000 | Sì | Questa quota viene applicata per tipo di risorsa che può fare riferimento a un elenco di prefissi. Ad esempio, è possibile avere 5.000 riferimenti a un elenco di prefissi in tutti i gruppi di sicurezza più 5.000 riferimenti a un elenco di prefissi in tutte le tabelle di routing di sottorete. Se condividi un elenco di prefissi con altri AWS account, i riferimenti degli altri account al tuo elenco di prefissi vengono conteggiati ai fini di questa quota. |

## Liste di controllo accessi (ACL) di rete

| Nome | Predefinita | Adattabile | Commenti |
| --- | --- | --- | --- |
| Liste di controllo degli accessi di rete per VPC | 200 | Sì | È possibile associare una sola lista di controllo degli accessi di rete a una o più sottoreti in un VPC. |
| Regole per lista di controllo degli accessi di rete | 20 | Sì | Questa quota determina sia il numero massimo di regole in entrata che il numero massimo di regole in uscita. Tale quota può essere incrementata fino a un massimo di 40 regole in entrata e 40 regole in uscita (per un totale di |

| Nome | Predefinita | Adattabile | Commenti |
| --- | --- | --- | --- |
| | | | 80 regole), ma le prestazioni della rete potrebbero risentirne. |

## Interfacce di rete

| Nome | Predefinita | Adattabile | Commenti |
| --- | --- | --- | --- |
| Interfacce di rete per istanza | Varia per tipo di istanza | No | Per ulteriori informazioni, consulta Interfacce di rete per tipo di istanza. |
| Interfacce di rete per Regione | 5.000 | Sì | Questa quota si applica ai VPC individuali e ai Account AWS VPC condivisi. Questo limite viene applicato per zona di disponibilità (AZ). Se, ad esempio, le interfacce di rete si trovano in tre AZ, ogni AZ avrà un limite di 5.000 e la regione avrà un limite di 15.000. |

## Tabelle di instradamento

| Nome | Predefinita | Adattabile | Commenti |
| --- | --- | --- | --- |
| Tabelle di routing per VPC | 200 | Sì | La tabella di instradamento principale viene conteggiata ai fini di questa quota. Tieni presente che se chiedi un aumento di quota per le tabelle di instradamento, puoi chiedere un aumento di quota anche per le sottoreti. Mentre le tabelle di instradamento possono essere condivise |

| Nome | Predefinita | Adattabile | Commenti |
| --- | --- | --- | --- |
| | | | con più sottoreti, una sottorete può essere associata solo a una singola tabella di instradamento. |
| Route per tabella di instradamento (route non propagate) | 50 | Sì | È possibile aumentare questa quota fino a un massimo di 1.000, ma potrebbero esserci ripercussioni sulle prestazioni di rete. Questa quota è applicata separatamente per le route IPv4 e IPv6.<br><br>Se hai più di 125 route, è consigliabile eseguire la paginazione delle chiamate per descrivere le tabelle di routing per migliorare le prestazioni. |
| Route propagate per tabella di routing | 100 | No | Se sono necessari prefissi aggiuntivi, annunciare un routing di default. |

## Gruppi di sicurezza

| Nome | Predefinita | Adattabile | Commenti |
| --- | --- | --- | --- |
| Gruppi di sicurezza VPC per Regione | 2.500 | Sì | Questa quota si applica ai VPC individuali e ai Account AWS VPC condivisi.<br><br>Se si aumenta questa quota a più di 5.000 gruppi di sicurezza in una Regione, è consigliabile eseguire l'impaginazione delle chiamate per descrivere i gruppi di sicurezza per migliorare le prestazioni. |
| Regole in entrata o in uscita per gruppo di sicurezza | 60 | Sì | Questa quota viene applicata separatamente per le regole in entrata e in uscita. |

| Nome | Predefinita | Adattabile | Commenti |
|---|---|---|---|
| | | | Pertanto, per un account con una quota predefinita di 60 regole, un gruppo di sicurezza può avere 60 regole in entrata e 60 regole in uscita. Questa quota, inoltre, viene applicata separatamente per le regole IPv4 e le regole IPv6. Pertanto, per un account con una quota predefinita di 60 regole, un gruppo di sicurezza può avere 60 regole in entrata per il traffico IPv4 e 60 regole in entrata per il traffico IPv6. Per ulteriori informazioni, consulta the section called “Dimensioni dei gruppi di sicurezza”.<br><br>La modifica della quota si applica alle regole in entrata e in uscita. Questa quota moltiplicata per la quota dei gruppi di sicurezza per interfaccia di rete non può essere superiore a 1.000. |
| Gruppi di sicurezza per interfaccia di rete | 5 | Sì<br><br>(fino a 16) | Questa quota moltiplicata per la quota di regole per gruppo di sicurezza non può essere superiore a 1.000. |

## Condivisione VPC

Ai VPC condivisi vengono applicate tutte le quote VPC standard.

| Nome | Predefinita | Adattabile | Commenti |
|---|---|---|---|
| Account partecipanti per VPC | 100 | Sì | Il numero massimo di account partecipanti distinti con cui è possibile condivide |

| Nome | Predefinita | Adattabile | Commenti |
| --- | --- | --- | --- |
| | | | re le sottoreti in un VPC. Si tratta di una quota VPC e si applica a tutte le sottoreti condivise in un VPC.<br><br>I proprietari di VPC possono visualizzare le interfacce di rete e i gruppi di sicurezza collegati alle risorse partecipanti. |
| Sottoreti che è possibile condividere con un account | 100 | Sì | Questo è il numero massimo di sottoreti che possono essere condivise con un account. AWS |

## Network Address Usage (NAU)

Network Address Usage (NAU) comprende indirizzi IP, interfacce di rete e CIDR negli elenchi di prefissi gestiti. NAU è un parametro applicato alle risorse in un VPC che consentono di pianificare e monitorare le dimensioni del tuo VPC. Per ulteriori informazioni, consulta Network Address Usage (NAU).

Le risorse che costituiscono il numero NAU hanno le proprie quote di servizio individuali. Anche se un VPC ha una capacità NAU disponibile, non sarà possibile avviare risorse nel VPC se le risorse hanno superato le relative quote di servizio.

| Nome | Predefinita | Adattabile | Commenti |
| --- | --- | --- | --- |
| Network Address Usage (NAU) | 64.000 | Yes (Sì) (fino a 256.000) | Il numero massimo di unità NAU per ogni VPC. |
| Network Address Usage con peering | 128.000 | Yes (Sì) (fino a 512.000) | Il numero massimo di unità NAU per un VPC e tutti i relativi VPC in peering intra-regionali. I VPC con peering in regioni |

| Nome | Predefinita | Adattabile | Commenti |
| --- | --- | --- | --- |
| | | | differenti non contribuiscono a questo numero. |

## Limitazione API Amazon EC2

Per informazioni sulla limitazione di Amazon EC2, consulta Limitazione delle richieste API nella Guida di riferimento dell'API Amazon EC2.

## Risorse aggiuntive delle quote

Per ulteriori informazioni, consulta gli argomenti seguenti:

- AWS Client VPN quote nella Guida per l'amministratore AWS Client VPN
- Quote di AWS Direct Connect nella guida per l'utente AWS Direct Connect
- Quote di peering nella Guida Amazon per il peering VPC
- PrivateLink quote nella Guida AWS PrivateLink
- Quote Site-to-Site VPN nella guida per l'utente AWS Site-to-Site VPN
- Quote di mirroring del traffico nella Guida per il mirroring del traffico Amazon VPC
- Quote del gateway di transito nella Guida per il gateway di transito di Amazon VPC

# Cronologia dei documenti

La tabella seguente descrive le modifiche importanti apportate a ogni versione della Guida per l'utente di Amazon VPC.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| Tempo di leasing preferito per IPv6 | Ora puoi scegliere la frequenza con cui un'istanza in esecuzione a cui è assegnato un IPv6 deve passare attraverso il rinnovo del lease DHCPv6. | 20 febbraio 2024 |
| AWS aggiornamento della politica gestita | Amazon VPC ha aggiornato AmazonVPCFullAccess e AmazonVPCReadOnlyAccess gestito le policy. | 8 febbraio 2024 |
| AWS aggiornamento della politica gestita | Amazon VPC ha aggiornato la policy AmazonVPCCrossAccountNetworkInterfaceOperations gestita. | 25 settembre 2023 |
| EC2-Classic è obsoleto | Con EC2-Classic, le istanze vengono eseguite in una singola rete semplice condivisa con altri clienti. Amazon VPC sostituisce EC2-Classic. Con Amazon VPC, le istanze vengono eseguite in un cloud privato virtuale (VPC) isolato a livello logico dall' Account AWS. | 31 luglio 2023 |
| Come aggiungere indirizzi IPv4 secondari a gateway NAT | Puoi aggiungere indirizzi IPv4 privati secondari a | 31 gennaio 2023 |

| | | |
|---|---|---|
| | gateway NAT pubblici e privati. Gli indirizzi IPv4 secondari incrementano il numero di porte disponibili e, di conseguenza, la quantità massima di connessioni simultanee che i carichi di lavoro possono stabilire utilizzando un gateway NAT. | |
| Allineamento alle best practice IAM | Guida aggiornata per allinearsi alle best practice IAM. Per ulteriori informazioni, consulta la sezione Best practice per la sicurezza in IAM | 4 gennaio 2023 |
| Scelta dell'indirizzo IP privato del gateway NAT | Quando crei un gateway NAT, ora puoi decidere di scegliere l'indirizzo IP privato assegnato al gateway NAT. In precedenza, l'indirizzo IP privato veniva assegnato automaticamente dall'intervallo di indirizzi IP della sottorete. | 17 novembre 2022 |
| Configurazione predefinita del router gateway IPv6 | Tre indirizzi IPv6 sono ora riservati all'uso da parte del router VPC predefinito. | 11 novembre 2022 |
| Trasferimento degli indirizzi IP elastici | Ora puoi trasferire indirizzi IP elastici da un AWS account all'altro. | 31 ottobre 2022 |
| Parametri di Network Address Usage | È possibile abilitare i parametri di Network Address Usage per il VPC per pianificare e monitorare le dimensioni del VPC. | 4 ottobre 2022 |

| | | |
|---|---|---|
| Pubblicazione dei log di flusso su Amazon Data Firehose | Puoi specificare un flusso di distribuzione di Amazon Data Firehose come destinazione per i dati del log di flusso. | 8 settembre 2022 |
| Larghezza di banda del gateway NAT | I gateway NAT ora supportano una larghezza di banda fino a 100 Gbps (con un aumento da 45 Gbps) e possono elaborare fino a dieci milioni di pacchetti al secondo (da quattro milioni di pacchetti). | 15 giugno 2022 |
| Più blocchi CIDR IPv6 | Puoi associare un massimo di cinque blocchi CIDR IPv6 a un VPC. | 12 maggio 2022 |
| Riorganizzazione | Riorganizzazione generale di questa Guida per l'utente di Amazon Virtual Private Cloud. | 2 gennaio 2022 |
| Gateway NAT da IPv6 a IPv4 | Il gateway NAT supporta la traduzione degli indirizzi di rete da IPv6 a IPv4, comunemente nota come NAT64. | 24 novembre 2021 |
| Sottoreti solo IPv6 nei VPC | È possibile creare sottoreti solo IPv6 in cui è possibile avviare istanze EC2 solo IPv6. | 23 novembre 2021 |
| Opzioni di consegna VPC Flow Logs ad Amazon S3 | È possibile specificare il formato del file di log di Apache Parquet, le partizioni orarie e i prefissi S3 compatibili con Hive. | 13 ottobre 2021 |

| | | |
|---|---|---|
| Amazon EC2 Global View | Amazon EC2 Global View consente di visualizzare VPC, sottoreti, istanze, gruppi di sicurezza e volumi in più AWS regioni in un'unica console. | 1 settembre 2021 |
| Route più specifiche | È possibile aggiungere alle tabelle di routing una route che sia più specifica della route locale. È possibile utilizzare route più specifich e per reindirizzare il traffico tra sottoreti all'interno di un VPC (traffico Est-Ovest) a un'appliance middlebox. La destinazione della route può essere impostata in modo da corrispondere all'intero blocco CIDR IPv4 o IPv6 di una sottorete nel VPC. | 30 agosto 2021 |
| ID risorse e supporto di assegnazione di tag per le regole dei gruppi di sicurezza | Puoi fare riferimento alle regole del gruppo di sicurezza in base all'ID risorsa. Puoi aggiungere i tag anche alle regole di un gruppo di sicurezza. | 7 luglio 2021 |
| Gateway NAT privati | Puoi utilizzare un gateway NAT privato per la comunicaz ione privata in uscita tra VPC o tra un VPC e la rete On-Premise. | 10 giugno 2021 |

| | | |
|---|---|---|
| Tag alla creazione | È possibile aggiungere tag quando si crea un VPC, opzioni DHCP, gateway Internet, gateway egress-on ly, ACL di rete e gruppo di sicurezza. | 30 giugno 2020 |
| Elenchi di prefissi gestiti | È possibile creare e gestire un set di blocchi CIDR nell'elenco dei prefissi. | 29 giugno 2020 |
| Miglioramenti ai log di flusso | Sono disponibili nuovi campi per i log di flusso ed è possibile specificare un formato personalizzato per i log di flusso che vengono pubblicati su Logs. CloudWatc h | 4 maggio 2020 |
| Supporto del tagging per i log di flusso | È possibile aggiungere tag ai log di flusso. | 16 marzo 2020 |
| Tag sulla creazione del gateway NAT | È possibile aggiungere un tag quando crei un gateway NAT. | 9 marzo 2020 |
| Intervallo di aggregazione massimo per log di flusso | Puoi specificare il periodo di tempo massimo durante il quale un flusso viene acquisito e aggregato in un record di log di flusso. | 4 febbraio 2020 |
| Configurazione del gruppo di confine di rete | È possibile configurare i gruppi di confine di rete per i VPC dalla Amazon Virtual Private Cloud Console. | 22 gennaio 2020 |

| | | |
|---|---|---|
| Nome DNS privato | Puoi accedere ai servizi AWS PrivateLink basati in modo privato dall'interno del tuo VPC utilizzando nomi DNS privati. | 6 gennaio 2020 |
| Tabelle di routing del gateway | È possibile associare una tabella di routing a un gateway e instradare il traffico VPC in ingresso a un'interfaccia di rete specifica nel VPC. | 3 dicembre 2019 |
| Miglioramenti ai log di flusso | Puoi specificare un formato personalizzato per il log di flusso e scegliere quali campi restituire nei record del log di flusso. | 11 settembre 2019 |
| Condivisione VPC | È possibile condividere sottoreti che si trovano nello stesso VPC con più account nella stessa organizzazione. AWS | 27 novembre 2018 |
| Creazione di una sottorete predefinita | Puoi creare una sottorete predefinita in una zona di disponibilità senza sottoreti. | 9 Novembre 2017 |
| Supporto del tagging per gateway NAT | È possibile contrassegnare con dei tag il gateway NAT. | 7 settembre 2017 |
| CloudWatch Parametri Amazon per i gateway NAT | Puoi visualizzare i CloudWatch parametri per il tuo gateway NAT. | 7 settembre 2017 |
| Descrizione della regola di gruppo di sicurezza | È possibile aggiungere descrizioni alle regole di un gruppo di sicurezza. | 31 agosto 2017 |

| | | |
|---|---|---|
| Blocchi CIDR IPv4 secondari per il VPC | Puoi aggiungere molteplici blocchi CIDR IPv4 al tuo VPC. | 29 agosto 2017 |
| Ripristino degli indirizzi IP elastici | Se rilasci un indirizzo IP elastico, dovresti riuscire a ripristinarlo. | 11 agosto 2017 |
| Creazione di un VPC predefinito | Puoi creare un nuovo VPC predefinito se Elimini quello esistente. | 27 luglio 2017 |
| Supporto IPv6 | Puoi associare un blocco CIDR IPv6 al VPC e assegnare indirizzi IPv6 alle risorse nel VPC. | 1 dicembre 2016 |
| Supporto per la risoluzione DNS per intervalli di indirizzi IP non RFC 1918 | Il server Amazon DNS può ora risolvere nomi host DNS privati in indirizzi IP privati per tutti gli spazi di indirizzi. | 24 ottobre 2016 |
| Gateway NAT | Puoi creare un gateway NAT in una sottorete pubblica e consentire alle istanze in una sottorete privata di avviare il traffico in uscita verso Internet o altri servizi AWS . | 17 dicembre 2015 |
| Log di flusso VPC | Puoi creare un log di flusso per acquisire informazioni sul traffico IP da e per l'interfaccia di rete nel VPC. | 10 giugno 2015 |

| | | |
|---|---|---|
| ClassicLink | Puoi utilizzarla ClassicLink per collegare la tua istanza EC2-Classic a un VPC nel tuo account. È possibile associare i gruppi di sicurezza VPC all'istanza EC2-Classic e consentire la comunicazione tra l'istanza EC2-Classic e le istanze del VPC tramite indirizzi IP privati. | 7 gennaio 2015 |
| Utilizzo di zone ospitate private | Puoi accedere a risorse nel VPC utilizzando nomi di dominio DNS personalizzati che definisci in una zona ospitata privata di Route 53. | 5 Novembre 2014 |
| Modifica dell'attributo di indirizzamento IP pubblico di una sottorete | Puoi modificare l'attributo di indirizzamento IP pubblico della sottorete per indicare se le istanze avviate in quella sottorete devono ricevere un indirizzo IP pubblico. | 21 giugno 2014 |
| Assegnazione di un indirizzo IP pubblico | Puoi assegnare un indirizzo IP pubblico a un'istanza durante l'avvio | 20 agosto 2013 |
| Abilitazione di nomi host DNS e disabilitazione della risoluzione DNS | Puoi modificare le impostazioni predefinite VPC e disabilitare la risoluzione DNS e abilitare i nomi host DNS. | 11 marzo 2013 |

| | | |
|---|---|---|
| VPC Everywhere | È stato aggiunto il supporto per VPC in cinque AWS regioni, VPC in più zone di disponibilità, più VPC per AWS account e più connessioni VPN per VPC. | 3 agosto 2011 |
| Istanze dedicate | Le istanze dedicate sono istanze di Amazon EC2 avviate nel VPC ed eseguite in hardware dedicato a un unico cliente. | 27 marzo 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.