aws

Guida per l'utente

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: Guida per l'utente

Table of Contents

Cos'è Amazon VPC? 1
Funzionalità 1
Nozioni di base su Amazon VPC 2
Uso di Amazon VPC 3
Prezzi per Amazon VPC 3
Come funziona Amazon VPC 6
VPC e sottoreti 7
VPC predefiniti e non predefiniti 7
Tabelle di routing 8
Accesso a Internet 8
Accesso a una rete domestica o aziendale 9
Connessione di VPC e reti 9
Rete globale privata AWS 10
Pianificazione del VPC 11
Iscriviti a un Account AWS 11
Verificare le autorizzazioni 12
Determina gli intervalli di indirizzi IP 12
Seleziona le tue zone di disponibilità 12
Pianifica la tua connettività Internet 13
Creazione di un VPC 13
Distribuzione dell'applicazione 14
Assegnazione di indirizzi IP 15
Indirizzi privati IPv4 16
Indirizzi pubblici IPv4 16
IPv6 indirizzi 18
Indirizzi pubblici IPv6 19
Indirizzi privati IPv6 19
Utilizzo dei propri indirizzi IP 21
Utilizzo di Gestione indirizzi IP di Amazon VPC 21
Blocchi CIDR del VPC 21
IPv4 Blocchi CIDR VPC 22
Gestisci i blocchi IPv4 CIDR per un VPC 23
IPv4 Restrizioni di associazione a blocchi CIDR 25
IPv6 Blocchi CIDR VPC 27

Blocchi CIDR di sottorete ... 28
Dimensionamento delle sottoreti per IPv4 ... 29
Dimensionamento della sottorete per IPv6 ... 29
Confronta IPv4 e IPv6 ... 30
Elenchi di prefissi gestiti ... 32
Concetti e regole degli elenchi di prefissi ... 33
Identity and access management per gli elenchi di prefissi ... 34
Elenchi di prefissi gestiti dal cliente ... 35
AWS Elenchi di prefissi gestiti da ... 45
Ottimizza la gestione AWS dell'infrastruttura con elenchi di prefissi ... 47
AWS Intervalli di indirizzi IP ... 50
Scarica ... 50
Controllo delle uscite ... 51
Feed di geolocalizzazione ... 51
Ricerca degli intervalli di indirizzi ... 51
Sintassi ... 58
Sottoscrizione alle notifiche di ... 63
IPv6 supporto per il tuo VPC ... 65
Aggiungi IPv6 il supporto per il tuo VPC ... 66
Esempio di VPC dual-stack ... 70
IPv6 supporto su AWS ... 72
Servizi che supportano IPv6 ... 72
Supporto aggiuntivo IPv6 ... 78
Ulteriori informazioni ... 79
Cloud privati virtuali ... 80
Nozioni di base sui VPC ... 81
Intervallo di indirizzi IP VPC ... 81
Diagramma di un VPC ... 81
Risorse VPC ... 82
Opzioni di configurazione del VPC ... 83
Predefinito VPCs ... 85
Componenti VPC predefiniti ... 85
Sottoreti predefinite ... 88
Utilizzo del VPC e delle sottoreti predefinite ... 89
Crea un VPC ... 93
Creazione di un VPC e di altre risorse VPC ... 93

Creare solo un VPC ... 95
Crea un VPC utilizzando il AWS CLI ... 97
Come visualizzare le risorse nel VPC ... 102
Aggiungere o rimuovere un blocco CIDR ... 104
Set di opzioni DHCP ... 106
Che cos'è il DHCP? ... 107
Concetti relativi ai set di opzioni DHCP ... 108
Utilizzo dei set di opzioni DHCP ... 111
Attributi DNS ... 116
Informazioni su Amazon DNS ... 116
Visualizza i nomi host DNS per la tua istanza EC2 ... 121
Visualizzazione e aggiornamento degli attributi DNS per il VPC ... 122
Utilizzo degli indirizzi di rete ... 123
Come viene calcolato il NAU ... 124
Esempi NAU ... 125
Condivisione di una sottorete VPC ... 126
Prerequisiti della sottorete condivisa ... 127
Lavorare con le sottoreti condivise ... 127
Fatturazione e misurazione per il proprietario e i partecipanti ... 130
Responsabilità e autorizzazioni per proprietari e partecipanti ... 131
AWS risorse e sottoreti VPC condivise ... 134
Come estendere un VPC ad altre zone ... 136
Sottoreti nelle AWS Local Zones ... 136
Sottoreti in AWS Wavelength ... 141
Sottoreti in AWS Outposts ... 145
Eliminazione del VPC ... 146
Eliminazione tramite la console ... 147
Eliminazione utilizzando la CLI ... 148
Generare IaC dalle azioni della console ... 149
Sottoreti ... 151
Nozioni di base sulla sottorete ... 151
Intervallo di indirizzi IP di sottorete ... 151
Tipi di sottorete ... 152
Diagramma sottorete ... 152
Routing della sottorete ... 153
Impostazioni sottorete ... 153

Sicurezza della sottorete ... 154
Creazione di una sottorete ... 154
Aggiungere o rimuovere un blocco IPv6 CIDR dalla sottorete ... 156
Modifica dell'attributo di assegnazione di indirizzi IP della sottorete ... 157
Prenotazioni della CIDR per la sottorete ... 158
Come lavorare con le prenotazioni del CIDR della sottorete tramite la console ... 159
Lavora con le prenotazioni CIDR di sottorete utilizzando il AWS CLI ... 160
Tabelle di instradamento ... 161
Concetti relativi alla tabella di instradamento ... 162
Tabelle di routing di sottoreti ... 163
Tabelle di routing del gateway ... 170
Priorità della route ... 173
Opzioni di routing di esempio ... 175
Modificare la tabella di routing di una sottorete ... 190
Sostituzione della tabella di instradamento principale ... 197
Controlla il traffico che entra nel tuo VPC con una tabella di routing del gateway ... 198
Sostituzione o ripristino della destinazione per una route locale ... 199
Risoluzione dei problemi di raggiungibilità ... 200
Procedura guidata di instradamento middlebox ... 200
Prerequisiti della procedura guidata per il routing middlebox ... 201
Reindirizzare il traffico VPC verso un'appliance di sicurezza ... 201
Considerazioni sulla procedura guidata di routing middlebox ... 203
Scenari middlebox ... 204
Eliminare una sottorete ... 214
Connettere il proprio VPC ... 216
Gateway Internet ... 217
Configurazione per l'accesso a Internet ... 218
Aggiunta di un accesso Internet a una sottorete ... 221
Internet Gateway egress-only ... 224
Nozioni di base sull'Internet Gateway egress-only ... 224
Aggiunta di un accesso Internet egress-only a una sottorete ... 225
Dispositivi NAT ... 228
Gateway NAT ... 230
Istanze NAT ... 277
Confronto dei dispositivi NAT ... 289
Indirizzi IP elastici ... 292

Concetti e regole degli indirizzi IP elastici ... 293
Iniziare a utilizzare gli indirizzi IP elastici ... 295
AWS Transit Gateway ... 304
AWS Virtual Private Network ... 305
Connessioni in peering di VPC ... 307
Monitoraggio ... 308
Log di flusso VPC ... 309
Nozioni di base sui log di flusso ... 310
Record di log di flusso ... 313
Esempi di record di log di flusso ... 324
Limitazioni del log di flusso ... 333
Prezzi ... 335
Utilizzo dei log di flusso ... 336
Pubblica nei registri CloudWatch ... 339
Pubblicazione su Amazon S3 ... 347
Pubblicazione in Amazon Data Firehose ... 356
Eseguire una query tramite Athena ... 364
Risoluzione dei problemi ... 368
CloudWatch metriche ... 371
Parametri e dimensioni di NAU ... 372
Abilita o disabilita il monitoraggio del NAU ... 375
Esempio di CloudWatch allarme NAU ... 376
Sicurezza ... 377
Protezione dei dati ... 378
Riservatezza del traffico Internet ... 379
Identity and Access Management ... 379
Destinatari ... 380
Autenticazione con identità ... 380
Gestione degli accessi tramite le policy ... 384
Come funziona Amazon VPC con IAM ... 386
Esempi di policy ... 391
Risoluzione dei problemi ... 403
AWS politiche gestite ... 405
Sicurezza dell'infrastruttura ... 408
Isolamento della rete ... 409
Controllo del traffico di rete ... 409

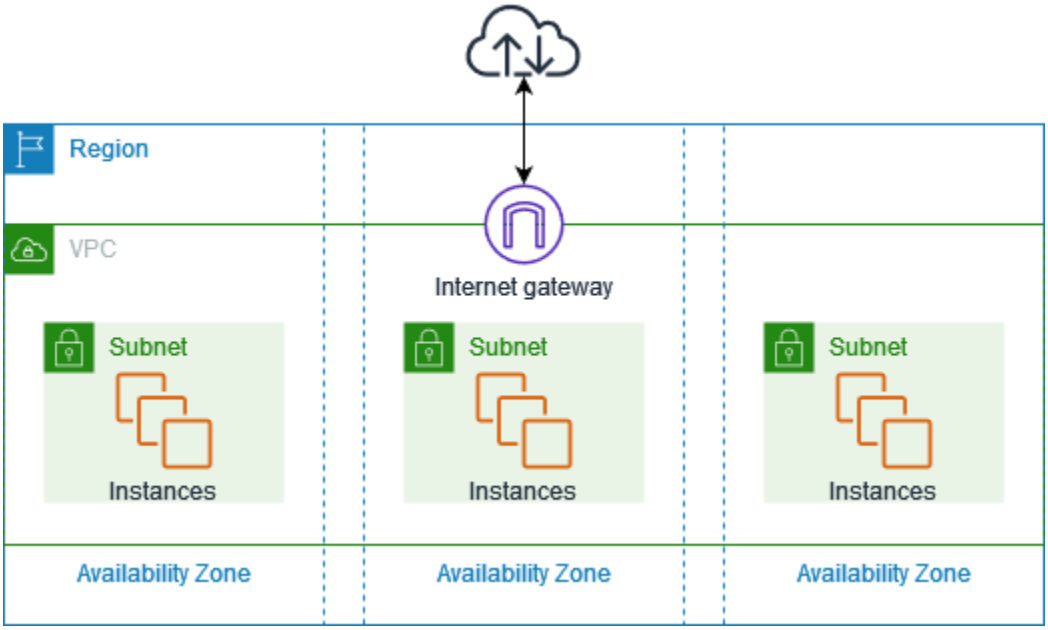
Confronta i gruppi di sicurezza e la rete ACLs 410
Gruppi di sicurezza 412
Nozioni di base sui gruppi di sicurezza 413
Esempio di gruppo di sicurezza 414
Regole del gruppo di sicurezza 415
Gruppi di sicurezza predefiniti 420
Creazione di un gruppo di sicurezza 422
Configurazione delle regole per i gruppi di sicurezza 424
Eliminare un gruppo di sicurezza 426
Associare gruppi di sicurezza a più gruppi di sicurezza VPCs 427
Condividi i gruppi di sicurezza con AWS Organizations 430
Rete ACLs 436
Informazioni di base sulla lista di controllo accessi di rete 437
Regole di liste di controllo accessi di rete 439
lista di controllo accessi di rete predefinita 440
Rete personalizzata ACLs 442
Porte Effimere 450
Rilevamento della MTU del percorso 451
Lavora con la rete ACLs 452
Esempio: controllo dell'accesso alle istanze in una sottorete 458
Risoluzione dei problemi di raggiungibilità 462
Resilienza 462
Convalida della conformità 463
Blocca l'accesso pubblico alle sottoreti VPCs e alle sottoreti 464
Nozioni di base su BPA 465
Valutazione dell'impatto di BPA e monitoraggio di BPA 471
Esempio avanzato 476
Best practice 529
Utilizzo con altri servizi 531
AWS PrivateLink 532
AWS Network Firewall 533
DNS Firewall per Route 53 Resolver 535
Reachability Analyzer 536
Esempi 537
Ambiente di test 538
Panoramica 538

1. Creazione del VPC 540
2. Distribuzione dell'applicazione 541
3. Test della configurazione 542
4. Eliminazione 542
Server Web e di database 542
Panoramica 543
1. Creazione del VPC 547
2. Distribuzione dell'applicazione 548
3. Test della configurazione 548
4. Eliminazione 549
Server privati 549
Panoramica 549
1. Creazione del VPC 552
2. Distribuzione dell'applicazione 553
3. Test della configurazione 554
4. Eliminazione 554
Quote 555
VPC e sottoreti 555
DNS 556
Indirizzi IP elastici 556
Gateway 556
Elenchi di prefissi gestiti dal cliente 557
Rete ACLs 559
Interfacce di rete 559
Tabelle di instradamento 560
Gruppi di sicurezza 561
Condivisione della sottorete VPC 562
Utilizzo degli indirizzi di rete 562
Limitazione EC2 delle API Amazon 563
Risorse aggiuntive delle quote 563
Cronologia dei documenti 564
..... dlxxiv

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 ciascuna delle zone di disponibilità della regione, EC2 istanze in ogni sottorete e un gateway Internet per consentire la comunicazione tra le risorse del 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 che, alla tua IPv4 e IPv6 alle sottoreti. VPCs Puoi anche trasferire i tuoi IPv4 indirizzi pubblici e IPv6 GUA AWS e allocarli alle risorse del tuo VPC, EC2 come istanze, 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

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

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 le tue VPCs connessioni VPN e AWS Direct Connect le connessioni.

Log di flusso VPC

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

Connessioni VPN

Connect VPCs le tue reti locali 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 Le impostazioni predefinite VPCs sono configurate in modo da poter iniziare immediatamente l'avvio e la connessione alle EC2 istanze. Per ulteriori informazioni, consulta Pianificazione del VPC.

Puoi scegliere di crearne altre VPCs 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 propri VPCs utilizzando una delle seguenti interfacce:

- AWS Management Console— Fornisce un'interfaccia web che è possibile utilizzare per accedere VPCs a.
- 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 SDKs— Fornisce informazioni specifiche per la lingua APIs 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 AWS SDKs.
- 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 le azioni di Amazon VPC nell'Amazon EC2 API Reference.

Prezzi per Amazon VPC

Non ci sono costi aggiuntivi per l'utilizzo di un VPC. Tuttavia, sono previsti addebiti per alcuni componenti VPC, come gateway NAT, IP Address Manager, mirroring del traffico, Reachability Analyzer e Strumento di analisi degli accessi alla rete. Per ulteriori informazioni, consulta la pagina dei Prezzi di Amazon VPC.

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

Amazon VPC consente di avviare servizi gestiti, come Elastic Load Balancing, Amazon RDS e Amazon EMR, senza dover prima configurare un VPC. Lo fa utilizzando il VPC predefinito nel tuo account, se ne hai uno. Eventuali IPv4 indirizzi pubblici forniti al tuo account dal servizio gestito verranno addebitati. Questi addebiti verranno associati al servizio Amazon VPC del tuo. AWS Cost and Usage Report

Prezzi per gli indirizzi pubblici IPv4

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

Se sei un cliente esistente o nuovo del piano AWS gratuito, riceverai 750 ore di utilizzo degli IPv4 indirizzi pubblici con il EC2 servizio gratuitamente. Se non utilizzi il EC2 servizio nel piano AWS gratuito, IPv4 gli indirizzi pubblici vengono addebitati. Per informazioni specifiche sui prezzi, consulta la scheda IPv4 Indirizzo pubblico nei prezzi di Amazon VPC.

IPv4 Gli indirizzi privati (RFC 1918) non vengono addebitati. Per ulteriori informazioni su come vengono addebitati IPv4 gli indirizzi pubblici per la condivisione VPCs, consulta Fatturazione e contabilizzazione per il proprietario e i partecipanti.

IPv4 Gli indirizzi pubblici hanno i seguenti tipi:

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

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

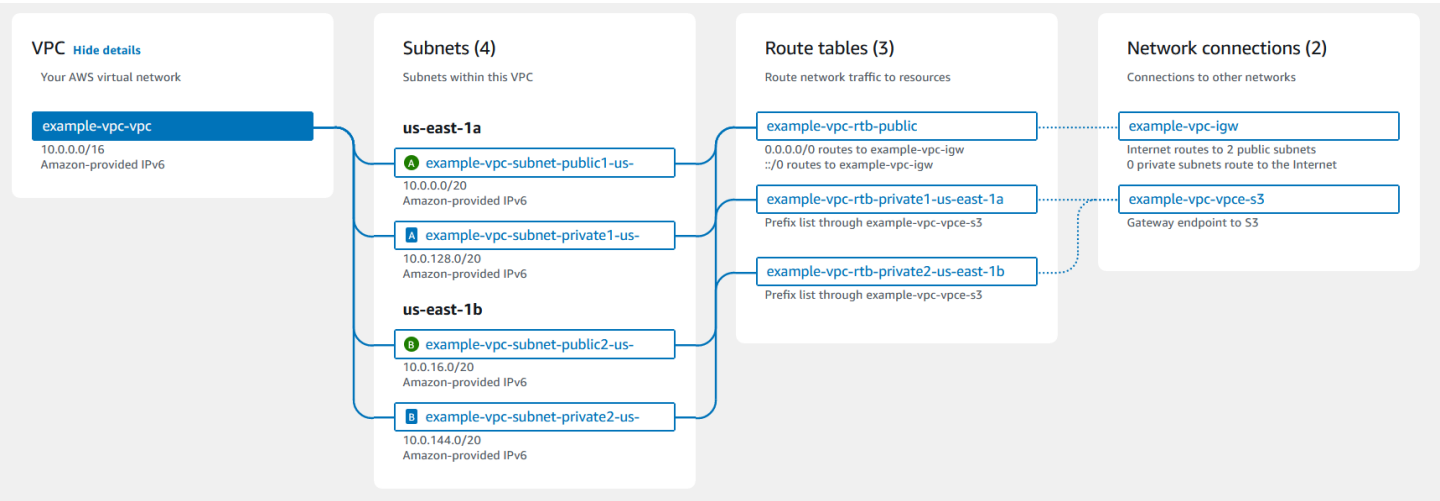
- Amazon AppStream 2.0
- AWS Client VPN
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR

- Amazon GameLift
- AWS Global Accelerator
- Modernizzazione del mainframe AWS
- 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) è possibile avviare risorse AWS in una rete virtuale isolata logicamente da te definita. 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
- Rete globale privata AWS

VPC e sottoreti

Un cloud privato virtuale (VPC) è una rete virtuale dedicata al tuo account AWS. Il VPC è isolato a livello logico dalle altre reti virtuali del 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 “Predefinito VPCs”
- 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

- Abilitazione dell'accesso di VPC a Internet tramite gateway Internet
- Abilita il IPv6 traffico in uscita utilizzando un gateway Internet solo in uscita
- Eseguire la connessione a Internet o ad altri VPC utilizzando dispositivi NAT

Accesso a una rete domestica o aziendale

Facoltativamente, puoi connettere il VPC al tuo data center aziendale utilizzando una connessione AWS Site-to-Site VPN IPsec, che rende il cloud AWS un'estensione del data center.

Una connessione Site-to-Site VPN è costituita da due tunnel VPN tra un dispositivo gateway virtuale privato o gateway di transito sul lato AWS e un dispositivo gateway 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

- Guida per l'utente di AWS Site-to-Site VPN
- 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 relativi allegati, che possono includere VPC, connessioni VPN, gateway AWS Direct Connect e connessioni peering del gateway di transito.

Ulteriori informazioni

- Amazon VPC Peering Guide
- Amazon VPC Transit Gateway

Rete globale privata AWS

AWS offre una rete globale privata ad alte prestazioni e a bassa latenza con 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, attraversa la rete globale privata AWS.
- Il traffico tra regioni viaggia sempre sulla rete globale privata AWS, ad eccezione del caso 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 (packet-loss rate, 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%.

Pianificazione del VPC

Completa le seguenti attività per prepararti a creare e connettere il tuo VPCs. Al termine dell'operazione, sari pronto a implementare l'applicazione su AWS.

Attività

- Iscriviti a 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 a 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 https://portal.aws.amazon.com/billing/registrazione.
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 best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo 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 VPCs crei delle sottoreti, puoi selezionare gli intervalli di indirizzi IP corrispondenti. Quando si distribuiscono risorse in una sottorete, ad esempio EC2 le istanze, queste ricevono gli indirizzi IP dall'intervallo di indirizzi IP della sottorete. Per ulteriori informazioni, consulta Assegnazione di indirizzi IP.

Quando scegli una dimensione per il tuo VPC, considera quanti indirizzi IP ti serviranno sul tuo Account AWS territorio. VPCs Assicurati che gli intervalli di indirizzi IP per la tua rete VPCs non si sovrappongano agli intervalli di indirizzi IP per la tua rete. Se hai bisogno di connettività tra più VPCs indirizzi IP, devi assicurarti 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 una posizione fisica 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 determinato il numero di sottoreti VPCs e di sottoreti di cui hai bisogno, quali blocchi CIDR assegnare alle tue VPCs e alle sottoreti e come connettere il tuo VPC a Internet, sei pronto per 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.

- Amazon EC2 Auto Scaling
- EC2 Parco istanze
- Amazon Elastic Container Service (Amazon ECS)

Ambiente di sviluppo o test

Per un ambiente di sviluppo o di test, puoi scegliere di avviare una singola EC2 istanza. Per ulteriori informazioni, consulta la sezione Guida introduttiva ad Amazon EC2 nella Amazon EC2 User Guide.

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

Per ulteriori informazioni, consulta Che cos'è CIDR?

Indice

- Indirizzi privati IPv4
- Indirizzi pubblici IPv4
- IPv6 indirizzi
- Utilizzo dei propri indirizzi IP
- Utilizzo di Gestione indirizzi IP di Amazon VPC
- Blocchi CIDR del VPC
- Blocchi CIDR di sottorete
- Confronta IPv4 e IPv6
- Consolidare e gestire i blocchi CIDR di rete con elenchi di prefissi gestiti
- AWS Intervalli di indirizzi IP
- IPv6 supporto per il tuo VPC

- AWS servizi che supportano IPv6

Indirizzi privati IPv4

IPv4 Gli indirizzi privati (denominati anche indirizzi IP privati in questo argomento) non sono raggiungibili su Internet e possono essere utilizzati per la comunicazione tra le istanze del VPC. Quando si avvia un'istanza in un VPC, un indirizzo IP privato primario dall'intervallo di IPv4 indirizzi della sottorete viene assegnato all'interfaccia di rete primaria (ad esempio, eth0) dell'istanza. 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 EC2 Denominazione delle istanze. 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 Indirizzi IP multipli nella Amazon EC2 User Guide.

Ci riferiamo agli indirizzi IP privati come gli indirizzi IP che rientrano nell'intervallo IPv4 CIDR 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 pubblicizziamo mai su Internet l'intervallo di IPv4 indirizzi di una sottorete.

Indirizzi pubblici IPv4

Tutte le sottoreti hanno un attributo che determina se un'interfaccia di rete creata nella sottorete riceve automaticamente un IPv4 indirizzo pubblico (denominato anche indirizzo IP pubblico in questo argomento). Pertanto, quando si avvia un'istanza in una sottorete con questo attributo abilitato, viene

assegnato un indirizzo IP pubblico all'interfaccia di rete principale creata per l'istanza. Un indirizzo IP pubblico è associato all'indirizzo IP privato primario tramite conversione degli indirizzi di rete (network address translation, NAT).

> **Note**
>
> AWS addebiti per tutti gli IPv4 indirizzi pubblici, inclusi gli IPv4 indirizzi pubblici associati alle istanze in esecuzione e gli indirizzi IP elastici. Per ulteriori informazioni, consulta la scheda IPv4 Indirizzo pubblico nella 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 di indirizzi IP della 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 alla tua 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 dall'istanza o gliene assegniamo uno nuovo. Per ulteriori informazioni, consulta Indirizzi IP pubblici nella Amazon EC2 User Guide.

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.

Se utilizzi Amazon VPC IP Address Manager (IPAM), puoi ottenere un blocco contiguo di IPv4 indirizzi pubblici AWS e utilizzarlo per allocare indirizzi IP elastici sequenziali alle risorse. AWS

L'utilizzo di blocchi di IPv4 indirizzi contigui può ridurre in modo significativo il sovraccarico di gestione degli elenchi di controllo degli accessi di sicurezza e semplificare l'allocazione e il tracciamento degli indirizzi IP per le aziende che vogliono crescere. AWS Per ulteriori informazioni, consulta Assegnare indirizzi IP elastici sequenziali da un pool IPAM nella Guida per l'utente di Amazon VPC IPAM.

IPv6 indirizzi

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 offre uno spazio di indirizzi più ampio rispetto a IPv4. IPv6 risolve il problema dell'esaurimento degli IPv4 indirizzi e consente di connettere più dispositivi a Internet. La transizione è graduale, ma man mano che IPv6 l'adozione cresce, è possibile semplificare le reti e sfruttare le funzionalità IPv6 avanzate per migliorare la connettività, le prestazioni e la sicurezza.

Molti AWS servizi, come Amazon EC2, Amazon S3 e Amazon, offrono supporto dual-stack (IPv4 e IPv6) o IPv6 solo CloudFront, consentendo l'assegnazione di IPv6 indirizzi e l'accesso alle risorse tramite il IPv6 protocollo e semplificando la configurazione e la gestione della rete per i clienti che lo adottano. IPv6 Altri servizi offrono supporto dual-stack e solo -only limitato o parziale. IPv6 Per ulteriori informazioni sui servizi che supportano, consulta. IPv6 AWS servizi che supportano IPv6

Si noti che alcuni IPv6 indirizzi sono riservati dall'Internet Engineering Task Force. Per ulteriori informazioni sugli intervalli di IPv6 indirizzi riservati, vedere IANA IPv6 Special-Purpose Address Registry e. RFC4291

> **Note**
>
> L' IPv6 indirizzamento pubblico e privato è disponibile in. AWS AWS considera gli indirizzi IP pubblici quelli da cui vengono pubblicizzati su Internet AWS, mentre gli indirizzi IP privati non lo sono e non possono essere pubblicizzati su Internet da. AWS

Indice

- Indirizzi pubblici IPv6
- Indirizzi privati IPv6

Indirizzi pubblici IPv6

IPv6 Gli indirizzi pubblici sono IPv6 indirizzi che possono essere configurati per rimanere privati o configurati per essere raggiungibili tramite Internet.

Questi sono alcuni dei modi in cui puoi prepararti a utilizzare IPv6 gli indirizzi pubblici per i tuoi carichi di lavoro:

- Crea un IPAM con Amazon VPC IP Address Manager e fornisci un intervallo di indirizzi IPv6 pubblici di proprietà di Amazon a un pool di indirizzi IPAM. Per ulteriori informazioni, consulta Create IPv6 pool nella Amazon VPC IPAM User Guide.
- Se disponi di un IPAM e possiedi un intervallo di IPv6 indirizzi pubblici, trasferisci in tutto o in parte l'intervallo di IPv6 indirizzi pubblici in IPAM e fornisci l'intervallo di IPv6 indirizzi pubblici a un pool di indirizzi IPAM. Per ulteriori informazioni, consulta Tutorial: trasferisci i tuoi indirizzi IP su IPAM nella Guida per l'utente IPAM di Amazon VPC.
- Se non disponi di un IPAM ma possiedi un intervallo di IPv6 indirizzi pubblici, trasferisci parte o tutto l'intervallo di indirizzi pubblici IPv6 a. AWS Per ulteriori informazioni, consulta Bring your own IP address (BYOIP) to Amazon EC2 nella Amazon EC2 User Guide.

Una volta che sei pronto a utilizzare IPv6 gli indirizzi pubblici, puoi assegnare IPv6 indirizzi pubblici alle istanze (vedi IPv6 gli indirizzi nella Amazon EC2 User Guide), puoi allocare un blocco IPv6 CIDR pubblico al tuo VPC (vediAggiungere o rimuovere un blocco CIDR dal VPC) e associare il blocco IPv6 CIDR alle tue sottoreti (vedi). Modifica dell'attributo di assegnazione di indirizzi IP della sottorete

Indirizzi privati IPv6

IPv6 Gli indirizzi privati sono IPv6 indirizzi che non vengono pubblicizzati e non possono essere pubblicizzati su Internet da. AWS

Puoi utilizzare un IPv6 indirizzo privato se desideri che le tue reti private supportino IPv6 e non hai intenzione di indirizzare il traffico da questi indirizzi a Internet. Se desideri connetterti a Internet da una risorsa con un IPv6 indirizzo privato, puoi farlo, ma per farlo devi indirizzare il traffico attraverso una risorsa in un'altra sottorete con un IPv6 indirizzo pubblico.

Esistono due tipi di IPv6 indirizzi privati:

- IPv6 Intervalli ULA: IPv6 indirizzi come definiti in RFC4193. Questi intervalli di indirizzi iniziano sempre con "fc" or "fd", il che li rende facilmente identificabili. Lo spazio IPv6 ULA valido è qualsiasi cosa inferiore a fd00: :/8 che non si sovrappone all'intervallo riservato di Amazon fd00: :/16.

- IPv6 Intervalli GUA: indirizzi come definiti in. IPv6 RFC3587 L'opzione per utilizzare gli intervalli IPv6 GUA come IPv6 indirizzi privati è disabilitata per impostazione predefinita e deve essere abilitata prima di poterla utilizzare. Per ulteriori informazioni, consulta Abilita il provisioning IPv6 GUA privato CIDRs nella Guida per l'utente IPAM di Amazon VPC.

Tieni presente quanto segue:

- IPv6 Gli indirizzi privati sono disponibili solo tramite Amazon VPC IP Address Manager (IPAM). IPAM rileva risorse con indirizzi IPv6 ULA e GUA e monitora i pool per individuare la sovrapposizione IPv6 di spazi di indirizzi ULA e GUA.
- Quando utilizzi intervalli IPv6 GUA privati, richiediamo che tu utilizzi intervalli IPv6 GUA di tua proprietà.
- IPv6 Gli indirizzi privati non sono e non possono essere pubblicizzati su Internet da AWS. AWS non consente l'accesso diretto alla rete Internet pubblica da una rete privata anche IPv6 se nel VPC è presente un gateway Internet o un gateway Internet di sola uscita. IPv6Gli indirizzi privati vengono automaticamente eliminati alla periferia del gateway Internet, in modo da non essere indirizzati pubblicamente.
- AWS riserva i primi 4 IPv6 indirizzi privati di sottorete e l'ultimo.
- Gli intervalli validi per l' IPv6 ULA privato sono compresi tra /9 e /60 a partire da fd80: :/9.
- Se disponi di un intervallo IPv6 GUA privato assegnato a un VPC, non puoi utilizzare uno spazio GUA IPv6 pubblico che si sovrappone allo spazio GUA IPv6 privato nello stesso VPC.
- È supportata la comunicazione tra risorse con intervalli di indirizzi IPv6 ULA e GUA privati (ad esempio tramite Direct Connect, peering VPC, gateway di transito o connessioni VPN).
- Puoi utilizzare IPv6 indirizzi privati con sottoreti VPC IPv6 -only e dual-stack, sistemi di bilanciamento del carico elastici ed endpoint.AWS Global Accelerator
- Non è IPv6 previsto alcun costo per gli indirizzi privati.

Questi sono alcuni dei modi in cui puoi prepararti a utilizzare IPv6 gli indirizzi privati per i tuoi carichi di lavoro:

- Crea un IPAM con Amazon VPC IP Address Manager e fornisci un intervallo ULA IPv6 privato a un pool di indirizzi IPAM. Per ulteriori informazioni, consulta Create IPv6 pool nella Amazon VPC IPAM User Guide.
- Crea un IPAM con Amazon VPC IP Address Manager e fornisci un intervallo GUA IPv6 privato a un pool di indirizzi IPAM. L'opzione per utilizzare gli intervalli IPv6 GUA come IPv6 indirizzi privati

è disabilitata per impostazione predefinita e deve essere abilitata sul tuo IPAM prima di poterla utilizzare. Per ulteriori informazioni, consulta Abilita il provisioning IPv6 GUA privato CIDRs nella Guida per l'utente IPAM di Amazon VPC.

Una volta che sei pronto a utilizzare IPv6 gli indirizzi privati, puoi allocare un blocco IPv6 CIDR privato da un pool IPAM al tuo VPC (vediAggiungere o rimuovere un blocco CIDR dal VPC) e associare il blocco IPv6 CIDR alle tue sottoreti (vedi). Modifica dell'attributo di assegnazione di indirizzi IP della sottorete

Utilizzo dei propri indirizzi IP

Puoi aggiungere una parte o la totalità del tuo intervallo di IPv4 indirizzi pubblici o del tuo intervallo di indirizzi al tuo account. IPv6 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. Puoi creare un indirizzo IP elastico dal tuo pool di IPv4 indirizzi e associare un blocco IPv6 CIDR dal tuo pool di IPv6 indirizzi 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 Puoi utilizzare IPAM per assegnare l'indirizzo CIDRs IP all'utilizzo di regole aziendali specifiche. VPCs

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 IPv4 CIDR associato. Facoltativamente, puoi associare blocchi IPv4 CIDR aggiuntivi e uno o più blocchi CIDR. IPv6 Per ulteriori informazioni, consulta Indirizzamento IP per le tue VPCs sottoreti.

Indice

- IPv4 Blocchi CIDR VPC

- Gestisci i blocchi IPv4 CIDR per un VPC
- IPv4 Restrizioni di associazione a blocchi CIDR
- IPv6 Blocchi CIDR VPC

IPv4 Blocchi CIDR VPC

Quando si crea un VPC, è necessario specificare un blocco IPv4 CIDR 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 tuo VPC, puoi associare blocchi IPv4 CIDR aggiuntivi al VPC. Per ulteriori informazioni, consulta Aggiungere o rimuovere un blocco CIDR dal VPC.

Quando crei un VPC, ti consigliamo di specificare un blocco CIDR dagli intervalli di IPv4 indirizzi privati come specificato nella 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
192.168.0.0 - 192.168.255.255 (prefisso 192.168/16)	192.168.0.0/20

> **Important**
>
> Alcuni AWS servizi utilizzano gli intervalli e CIDR`172.17.0.0/16`. `172.16.0.0/12` I servizi possono riscontrare conflitti di indirizzi IP se gli intervalli di indirizzi IP sono già in uso in qualsiasi punto della rete. Ad esempio, AWS Cloud9 e l'utilizzo di Amazon SageMaker AI `172.17.0.0/16` e Amazon RDS. `172.16.0.0/12` Per evitare conflitti, non utilizzare questi intervalli durante la creazione del VPC. Per ulteriori informazioni, consulta Impossibile connettersi all' EC2 ambiente perché gli indirizzi IP di VPC vengono utilizzati da Docker nella Guida per l'AWS Cloud9 utente.

È possibile creare un VPC con un blocco CIDR instradabile pubblicamente che non rientra negli intervalli di IPv4 indirizzi privati specificati nella RFC 1918. Tuttavia, ai fini di questa documentazione,

ci riferiamo agli indirizzi IP privati come gli IPv4 indirizzi che rientrano nell'intervallo CIDR del tuo VPC.

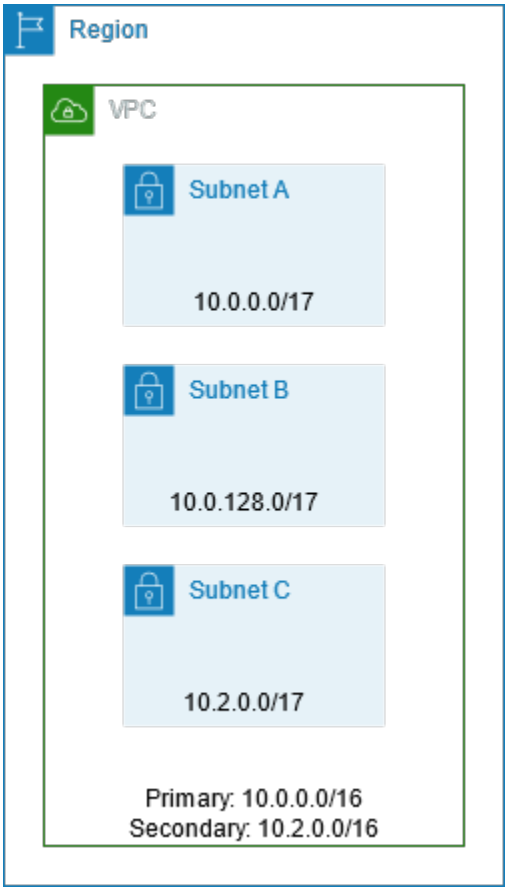
Quando crei un VPC da utilizzare con un AWS servizio, consulta la documentazione del servizio per verificare se esistono requisiti specifici per la sua configurazione.

Se crei un VPC utilizzando uno strumento da riga di comando o l' EC2 API Amazon, il blocco CIDR viene automaticamente modificato nella sua forma canonica. 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.

Gestisci i blocchi IPv4 CIDR per un VPC

Puoi associare blocchi IPv4 CIDR secondari al tuo 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 restrizioni sugli intervalli di IPv4 indirizzi che è possibile utilizzare. Per ulteriori informazioni, consulta IPv4 Restrizioni di associazione a blocchi CIDR.
- 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 IPv4 CIDR 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 AWS Direct Connect per connetterti a più utenti VPCs tramite un gateway Direct Connect, VPCs i blocchi CIDR associati al gateway Direct Connect non devono avere blocchi CIDR sovrapposti. Se aggiungi un blocco CIDR a uno dei blocchi associati al VPCs gateway Direct Connect, assicurati che il nuovo blocco CIDR non si sovrapponga a un blocco CIDR esistente di nessun 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 tuo VPC nella console Amazon VPC, scegli VPCs Your, seleziona la casella di controllo relativa al tuo VPC e scegli la scheda. CIDRs 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
```

IPv4 Restrizioni di associazione a blocchi CIDR

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). Se uno qualsiasi dei blocchi CIDR associati al VPC è compreso nell'intervallo 10.0.0.0/15 (da 10.0.0.0 a 10.1.255.255), non potrai aggiungere un blocco CIDR dall'intervallo 10.0.0.0/16 (da 10.0.0.0 a 10.0.255.255). Blocchi CIDR dall'intervallo 198.19.0.0/16.	Qualsiasi altro blocco CIDR dall'intervallo 10.0.0.0/8 tra una netmask /16 e una netmask /28 che non è soggetto a limitazioni. Qualsiasi blocco IPv4 CIDR indirizzabile pubblicamente (non RFC 1918) compreso 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.
169.254.0.0/16	I blocchi CIDR del blocco «link local» sono riservati come descritto nella RFC 5735 e non possono essere assegnati a. VPCs	
172.16.0.0/12	Blocchi CIDR da altri intervalli RFC 1918* (10.0.0.0/8 e 192.168.0.0/16). Blocchi CIDR dall'intervallo 172.31.0.0/16. Blocchi CIDR dall'intervallo 198.19.0.0/16.	Qualsiasi altro blocco CIDR dall'intervallo 172.16.0.0/12 tra una netmask /16 e una netmask /28 che non è soggetto a limitazioni. Qualsiasi blocco IPv4 CIDR 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.
192.168.0.0/16	Blocchi CIDR da altri intervalli RFC 1918* (10.0.0.0/8 e 172.16.0.0/12).	Qualsiasi altro blocco CIDR dall'intervallo 192.168.0.0/16 tra una netmask /16 e una netmask /28.

Intervallo di indirizzo IP	Associazioni limitate	Associazioni consentite
	Blocchi CIDR dall'intervallo 198.19.0.0/16.	Qualsiasi blocco IPv4 CIDR 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 IPv4 CIDR 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.
Blocco CIDR indirizzabile pubblicamente (non RFC 1918) o un blocco CIDR dall'intervallo 100.64.0.0/10	Blocchi CIDR dagli intervalli RFC 1918*. Blocchi CIDR dall'intervallo 198.19.0.0/16.	Qualsiasi altro blocco IPv4 CIDR 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. Puoi anche associare un CIDR in uno degli intervalli RFC 1918, ma per farlo devi prima aggiungere quel CIDR quando crei il VPC e poi aggiungere il CIDR non RFC 1918.

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

IPv6 Blocchi CIDR VPC

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

Se hai associato un blocco IPv6 CIDR al tuo VPC, puoi associare IPv6 un blocco CIDR a una sottorete esistente nel tuo VPC o quando crei una nuova sottorete. Per ulteriori informazioni, consulta the section called “Dimensionamento della sottorete per IPv6”.

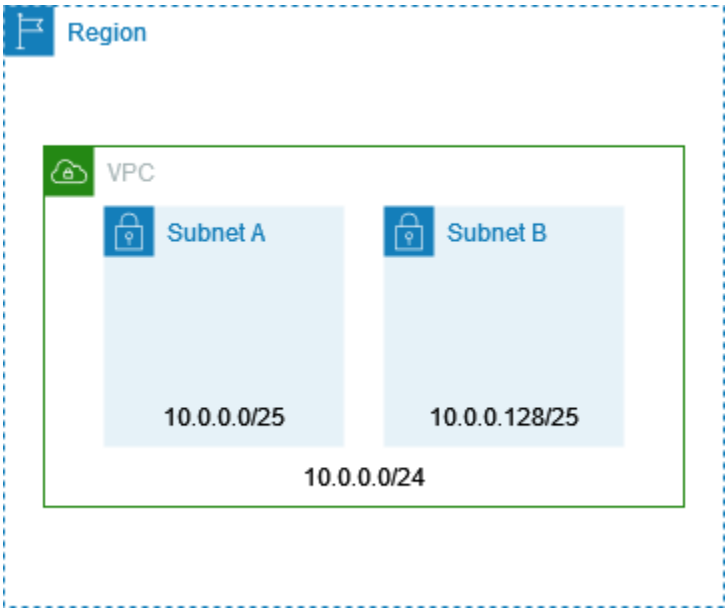
Ad esempio, crei un VPC e specifichi che desideri associare un IPv6 blocco CIDR fornito da Amazon al VPC. Amazon assegna il seguente blocco IPv6 CIDR al tuo VPC:. `2001:db8:1234:1a00::/56` Non puoi scegliere autonomamente l'intervallo di indirizzi IP. Puoi creare una sottorete e associare un blocco IPv6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

È possibile dissociare un blocco IPv6 CIDR da un VPC. Dopo aver dissociato un blocco IPv6 CIDR da un VPC, non puoi aspettarti di ricevere lo stesso CIDR se associ nuovamente un blocco CIDR al tuo VPC in un IPv6 secondo momento.

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 strumenti che consentono di calcolare e creare IPv4 blocchi CIDR e suddividere in IPv6 sottoreti. Puoi trovare strumenti che soddisfano le tue esigenze cercando termini come "calcolatore di sottoreti" o "calcolatore CIDR". Il vostro gruppo di tecnici di rete può anche aiutarvi a determinare i IPv4 blocchi IPv6 CIDR da specificare per le vostre sottoreti.

Dimensionamento delle sottoreti per IPv4

La dimensione del blocco IPv4 CIDR consentita per una sottorete è compresa tra una maschera di rete e una `/28` maschera di rete. `/16` I primi quattro indirizzi IP e l'ultimo indirizzo IP in ogni blocco CIDR di sottorete non sono disponibili per l'uso e non possono essere assegnati a una risorsa, ad esempio 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 VPCs i blocchi CIDR multipli, l'indirizzo IP del server DNS si trova nel CIDR primario. 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 crei una sottorete utilizzando uno strumento da riga di comando o l' EC2 API Amazon, il blocco CIDR viene automaticamente modificato nella sua forma canonica. 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 AWS utilizzi BYOIP per un intervallo di IPv4 indirizzi, puoi utilizzare tutti gli indirizzi IP dell'intervallo, incluso il primo indirizzo (l'indirizzo di rete) e l'ultimo indirizzo (l'indirizzo di trasmissione).

Dimensionamento della sottorete per IPv6

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

Su Internet sono disponibili strumenti che consentono di calcolare e creare blocchi CIDR di IPv6 sottorete. Puoi trovare strumenti adatti alle tue esigenze cercando termini come «calcolatore di IPv6 sottorete» o «calcolatore CIDR». IPv6 Il vostro gruppo di ingegneria di rete può anche aiutarvi a determinare i blocchi IPv6 CIDR da specificare per le vostre sottoreti.

I primi quattro IPv6 indirizzi e l'ultimo IPv6 indirizzo in ogni blocco CIDR di sottorete non sono disponibili per l'uso 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 IPv6 indirizzi sono riservati al router VPC predefinito:

- Un IPv6 indirizzo locale del collegamento nell'intervallo FE8 0: :/10 generato utilizzando EUI-64. Per ulteriori informazioni sugli indirizzi locali del collegamento, consulta Indirizzo locale del collegamento.
- L' IPv6 indirizzo `FE80:ec2::1` locale del collegamento.

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.

Confronta IPv4 e IPv6

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

Caratteristica	IPv4	IPv6
Dimensione VPC	Fino a 5 da /16 a /28. CIDRs Questa quota è modificabile.	Fino a 5 CIDRs 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	Puoi scegliere il blocco IPv4 CIDR per il tuo VPC o 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 IPv6 CIDR AWS per 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'istanz a un indirizzo pubblico statico e permanente. EC2 IPv4	Non supportato. EIPs mantiene l' IPv4 indirizzo pubblico di un'istanza statico al riavvio dell'istanza. IPv6 gli indirizzi sono statici per impostazione predefinita.
Gateway NAT	Supportato. Le istanze in sottoreti private possono connettersi a Internet utilizzando un gateway NAT pubblico o a risorse in altre sottoreti VPCs utilizzando un gateway NAT privato.	Supportato. È possibile utilizzare un gateway NAT NAT64 per consentir e alle istanze in sottoreti IPv6 -only di comunicare con risorse IPv4 -only all'interno VPCs, tra VPCs, nelle reti locali o su Internet.

Caratteristica	IPv4	IPv6
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.

Consolidare e gestire i blocchi CIDR di rete con 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

- Concetti e regole degli elenchi di prefissi
- Identity and access management per gli elenchi di prefissi
- Elenchi di prefissi gestiti dal cliente
- AWS Elenchi di prefissi gestiti da

- Ottimizza la gestione AWS dell'infrastruttura con elenchi di prefissi

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 tipo di indirizzamento IP (IPv4 o). IPv6 Non è possibile combinare IPv4 blocchi IPv6 CIDR 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 Priorità di route per gli elenchi di prefissi.
- 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 GovCloud (incluse le regioni degli Stati Uniti e della 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 di azioni Amazon VPC e le risorse e le chiavi di condizione che puoi utilizzare in una policy IAM, consulta Azioni, risorse e chiavi di condizione per Amazon EC2 nel Service Authorization Reference.

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.

Elenchi di prefissi gestiti dal cliente

Gli elenchi di prefissi gestiti dal cliente consentono di definire e gestire set personalizzati di intervalli di indirizzi IP, noti come prefissi, all'interno di AWS. Invece di codificare questi indirizzi IP nelle varie risorse, puoi creare un elenco di prefissi centralizzato e farvi riferimento laddove necessario. Ciò non solo semplifica la gestione degli indirizzi IP, ma promuove anche la coerenza e la riutilizzabilità in tutto il panorama. AWS

Una delle caratteristiche principali degli elenchi di prefissi gestiti dai clienti è la possibilità di condividerli con altri account. AWS Concedendo l'accesso agli elenchi di prefissi, è possibile consentire ad altri team od organizzazioni di sfruttare gli intervalli di indirizzi IP definiti nelle proprie risorse. Questo approccio collaborativo favorisce un'esperienza cloud più coesa ed efficiente, in cui la gestione degli indirizzi IP è condivisa e sincronizzata.

Nelle sezioni che seguono, approfondiremo gli aspetti pratici dell'utilizzo degli elenchi di prefissi gestiti dai clienti, incluse le step-by-step indicazioni sulla creazione, la gestione e la condivisione degli intervalli di indirizzi IP.

Attività

- Utilizzo degli elenchi di prefissi gestiti dal cliente

Utilizzo degli elenchi di prefissi gestiti dal cliente

In questa sezione viene descritto come lavorare con elenchi di prefissi gestiti dal cliente.

Indice

- 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
- Condividere gli elenchi di prefissi gestiti dal cliente

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. Apri la 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, scegli se l'elenco di prefissi supporta o più voci. IPv4 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. Apri la 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. Apri la 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 IDs le risorse associate all'elenco dei prefissi e i relativi proprietari. 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 a un elenco di prefissi AWS-managed.

Per visualizzare le associazioni degli elenchi di prefissi utilizzando la console

1. Apri la 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. Apri la 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. Apri la 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. Apri la 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. Apri la 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.

Condividere gli elenchi di prefissi gestiti dal cliente

Con AWS Resource Access Manager (AWS RAM), il proprietario di un elenco di prefissi gestito dal cliente può condividere l'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. Per ulteriori informazioni sulle quote, vedere Quote di servizio nella Guida per l' AWS RAM utente.

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

Indice

- Autorizzazioni dell'elenco di prefissi condivisi
- Utilizzo di elenchi di prefissi condivisi

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 le AWS risorse che fanno riferimento all'elenco IDs 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.

Utilizzo di elenchi di prefissi condivisi

AWS Gli elenchi di prefissi forniscono un modo pratico per gestire e fare riferimento agli intervalli di indirizzi IP utilizzati da vari servizi. AWS Oltre agli elenchi di prefissi AWS gestiti, puoi anche creare e condividere i tuoi elenchi di prefissi gestiti dal cliente con altri account. AWS

La condivisione degli elenchi di prefissi può essere particolarmente utile per le organizzazioni con requisiti di rete complessi o per quelle che devono coordinare l'utilizzo degli indirizzi IP su più carichi

di lavoro. AWS Condividendo un elenco di prefissi, puoi garantire una gestione coerente degli indirizzi IP e semplificare le configurazioni di rete per i tuoi collaboratori.

Questa sezione descrive come condividere gli elenchi di prefissi e come identificare e utilizzare gli elenchi di prefissi condivisi con il tuo account.

Indice

- Condivisione di un elenco di prefissi
- Annullamento della condivisione di un elenco di prefissi condiviso
- Identificazione di un elenco di prefissi condiviso
- Identificazione dei riferimenti a un elenco di prefissi condiviso

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 in AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso all'elenco di prefissi condiviso. 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.

Important

- 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 AWS di prefissi gestito.
- 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 .

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

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.

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. Apri la 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 il 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. Apri la 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. Le risorse che fanno riferimento all'elenco IDs dei prefissi sono elencate nella colonna Resource ID. 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.

AWS Elenchi di prefissi gestiti da

AWS Gli elenchi di prefissi -managed sono insiemi di intervalli di indirizzi IP per i servizi. AWS Questi elenchi di prefissi sono gestiti da Amazon Web Services e forniscono un modo per fare riferimento agli indirizzi IP utilizzati da varie AWS offerte. Ciò può essere particolarmente utile quando si configurano gruppi di sicurezza o altri controlli a livello di rete all'interno di un VPC.

Gli elenchi di prefissi coprono un'ampia gamma di AWS servizi, tra cui S3 e DynamoDB e molti altri. Utilizzando gli elenchi di prefissi gestiti, puoi assicurarti che le tue configurazioni di rete siano corrette up-to-date e tengano conto correttamente degli indirizzi IP utilizzati dai servizi da cui dipendi. AWS Questo può contribuire a semplificare le attività di rete e ridurre il sovraccarico amministrativo legato alla gestione manuale degli elenchi di indirizzi IP.

Oltre ai vantaggi pratici, l'utilizzo degli elenchi di prefissi gestiti è conforme AWS anche alle migliori pratiche di sicurezza. Affidandoti alle informazioni autorevoli sull'indirizzo IP fornite da AWS, puoi ridurre al minimo il rischio di errori di configurazione o problemi di connettività imprevisti. Ciò può essere particolarmente importante per applicazioni o carichi di lavoro mission-critical con requisiti di conformità rigorosi.

Indice

- Elenchi di prefissi gestiti disponibili AWS
- Peso dell'elenco dei prefissi gestiti da AWS
- Usa un elenco di AWS prefissi -managed

Elenchi di prefissi gestiti disponibili AWS

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*.dinamodb	1
Amazon EC2 Instance Connect	com.amazonaws. *region*.ec2-instance-connect	2

Servizio AWS	Nome elenco dei prefissi	Weight
	com.amazonaws. *region*.ipv6.ec2-instance-connect	2
AWS Ground Station	com.amazonaws.global.groundstation	5
Amazon Route 53	com.amazonaws. *region*.ipv6.route53 - controlli sanitari	25
	com.amazonaws. *region*.route 53 - controlli sanitari	25
Amazon S3	com.amazonaws. *region*.s3	1
Amazon S3 Express One Zone	com.amazonaws. *region*.s3 express	6
Amazon VPC Lattice	com.amazonaws. *region*.vpc-reticolo	10
	com.amazonaws. *region*.ipv6.vpc-reticolo	10

Per visualizzare gli elenchi di prefissi -managed utilizzando la console AWS

1. Apri la 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
```

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.

Usa un elenco di AWS prefissi -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 Ottimizza la gestione AWS dell'infrastruttura con elenchi di prefissi.

Ottimizza la gestione AWS dell'infrastruttura con elenchi di prefissi

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

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.

> **Important**
>
> Non è possibile modificare una regola esistente per utilizzare una lista di prefissi. È necessario creare una nuova regola per utilizzare un elenco di prefissi.

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

1. Apri la 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), scegli Personalizza. Quindi, nel campo successivo, in Elenchi prefissi, scegli l'ID dell'elenco dei prefissi.
6. Scegliere Salva regole.

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

Utilizza i comandi authorize-security-group-ingress e authorize-security-group-egress. 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 instradamento utilizzando la console

1. Apri la 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 instradamento.
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. Scegli Save changes (Salva modifiche).

Per fare riferimento a un elenco di prefissi in una tabella di routing utilizzando il 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 CIDRs prefissi 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 Gestione dei routing nella relativa tabella del gateway locale nella Guida per l'utente per i rack AWS Outposts .

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. AWS Puoi anche utilizzare queste informazioni per concedere o negare il traffico da o verso alcuni servizi Servizi AWS.

Considerazioni

- Pubblichiamo gli intervalli di indirizzi IP per i servizi che i clienti utilizzano comunemente per eseguire il filtraggio in uscita. Non pubblichiamo gli intervalli di indirizzi IP per tutti i servizi.
- I servizi utilizzano i relativi intervalli di indirizzi IP per comunicare con altri servizi o con una rete di clienti.
- Gli intervalli di indirizzi IP trasferiti AWS tramite Bring your own IP address (BYOIP) non sono inclusi nel `.json` file. Per ulteriori informazioni, consulta Pubblicizza il tuo intervallo di indirizzi AWS nella Amazon EC2 User Guide.

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

Indice

- Download del file JSON
- Controllo delle uscite
- Feed di geolocalizzazione
- Trova gli intervalli di indirizzi IP per Servizi AWS
- Sintassi per l'intervallo di indirizzi AWS IP JSON
- AWS Notifiche degli intervalli di indirizzi IP

Download del file JSON

Per visualizzare gli intervalli di indirizzi correnti, scarica ip-ranges.json. Per mantenere la cronologia, salva le versioni successive del file JSON nel tuo computer. 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.

Di seguito è riportato un comando curl di esempio che salva il file JSON nella directory corrente.

```
curl -O https://ip-ranges.amazonaws.com/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.

Per ricevere notifiche di aggiornamenti al file JSON, consulta the section called “Sottoscrizione alle notifiche di ”.

Controllo delle uscite

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 sullo spazio degli indirizzi IP e lo utilizzano. EC2 EC2 Se blocchi il traffico verso lo spazio degli indirizzi EC2 IP, blocchi anche il traffico verso questi non EC2 servizi.

Feed di geolocalizzazione

Gli intervalli di indirizzi IP `ip-ranges.json` inclusi sono di Regione AWS. Tuttavia, una zona locale non si trova nella stessa posizione fisica della Regione principale. I dati di geolocalizzazione pubblicati negli account geo-ip-feed.csv per Local Zones. I dati seguono la norma RFC 8805.

Trova gli intervalli di indirizzi IP per Servizi AWS

Il file JSON con intervallo di indirizzi AWS IP fornito da AWS può essere una risorsa preziosa per trovare gli indirizzi IP di vari AWS servizi e sfruttare tali informazioni per migliorare la sicurezza della rete e il controllo degli accessi. Analizzando i dati dettagliati contenuti in questo file JSON, è possibile identificare con precisione gli intervalli di indirizzi IP associati a Regioni e Servizi AWS specifici.

Ad esempio, è possibile utilizzare gli intervalli di indirizzi IP al fine di configurare solide policy di sicurezza di rete e impostare regole firewall granulari per consentire o negare l'accesso a determinate

risorse AWS . Queste informazioni possono essere utili anche per una serie di AWS Network Firewall attività. Questo livello di controllo è fondamentale per proteggere le applicazioni e i dati, garantendo che solo il traffico autorizzato possa raggiungere i Servizi AWS necessari. Inoltre, disporre di questa intelligenza IP può aiutarvi a garantire che le applicazioni siano configurate correttamente per comunicare con gli AWS endpoint giusti, migliorando l'affidabilità e le prestazioni complessive.

Oltre alle semplici regole del firewall, il file `ip-ranges.json` può essere utilizzato anche per configurare sofisticati filtri in uscita sull'infrastruttura di rete. Comprendendo i diversi intervalli di indirizzi IP di destinazione Servizi AWS, è possibile impostare politiche di routing o sfruttare soluzioni di sicurezza di rete avanzate, ad esempio autorizzare o bloccare selettivamente il traffico in uscita in base alla destinazione prevista. Questo controllo delle uscite è essenziale per mitigare il rischio di perdita di dati e accesso non autorizzato.

È importante notare che il `ip-ranges.json` file viene aggiornato regolarmente, quindi mantenere una copia up-to-date locale è fondamentale per garantire le informazioni più accurate e aggiornate. Sfruttando continuamente il contenuto di questo file, è possibile gestire in modo efficiente l'accesso alla rete e la sicurezza per le applicazioni AWS basate, rafforzando la posizione generale di sicurezza del cloud.

Gli esempi seguenti possono aiutarti a filtrare gli intervalli di indirizzi AWS IP in base a ciò che stai cercando. Su Linux, puoi scaricare e utilizzare lo strumento jq per analizzare una copia locale del file JSON. AWS Tools for Windows PowerShellInclude un cmdlet, Get- AWSPublic IpAddressRange, che è possibile utilizzare per analizzare questo file JSON. Per ulteriori informazioni, consulta il seguente blog: Querying the Public IP Address Ranges for AWS.

Per ottenere il file JSON, consulta the section called “Scarica”. Per ulteriori informazioni sulla sintassi del file JSON, consulta the section called “Sintassi”.

Esempi

- Come ottenere la data di creazione
- Come ottenere gli indirizzi IP per una Regione specifica
- Ottieni tutti gli indirizzi IPv4
- Ottieni tutti gli IPv4 indirizzi per un servizio specifico
- Ottieni tutti IPv4 gli indirizzi per un servizio specifico in una regione specifica
- Ottieni tutti gli indirizzi IPv6
- Ottieni tutti gli IPv6 indirizzi per un servizio specifico

- Come ottenere tutti gli indirizzi IP per un gruppo di confine specifico

Come ottenere la data di creazione

Nell'esempio seguente viene recuperata la data di creazione di `ip-ranges.json`.

jq

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

"2024-08-01-17-22-15"
```

PowerShell

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

Thursday, August 1, 2024 9:22:35 PM
```

Come ottenere gli indirizzi IP per una Regione specifica

Nell'esempio seguente viene filtrato il file JSON per ottenere gli indirizzi IP per la Regione specificata.

jq

```
$ 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"
},
...
```

PowerShell

```
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
...
```

Ottieni tutti gli indirizzi IPv4

L'esempio seguente filtra il file JSON per gli IPv4 indirizzi.

jq

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

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

PowerShell

```
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
...
```

Ottieni tutti gli IPv4 indirizzi per un servizio specifico

L'esempio seguente filtra il file JSON per gli IPv4 indirizzi del servizio specificato.

jq

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

13.248.117.0/24
15.197.34.0/23
15.197.36.0/22
...
```

PowerShell

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

IpPrefix
--------
13.248.117.0/24
15.197.34.0/23
15.197.36.0/22
...
```

Ottieni tutti IPv4 gli indirizzi per un servizio specifico in una regione specifica

L'esempio seguente filtra il file JSON per gli IPv4 indirizzi del servizio specificato nella regione specificata.

jq

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

13.248.124.0/24
99.82.166.0/24
99.82.171.0/24
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1 -ServiceKey GLOBALACCELERATOR
 | where {$_.IpAddressFormat -eq "Ipv4"} | select IpPrefix

IpPrefix
--------
13.248.117.0/24
99.82.166.0/24
99.82.171.0/24
...
```

Ottieni tutti gli indirizzi IPv6

L'esempio seguente filtra il file JSON per gli IPv6 indirizzi.

jq

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

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

PowerShell

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

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

Ottieni tutti gli IPv6 indirizzi per un servizio specifico

L'esempio seguente filtra il file JSON per gli IPv6 indirizzi del servizio specificato.

jq

```
$ jq -r '.ipv6_prefixes[] | select(.service=="GLOBALACCELERATOR") | .ipv6_prefix' <
 ip-ranges.json

2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
2600:9000:a800::/40
...
```

PowerShell

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

IpPrefix
--------
2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
2600:9000:a800::/40
...
```

Come ottenere tutti gli indirizzi IP per un gruppo di confine specifico

Nell'esempio seguente viene filtrato il file JSON per ottenere gli indirizzi IP per il gruppo di confine specificato.

jq

```
$ jq -r '.prefixes[] | 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
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.NetworkBorderGroup -eq "us-west-2-
lax-1"} | select IpPrefix

IpPrefix
--------
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

Sintassi per l'intervallo di indirizzi AWS IP JSON

AWS pubblica gli intervalli di indirizzi IP correnti in formato JSON. Per ottenere il file JSON, consulta the section called “Scarica”. La sintassi del file JSON è riportata di seguito.

```
{
  "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 IPv4 indirizzi pubblici, in 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 IPv6 indirizzi pubblici, in 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`GL0BAL`. Il traffico per `GL0BAL` 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` | `ap-southeast-5` | `ap-southeast-7` `ca-central-1` | `ca-west-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` | `il-central-1` | `mx-central-1` | `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 risorse del servizio B, esistono intervalli di indirizzi IP restituiti dai codici di servizio sia per il servizio A che per il servizio B. Tuttavia, questi intervalli di indirizzi IP vengono utilizzati esclusivamente dal servizio A e non possono essere utilizzati dal servizio B. Ad esempio, Amazon S3 utilizza risorse di Amazon EC2, quindi esistono intervalli di indirizzi IP che vengono restituiti sia dai codici di `EC2` servizio che da. `S3` 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, trova gli intervalli di indirizzi IP restituiti dal codice di `EC2` servizio ma non dal codice di `S3` servizio.

Ulteriori informazioni

Questa sezione fornisce i collegamenti alle informazioni aggiuntive per i diversi codici di servizio.

- `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`— IPV4 Indirizzi 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`— PCoserver gateway IP

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
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

Descrizione	Data di rilascio
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
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
È stato aggiunto il supporto per gli intervalli di IPv6 indirizzi.	22 agosto 2016
Rilascio iniziale	19 Novembre 2014

AWS Notifiche degli intervalli di indirizzi IP

AWS pubblica gli intervalli di indirizzi IP correnti in formato JSON. Ogni volta che viene apportata una modifica agli intervalli di indirizzi AWS IP, inviamo notifiche agli abbonati dell'argomento Amazon SNS denominato. `AmazonIpSpaceChanged` Per ulteriori informazioni sulla sintassi del file JSON, consulta the section called “Sintassi”.

Il payload della notifica 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`. Per ulteriori informazioni, consulta the section called "Scarica".

Puoi iscriverti per ricevere notifiche come segue.

Per sottoscrivere le notifiche relative all' AWS intervallo di indirizzi IP

1. Apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/
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 nome della risorsa Amazon (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 nella versione v3/home. https://console.aws.amazon.com/sns/
2. Nel riquadro di navigazione scegliere Subscriptions (Iscrizioni).
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.

IPv6 supporto per il tuo VPC

Se disponi di un VPC esistente che supporta IPv4 solo il VPC e di risorse nella sottorete configurate per l'uso IPv4 esclusivo, puoi aggiungere il IPv6 supporto per il tuo VPC e le tue risorse. Il tuo VPC può funzionare in modalità dual-stack: le tue risorse possono comunicare tramite IPv4 o entrambi. IPv6 IPv4 e le IPv6 comunicazioni sono indipendenti l'una dall'altra.

Non puoi disabilitare il IPv4 supporto per il tuo VPC e le sottoreti; questo è il sistema di indirizzamento IP predefinito per Amazon VPC e Amazon. EC2

Considerazioni

- Non esiste un percorso di migrazione dalle sottoreti -only alle IPv4 sottoreti -only. 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, vedere. the section called “Crea un VPC”
- Prima di iniziare a utilizzare IPv6, assicurati di aver letto le funzionalità di IPv6 indirizzamento per Amazon VPC:. Confronta IPv4 e IPv6

Indice

- Aggiungi IPv6 il supporto per il tuo VPC
- Esempio di configurazione di VPC dual-stack

Aggiungi IPv6 il supporto per il tuo VPC

La tabella seguente fornisce una panoramica del processo da abilitare IPv6 per il tuo VPC.

Indice

- Fase 1: Associare un blocco IPv6 CIDR al VPC e alle sottoreti
- Fase 2: aggiornamento delle tabelle di routing
- Fase 3: aggiornamento delle regole di gruppo di sicurezza
- Passaggio 4: assegna IPv6 gli indirizzi alle istanze

Fase	Note
Fase 1: Associare un blocco IPv6 CIDR al VPC e alle sottoreti	Associa un IPv6 blocco CIDR fornito da Amazon o BYOIP al tuo VPC e alle tue sottoreti .
Fase 2: aggiornamento delle tabelle di routing	Aggiorna le tabelle dei percorsi per indirizza re il traffico. IPv6 Per una sottorete pubblica, create un percorso che indirizzi tutto il IPv6 traffico dalla sottorete al gateway Internet. Per una sottorete privata, create un percorso che indirizzi tutto il IPv6 traffico legato a Internet dalla sottorete a un gateway Internet solo in uscita.

Fase	Note
Fase 3: aggiornamento delle regole di gruppo di sicurezza	Aggiorna le regole del gruppo di sicurezza per includere regole per gli indirizzi. IPv6 Ciò consente al IPv6 traffico di fluire da e verso le tue istanze. Se hai creato regole ACL di rete personalizzate per controllare il flusso di traffico da e verso la sottorete, devi includere regole per il traffico. IPv6
Passaggio 4: assegna IPv6 gli indirizzi alle istanze	Assegna IPv6 indirizzi alle istanze dall'intervallo di IPv6 indirizzi della sottorete.

Fase 1: Associare un blocco IPv6 CIDR al VPC e alle sottoreti

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

Per associare un blocco IPv6 CIDR a un VPC

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Your. VPCs
3. Seleziona il tuo VPC.
4. Scegli Azioni, Modifica CIDRs, quindi scegli Aggiungi nuovo IPv6 CIDR.
5. Seleziona una delle seguenti opzioni, quindi Seleziona CIDR:
   - Blocco IPv6 CIDR fornito da Amazon: utilizza un IPv6 blocco CIDR dal pool di indirizzi di Amazon. IPv6 Per Network Border Group, scegli il gruppo da cui AWS pubblicizza gli indirizzi IP.
   - Blocco CIDR allocato tramite IPAM: utilizza un blocco IPv6 CIDR da un pool IPv6 IPAM. Scegli il pool IPAM e il blocco CIDR. IPv6
   - IPv6 CIDR di mia proprietà: utilizza un blocco IPv6 CIDR dal tuo pool di IPv6 indirizzi (BYOIP). Scegli il pool di IPv6 indirizzi e il blocco CIDR. IPv6
6. Scegli Chiudi.

Per associare un blocco IPv6 CIDR a una sottorete

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

Per ulteriori informazioni, consulta IPv6 Blocchi CIDR VPC.

Fase 2: aggiornamento delle tabelle di routing

Quando associ un blocco IPv6 CIDR al tuo VPC, aggiungiamo automaticamente un percorso locale a ciascuna tabella di routing affinché il VPC consenta il IPv6 traffico 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 il gateway Internet per il traffico. IPv6 È inoltre necessario aggiornare le tabelle di routing per le sottoreti private per consentire alle istanze (come le istanze di database) di utilizzare un gateway Internet di sola uscita per il traffico, poiché i gateway NAT non supportano. IPv6 IPv6

Aggiornare la tabella di routing per una sottorete pubblica

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli 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. Scegli Save changes (Salva modifiche).

Aggiornare la tabella di routing per una sottorete privata

1. Apri la 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 Abilita il IPv6 traffico in uscita utilizzando un gateway Internet solo in uscita.
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. Scegli Save changes (Salva 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 IPv6, è necessario aggiornare le regole del gruppo di sicurezza in modo da includere 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 consentano l'accesso HTTP, HTTPS e SSH in entrata dagli indirizzi. IPv6 Non è necessario apportare modifiche alle regole in entrata per il gruppo di sicurezza del database; la regola che consente tutte le comunicazioni da `sg-11aa22bb11aa22bb1` e verso l'esterno include la comunicazione. IPv6

Aggiornare le regole di gruppo di sicurezza in entrata

1. Apri la 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 IPv4 il traffico, scegli Aggiungi regola e configura la regola per consentire il IPv6 traffico corrispondente. Ad esempio, per aggiungere una regola che consenta l'invio di tutto il traffico HTTP IPv6, scegli 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 associ un blocco IPv6 CIDR al tuo VPC, aggiungiamo automaticamente una regola in uscita ai gruppi di sicurezza per il VPC che consente tutto il traffico. IPv6 Tuttavia, se hai modificato le regole in uscita originali per il tuo gruppo di sicurezza, questa regola non viene aggiunta automaticamente e devi aggiungere regole in uscita equivalenti per il traffico. IPv6

Aggiornamento delle regole di lista di controllo accessi di rete

Quando associ un blocco IPv6 CIDR a un VPC, aggiungiamo automaticamente regole all'ACL di rete predefinito per consentire il traffico. IPv6 Tuttavia, se hai modificato l'ACL di rete predefinito o se hai creato un ACL di rete personalizzato, devi aggiungere manualmente le regole per il traffico. IPv6 Per ulteriori informazioni, consulta Lavora con la rete ACLs.

Passaggio 4: assegna IPv6 gli indirizzi alle istanze

Supporta tutti i tipi di istanze dell'attuale generazione. IPv6 Se il tipo di istanza non lo supporta IPv6, è necessario ridimensionare l'istanza in base a un tipo di istanza supportato prima di poter assegnare un IPv6 indirizzo. 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 Amazon EC2 User Guide. Se devi avviare un'istanza da una nuova AMI da supportare IPv6, puoi assegnare un IPv6 indirizzo all'istanza durante l'avvio.

Dopo aver verificato che il tipo di istanza lo supporti IPv6, puoi assegnare un IPv6 indirizzo all'istanza utilizzando la EC2 console Amazon. L' IPv6 indirizzo viene assegnato all'interfaccia di rete principale (ad esempio, eth0) per l'istanza. Per ulteriori informazioni, consulta Assegnare un IPv6 indirizzo a un'istanza nella Amazon EC2 User Guide.

Puoi connetterti a un'istanza usando il suo IPv6 indirizzo. Per ulteriori informazioni, consulta Connect to your Linux using an SSH client nella Amazon EC2 User Guide.

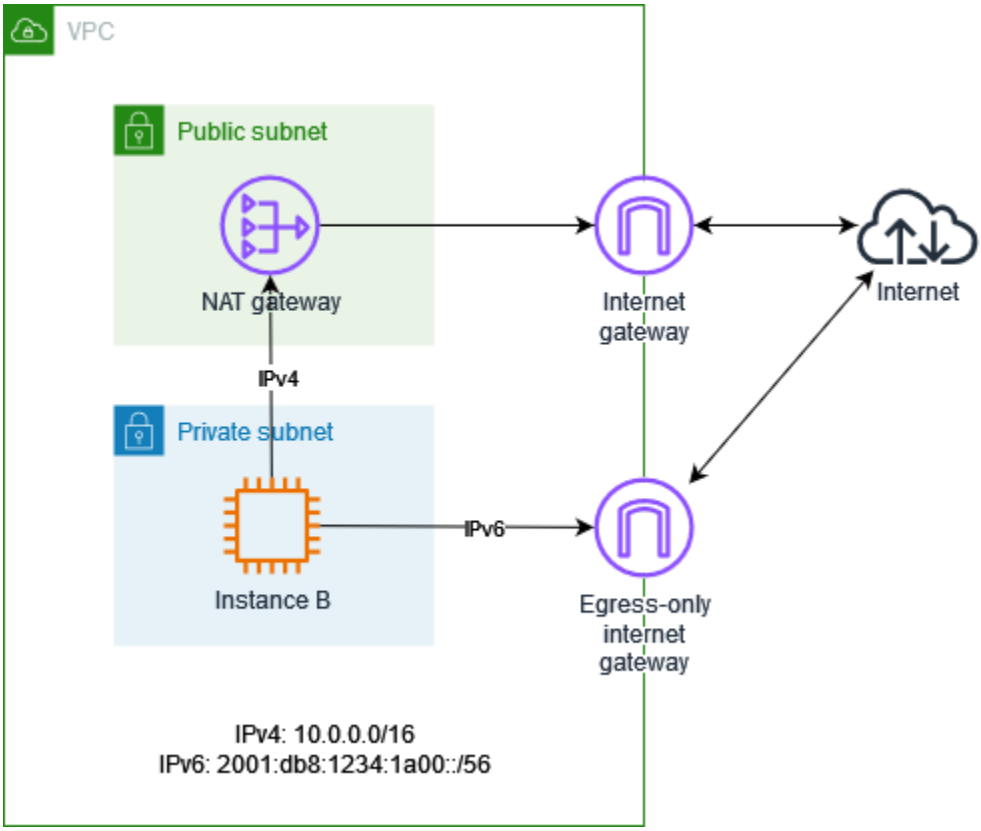
Se hai avviato l'istanza utilizzando un'AMI per una versione corrente del tuo sistema operativo, l'istanza è configurata per IPv6. Se non riesci a eseguire il ping di un IPv6 indirizzo dalla tua istanza, consulta la documentazione del tuo sistema operativo per la configurazione IPv6.

Esempio di configurazione di VPC dual-stack

Con una configurazione dual-stack, puoi utilizzare entrambi IPv4 IPv6 gli indirizzi per la comunicazione tra le risorse del tuo VPC e le risorse su Internet.

Il diagramma seguente rappresenta l'architettura del tuo VPC. Il VPC dispone di una sottorete pubblica e una privata. Il VPC e le sottoreti hanno sia un blocco CIDR che un blocco IPv4 CIDR.

IPv6 Esiste un' EC2 istanza nella sottorete privata che ha sia un indirizzo che un indirizzo. IPv4 IPv6 L'istanza può inviare IPv4 traffico in uscita a Internet utilizzando un gateway NAT e IPv6 traffico in uscita verso Internet utilizzando un gateway Internet solo in uscita.



Di seguito è riportata una tabella di routing per la sottorete pubblica. Le prime due voci riguardano le route locali. La terza voce invia tutto IPv4 il traffico al gateway Internet.

Destinazione	Target
VPC IPv4 CIDR	local
VPC IPv6 CIDR	locale
0.0.0.0/0	*internet-gateway-id*

Di seguito è riportata una tabella di routing per la sottorete privata. Le prime due voci riguardano le route locali. La terza entrata invia tutto il IPv4 traffico al gateway NAT. L'ultima voce invia tutto il IPv6 traffico al gateway Internet di sola uscita.

Destinazione	Target
VPC IPv4 CIDR	local
VPC IPv6 CIDR	locale
0.0.0.0/0	*nat-gateway-id*
::/0	*egress-only-gateway-id*

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 offre 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 IPv6 solo per le configurazioni. 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, puoi creare sottoreti che sono IPv4 solo, 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 lo fanno IPv6 tramite i propri endpoint pubblici. Gli endpoint che lo 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, IPv6 solo il supporto e gli endpoint che lo supportano. IPv6 Aggiorneremo questa tabella non appena verrà rilasciato supporto aggiuntivo per. IPv6 Per informazioni specifiche sul supporto di un servizio IPv6, consulta la documentazione del servizio.

Nome servizio	Supporto dual stack	IPv6 solo supporto	Supporto pubblico per endpoint IPv6	Supporto per endpoint privati 1 IPv6
Amazon API Gateway	No	No	No	Sì
AWS App Mesh	Sì	Sì	Sì	No
AWS Application Discovery Service	Sì	No	Sì	Sì
Amazon AppStream 2.0	Sì	No	No	No
Amazon Athena	Sì	No	Sì	Sì
Amazon Aurora	Sì	No	Sì	No
AWS Backup	Sì	No	Sì	Sì
Amazon Braket	Sì	Sì	Sì	Sì
AWS Cloud9	Sì	No	Sì	
AWS Cloud Control API	Sì	No	Sì	Sì
Amazon CloudFront	Sì	No	No	
AWS CloudHSM	Sì	No	Sì	Sì

Nome servizio	Supporto dual stack	IPv6 solo supporto	Supporto pubblico per endpoint IPv6	Supporto per endpoint privati 1 IPv6
AWS CloudTrail	Sì	No	Sì	Sì
CloudWatch Registri Amazon	Sì	No	Sì	No
AWS Cloud Map	Sì	Sì	Sì	Sì
AWS WAN nel cloud	Sì	No	Sì	No
AWS CodeArtifact	Sì	No	Sì	Sì
Amazon CodeGuru Profiler	Sì	No	Sì	Sì
Centrale ottimizzazione costi AWS	Sì	No	Sì	Sì
AWS Elastic Beanstalk	No	No	Sì	Sì
Amazon Cognito	Sì	No	Sì	
Amazon Data Firehose	No	No	Sì	Sì
AWS Database Migration Service	Sì	No	No	No
AWS Direct Connect	Sì	Sì	No	

Nome servizio	Supporto dual stack	IPv6 solo supporto	Supporto pubblico per endpoint IPv6	Supporto per endpoint privati 1 IPv6
Amazon EBS diretto APIs	Sì	Sì	Sì	Sì
Amazon EC2	Sì	Sì	Sì	No
Amazon ECS	Sì	No	No	No
Amazon EKS	Parziale	Parziale	Sì	Sì
Sistema di bilanciamento del carico elastico	Parziale	Parziale	No	No
Amazon ElastiCache	Sì	Sì	No	No
AWS Messaggistica sociale per utenti finali	Sì	No	Sì	No
AWS Fargate	Sì	No	No	No
Grafana 2 gestita da Amazon	Sì	No	Sì	Sì
AWS Global Accelerator	Sì	No	No	
AWS Glue	Sì	No	No	Sì
AWS IoT	Sì	No	Sì	No

Nome servizio	Supporto dual stack	IPv6 solo supporto	Supporto pubblico per endpoint IPv6	Supporto per endpoint privati 1 IPv6
AWS IoT FleetWise	Sì	No	Sì	Sì
Wireless AWS IoT	Sì	No	Sì	Sì
AWS Lake Formation	No	No	No	Sì
AWS Lambda	Sì	No	Sì	No
Amazon Lightsail	Sì	Sì	Sì	No
Amazon Macie	Sì	No	Sì	Sì
Modernizzazione del mainframe AWS	Sì	No	Sì	Sì
AWS Network Firewall	Sì	Sì	No	No
OpenSearch Servizio Amazon	Sì	No	Sì	No
Amazon Pinpoint	Sì	No	Sì	No
Amazon Polly	Sì	No	Sì	Sì
AWS Private CA Connettore per SCEP	Sì	Sì	Sì	Sì

Nome servizio	Supporto dual stack	IPv6 solo supporto	Supporto pubblico per endpoint IPv6	Supporto per endpoint privati 1 IPv6
AWS PrivateLink	Sì	Sì	Sì	
Amazon Managed Service per Prometheus	Sì	No	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	
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

Nome servizio	Supporto dual stack	IPv6 solo supporto	Supporto pubblico per endpoint IPv6	Supporto per endpoint privati 1 IPv6
AWS X-Ray	Sì	No	Sì	Sì

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

[2] Questa voce rappresenta il IPv6 supporto per le operazioni di gestione dell'area di lavoro Grafana, come l'aggiornamento delle aree di lavoro e delle autorizzazioni dell'area di lavoro. Non è disponibile alcun IPv6 supporto per le operazioni generali dell'area di lavoro Grafana, come la creazione e la modifica di dashboard o l'interrogazione delle fonti di dati.

Supporto aggiuntivo IPv6

Calcolo

- Amazon EC2 supporta il lancio di istanze basate su Nitro System in IPv6 sottoreti -only.
- Amazon EC2 fornisce IPv6 endpoint per Instance Metadata Service (IMDS) e Amazon Time Sync Service.

Reti e distribuzione di contenuti

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

Sicurezza, identità e conformità

- AWS Identity and Access Management (IAM) supporta IPv6 gli indirizzi nelle politiche basate sull'identità IAM.
- Amazon Macie supporta IPv6 gli indirizzi nelle informazioni di identificazione personale (PII).

Gestione e governance

- AWS CloudTrail i record includono informazioni sulla fonte. IPv6

- AWS CLI v2 supporta il download tramite IPv6 connessioni IPv6 solo per i client.

Ulteriori informazioni

- IPv6 su AWS
- Architetture di riferimento Dual Stack e solo IPv6 Amazon VPC (PDF)

Configurare un cloud privato virtuale

Il cloud privato virtuale (VPC) di Amazon è un elemento fondamentale che consente di fornire una rete virtuale logicamente isolata all'interno del cloud AWS. Creando il proprio VPC, si ottiene il pieno controllo sull'ambiente di rete, inclusa la possibilità di definire intervalli di indirizzi IP, sottoreti, tabelle di routing e opzioni di connettività.

L'account AWS contiene un VPC predefinito per ogni area AWS. Questo VPC predefinito è preconfigurato con impostazioni che lo rendono una comoda opzione per avviare rapidamente le risorse. Tuttavia, il VPC predefinito potrebbe non essere sempre in linea con le proprie esigenze di rete a lungo termine. È qui che la creazione di VPC aggiuntivi può essere vantaggiosa.

La creazione di VPC aggiuntivi offre diversi vantaggi rispetto all'utilizzo del VPC predefinito fornito con ogni nuovo account AWS. Con un VPC autogestito, è possibile progettare la topologia di rete per allinearla con precisione ai propri requisiti specifici, che si tratti di implementare un'applicazione multilivello, connettersi a risorse on-premises o segregare i carichi di lavoro per reparto o unità aziendale.

Inoltre, la creazione di più VPC può consentire una maggiore sicurezza e isolamento tra le diverse applicazioni o unità aziendali. Ogni VPC funge da rete virtuale separata, che consente di applicare policy di sicurezza, controlli di accesso e configurazioni di routing distinti, fatti su misura per ciascun ambiente.

In definitiva, la decisione di utilizzare il VPC predefinito o creare uno (o più) VPC personalizzati dovrebbe basarsi sui requisiti applicativi specifici, sulle esigenze di sicurezza e sugli obiettivi di scalabilità a lungo termine. Investire del tempo nella progettazione attenta della propria infrastruttura VPC può dare i suoi frutti sotto forma di una base di cloud networking solida, sicura e adattabile.

Indice

- Nozioni di base sui VPC
- Opzioni di configurazione del VPC
- Predefinito VPCs
- Crea un VPC
- Come visualizzare le risorse nel VPC
- Aggiungere o rimuovere un blocco CIDR dal VPC
- Set di opzioni DHCP in Amazon VPC

- Attributi DNS per il VPC
- NAU (Network Address Usage) per il tuo VPC
- Condividere le sottoreti VPC con altri account
- Estendere un VPC a una zona locale, una zona Wavelength o un Outpost
- Eliminazione del VPC
- Generare infrastructure-as-code dalle azioni della console VPC con Console-to-Code

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, consultare Sottoreti.

Indice

- Intervallo di indirizzi IP VPC
- Diagramma di un VPC
- Risorse VPC

Intervallo di indirizzi IP VPC

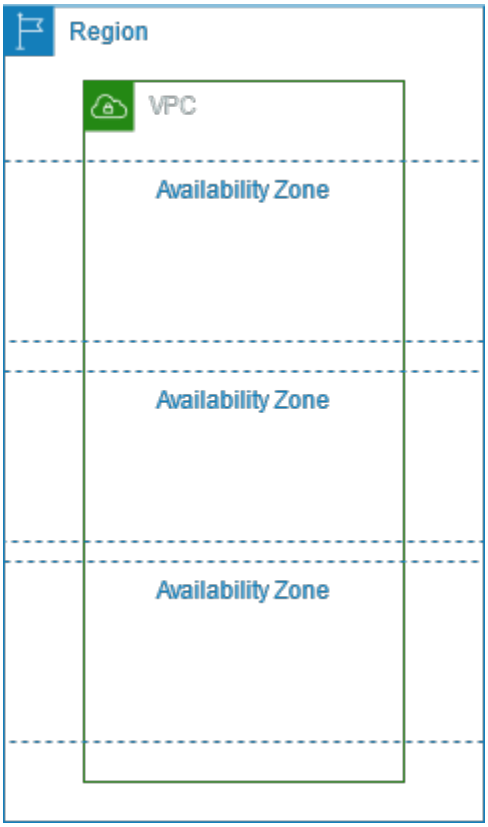
Quando crei un VPC, devi specificare i relativi indirizzi IP come segue:

- 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, consultare Indirizzamento IP per le tue VPCs 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

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, consultare Indirizzamento IP per le tue VPCs 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, consultare 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 le risorse AWS, ad esempio istanze EC2, nelle 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 che la tenancy del VPC sia `Default`, le istanze EC2 avviate in questo VPC utilizzeranno l'attributo di tenancy specificato quando avvii l'istanza. Per ulteriori informazioni, consulta Avvio di un'istanza utilizzando parametri definiti nella Guida per l'utente di Amazon EC2. 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, il tuo Outpost richiede una connettività privata; è necessario utilizzare la tenancy di `Default`.

Predefinito VPCs

Quando inizi a usare Amazon VPC, hai 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. Pertanto, puoi iniziare immediatamente a lanciare EC2 istanze Amazon in un VPC predefinito. 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
- Sottoreti predefinite
- Utilizzo del VPC e delle sottoreti predefinite

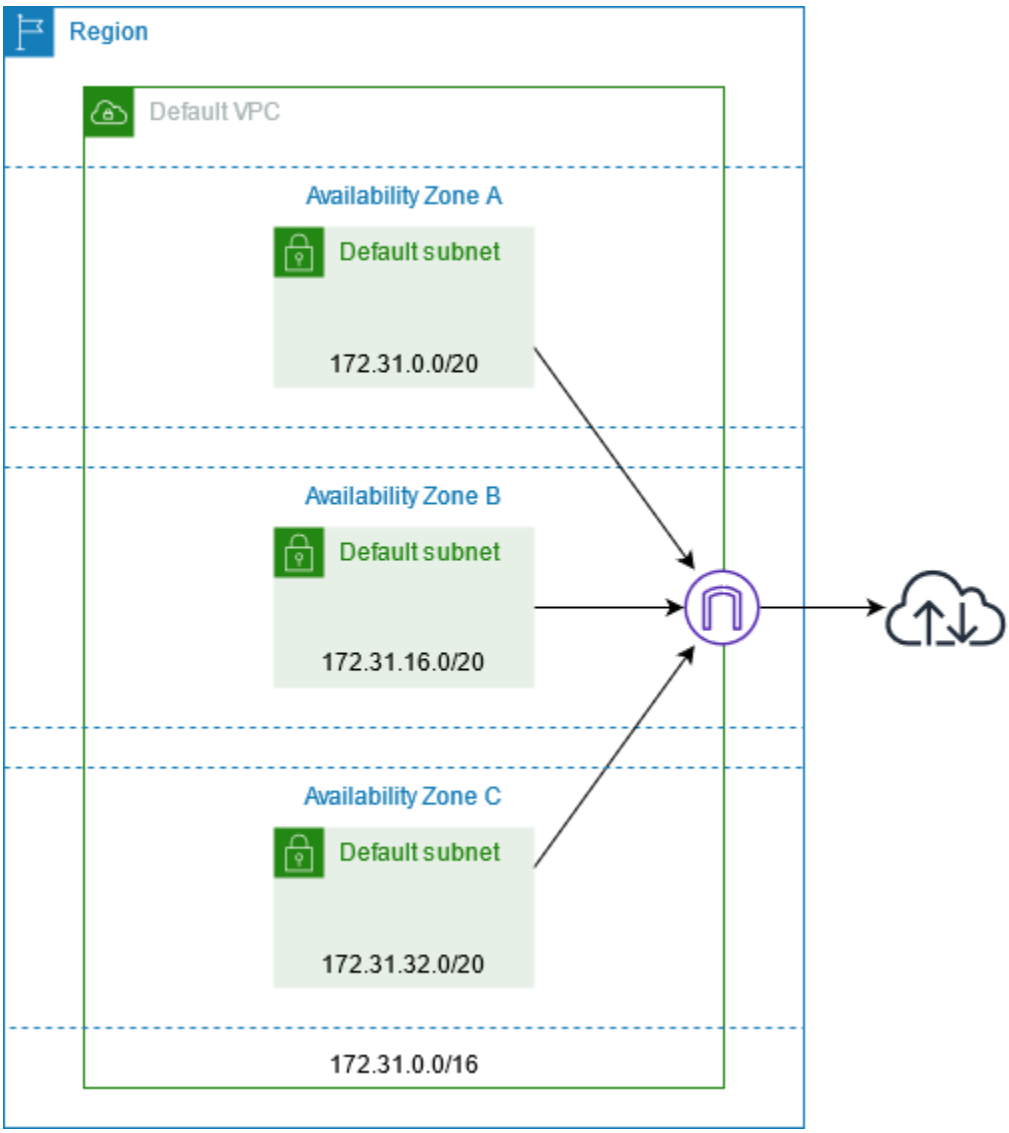
Componenti VPC predefiniti

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

- Crea un VPC con un blocco `/16` IPv4 CIDR di dimensioni (). `172.31.0.0/16` Ciò fornisce fino a 65.536 indirizzi privati. IPv4
- 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.
- Associa le opzioni DHCP predefinite impostate per il tuo AWS account al tuo 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 disponi di una policy IAM che nega la possibilità di chiamare CreateInternetGateway e quindi effettui una chiamata CreateDefaultVpc, il gateway Internet nel VPC predefinito viene comunque creato. Per impedire ad Amazon di creare un gateway Internet, dovresti negare CreateDefaultVpc e CreateInternetGateway.
> - Per bloccare tutto il traffico da e verso i gateway Internet nel tuo account, consulta Blocca l'accesso pubblico alle sottoreti VPCs e alle sottoreti.

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.
- Aggiungi AWS Site-to-Site VPN connessioni.
- Aggiungi altri blocchi IPv4 CIDR.
- Accesso VPCs in una regione 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 .

È possibile utilizzare una sottorete predefinita come qualsiasi altra sottorete; aggiungere tabelle di routing personalizzate e impostare la rete. ACLs È inoltre possibile specificare una sottorete predefinita specifica quando si avvia un'istanza. EC2

Facoltativamente, puoi associare un blocco IPv6 CIDR al tuo 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, se si esegue questa operazione, nessuna EC2 istanza in esecuzione in quella sottorete può accedere a Internet.

Le istanze avviate in una sottorete predefinita ricevono sia un IPv4 indirizzo pubblico che un IPv4 indirizzo privato e nomi host DNS pubblici e privati. Le istanze avviate in una sottorete non predefinita in un VPC predefinito non ricevono un IPv4 indirizzo 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 di indirizzi IP della sottorete.

Di tanto in tanto, 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.

Utilizzo del VPC e delle sottoreti predefinite

Questa sezione descrive come lavorare con le sottoreti predefinite VPCs e predefinite.

Indice

- Visualizzazione del VPC predefinito e delle sottoreti predefinite
- Creazione di un VPC predefinito
- Creazione di una sottorete predefinita
- Eliminazione delle sottoreti predefinite e del VPC predefinito

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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Your. VPCs
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)
- Usa il 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)
- Usa il 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Your VPCs.
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

È possibile utilizzare il comando create-default-vpc 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, puoi utilizzare il PowerShell comando New-EC2DefaultVpcTools for Windows o l'azione CreateDefaultVpcAmazon EC2 API.

Creazione di una sottorete predefinita

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

Puoi creare una sottorete predefinita in una zona di disponibilità senza sottoreti. Ad esempio, potresti voler creare una sottorete predefinita se hai eliminato una sottorete predefinita o se hai AWS aggiunto una nuova zona di disponibilità e non hai creato automaticamente una sottorete predefinita per quella zona nel tuo VPC predefinito.

Quando si crea una sottorete predefinita, questa viene creata con un blocco `/20` IPv4 CIDR di dimensioni 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 hai bisogno di più spazio per gli indirizzi, puoi aggiungere un blocco IPv4 CIDR al tuo VPC.

Se hai associato un blocco IPv6 CIDR al tuo VPC predefinito, la nuova sottorete predefinita non riceve IPv6 automaticamente un blocco CIDR. Puoi invece associare un blocco IPv6 CIDR alla sottorete predefinita dopo averlo creato. Per ulteriori informazioni, consulta Aggiungere o rimuovere un blocco IPv6 CIDR dalla sottorete.

Per creare una sottorete predefinita utilizzando il AWS CLI

Utilizzare il create-default-subnet AWS CLI comando e specificare 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 di AWS CLI, consulta la Guida per l'AWS Command Line Interface utente.

In alternativa, puoi utilizzare il PowerShell comando New-EC2DefaultSubnetTools for Windows o l'azione CreateDefaultSubnetAmazon 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 esplicitamente una sottorete in una delle tue istanze When you launch. VPCs 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 di indirizzi IP della 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

- Creazione di un VPC e di altre risorse VPC
- Creare solo un VPC
- Crea un VPC utilizzando il AWS CLI

Per informazioni sulla visualizzazione o la modifica di un VPC, consultare the section called “Aggiungere o rimuovere un blocco CIDR”.

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 la 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. Per creare tag dei nomi per le risorse VPC, mantieni selezionata Generazione automatica dei tag dei nomi altrimenti deselezionala per scegliere autonomamente tag dei nomi per le risorse VPC.
5. Per il blocco IPv4 CIDR, inserisci un intervallo di IPv4 indirizzi per il VPC. Un VPC deve avere un intervallo di IPv4 indirizzi.
6. (Facoltativo) Per supportare il IPv6 traffico, scegli il blocco IPv6 CIDR, il blocco CIDR fornito da Amazon IPv6 .
7. Scegli un'opzione di tenancy. Questa opzione definisce se EC2 le istanze che avvii nel VPC verranno eseguite su hardware condiviso con Account AWS altri o su hardware dedicato esclusivamente al tuo utilizzo. Se scegli la tenancy del VPC EC2 , le istanze `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 Number of Availability Zones (AZs), consigliamo di effettuare il provisioning delle sottoreti in almeno due zone di disponibilità per un ambiente di produzione. Per scegliere le AZs sottoreti, espandi Personalizza. AZs Altrimenti, lascia che le 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. (Facoltativo) Se le risorse di una sottorete privata devono accedere alla rete Internet pubblica IPv4, per i gateway NAT, scegli il numero di gateway NAT AZs 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 per i gateway NAT.
11. (Facoltativo) Se le risorse di una sottorete privata devono accedere alla rete Internet pubblica IPv6, per il gateway Internet solo Egress, 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 Gateway Endpoints nella Guida.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 la 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 il blocco IPv4 CIDR, effettuate una delle seguenti operazioni:
   - Scegli l'immissione manuale IPv4 CIDR e inserisci un intervallo di IPv4 indirizzi per il tuo VPC.
   - Scegli il blocco IPv4 CIDR allocato su IPAM, seleziona il pool di indirizzi IPAM (Amazon VPC IP Address Manager) e una netmask. IPv4 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, consultare la Guida per l'utente Amazon VPC IPAM.

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 VPC dual stack, specifica IPv6 un intervallo di indirizzi per il tuo VPC. Per il blocco IPv6 CIDR, esegui una delle seguenti operazioni:

   - Scegli il blocco IPv6 CIDR allocato su IPAM se utilizzi Amazon VPC IP Address Manager e desideri effettuare il provisioning di un CIDR da un pool IPAM. IPv6 Se si utilizza il blocco IPv6 CIDR allocato su IPAM a cui effettuare il provisioning IPv6 CIDRs VPCs, si ottiene il vantaggio di contiguous for VPC. IPv6 CIDRs Le allocazioni contigue sono quelle allocate in sequenza. CIDRs CIDRs Consentono di semplificare le regole di sicurezza e di rete; IPv6 CIDRs possono essere aggregate in un'unica voce attraverso costrutti di rete e sicurezza come elenchi di controllo degli accessi, tabelle di routing, gruppi di sicurezza e firewall.

     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 opzionale di allocazione della lunghezza della maschera di rete predefinita, consulta Create a Regional IPv6 pool nella Amazon VPC IPAM User Guide.
       - 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.
     - 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 della IPv6 netmask sono comprese tra /44 e /60 con incrementi di /4.

- Scegli il blocco IPv6 CIDR fornito da Amazon per richiedere un blocco IPv6 CIDR da un pool di indirizzi Amazon. IPv6 Per Network Border Group, seleziona il gruppo da cui AWS pubblicizza gli indirizzi IP. Amazon fornisce una dimensione fissa del blocco IPv6 CIDR di /56.
- Scegli IPv6 CIDR di mia proprietà per fornire un IPv6 CIDR a cui hai già fornito. AWS Per ulteriori informazioni su come trasferire i tuoi intervalli di indirizzi IP su AWS, consulta Bring your own IP address (BYOIP) nella Amazon EC2 User Guide. È possibile effettuare il provisioning di 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.
  - Seleziona un CIDR: scegli questa opzione per inserire manualmente un IPv6 indirizzo e 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 della IPv6 maschera di rete sono comprese tra /44 e /60 con incrementi di /4.

7. (Facoltativo) Scegli un'opzione di tenancy. Questa opzione definisce se EC2 le istanze che avvii nel VPC verranno eseguite su hardware condiviso con Account AWS altri o su hardware dedicato esclusivamente al tuo utilizzo. Se scegli la tenancy del VPC EC2 , le istanze *`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 User Guide. EC2 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 seguente comando create-vpc per creare un VPC con il blocco CIDR specificato. IPv4

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

   In alternativa, per creare un VPC dual stack, aggiungi `--amazon-provided-ipv6-cidr-block` l'opzione 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 IPv6 il blocco CIDR associato al tuo VPC utilizzando il seguente comando describe-vpcs.

```
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.
   - IPv4-only subnet — Per creare una sottorete con un blocco CIDR specifico, usa il seguente comando create-subnet. IPv4

     ```
     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
     ```

   - IPv6-only subnet: se hai creato un VPC dual stack, puoi utilizzare `--ipv6-native` l'opzione per creare IPv6 una sottorete -only, come illustrato 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 comando seguente. 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 tuo VPC utilizzando il seguente attach-internet-gatewaycomando. 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 tua sottorete pubblica utilizzando il comando seguente create-route-table. 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 una route nella tabella delle rotte che invii tutto il IPv4 traffico al gateway Internet utilizzando il seguente comando create-route. 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. Associate la tabella delle rotte alla sottorete pubblica utilizzando il comando seguente. associate-route-table 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] È possibile aggiungere un gateway Internet solo in uscita in modo che le istanze in una sottorete privata possano accedere a Internet IPv6 (ad esempio, per ottenere aggiornamenti software), ma gli host su Internet non possano accedere alle istanze.

   a. Crea un gateway Internet solo in uscita utilizzando il seguente comando -gateway. create-egress-only-internet 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 tua sottorete privata utilizzando il comando seguente. create-route-table 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 una route nella tabella di routing per la sottorete privata che invia tutto il IPv6 traffico al gateway Internet di sola uscita utilizzando il seguente comando create-route. 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. Associate la tabella di routing alla sottorete privata utilizzando il comando seguente. associate-route-table

```
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. Creare il gateway NAT nella sottorete pubblica utilizzando il comando seguente. 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. Altrimenti, usa il seguente create-route-tablecomando per creare una tabella di routing per la tua 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 una route nella tabella delle rotte per la sottorete privata che invia tutto il IPv4 traffico al gateway NAT utilizzando il seguente comando create-route. 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. Altrimenti, usa il seguente associate-route-tablecomando per associare la tabella delle rotte 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
```

Come visualizzare le risorse nel VPC

Questa sezione descrive come 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. Accedi 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 è presente un endpoint gateway, esiste una risorsa endpoint gateway con il nome di servizio AWS (Amazon S3 o Amazon DynamoDB) a cui puoi connetterti 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.

Aggiungere o rimuovere un blocco CIDR dal VPC

Questa sezione descrive come aggiungere o rimuovere IPv4 blocchi IPv6 CIDR da un VPC.

⚠ Important

- Il tuo VPC può avere fino a cinque o cinque IPv4 blocchi IPv6 CIDR per impostazione predefinita, ma questo limite è regolabile. Per ulteriori informazioni, consulta Quote Amazon VPC. Per informazioni riguardo le restrizioni sui blocchi CIDR di un VPC, consulta Blocchi CIDR del VPC.
- Se al tuo VPC è associato più di un blocco IPv4 CIDR, puoi rimuovere un blocco IPv4 CIDR dal VPC. Non è possibile rimuovere il blocco CIDR primario. IPv4 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.
- Se non desideri più il IPv6 supporto nel tuo VPC, ma desideri continuare a utilizzare il tuo VPC per creare e comunicare con IPv4 le risorse, puoi rimuovere il blocco CIDR. IPv6
- Per rimuovere un blocco IPv6 CIDR, devi prima annullare l'assegnazione di tutti IPv6 gli indirizzi assegnati a qualsiasi istanza nella sottorete.
- La rimozione di un blocco IPv6 CIDR non elimina automaticamente le regole dei gruppi di sicurezza, le regole ACL di rete o i percorsi delle tabelle di routing configurati per la rete. IPv6 Devi modificare o eliminare manualmente queste regole o route.

Per aggiungere o rimuovere un blocco CIDR da un VPC tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Your. VPCs
3. Seleziona il VPC, quindi scegli Azioni, Modifica. CIDRs

4. Per rimuovere un CIDR, scegliere Rimuovi accanto a esso.
5. Per aggiungere un CIDR, scegli Aggiungi nuovo IPv4 CIDR o Aggiungi nuovo CIDR. IPv6
6. Per aggiungere un CIDR per IPv4 un blocco CIDR, esegui una delle seguenti operazioni:
   - Scegliete l'immissione manuale IPv4 CIDR e inserite un IPv4 blocco CIDR.
   - Scegli CIDR allocato su IPAM e seleziona un IPv4 CIDR da un pool IPAM. IPv4
   - Seleziona Salva.
7. Per aggiungere un CIDR per un blocco CIDR, procedi come segue: IPv6

   - Scegli il blocco IPv6 CIDR allocato su IPAM se utilizzi Amazon VPC IP Address Manager e desideri effettuare il provisioning di un CIDR da un pool IPAM. IPv6 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 opzionale di allocazione della lunghezza della maschera di rete predefinita, consulta Create a Regional IPv6 pool nella Amazon VPC IPAM User Guide.
       - 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.
     - 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 della IPv6 netmask sono comprese tra /44 e /60 con incrementi di /4.
   - Scegli il blocco IPv6 CIDR fornito da Amazon per richiedere un blocco IPv6 CIDR da un pool di indirizzi Amazon. IPv6 Per Network Border Group, seleziona il gruppo da cui AWS pubblicizza gli indirizzi IP. Amazon fornisce una dimensione fissa del blocco IPv6 CIDR di /56.

- Scegli IPv6 CIDR di mia proprietà per fornire un IPv6 CIDR a cui hai già fornito. AWS Per ulteriori informazioni su come trasferire i tuoi 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.
  - Seleziona un CIDR: scegli questa opzione per inserire manualmente un IPv6 indirizzo e 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 della IPv6 maschera di rete sono comprese tra /44 e /60 con incrementi di /4.
  - Al termine, scegliere Seleziona CIDR.

8. Scegli Chiudi.
9. Se è stato aggiunto un blocco CIDR al VPC, è possibile creare sottoreti che utilizzano il nuovo blocco CIDR. Per ulteriori informazioni, consulta Creazione di una sottorete.

Per associare o dissociare un blocco CIDR da un VPC utilizzando AWS CLI

Utilizza i comandi associate-vpc-cidr-block e 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?
- Concetti relativi ai set di opzioni DHCP

- Utilizzo dei set di opzioni DHCP

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 EC2 istanze possono comunicare con i server Amazon DHCP in base alle esigenze per recuperare il lease dell'indirizzo IP o altre informazioni di configurazione di rete (come l'indirizzo IP di un server Amazon DNS o l'indirizzo IP del router nel tuo 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 disponi di una configurazione VPC che richiede alle tue applicazioni di effettuare richieste dirette al server Amazon IPv6 DHCP, tieni presente quanto segue:

- Un' EC2 istanza in una sottorete dual-stack può recuperare il proprio indirizzo solo dal server DHCP. IPv6 IPv6 Non può recuperare configurazioni di rete aggiuntive dal server IPv6 DHCP, ad esempio nomi di server DNS o nomi di dominio.
- Un' EC2 istanza in una sottorete IPv6 -only può recuperare il proprio IPv6 indirizzo dal server IPv6 DHCP e può recuperare informazioni di configurazione di rete aggiuntive, come nomi di server DNS e nomi di dominio.
- Per un' EC2 istanza in una sottorete IPv6 -only, il server IPv4 DHCP 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 IPv4 DHCP non restituirà un indirizzo indipendentemente dal fatto che nell'insieme di opzioni siano menzionati o meno altri name server. IPv4

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

Concetti relativi ai set di opzioni DHCP

Un set di opzioni DHCP è un gruppo di impostazioni di rete utilizzate dalle risorse del VPC, ad esempio EC2 le istanze, per comunicare sulla 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 EC2 le istanze create su Nitro System, si AWS configura `169.254.169.253` come server dei nomi di dominio predefinito.
- Per EC2 le istanze basate su Xen, non sono configurati server di nomi di dominio e, poiché le istanze nel VPC non hanno accesso a un server DNS, non possono accedere a Internet.

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

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

Indice

- Set di opzioni DHCP predefinito
- Set di opzioni DHCP personalizzato

Set di opzioni DHCP predefinito

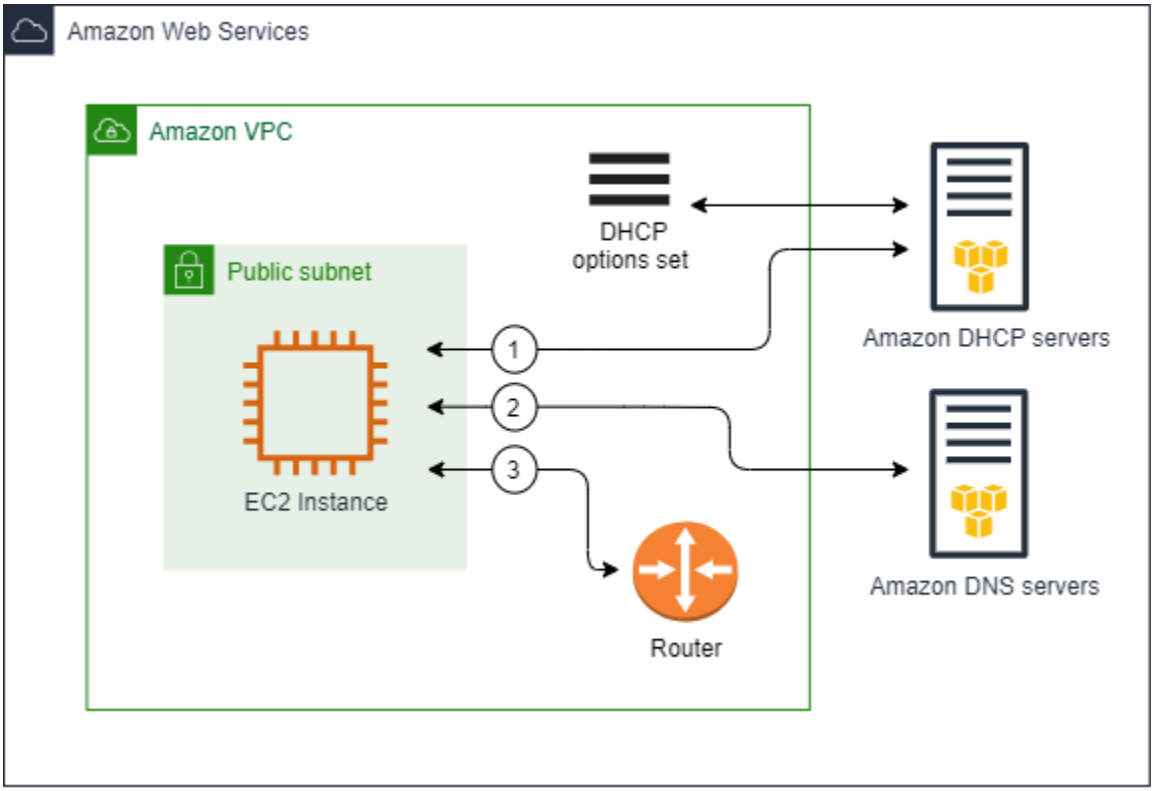
Il set di opzioni DHCP predefinito contiene le seguenti impostazioni:

- 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 EC2 le istanze, consulta i nomi host delle EC2 istanze Amazon.
- IPv6 Tempo di leasing preferito: con quale frequenza viene rinnovato il leasing di un'istanza in esecuzione a cui è IPv6 assegnata un'istanza. DHCPv6 Il tempo di leasing predefinito è 140 secondi. Il rinnovo avviene in genere quando è trascorsa la metà del tempo di leasing.

Quando si utilizza 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, EC2 le istanze utilizzano Amazon Time Sync Service per recuperare l'ora.
- Server dei nomi NetBIOS: per EC2 le istanze 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 EC2 le istanze 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.

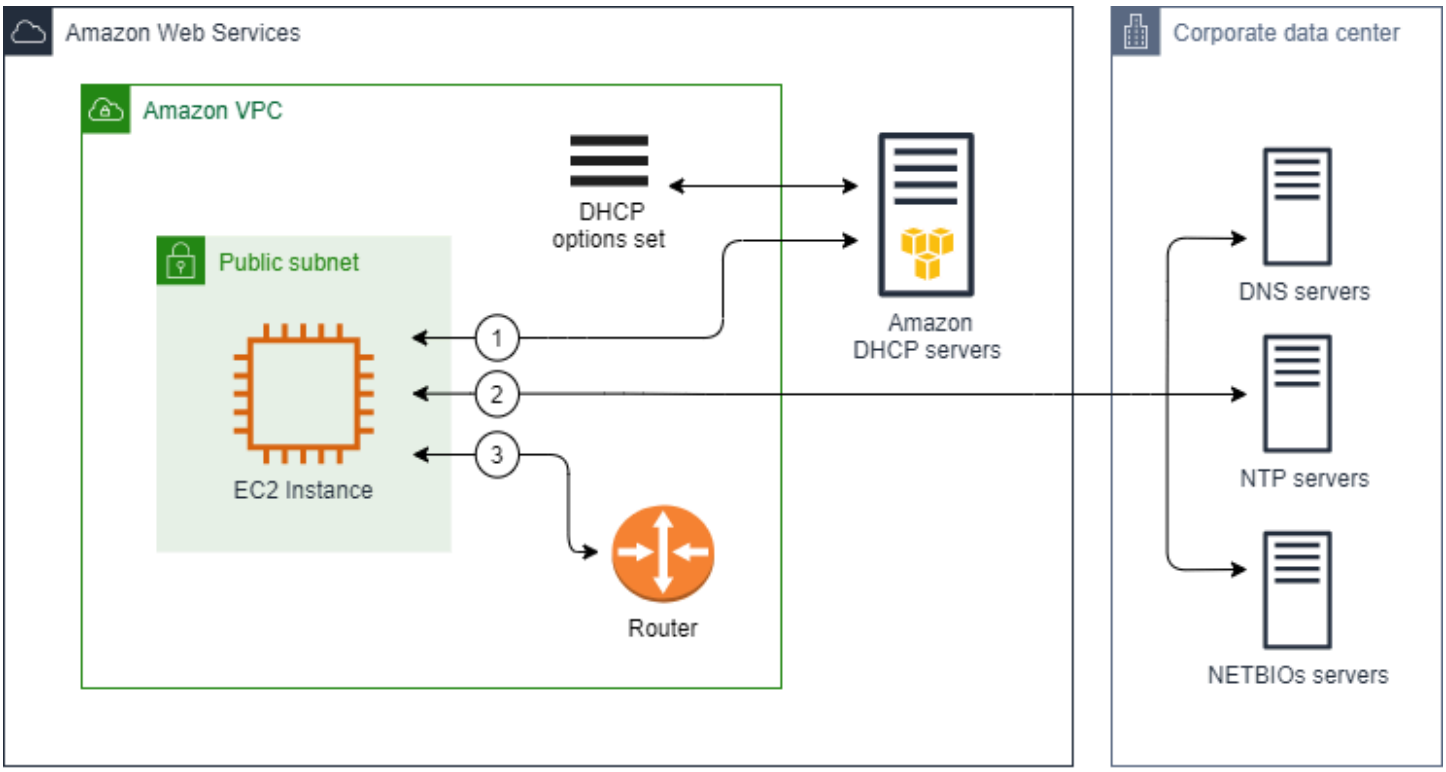


Set di opzioni DHCP personalizzato

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 dei nomi NetBIOS: per EC2 le istanze 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 EC2 le istanze che eseguono Windows, il metodo utilizzato dalle istanze per risolvere i nomi NetBIOS in indirizzi IP.
- IPv6 Tempo di leasing preferito (opzionale): un valore (in secondi, minuti, ore o anni) che indica la frequenza con cui un'istanza in esecuzione a cui è IPv6 assegnata un'istanza viene rinnovata. DHCPv6 I valori accettabili sono compresi tra 140 e 4294967295 secondi (circa 138 anni). Il tempo di leasing predefinito è pari a 140 secondi se non vengono inseriti valori. Se si utilizza l'indirizzamento a lungo termine per EC2 le istanze, è possibile aumentare la durata del leasing ed evitare frequenti richieste di rinnovo del leasing. Il rinnovo avviene in genere quando è trascorsa la metà del tempo 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

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

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 la 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 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.

     > **Note**
     >
     > Usa solo nomi di dominio che controlli completamente.

     Alcuni sistemi operativi Linux accettano più nomi di dominio separati da spazi. Tuttavia, Windows e altri sistemi operativi Linux considerano il valore come un singolo dominio, il che determina un comportamento imprevisto. Se il set di opzioni DHCP è associato a un VPC contenente istanze che eseguono sistemi operativi che considerano 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. Puoi inserire gli indirizzi IP di un massimo di quattro server di nomi di IPv4 dominio (o fino a tre server di nomi di IPv4 dominio e**`AmazonProvidedDNS`**) e quattro server di nomi di IPv6 dominio 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.

- Server NTP (opzionali): inserisci gli indirizzi IP di un massimo di otto server Network Time Protocol (NTP) (quattro indirizzi e quattro IPv4 indirizzi). IPv6

  I server NTP forniscono il tempo alla rete. Puoi specificare Amazon Time Sync Service all' IPv4 indirizzo `169.254.169.123` o all' IPv6 indirizzo`fd00:ec2::123`. Di default, le istanze comunicano con Amazon Time Sync Service. Tieni presente che l' IPv6 indirizzo è accessibile solo sulle EC2 istanze create 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 Imposta l'ora per la tua istanza 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 EC2 le istanze 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**. Si consiglia 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 nodi, vedere la sezione 8.7 di RFC 2132 e la sezione 10 di 001. RFC1

Per EC2 le istanze 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 Tempo di leasing preferito (opzionale): un valore (in secondi, minuti, ore o anni) che indica la frequenza con cui un'istanza in esecuzione a cui è IPv6 assegnata un'istanza viene rinnovata. DHCPv6 I valori accettabili sono compresi tra 140 e 2147483647 secondi (circa 68 anni). Il tempo di leasing predefinito è pari a 140 secondi se non vengono inseriti valori. Se si utilizza l'indirizzamento a lungo termine per EC2 le istanze, è possibile aumentare la durata del leasing ed evitare frequenti richieste di rinnovo del leasing. Il rinnovo avviene in genere quando è trascorsa la metà del tempo 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

- 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. VPCs 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Your VPCs.
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. Seleziona Salva.

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

- 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 la 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

- 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.

IPv4 Gli indirizzi pubblici consentono la comunicazione su Internet, mentre IPv4 gli indirizzi privati consentono la comunicazione all'interno della rete dell'istanza. Per ulteriori informazioni, consulta Indirizzamento IP per le tue VPCs 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

- Informazioni su Amazon DNS
- Visualizza i nomi host DNS per la tua istanza EC2
- Visualizzazione e aggiornamento degli attributi DNS per il VPC

Informazioni su Amazon DNS

In qualità di AWS architetto o amministratore, uno dei componenti di rete fondamentali che incontrerai è il server Amazon DNS, noto anche come Route 53 Resolver. Questo servizio di resolver DNS è integrato nativamente in ogni zona di disponibilità all'interno AWS della regione, fornendo una soluzione affidabile e scalabile per la risoluzione dei nomi di dominio all'interno del Virtual Private Cloud (VPC). In questa sezione verranno illustrati gli indirizzi IP del server Amazon DNS, i nomi host DNS privati che può risolvere e le regole che ne regolano l'utilizzo.

Indice

- Server DNS Amazon
- Regole e considerazioni
- Hostname DNS
- Attributi DNS nel VPC
- Quote per DNS

- Zone ospitate private

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 Route 53 Resolver si trova in `169.254.169.253` (IPv4), `fd00:ec2::253` (IPv6) e nell'intervallo IPV4 CIDR privato principale fornito al tuo VPC più due. Ad esempio, se disponi di un VPC con un IPv4 CIDR di `10.0.0.0/16` e un IPv6 CIDR di`2001:db8::/32`, puoi raggiungere il Route 53 Resolver all'indirizzo `169.254.169.253` (IPv4), `fd00:ec2::253` () o (). IPv6 `10.0.0.2` IPv4 Le risorse all'interno di un VPC utilizzano un indirizzo link-local per le query DNS. Queste query vengono trasferite privatamente al Route 53 Resolver e non sono visibili sulla rete. In una sottorete IPv6 solo, l'indirizzo IPv4 locale del collegamento (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. Forniamo anche un nome host DNS pubblico se l'istanza è configurata con un IPv4 indirizzo pubblico e gli attributi DNS VPC sono abilitati.

Il formato del nome host DNS privato dipende da come configuri l'istanza al momento dell' EC2 avvio. Per ulteriori informazioni sui tipi di nomi host DNS privati, consulta i tipi di hostname delle EC2 istanze Amazon nella Amazon EC2 User Guide.

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 puoi filtrare il traffico da o verso il server Amazon DNS utilizzando gruppi di rete ACLs o 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 IPv4 indirizzo privato e un nome host DNS privato che corrisponde al suo indirizzo privato. IPv4 Se l'istanza ha un IPv4 indirizzo pubblico, gli attributi DNS del relativo VPC determinano se riceve un nome host DNS pubblico che corrisponde all'indirizzo pubblico. IPv4 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

È possibile utilizzare il nome host DNS IP privato (IPv4 solo) per la comunicazione tra istanze nello stesso VPC. È possibile risolvere i nomi host del nome DNS IP privato (IPv4 solo) di altre istanze in altre istanze VPCs purché le istanze si trovino nella stessa AWS regione e il nome host dell'altra istanza si trovi nell'intervallo dello spazio di indirizzi privato definito da RFC 1918:, e. `10.0.0.0 - 10.255.255.255 (10/8 prefix)` `172.16.0.0 - 172.31.255.255 (172.16/12 prefix)` `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 in sottoreti dual-stack e -only. IPv6 Per ulteriori informazioni su RBN, consulta Tipi di hostname delle istanze. EC2

DNS pubblico IPv4

Un hostname IPv4 DNS pubblico (esterno) assume il formato `ec2-`*`public-ipv4-address`*`.compute-1.amazonaws.com` per la `us-east-1` regione e `ec2-`*`public-ipv4-address.region`*`.compute.amazonaws.com` per le altre regioni. Il server Amazon DNS risolve un nome host DNS pubblico nell' IPv4indirizzo pubblico dell'istanza all'esterno della rete dell'istanza e nell' IPv4 indirizzo privato dell'istanza all'interno della rete dell'istanza. Per ulteriori informazioni, IPv4consulta Indirizzi 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, un'istanza lanciata nel VPC riceve un nome host DNS pubblico se le viene assegnato un IPv4 indirizzo pubblico o un indirizzo IP elastico al momento della creazione. Se abiliti entrambi gli attributi per un VPC che in precedenza non li aveva entrambi abilitati, le istanze già avviate in quel VPC ricevono nomi host DNS pubblici se hanno un indirizzo pubblico o un indirizzo IP elastico IPv4 .

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. Il valore di default per questo attributo è `false` a meno che il VPC non sia un VPC di default. Esamina le regole e considera zioni relative a questo attributo riportate di seguito.
`enableDnsSupport`	Determina se il VPC supporti la risoluzione DNS tramite il server DNS fornito da Amazon. Se questo attributo è `true`, le query al DNS fornito da Amazon hanno esito positivo. Per ulteriori informazioni, consulta Server DNS Amazon. Il valore di default per questo attributo è `true`. Esamina le regole e 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 IPv4 indirizzi privati per tutti gli spazi di indirizzi, incluso il caso in cui l'intervallo di IPv4 indirizzi del tuo VPC non rientra negli intervalli di IPv4 indirizzi privati specificati da RFC 1918. Tuttavia, se hai creato il tuo VPC prima di ottobre 2016, non Amazon Route 53 Resolver risolve i nomi host DNS privati se l'intervallo di IPv4 indirizzi del tuo VPC non rientra in questi intervalli. Per abilitare il supporto, contatta Supporto.
- Se utilizzi il peering VPC, devi abilitare entrambi gli attributi per entrambi e devi abilitare VPCs la risoluzione DNS per la connessione peering. Per ulteriori informazioni, consulta Abilitazione della risoluzione DNS per una connessione peering VPC.

Quote per DNS

Esiste un limite di 1024 pacchetti al secondo (PPS) per i servizi che utilizzano indirizzi link-local. Questo limite include l'aggregato di query DNS di Route 53 Resolver, richieste del servizio di metadati di istanza (IMDS), richieste Amazon Time Service Network Time Protocol (NTP) e richieste Windows Licensing Service (per istanze basate su Microsoft Windows). 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 User Guide. EC2

Zone ospitate private

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

Visualizza i nomi host DNS per la tua istanza EC2

Puoi visualizzare i nomi host DNS per un'istanza in esecuzione o un'interfaccia di rete utilizzando la EC2 console Amazon o la riga di comando. Conoscere questi nomi host è importante per connetterti alle tue risorse.

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

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

- 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. Apri la EC2 console Amazon 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) mostra il nome host DNS privato.

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

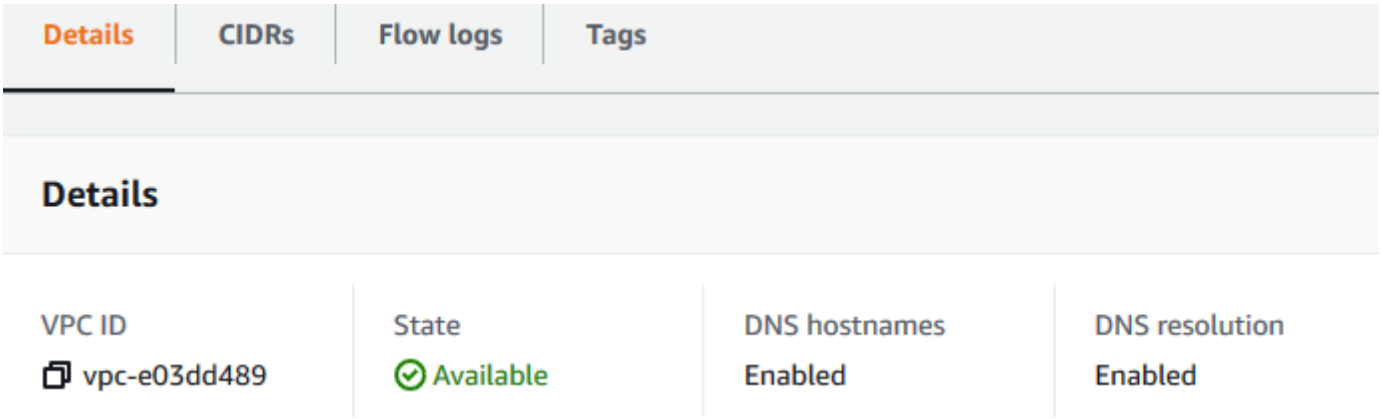
- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

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. Queste impostazioni controllano se le tue istanze ricevono nomi host DNS pubblici e se il server Amazon DNS è in grado di risolvere quelli privati. La configurazione corretta di questi attributi è fondamentale per garantire una comunicazione senza interruzioni all'interno del VPC.

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

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Your. VPCs
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

- 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

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

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.
- Utilizzo degli indirizzi di rete peer-to-peer: il numero massimo di unità NAU per un VPC e tutte le unità peer-ered. VPCs Se un VPC è collegato in peering con altri VPCs nella stessa regione, la VPCs combinazione può avere fino a 128.000 unità NAU per impostazione predefinita. Puoi richiedere un aumento della quota fino a 512.000. VPCs che vengono scambiati tra regioni diverse non contribuiscono al raggiungimento di questo limite.

Puoi utilizzare il NAU nei modi seguenti:

- Prima di creare la rete virtuale, calcola le unità NAU per decidere se distribuire i carichi di lavoro su più piattaforme. VPCs
- 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 “CloudWatch metriche”.

Come viene calcolato il NAU

Se conosci bene come viene calcolato il NAU, può aiutarti a pianificare la scalabilità del tuo. VPCs

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 altre risorse sono rappresentate come più unità NAU. Puoi usare la tabella per imparare a calcolare il NAU.

Risorsa	Unità NAU
Ogni indirizzo privato o pubblico IPv4 e ogni IPv6 indirizzo assegnato a un'interfaccia di rete per un' EC2istanza nel VPC	1
Interfacce di rete aggiuntive collegate a un'istanza EC2	1
Prefissi assegnati a un'interfaccia di rete	1

Risorsa	Unità NAU
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
Obiettivo di montaggio EFS	6
Interfaccia EFA (EFA con un dispositivo ENA) o interfaccia solo EFA	1
Pod Amazon EKS	1

Esempi NAU

Gli esempi seguenti mostrano come calcolare il NAU.

Esempio 1 - Due VPCs connessioni tramite peering VPC

I peer VPCs 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 IPv4 indirizzo e un IPv6 indirizzo) in una sottorete e 5.000 istanze (ciascuna con un IPv4 indirizzo e un IPv6 indirizzo) 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 IPv4 indirizzo e un IPv6 indirizzo) in una sottorete e 5.000 istanze (ciascuna con un indirizzo e un IPv4 indirizzo) in un'altra sottorete: 20.000 unità IPv6
  - 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 VPCs connessioni tramite un gateway di transito

VPCs che sono connessi tramite un gateway di transito non contribuiscono a una quota NAU combinata come accade per le connessioni VPCs peer-to-peer.

- VPC 1
  - 50 Network Load Balancer in 2 sottoreti in zone di disponibilità separate: 600 unità NAU
  - 5.000 istanze (ciascuna con un IPv4 indirizzo e un IPv6 indirizzo) in una sottorete e 5.000 istanze (ciascuna con un IPv4 indirizzo e un IPv6 indirizzo) 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 IPv4 indirizzo e un IPv6 indirizzo) in una sottorete e 5.000 istanze (ciascuna con un indirizzo e un IPv4 indirizzo) in un'altra sottorete: 20.000 unità IPv6
  - 100 funzioni Lambda: 600 unità NAU
- Numero totale di NAU per VPC: 21.200 unità
- Quota NAU predefinita per VPC: 64.000 unità

Condividere le sottoreti VPC con altri account

La condivisione di sottoreti VPC consente Account AWS a più utenti di creare le proprie risorse applicative, come EC2 istanze Amazon, database Amazon Relational Database Service (RDS), cluster Amazon Redshift e funzioni, in cloud privati virtuali condivisi e gestiti centralmente (). AWS Lambda VPCs 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 le sottoreti 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. In questo modo si riduce il numero di VPCs account creati e gestiti, utilizzando al contempo account separati per la fatturazione e il controllo degli accessi. Puoi semplificare le topologie di rete interconnettendo sottoreti Amazon VPC condivise utilizzando funzionalità di connettività, come gateway di AWS PrivateLink transito e peering VPC. Per ulteriori informazioni sui vantaggi della condivisione della sottorete VPC, consulta Condivisione di VPC: un nuovo approccio a più account e gestione dei VPC.

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

Indice

- Prerequisiti della sottorete condivisa
- Lavorare con le sottoreti condivise
- Fatturazione e misurazione per il proprietario e i partecipanti
- Responsabilità e autorizzazioni per proprietari e partecipanti
- AWS risorse e sottoreti VPC condivise

Prerequisiti della sottorete condivisa

Questa sezione contiene i prerequisiti per l'utilizzo di sottoreti condivise:

- 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 con AWS Organizations nella Guida per l'utente di AWS RAM .
- Devi creare una condivisione di risorse. Puoi specificare le sottoreti da condividere quando crei 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 .

Lavorare con le sottoreti condivise

Questa sezione descrive come utilizzare le sottoreti condivise nella AWS console e. AWS CLI

Indice

- Condivisione di una sottorete
- Annullamento della condivisione di una sottorete condivisa
- Identificazione del proprietario di una sottorete condivisa

Condivisione di una sottorete

Puoi condividere le sottoreti non predefinite con altri account all'interno dell'organizzazione come riportato qui di seguito. Inoltre, puoi condividere gruppi di sicurezza tra AWS Organizations. Per ulteriori informazioni, consulta Condividi i gruppi di sicurezza con AWS Organizations.

Per condividere una sottorete utilizzando la console

1. Apri la 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 il AWS CLI

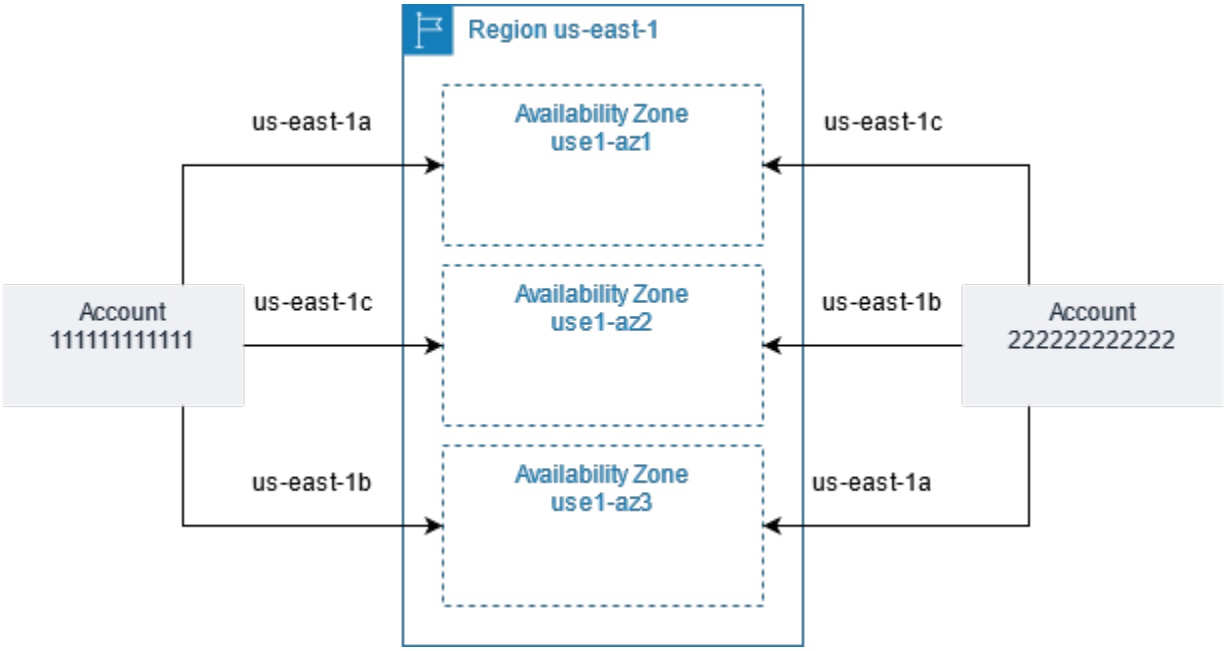
Utilizza i comandi create-resource-share e associate-resource-share.

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`. Utilizza AZ IDs per determinare 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. Apri la 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 il 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. Apri la 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.

Fatturazione e misurazione per il proprietario e i partecipanti

Questa sezione contiene i dettagli di fatturazione e misurazione per coloro che possiedono la sottorete condivisa e per coloro che ci lavorano:

- In un VPC condiviso, ogni partecipante paga per le proprie risorse applicative, tra cui EC2 istanze Amazon, 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, IPv4 gli indirizzi pubblici utilizzati in modalità condivisa VPCs vengono fatturati ai proprietari di VPC. Per ulteriori informazioni sui prezzi IPv4 degli indirizzi pubblici, consulta la scheda IPv4 Indirizzo 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

Questa sezione include dettagli sulle responsabilità e le autorizzazioni per coloro che possiedono la sottorete condivisa (proprietario) e per coloro che la utilizzano (partecipante).

Risorse del proprietario

I proprietari sono responsabili delle risorse VPC di loro proprietà. I proprietari di VPC sono responsabili della creazione, della gestione e dell'eliminazione delle risorse associate a un VPC condiviso. Questi includono sottoreti, tabelle di routing, connessioni di rete e peering ACLs, endpoint gateway, endpoint di interfaccia, endpoint, gateway Internet, Amazon Route 53 Resolver gateway NAT, gateway privati virtuali e allegati ai gateway di transito.

Risorse dei partecipanti

I partecipanti sono responsabili delle risorse VPC di loro proprietà. 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 della sottorete VPC.

Risorse VPC

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

Log di flusso

- I partecipanti possono creare, eliminare o descrivere i log di flusso per le interfacce di rete di loro proprietà in una sottorete VPC condivisa.
- I partecipanti non possono creare, eliminare o descrivere i log di flusso per le interfacce di rete non di loro proprietà in una sottorete VPC condivisa.
- I partecipanti non possono creare, eliminare o descrivere i log di flusso per una sottorete VPC condivisa.

- I proprietari dei VPC possono creare, eliminare o descrivere i log di flusso per le interfacce di rete non di loro proprietà in una sottorete VPC condivisa.
- I proprietari dei VPC possono creare, eliminare o descrivere i log di flusso per una sottorete VPC condivisa.
- 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 e 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.

Elenchi di controllo degli accessi alla rete () NACLs

- I partecipanti non possono creare, eliminare o sostituire NACLs in una sottorete VPC condivisa. I partecipanti possono descrivere i NACLs contenuti creati 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 del VPC non possono utilizzare in altro modo le interfacce di rete di proprietà dei partecipanti, 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 in una sottorete VPC condivisa di loro proprietà. I partecipanti possono lavorare con i gruppi di sicurezza creati dai proprietari del VPC se il proprietario del VPC condivide il gruppo di sicurezza con il partecipante.
- 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 il gruppo di sicurezza predefinito per il VPC, in quanto questo appartiene al proprietario.
- I partecipanti non possono avviare le istanze utilizzando i gruppi di sicurezza non predefiniti di proprietà di altri partecipanti o del proprietario del VPC, a meno che il gruppo di sicurezza non sia stato condiviso con loro.
- I partecipanti possono descrivere i gruppi di sicurezza creati dai partecipanti in una sottorete VPC condivisa. I proprietari del VPC non possono utilizzare in altro modo i gruppi di sicurezza creati dai partecipanti. 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.

VPCs

- I partecipanti non possono modificare i VPCs relativi attributi. Solo il proprietario del VPC può farlo. I partecipanti possono descrivere VPCs, i propri 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.
- I partecipanti possono associare i propri gruppi di sicurezza a un VPC condiviso. Ciò consente al partecipante di utilizzare il gruppo di sicurezza con interfacce di rete elastiche di sua proprietà nel VPC condiviso.

AWS risorse e sottoreti VPC condivise

Le risorse Servizi AWS elencate in questa sezione supportano le risorse 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 ECS
- Amazon ElastiCache (sistema operativo Redis)
- Amazon EFS
- 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
- Amazon MQ con Apache MQ (non Rabbit MQ)
- MSK Amazon
- AWS Network Manager
  - AWS WAN nel cloud
  - Strumento di analisi degli accessi alla rete
  - Reachability Analyzer
- OpenSearch Servizio Amazon
- 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

L'elenco in questa sezione rappresenta il nostro maggiore sforzo di documentare quali servizi supportano l'avvio di risorse in sottoreti VPC condivise. Potrebbero esserci altri servizi non elencati che supportano l'avvio di risorse in sottoreti VPC condivise. Consigliamo di inviare commenti in caso di domande su risorse non presenti in questo elenco.

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 offre AWS servizi, infrastrutture e modelli operativi nativi praticamente a qualsiasi data center, spazio di co-ubicazione o struttura locale.
- Le zone Wavelength consentono agli sviluppatori di creare applicazioni che offrono latenze molto basse a dispositivi 5G e utenti finali. Wavelength implementa servizi di elaborazione e archiviazione AWS standard ai margini delle reti 5G dei gestori di telecomunicazioni.

AWS gestisce data center state-of-the-art ad alta disponibilità. 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.

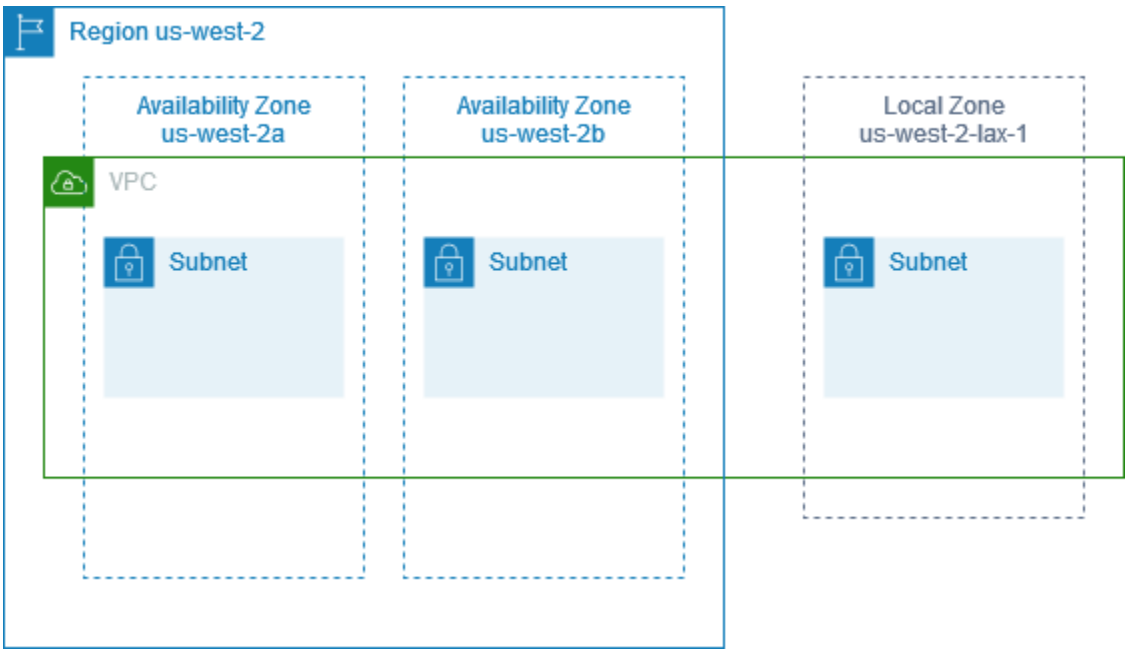
Sottoreti nelle AWS Local Zones

AWS Le Local Zones ti consentono di avvicinare le risorse agli utenti e di connetterti senza problemi all'intera gamma di servizi della AWS regione, utilizzando set di strumenti APIs e 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 a points-of-presence (PoPs) senza attraversare la regione madre della zona locale, consentendo l'accesso all'elaborazione 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 e la rete. ACLs
- 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 lo supporta IPv6, puoi richiedere gli indirizzi IP IPv6 forniti da Amazon e associarli al gruppo di confine di rete per un VPC nuovo o esistente. Per l'elenco delle Local Zones supportate IPv6, consulta Considerazioni nella AWS Local Zones User Guide

- 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 AWS Direct Connect posizione in una regione. Il data center locale dispone di una AWS Direct Connect connessione alla AWS Direct Connect posizione.

> **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. È possibile visualizzare il VPC per la sottorete nella pagina dei dettagli della subnet in Amazon Virtual Private Cloud Console, oppure utilizzare il comando describe-subnets.

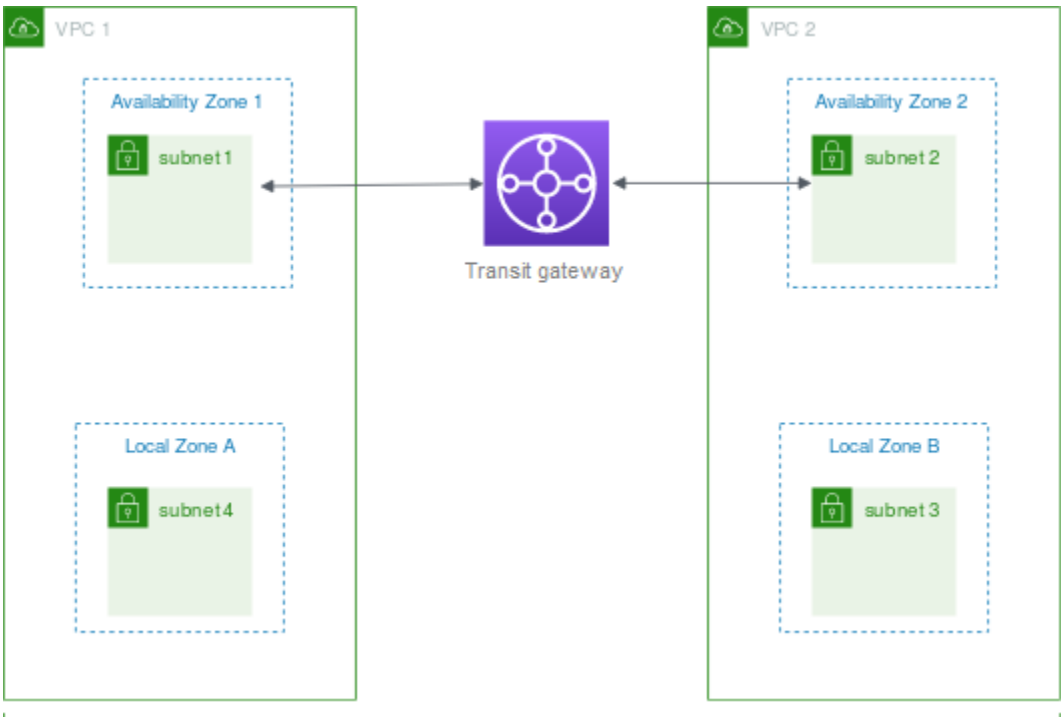
  Per informazioni su come creare un gateway virtuale privato, consulta Creazione di un gateway di destinazione nella Guida per l'utente di AWS Site-to-Site VPN .
- Una connessione Direct Connect. Per prestazioni di latenza ottimali, ti AWS consigliamo di utilizzare la posizione Direct Connect più vicina alla zona locale a cui estenderai la 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 .
- Un'interfaccia virtuale privata sulla connessione dalla AWS Direct Connect posizione al data center locale. 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 delle sottoreti dell'area locale che hanno l'altro CIDR VPC come destinazione e l'ID dell'interfaccia di rete per il collegamento del gateway di transito alla VPN 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
VPC 1 CIDR	*local*
VPC 2 CIDR	*vpc1-attachment-network-interface-id*

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

Destinazione	Target
VPC 2 CIDR	*local*
VPC 1 CIDR	*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
VPC 1 CIDR	*Attachment for VPC 1*	propagata
VPC 2 CIDR	*Attachment for 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 estendere un cloud privato virtuale (VPC) a una o più Wavelength Zone e quindi utilizzare

risorse AWS come le EC2 istanze Amazon per eseguire applicazioni che richiedono una latenza estremamente bassa e connettersi alla regione. Servizi AWS

Per utilizzare le zone Wavelength, devi prima scegliere la zona. Creare quindi una sottorete nella zona Wavelength. Puoi creare EC2 istanze Amazon, volumi Amazon EBS e sottoreti Amazon VPC e carrier gateway in Wavelength Zones. Puoi anche utilizzare servizi che orchestrano o funzionano con EBS e VPC EC2, come Amazon EC2 Auto Scaling, cluster Amazon EKS, cluster Amazon ECS, Amazon Systems EC2 Manager, Amazon e. CloudWatch AWS CloudTrail AWS CloudFormation I servizi in Wavelength fanno parte di un VPC connesso tramite una connessione affidabile e ad alta larghezza di banda a una regione per AWS un facile accesso a servizi tra cui 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' EC2 istanza in una sottorete in una Wavelength Zone, le si assegna un indirizzo IP dell'operatore. 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 IPv4 indirizzi, set di opzioni DHCP e rete. ACLs
- 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

EC2 le istanze che si trovano in zone Wavelength diverse nello stesso VPC non possono comunicare tra loro. Se è necessaria la comunicazione da Wavelength Zone a Wavelength Zone, si consiglia di utilizzarne più VPCs di una AWS , una per ogni Wavelength Zone. È possibile utilizzare un gateway di transito per connettere il. VPCs Questa configurazione consente la comunicazione tra istanze nelle zone Wavelength.

Percorsi di traffico da Wavelength Zone a Wavelength Zone 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”. Usa il describe-availability-zonescomando per trovare la zona principale.
- Un gateway di transito. Il gateway di transito collega il VPCs. 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”.

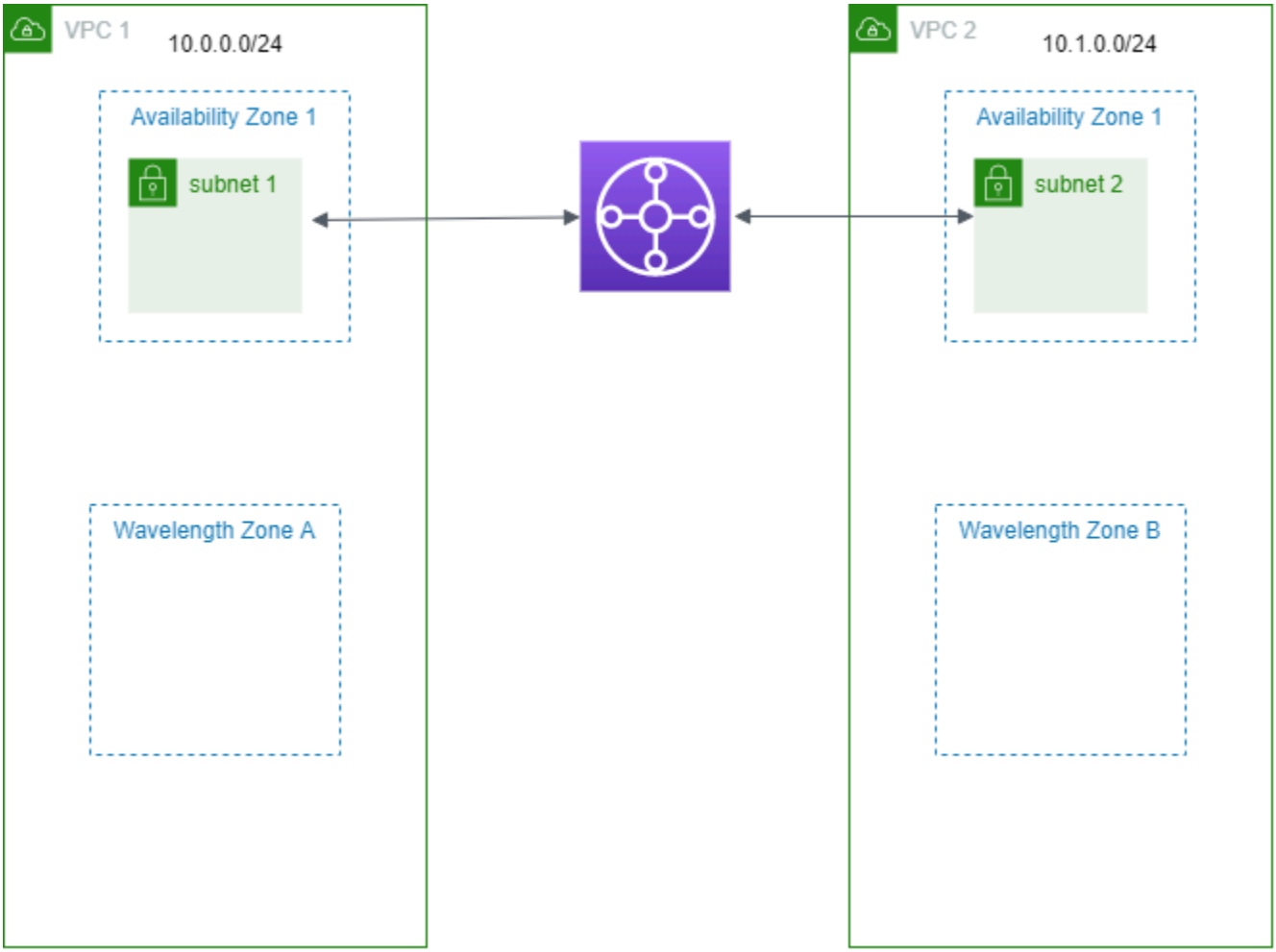
  Nell'esempio, la tabella di instradamento per VPC 1 ha la seguente voce:

Destinazione	Target

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



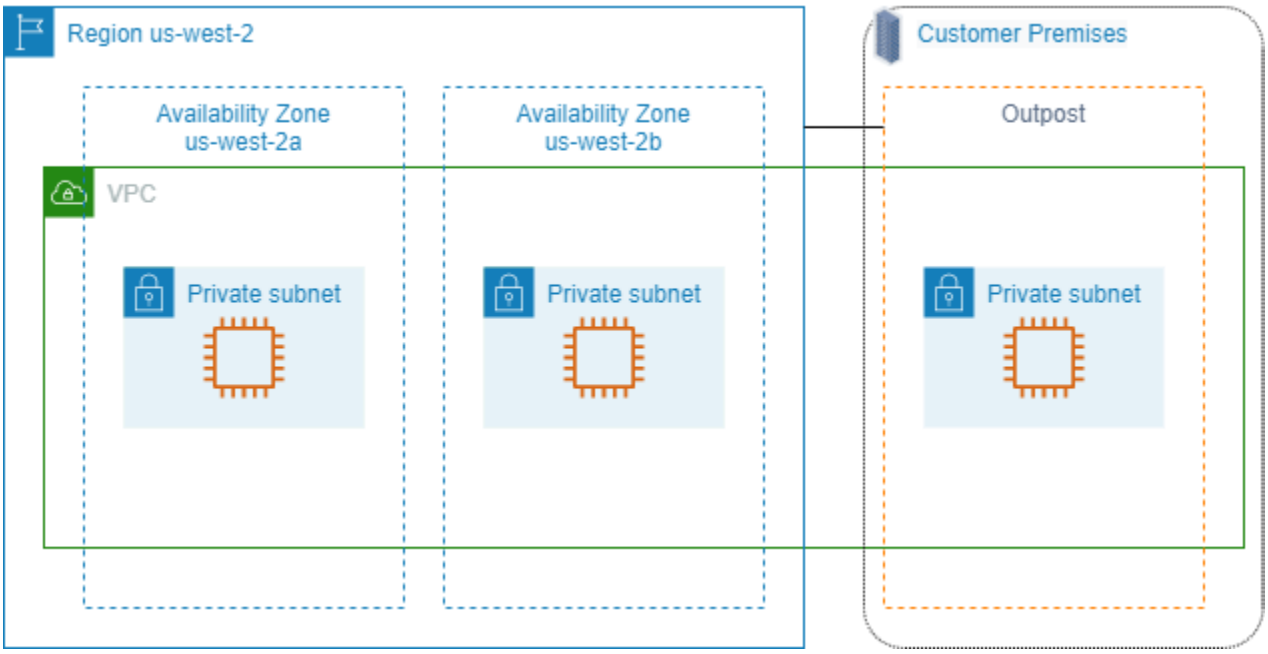
Sottoreti in AWS Outposts

AWS Outposts ti offre la stessa infrastruttura AWS hardware, gli stessi servizi e gli stessi strumenti per creare ed eseguire le tue applicazioni on-premise e nel cloud. APIs AWS Outposts è ideale per carichi di lavoro che richiedono un accesso a bassa latenza ad applicazioni o sistemi locali e per carichi di lavoro che devono archiviare ed elaborare i dati localmente. Per ulteriori informazioni su, vedere. AWS OutpostsAWS Outposts

Un VPC si estende su 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.

Le seguenti regole si applicano 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, è necessario terminare EC2 le istanze ed eliminare i sistemi di bilanciamento del carico, i gateway NAT, gli allegati VPC del gateway di transito e gli endpoint VPC di interfaccia.

> **Note**
>
> Se hai creato un log di flusso per il VPC che stai eliminando, tieni presente che i log di flusso per l'eliminazione VPCs vengono infine rimossi automaticamente.

Indice

- Eliminazione di un VPC tramite la console
- Eliminazione di un VPC utilizzando la riga di comando

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
- Rete ACLs
- Tabelle di instradamento
- Gruppi di sicurezza
- Sottoreti

Per eliminare il VPC tramite la console

1. Apri la EC2 console Amazon 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
4. Nel pannello di navigazione, scegli Your VPCs.
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 Site-to-Site VPN, puoi selezionare l'opzione per eliminarla. Se prevedi 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 Site-to-Site connessione 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. È inoltre necessario eliminare o scollegare tutte le risorse VPC create, ad esempio sottoreti, gruppi di sicurezza, ACLs rete, tabelle di routing, gateway Internet e gateway Internet solo in uscita. 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. Eliminare il gruppo di sicurezza utilizzando il delete-security-groupcomando.

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

2. Eliminare ogni ACL di rete utilizzando il delete-network-aclcomando.

```
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. Eliminare ogni tabella di routing personalizzata utilizzando il delete-route-tablecomando.

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

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

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-id --vpc-id vpc-id
```

6. Elimina il tuo gateway Internet utilizzando il delete-internet-gatewaycomando.

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-id
```

7. [VPC dual stack] Elimina il gateway Internet di sola uscita utilizzando il comando -gateway. delete-egress-only-internet

```
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
```

Generare infrastructure-as-code dalle azioni della console VPC con Console-to-Code

La console fornisce un percorso guidato per creare risorse e testare prototipi. Se vuoi creare le stesse risorse su larga scala, avrai bisogno del codice di automazione. Console-to-Code è una funzionalità di Amazon Q Developer che può essere utile per iniziare a usare il codice di automazione. Console-to-Code registra le operazioni della console, inclusi i valori predefiniti e i parametri compatibili. Utilizza quindi l'IA generativa per suggerire il codice nel formato infrastructure-as code (IaC) preferito per le operazioni desiderate. Poiché il flusso di lavoro della console assicura che i valori dei parametri specificati siano validi insieme, il codice generato utilizzando Console-to-Code ha valori di parametro compatibili. Puoi usare il codice come punto di partenza, personalizzandolo in seguito al fine di renderlo pronto per la produzione per il tuo caso d'uso specifico.

Ad esempio, con Console-to-Code puoi registrarti utilizzando la console VPC per creare sottoreti, gruppi di sicurezza, NACL, una tabella di routing personalizzata e un gateway Internet così da generare un codice in formato JSON AWS CloudFormation. Quindi, puoi copiare quel codice e personalizzarlo per utilizzarlo nel tuo modello AWS CloudFormation.

Al momento Console-to-Code può generare infrastructure-as-code (IaC) nelle seguenti lingue e formati:

- Java CDK
- Python CDK
- TypeScript CDK
- JSON CloudFormation
- YAML CloudFormation

Per ulteriori informazioni e istruzioni su come utilizzare Console-to-Code, consultare Automazione dei servizi AWS con Amazon Q Developer Console-to-Code nella Guida per l'utente Amazon Q Developer.

Sottoreti per il VPC

una sottorete è un intervallo di indirizzi IP nel VPC; È possibile creare AWS risorse, ad esempio EC2 istanze, in sottoreti specifiche.

Indice

- Nozioni di base sulla sottorete
- Sicurezza della sottorete
- Creazione di una sottorete
- Aggiungere o rimuovere un blocco IPv6 CIDR dalla sottorete
- Modifica dell'attributo di assegnazione di indirizzi IP della sottorete
- Prenotazioni della CIDR per la sottorete
- Configurare le tabelle di routing
- Procedura guidata di instradamento middlebox
- Eliminare una sottorete

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 dai guasti di una singola zona di disponibilità.

Indice

- Intervallo di indirizzi IP di sottorete
- Tipi di sottorete
- Diagramma sottorete
- Routing della sottorete
- Impostazioni sottorete

Intervallo di indirizzi IP di sottorete

Quando crei una sottorete, devi specificare i relativi indirizzi IP, a seconda della configurazione del VPC:

- IPv4 solo: la sottorete ha un blocco IPv4 CIDR ma non ha un IPv6 blocco CIDR. Le risorse in una sottorete IPv4 -only devono comunicare tramite. IPv4
- Dual stack: la sottorete ha sia un blocco CIDR che un blocco IPv4 CIDR. IPv6 Il VPC deve avere sia un blocco IPv4 CIDR che un blocco CIDR. IPv6 Le risorse in una sottorete dual-stack possono comunicare tramite e. IPv4 IPv6
- IPv6 solo: la sottorete ha un blocco IPv6 CIDR ma non ha un blocco CIDR. IPv4 Il VPC deve avere un blocco IPv6 CIDR. Le risorse in una sottorete IPv6 -only devono comunicare tramite. IPv6

> **Note**
>
> Alle risorse nelle sottoreti IPv6 -only vengono assegnati IPv4 indirizzi locali del collegamento dal blocco CIDR 169.254.0.0/16. Questi indirizzi vengono utilizzati per comunicare con servizi disponibili solo nel VPC. Per esempi, consulta Link-local address nella Amazon EC2 User Guide.

Per ulteriori informazioni, consulta Indirizzamento IP per le tue VPCs sottoreti.

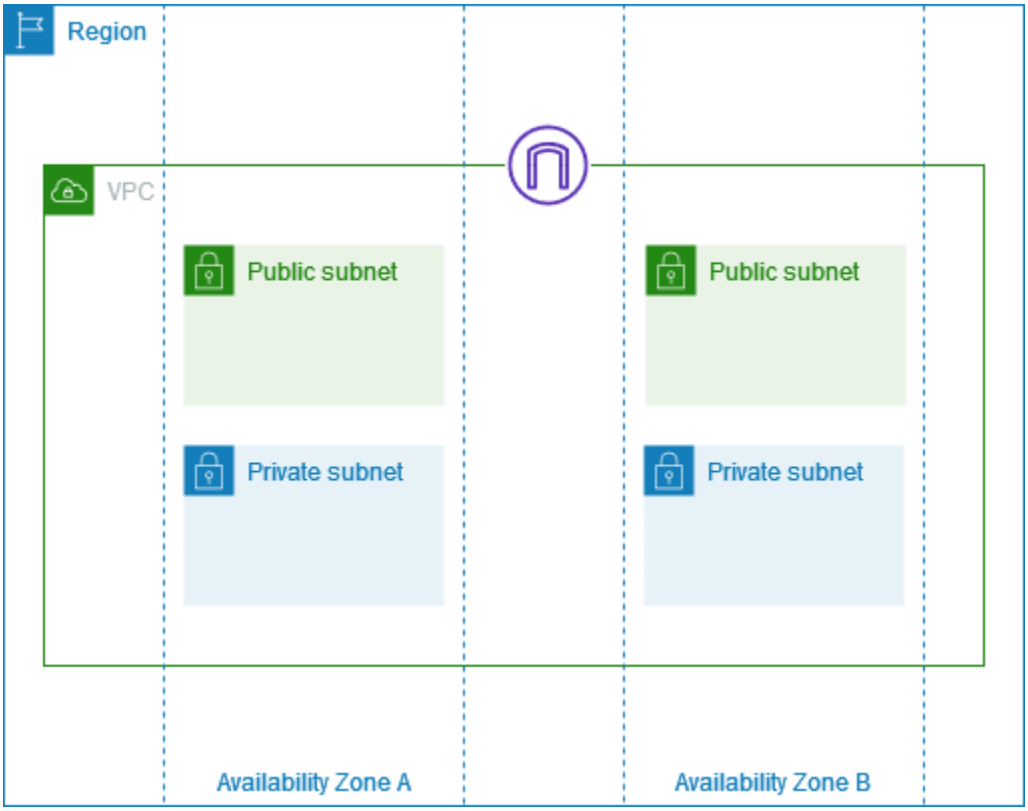
Tipi di sottorete

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.
- Subnet solo VPN: la sottorete ha un percorso verso una Site-to-Site connessione VPN attraverso 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 un VPC con sottoreti in due zone di disponibilità e un gateway Internet. Ogni zona di disponibilità ha una sottorete pubblica e una privata.



Per i diagrammi che mostrano le sottoreti in Local Zones e Wavelength Zones, vedere How AWS Local Zones work e How works. AWS Wavelength

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 a un'interfaccia di rete creata in quella sottorete viene assegnato un indirizzo pubblico e, se applicabile, un indirizzo. IPv4 IPv6 Ciò include l'interfaccia di rete principale (ad esempio eth0) creata per un'istanza quando si avvia un'istanza in quella 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:

- Assegnazione automatica delle impostazioni IP: consente di configurare le impostazioni IP di assegnazione automatica per richiedere automaticamente un pubblico IPv4 o un IPv6 indirizzo per una nuova interfaccia di rete in questa sottorete.
- Impostazioni RBN (Resource-based Name): consentono di specificare il tipo di nome host per le EC2 istanze in questa sottorete e di configurare la modalità di gestione delle query di record DNS A e AAAA. Per ulteriori informazioni, consulta i tipi di hostname delle EC2 istanze Amazon nella Amazon EC2 User Guide.

Sicurezza della sottorete

Per proteggere AWS le tue risorse, ti consigliamo di utilizzare sottoreti private. Usa un host bastion o un dispositivo NAT per fornire l'accesso a Internet a risorse, come le EC2 istanze, 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 per le risorse associate, come le istanze. EC2 La rete ACLs consente o nega 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. Tuttavia, è possibile utilizzare la rete ACLs se si desidera un ulteriore livello di sicurezza. Per ulteriori informazioni, consulta the section called “Confronta i gruppi di sicurezza e la rete ACLs”.

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 predefinito o creare una rete personalizzata ACLs e associarla alle sottoreti. Per ulteriori informazioni, consulta Controllo del traffico della sottorete con le liste di controllo degli accessi alla 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 IPv4 CIDR per la sottorete dall'intervallo del VPC. Facoltativamente, puoi specificare un blocco IPv6 CIDR per una sottorete se esiste un blocco IPv6 CIDR associato al VPC. Per ulteriori informazioni, consulta Indirizzamento IP per le tue VPCs sottoreti.
- Se crei una sottorete IPv6 solo per la rete, tenete presente quanto segue. Un' EC2 istanza avviata in una sottorete IPv6 -only riceve un IPv6 indirizzo ma non un indirizzo. IPv4 Tutte le istanze avviate in una sottorete IPv6 -only devono essere istanze create sul sistema Nitro.
- Per creare la sottorete in una zona locale o in una zona Wavelength, è necessario abilitare la zona. Per ulteriori informazioni, consulta Regioni e zone nella Amazon EC2 User Guide.

Per aggiungere una sottorete al VPC

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli 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 il blocco IPv4 CIDR, seleziona Inserimento manuale per inserire un blocco IPv4 CIDR per la sottorete (ad esempio**`10.0.1.0/24`**) oppure seleziona 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 il blocco IPv6 CIDR, seleziona Input manuale per scegliere il CIDR del VPC in cui desideri creare una sottorete. IPv6 Questa opzione è disponibile solo se al VPC è associato un blocco IPv6 CIDR. 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 blocco IPv6 CIDR VPC.
10. Per il blocco CIDR della IPv6 sottorete, scegli un CIDR per la sottorete 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 IPv6 maschere di rete sono comprese tra /44 e /64 in 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.
- Modificare il comportamento di assegnazione di indirizzi IP. È possibile specificare se le istanze avviate nella sottorete ricevono un IPv4 indirizzo pubblico, un IPv6 indirizzo o entrambi. Per ulteriori informazioni, consulta Modifica dell'attributo di assegnazione di indirizzi IP della sottorete.
- Modifica le impostazioni del nome basato sulle risorse (RBN). Per ulteriori informazioni, consulta i tipi di hostname delle EC2 istanze Amazon.
- Crea o modifica la tua rete ACLs. Per ulteriori informazioni, consulta Controllo del traffico della sottorete con le liste di controllo degli accessi alla rete.
- Condividere la sottorete con altri account. Per ulteriori informazioni, consulta ???.

Aggiungere o rimuovere un blocco IPv6 CIDR dalla sottorete

Puoi associare un blocco IPv6 CIDR a una sottorete esistente nel tuo VPC. Alla sottorete non deve essere associato un blocco IPv6 CIDR esistente.

Se non desideri più il IPv6 supporto nella tua sottorete, ma desideri continuare a utilizzare la sottorete per creare e comunicare con IPv4 le risorse, puoi rimuovere il blocco CIDR. IPv6

Prima di poter rimuovere un blocco IPv6 CIDR, è necessario innanzitutto annullare l'assegnazione di tutti IPv6 gli indirizzi assegnati a qualsiasi istanza nella sottorete.

Per aggiungere o rimuovere un blocco CIDR a una IPv6 sottorete

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Subnets (Sottoreti).
3. Seleziona la tua sottorete e scegli Azioni, Modifica. IPv6 CIDRs
4. Per aggiungere un CIDR, scegli Aggiungi IPv6 CIDR, scegli un blocco CIDR VPC, inserisci un blocco CIDR di sottorete e 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 della IPv6 netmask sono comprese tra /44 e /64 in incrementi di /4.
5. Per rimuovere un CIDR, trova il blocco CIDR e scegli Rimuovi. IPv6
6. Seleziona Salva.

Per associare un blocco IPv6 CIDR a una sottorete utilizzando AWS CLI

Utilizza il comando associate-subnet-cidr-block.

Per dissociare un blocco IPv6 CIDR da una sottorete utilizzando AWS CLI

Utilizza il comando disassociate-subnet-cidr-block.

Modifica dell'attributo di assegnazione di indirizzi IP della sottorete

Per impostazione predefinita, le sottoreti non predefinite hanno l'attributo di indirizzamento IPv4 pubblico impostato su e le `false` sottoreti predefinite hanno questo attributo impostato su. `true` Un'eccezione è una sottorete non predefinita creata dalla procedura guidata di EC2 avvio dell'istanza di Amazon: la procedura guidata imposta l'attributo su. `true` L'attributo è modificabile tramite la console Amazon VPC.

Per impostazione predefinita, tutte le sottoreti hanno l'attributo di indirizzamento impostato su. IPv6 `false` L'attributo è modificabile tramite la console Amazon VPC. Se si abilita l'attributo di IPv6 indirizzamento per la sottorete, le interfacce di rete create nella sottorete ricevono un IPv6

indirizzo dall'intervallo della sottorete. Le istanze avviate nella sottorete ricevono un IPv6 indirizzo sull'interfaccia di rete principale.

La sottorete deve avere un blocco CIDR associato IPv6 .

> **Note**
>
> Se abiliti la funzionalità di IPv6 indirizzamento per la sottorete, l'interfaccia o l'istanza di rete riceve un IPv6 indirizzo solo se è stata creata utilizzando una versione `2016-11-15` o successiva dell' EC2 API Amazon. La EC2 console Amazon utilizza l'ultima versione dell'API.

Per modificare il comportamento di assegnazione di indirizzi IP della sottorete

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Subnets (Sottoreti).
3. Selezionare la sottorete e scegliere Actions (Operazioni), Edit subnet (Modifica sottorete).
4. La casella di controllo Abilita l'assegnazione automatica IPv4 dell'indirizzo pubblico, se selezionata, richiede un IPv4 indirizzo pubblico per tutte le istanze avviate nella sottorete selezionata. Selezionare o deselezionare la casella di controllo in base alle Esigenze, quindi selezionare Save (Salva).
5. La casella di controllo Abilita assegnazione automatica IPv6 degli indirizzi, se selezionata, richiede un IPv6 indirizzo 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

Utilizza il comando modify-subnet-attribute.

Prenotazioni della CIDR per la sottorete

Una prenotazione CIDR di sottorete è un intervallo di IPv4 o IPv6 indirizzi che metti da parte in modo da non AWS poterli assegnare alle interfacce di rete. Ciò consente di riservare blocchi IPv4 IPv6 CIDR (chiamati anche «prefissi») da utilizzare con le 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 EC2 rete Amazon nella Amazon User Guide. EC2
- 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 possono essere assegnati AWS alle interfacce di rete. 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.

Indice

- Come lavorare con le prenotazioni del CIDR della sottorete tramite la console
- Lavora con le prenotazioni CIDR di sottorete utilizzando il AWS CLI

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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli 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 IPv4 CIDR, scegli IPv4Aggiungi prenotazione CIDR. IPv4 Scegli il tipo di prenotazione, inserisci l'intervallo CIDR e scegli Add (Aggiungi).
   - Per aggiungere una prenotazione IPv6 CIDR IPv6, scegli Aggiungi IPv6 prenotazione CIDR. 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-reservationper creare una prenotazione CIDR su 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-reservationsper visualizzare i dettagli di una prenotazione CIDR su 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-reservationper eliminare una prenotazione CIDR su 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
- Tabelle di routing di sottoreti
- Tabelle di routing del gateway
- Priorità della route
- Opzioni di routing di esempio
- Modificare la tabella di routing di una sottorete
- Sostituzione della tabella di instradamento principale
- Controlla il traffico che entra nel tuo VPC con una tabella di routing del gateway
- Sostituzione o ripristino della destinazione per una route locale
- Risoluzione dei problemi di raggiungibilità

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 le opzioni di routing Site-to-Site VPN nella Guida per l'utente della Site-to-Site VPN.
- 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
- Tabella di routing principale
- Tabelle di routing personalizzate
- Associazione di tabelle di routing della sottorete

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 del percorso è`0.0.0.0/0`, che rappresenta tutti gli IPv4 indirizzi. 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 vengono trattati separatamente. Ad esempio, un percorso con un CIDR di destinazione `0.0.0.0/0` non include automaticamente tutti gli IPv6 indirizzi. È necessario creare un percorso con un CIDR di destinazione `::/0` per tutti gli IPv6 indirizzi.

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 tuo VPC ha più di un blocco IPv4 CIDR, le tabelle di routing contengono una route locale per ogni IPv4 blocco CIDR. Se hai associato un blocco IPv6 CIDR al tuo VPC, le tabelle di routing contengono una route locale per IPv6 il blocco CIDR. 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 IPv4 IPv6 CIDR di una sottorete nel tuo 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 puoi aggiungere percorsi a IPv4 indirizzi che corrispondono esattamente o appartengono a 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 di questo intervallo per servizi accessibili solo da EC2 istanze, 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 puoi aggiungere percorsi a IPv6 indirizzi che corrispondono esattamente o appartengono a 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 dei servizi. AWS Ad esempio, Amazon EC2 utilizza gli indirizzi di questo intervallo per servizi accessibili solo da EC2 istanze, 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, consulta the section called “Routing per un'appliance middlebox”.

Esempio

Nell'esempio seguente, supponiamo che il VPC abbia sia IPv4 un blocco CIDR che un blocco CIDR. IPv6 IPv4 e IPv6 il traffico vengono trattati separatamente, come illustrato nella seguente tabella di percorso.

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

- IPv4 il traffico da instradare all'interno del VPC (10.0.0.0/16) è coperto dal Local percorso.
- IPv6 il traffico da instradare all'interno del VPC (2001:db 8:1234:1 a00: :/56) è coperto dal Local percorso.
- Il percorso per 172.31.0.0/16 invia il traffico a una connessione peering.
- Il percorso per tutto il IPv4 traffico (0.0.0.0/0) invia il traffico a un gateway Internet. Pertanto, tutto IPv4 il traffico, ad eccezione del traffico all'interno del VPC e della connessione peering, viene indirizzato al gateway Internet.
- Il percorso per tutto il IPv6 traffico (:: /0) invia il traffico a un gateway Internet solo in uscita. Pertanto, tutto IPv6 il traffico, 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.

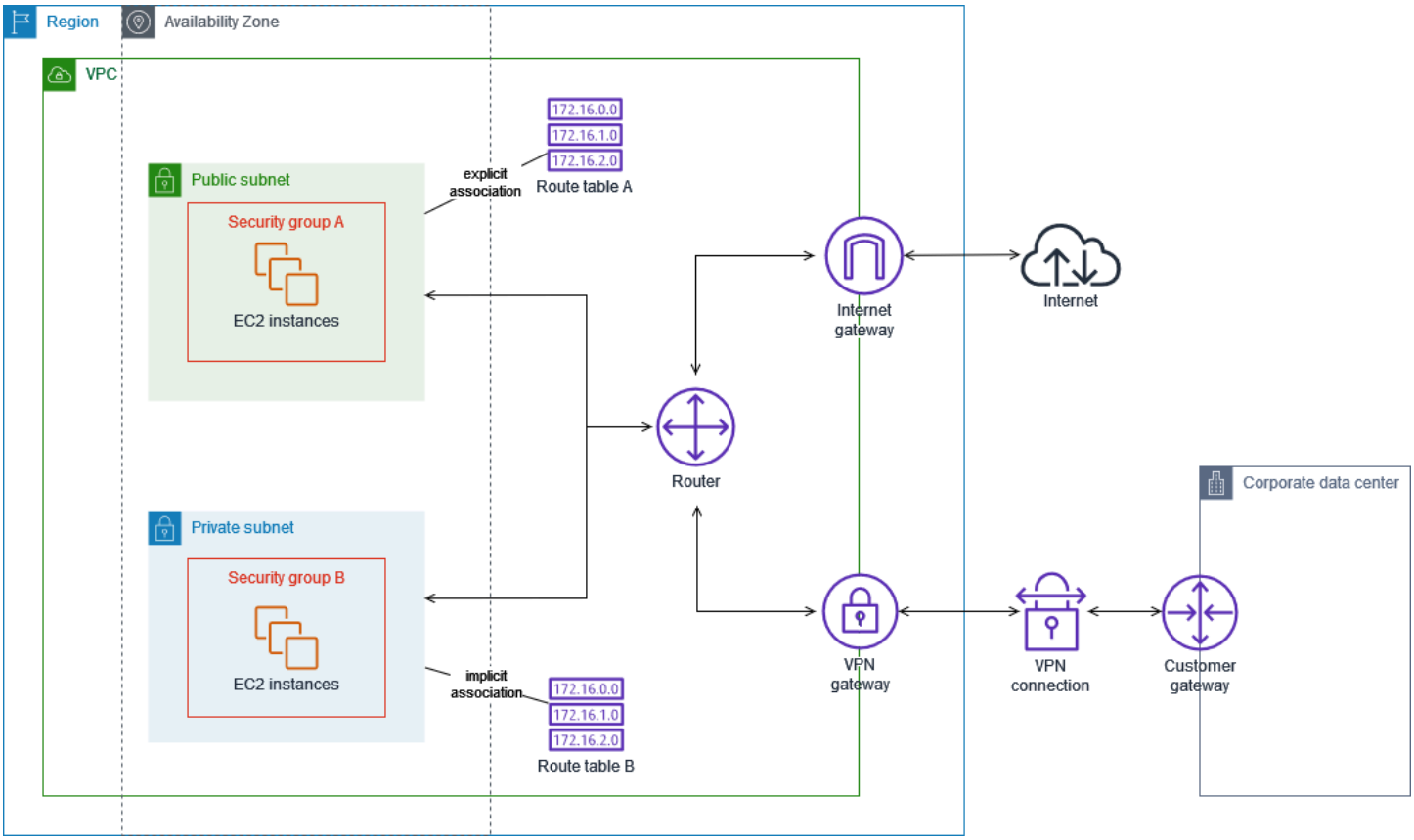
Associazione di tabelle di routing della sottorete

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 VPCs associate a Outposts possono avere un tipo di destinazione aggiuntivo di 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
VPC CIDR	Locale
0.0.0.0/0	*igw-id*

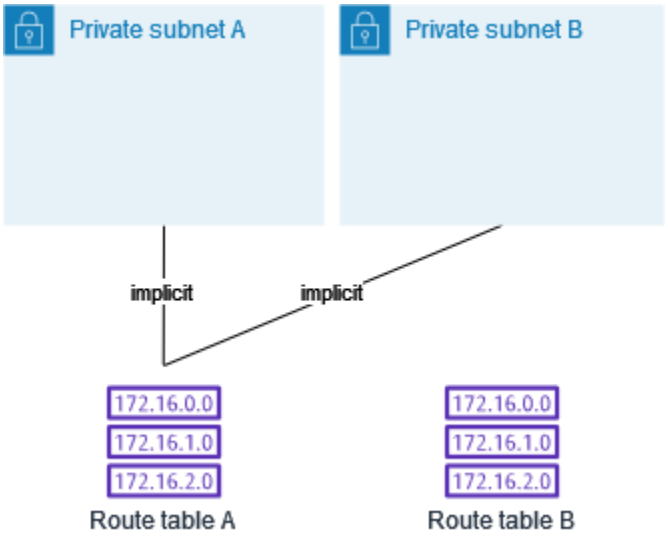
La tabella di instradamento B è la tabella di instradamento principale. È associato implicitamente alla sottorete privata. Ha un percorso che invia tutto il traffico al gateway privato virtuale ma nessun percorso verso il gateway Internet, che è ciò che rende la sottorete una sottorete solo VPN. Se crei 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
VPC CIDR	Locale
0.0.0.0/0	*vgw-id*

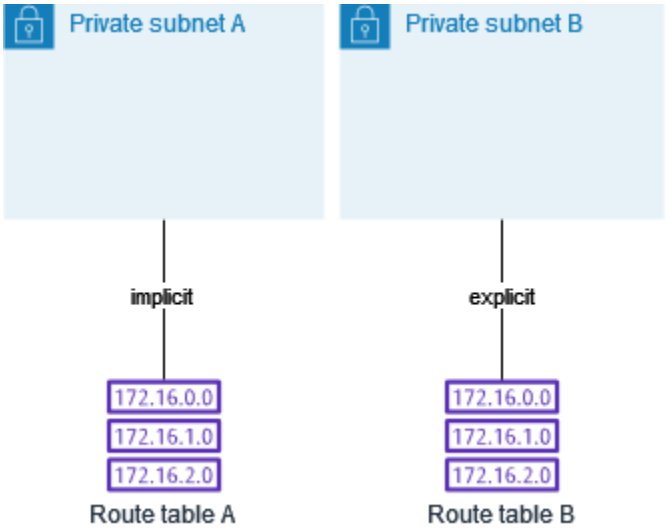
Esempio 2: Sostituzione della tabella di instradamento principale

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.

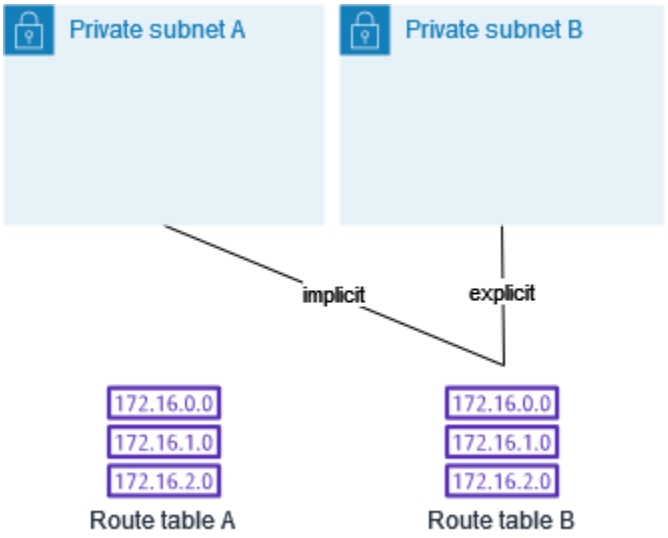
Il diagramma seguente mostra due sottoreti e due tabelle di routing. La sottorete A è associata implicitamente alla tabella di routing A, la tabella di routing principale. La sottorete B è associata implicitamente alla tabella di routing A. La tabella di routing B, una tabella di routing personalizzata, 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.

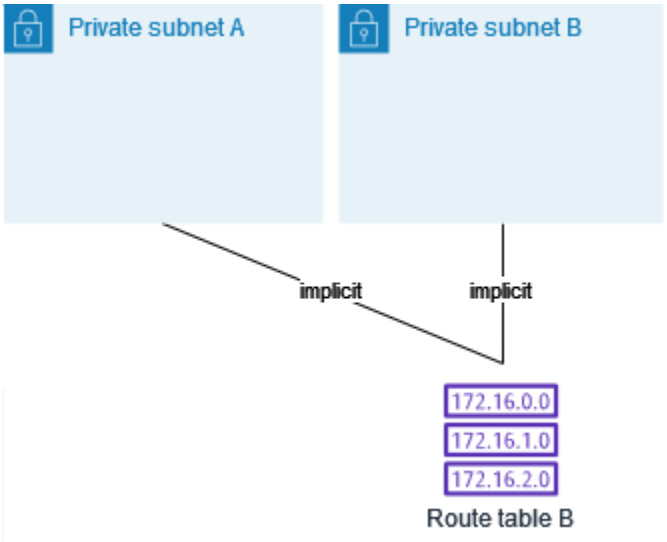


Tabelle di routing del gateway

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
- Regole e considerazioni

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 IPv4 IPv6 CIDR del tuo VPC. In questo caso, sostituisci il target della route locale predefinita.
- L'intero blocco IPv4 IPv6 CIDR di una sottorete nel tuo 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.

L'elenco seguente mostra un riepilogo della priorità di route con collegamenti alle sezioni successive contenenti informazioni più dettagliate ed esempi:

1. Prefisso più lungo (ad esempio, 10.10.2.15/32 ha la priorità rispetto a 10.10.2.0/24)
2. Route statiche (come peering VPC e connessioni gateway Internet)
3. Route con elenco di prefissi
4. Route propagate
   a. Percorsi Direct Connect BGP (route dinamiche)
   b. Route statiche VPN
   c. Route VPN BGP (route dinamiche) (come i gateway privati virtuali)

Corrispondenza prefisso più lungo

I percorsi IPv4 e gli IPv6 indirizzi o i blocchi CIDR sono indipendenti l'uno dall'altro. Utilizziamo il percorso più specifico che corrisponde al IPv4 traffico o al IPv6 traffico per determinare come indirizzare il traffico.

L'esempio seguente di tabella di routing di sottorete contiene un percorso per il traffico IPv4 Internet (`0.0.0.0/0`) che punta a un gateway Internet e un percorso per il `172.31.0.0/16` IPv4 traffico 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 di route per route statiche e propagate dinamicamente

Se hai collegato un gateway privato virtuale al tuo VPC e abilitato la propagazione delle route sulla tabella di routing della subnet, le route che rappresentano la tua connessione Site-to-Site VPN vengono automaticamente visualizzate come route propagate nella tabella di routing.

Se la destinazione di una route propagata è identica alla destinazione di una statica, quest'ultima ha la priorità. Le seguenti risorse utilizzano route statiche:

- 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

Priorità di route per gli elenchi di prefissi

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.

Opzioni di routing di esempio

I seguenti argomenti descrivono il routing per specifici gateway o connessioni nel VPC.

Indice

- Routing a un Internet gateway
- Routing a un dispositivo NAT
- Routing a un gateway virtuale privato
- Instradamento verso un gateway locale AWS Outposts
- Routing a una connessione peering VPC
- Routing a un endpoint VPC del gateway
- Routing a un Internet gateway egress-only

- Routing per un gateway di transito
- Routing per un'appliance middlebox
- Routing mediante un elenco di prefissi
- Routing a un endpoint Gateway Load Balancer

Routing a un Internet gateway

Puoi rendere pubblica una sottorete aggiungendo una route nella tabella di instradamento della sottorete a un Internet gateway. A tale scopo, crea e collega un gateway Internet al tuo VPC, quindi aggiungi un percorso con una destinazione per il IPv4 traffico o `0.0.0.0/0` `::/0` per il IPv6 traffico e una destinazione dell'ID del gateway Internet ()`igw-xxxxxxxxxxxxxxxxx`.

Destinazione	Target
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Per ulteriori informazioni, consulta Abilitazione dell'accesso di VPC a Internet tramite 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. Quindi aggiungete un percorso per la tabella di routing della sottorete privata che indirizza il traffico IPv4 Internet (`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*

Puoi quindi creare e configurare la tua Site-to-Site connessione 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 privato virtuale non supporta il IPv6 traffico. Tuttavia, supportiamo il IPv6 traffico indirizzato verso una AWS Direct Connect connessione attraverso un gateway privato virtuale. Per ulteriori informazioni, consulta la Guida per l'utente AWS Direct Connect.

Instradamento 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
- Abilita il traffico tra sottoreti nello stesso VPC su Outposts

Abilita il traffico tra le sottoreti Outpost e la rete locale

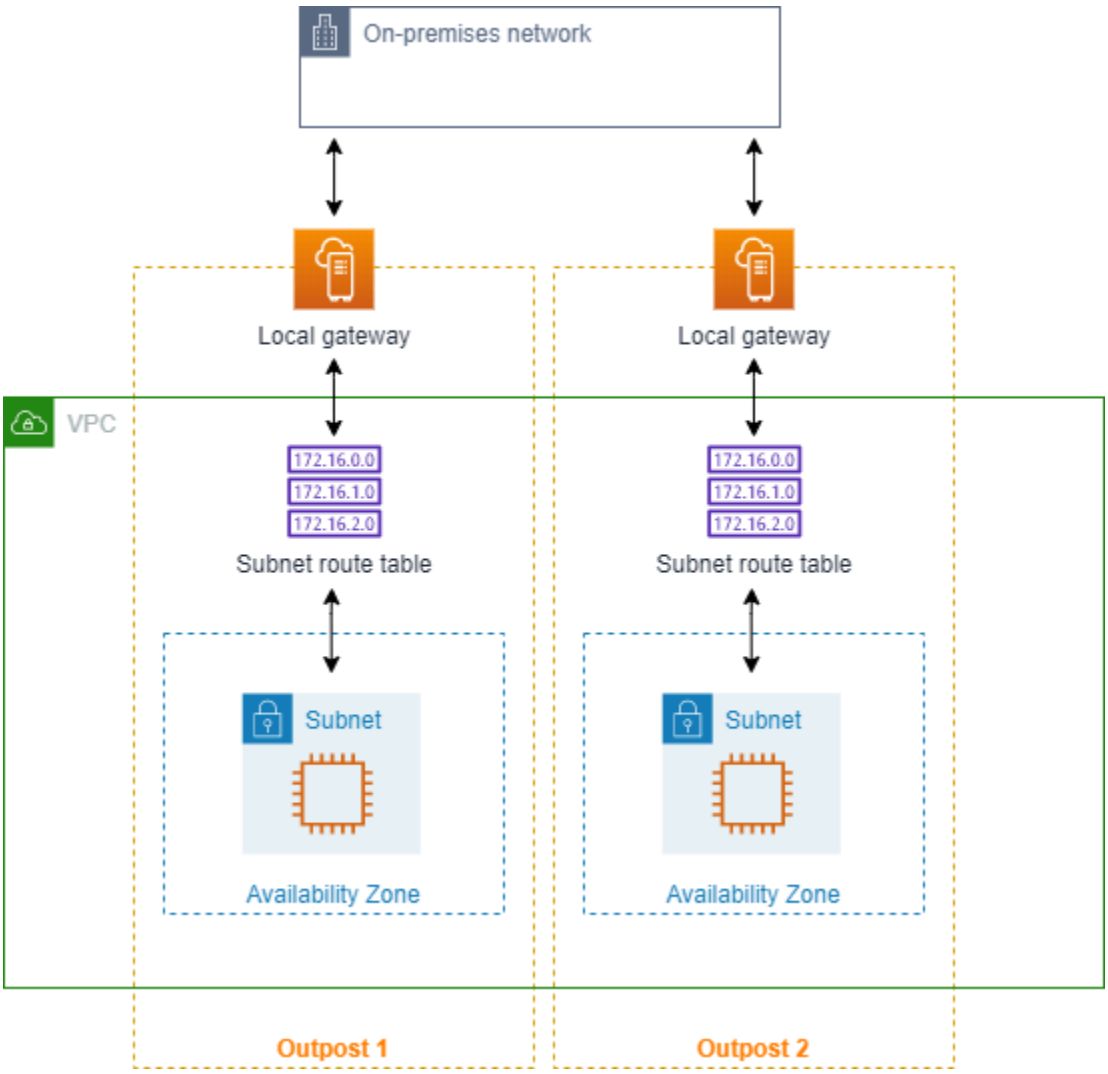
Le sottoreti VPCs associate a AWS Outposts possono avere un tipo di destinazione aggiuntivo di gateway locale. Considera il caso in cui desideri che il gateway locale instradi il traffico con un indirizzo di destinazione 192.168.10.0/24 alla rete del cliente. Per farlo, aggiungi la route seguente con 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 Multi-availability Zone (AZ) per le applicazioni locali in esecuzione sui rack Outposts stabilendo la connettività tra rack Outposts ancorati a diversi rack Outposts. AZs



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 del percorso deve corrispondere all'intero IPv4 blocco della sottorete nel tuo 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 un gruppo di sicurezza. IDs
- 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 VPCs che consente di instradare il traffico tra di loro utilizzando indirizzi privati. IPv4 Le istanze nei due VPC possono comunicare tra loro come se facessero parte della stessa rete.

Per abilitare l'instradamento del traffico tra VPCs una connessione peering VPC, è necessario aggiungere un percorso a una o più tabelle di routing della subnet 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 VPCs, 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 VPCs e consentire l'accesso all'intero blocco IPv4 CIDR di entrambi i VPC, la tabella di routing VPC A è configurata come segue.

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 anche supportare la IPv6 comunicazione tra istanze in VPCs, se le istanze VPCs e sono abilitate per la comunicazione. IPv6 Per abilitare l'instradamento del IPv6 traffico tra VPCs, è necessario aggiungere un percorso alla tabella dei percorsi che punti alla connessione peering VPC per accedere a tutto o parte del blocco CIDR IPv6 del VPC peer.

Ad esempio, utilizzando la stessa connessione peering VPC (`pcx-11223344556677889`) riportata sopra, supponiamo che VPCs dispongano delle seguenti informazioni:

- VPC A: il blocco IPv6 CIDR è `2001:db8:1234:1a00::/56`
- VPC B: il blocco IPv6 CIDR è `2001:db8:5678:2b00::/56`

Per abilitare la IPv6 comunicazione tramite la connessione peering VPC, aggiungi la seguente route alla tabella di routing di sottorete 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 gateway Internet solo in uscita viene utilizzato solo per il traffico. IPv6 Per configurare il routing per un gateway Internet solo in uscita, aggiungi una route nella tabella di routing della sottorete privata che indirizza il traffico IPv6 Internet () verso il gateway Internet solo in uscita. `::/0`

Destinazione	Target
::/0	*eigw-id*

Per ulteriori informazioni, consulta Abilita il IPv6 traffico in uscita utilizzando un gateway Internet solo in uscita.

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.

Considerate lo scenario seguente in cui ne avete tre VPCs 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, ne avete due VPCs, 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 il gateway di transito VPCs e consentire l'accesso al gateway di transito, la tabella di routing VPC A è configurata come segue.

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 EC2 istanza Amazon in una sottorete del 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 instradamento 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
- Routing del traffico tra un gateway e un'appliance
- Routing del traffico tra sottoreti a un'appliance

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:

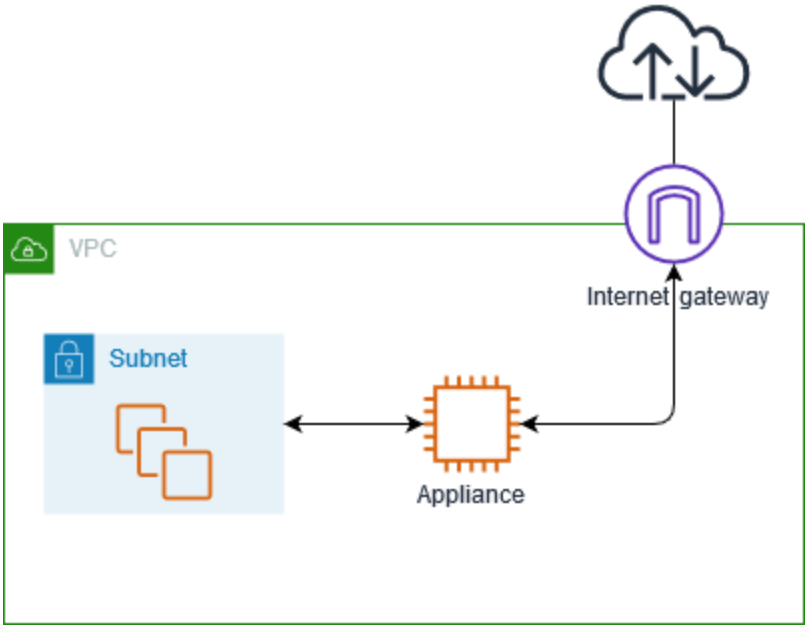
- L'appliance deve essere configurata in una sottorete separata per il traffico di origine o di destinazione.
- Devi disabilitare i controlli dell'origine/della destinazione sull'appliance. Per ulteriori informazioni, consulta Changing the Source or Destination Checking nella Amazon EC2 User Guide.
- 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 del percorso deve corrispondere all'intero blocco IPv4 o IPv6 CIDR di una sottorete nel tuo VPC.

- Per intercettare il IPv6 traffico, assicurati che il tuo VPC, la sottorete e l'appliance siano supportati. IPv6 I gateway privati virtuali 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 IPv4 traffico destinato alla sottorete all'interfaccia di rete dell'appliance. Questa è una route più specifica rispetto alla route locale.

Destinazione	Target
VPC CIDR	Locale
Subnet CIDR	*Appliance network interface ID*

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
VPC CIDR	*Appliance network interface ID*

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, specificare `0.0.0.0/0` (tutti IPv4 gli indirizzi) per la destinazione.

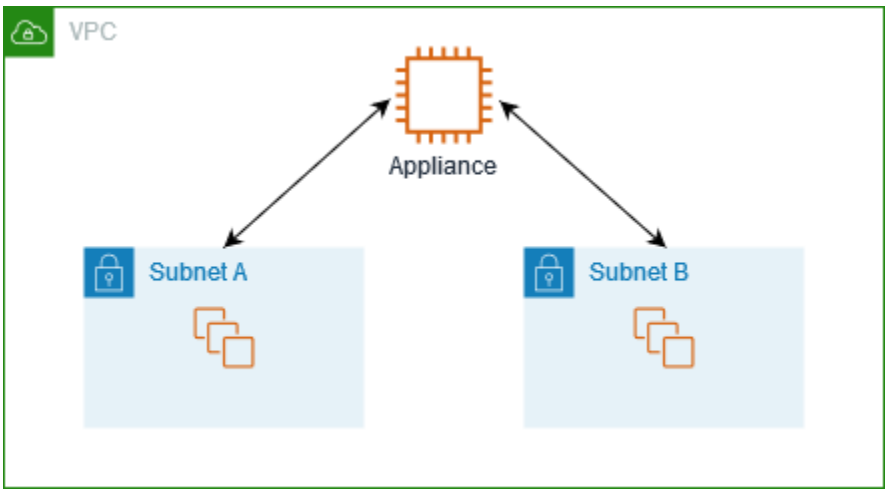
Destinazione	Target
VPC CIDR	Locale
0.0.0.0/0	*Appliance network interface ID*

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
VPC CIDR	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
VPC CIDR	Locale
Subnet B CIDR	*Appliance network interface ID*

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
VPC CIDR	Locale
Subnet A CIDR	*Appliance network interface ID*

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
VPC CIDR	*Appliance network interface ID*

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. VPCsDevono essere in grado di comunicare con due allegati VPC specifici che hanno 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
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 creare un Gateway Load Balancer, configurare un servizio endpoint Gateway Load Balancer e quindi creare un endpoint Gateway Load Balancer nel tuo VPC per collegarlo 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.

Modificare la tabella di routing di una sottorete

In questa sezione viene spiegato come lavorae con le tabelle di instradamento. Occorre tenere presente che questa sezione è un raggruppamento di procedure tutte relative alla modifica della tabella di routing della sottorete.

Indice

- Determinazione della tabella di instradamento per una sottorete
- Determinazione delle sottoreti o dei gateway associati esplicitamente
- Creazione di una tabella di routing personalizzata
- Aggiunta e rimozione di route da una tabella di instradamento

- Abilitazione o disabilitazione della propagazione delle route
- Modifica della tabella di instradamento per una sottorete
- Associare o dissociare una sottorete da una tabella di routing

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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli 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. Apri la 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. 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 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.

> **Note**
>
> 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.

Per creare una tabella di instradamento personalizzata utilizzando la console

1. Apri la 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 delle route statiche per una connessione Site-to-Site VPN, consulta Modifica delle route statiche per una connessione Site-to-Site VPN nella Guida per l'utente.AWS Site-to-Site VPN

> **Note**
>
> 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.

Per aggiornare i routing per una tabella di instradamento utilizzando la console

1. Apri la 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. Scegli Save changes (Salva 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 le opzioni di routing Site-to-Site VPN nella Guida per l'utente Site-to-Site VPN.

Per abilitare la propagazione della route tramite la console

1. Apri la 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. Apri la 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)

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. Apri la 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. Seleziona 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)

Associare o dissociare una sottorete da una tabella di routing

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.

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.

Associare o dissociare una tabella di routing a una sottorete utilizzando la console

1. Apri la 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 o deselziona la casella di controllo per la sottorete da associare alla tabella di routing.
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)

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

Questa sezione descrive come sostituire la tabella di routing principale nel VPC.

Per sostituire la tabella di instradamento principale utilizzando la console

1. Apri la 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 instradamento principale

1. Apri la 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.

Controlla il traffico che entra nel tuo VPC con una tabella di routing del gateway

Per controllare il traffico che entra nel VPC con una tabella di routing del gateway, puoi associare o dissociare un gateway Internet o un gateway virtuale privato a una tabella di routing. Per ulteriori informazioni, consulta Tabelle di routing del gateway.

Per associare o dissociare un gateway a una tabella di routing utilizzando la console

1. Apri la 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 o deselezionare la casella di controllo relativa al gateway.
5. Scegli Save changes (Salva modifiche).

Per associare o dissociare un gateway da una tabella di routing utilizzando il AWS CLI

Utilizza 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
```

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. Apri la 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. Scegli Save changes (Salva modifiche).

Per ripristinare il target per una route locale utilizzando la console

1. Apri la 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. Scegli Save changes (Salva modifiche).

Per sostituire la destinazione di una route 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
```

Risoluzione dei problemi di raggiungibilità

Reachability Analyzer è uno strumento di analisi statica della configurazione. Utilizza questo strumento per analizzare ed eseguire il debug della raggiungibilità di rete tra due risorse nel 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 route delle tabelle di routing mancanti o configurate in modo errato.

Per ulteriori informazioni, consulta la Guida di Reachability Analyzer.

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, consultare the section called “Scenari middlebox”.

Indice

- Prerequisiti della procedura guidata per il routing middlebox
- Reindirizzare il traffico VPC verso un'appliance di sicurezza
- Considerazioni sulla procedura guidata di routing middlebox
- Scenari middlebox

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.

Reindirizzare il traffico VPC verso un'appliance di sicurezza

La procedura guidata di routing middlebox è disponibile nella Amazon Virtual Private Cloud Console.

Indice

- 1. Creazione di route utilizzando la procedura guidata di routing middlebox
- 2. Modifica delle route middlebox
- 3. Eliminazione della configurazione della procedura guidata di routing middlebox

1. Creazione di route utilizzando la procedura guidata di routing middlebox

Come creare route utilizzando la procedura guidata di routing middlebox

1. Accedi 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 Next (Successivo).
9. Nella pagina Rivedi e crea verificare le route, quindi selezionare Crea route.

2. 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. Accedi 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 Next (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.

3. 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.

   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.

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 Modifica del controllo di origine o di destinazione 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, consultare 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

Amazon Virtual Private Cloud (VPC) offre un'ampia gamma di funzionalità di rete che consentono di personalizzare e controllare il routing del traffico all'interno della rete virtuale. Una di queste funzionalità è la procedura guidata di routing middlebox, che consente un controllo granulare sul percorso di routing del traffico che entra o esce dal VPC.

Se è necessario reindirizzare il traffico verso un'appliance di sicurezza, un bilanciatore del carico o un altro dispositivo di rete per scopi di ispezione, monitoraggio oppure ottimizzazione, la procedura guidata di routing middlebox può semplificare il processo. Questa procedura guidata crea automaticamente le tabelle di routing e i percorsi (hop) necessari per reindirizzare il traffico specificato in base alle esigenze, eliminando lo sforzo manuale richiesto per impostare configurazioni di routing complesse.

La procedura guidata di routing middlebox supporta diversi scenari. Ad esempio, puoi utilizzarla per esaminare il traffico destinato a una particolare sottorete, configurare il routing e l'ispezione

del traffico middlebox sull'intero VPC o ispezionare selettivamente il traffico tra sottoreti specifiche. Questo controllo granulare sul routing del traffico consente di implementare policy di sicurezza avanzate, abilitare il monitoraggio centralizzato della rete oppure ottimizzare le prestazioni delle applicazioni basate sul cloud.

Gli esempi seguenti descrivono gli scenari per la procedura guidata di instradamento middlebox.

Indice

- Ispezione del traffico destinato a una sottorete
- Configurazione del routing e dell'ispezione del traffico middlebox in un VPC
- Controllo del traffico tra sottoreti

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 dispositivo firewall installato su un'istanza. EC2 L'appliance firewall deve essere installata e configurata su un' EC2 istanza in una sottorete separata dalla sottorete B del VPC, ad esempio la sottorete C. È quindi possibile utilizzare la procedura guidata di routing middlebox per configurare le rotte 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.

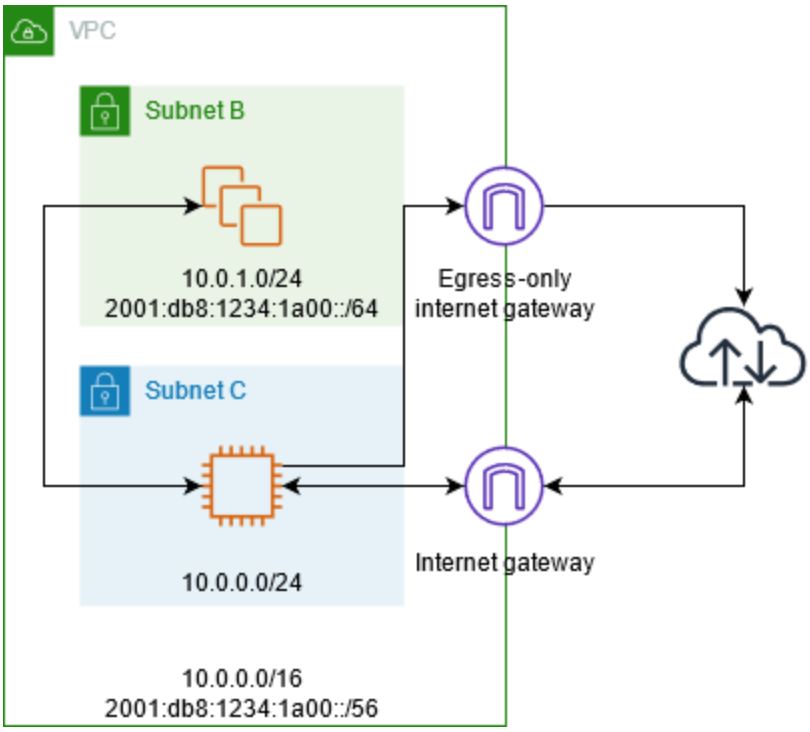


Tabella di routing del gateway Internet

Aggiungi le seguenti route alla tabella di routing per il gateway Internet.

Destinazione	Target	Scopo
10.0.0.0/16	Locale	Percorso locale per IPv4
10.0.1.0/24	*appliance-eni*	IPv4 Indirizza il traffico destinato alla sottorete B verso il middlebox
2001:db8:1234:1a00::/56	Locale	Percorso locale per IPv6

Destinazione	Target	Scopo
2001:db8:1234:1a00::/64	*appliance-eni*	IPv6 Indirizza il traffico destinato alla sottorete B verso il 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	Percorso locale per IPv4
0.0.0.0/0	*appliance-eni*	IPv4 Indirizza il traffico destinato a Internet verso il middlebox
2001:db8:1234:1a00::/56	Locale	Percorso locale per IPv6
::/0	*appliance-eni*	IPv6 Indirizza il traffico destinato a Internet verso il 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	Percorso locale per IPv4
0.0.0.0/0	*igw-id*	Indirizza il IPv4 traffico verso il gateway Internet
2001:db8:1234:1a00::/56	Locale	Percorso locale per IPv6
::/0	*eigw-id*	Indirizza il IPv6 traffico verso il gateway Internet solo in uscita

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")

Configurazione del routing e dell'ispezione del traffico middlebox in un VPC

Si consideri lo scenario in cui è necessario ispezionare il traffico che entra in un VPC dal gateway Internet e destinato a una sottorete, utilizzando una flotta di dispositivi di sicurezza configurati dietro 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 seguenti operazioni:

- 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.

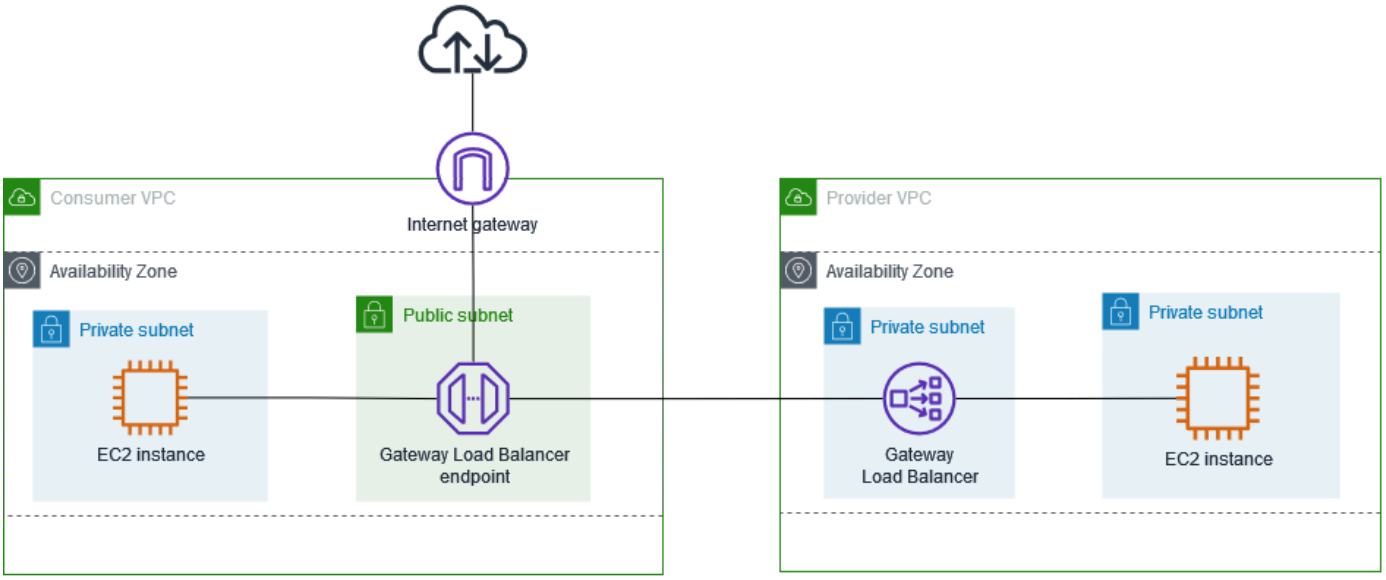


Tabella di routing del gateway Internet

La tabella di instradamento del gateway Internet ha gli instradamenti seguenti:

Destinazione	Target	Scopo
Consumer VPC CIDR	Locale	Route locale
Application subnet CIDR	*endpoint-id*	Instrada 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
Consumer VPC CIDR	Locale	Route locale
0.0.0.0/0	*endpoint-id*	Indirizza il traffico dai server delle applicazioni all'endpoint Gateway Load Balancer prima che venga indirizzato a 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
Provider VPC CIDR	Locale	Instradamento locale. Assicura che il traffico proveniente da Internet venga indirizzato ai server delle applicazioni
0.0.0.0/0	*igw-id*	Indirizza tutto il traffico al gateway Internet.

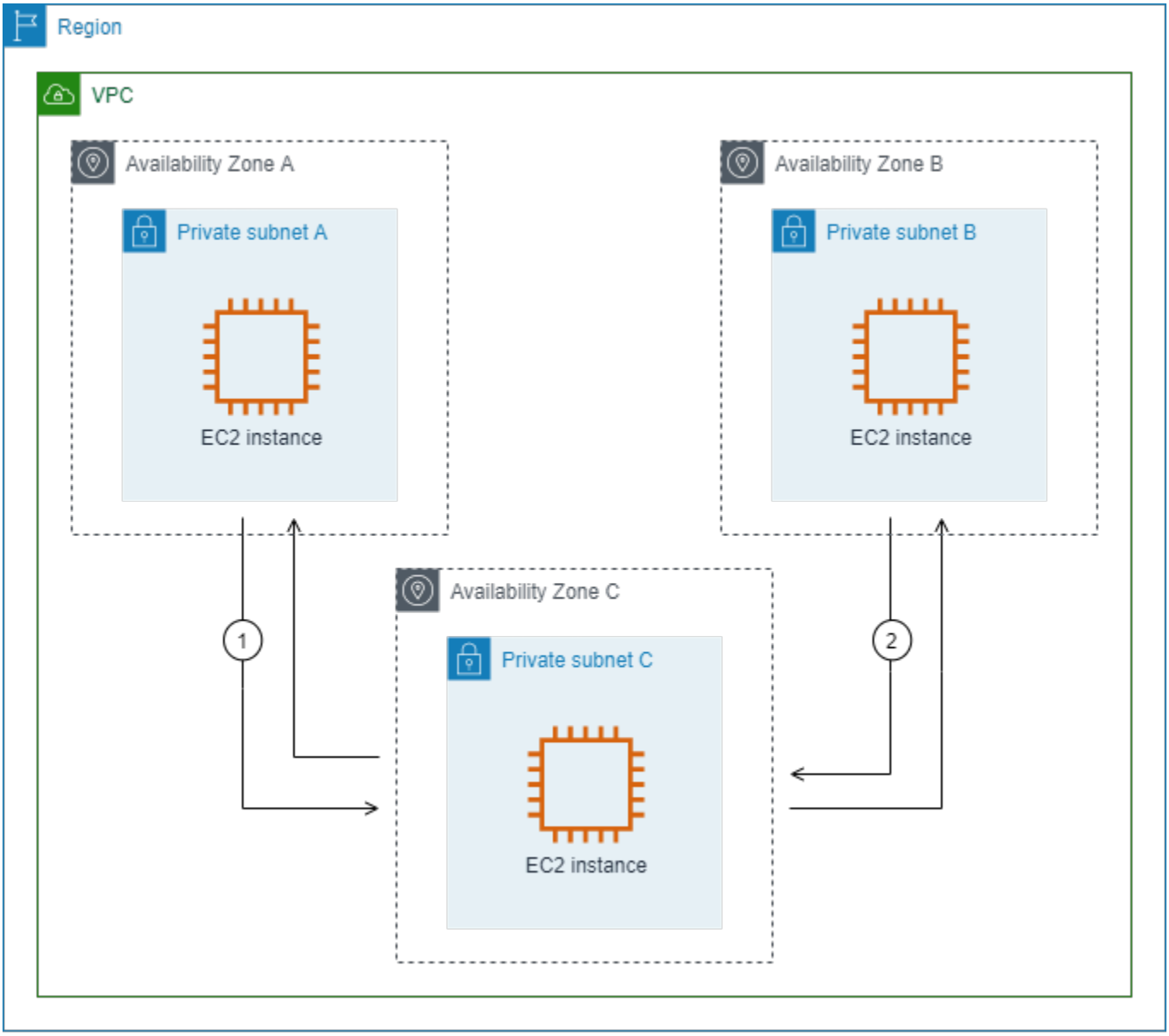
Quando utilizzi la procedura guidata di instradamento middlebox, alla tabella di instradamento sono associati i tag seguenti:

- 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 su un' EC2 istanza in una sottorete separata del tuo VPC.

Il diagramma seguente mostra un'appliance firewall installata su un' EC2 istanza nella sottorete C. L'appliance ispeziona tutto il traffico che viaggia dalla sottorete A alla sottorete B (vedere 1) e dalla sottorete B alla sottorete A (vedere 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
VPC CIDR	Locale	Route locale
Subnet B CIDR	*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
VPC CIDR	Locale	Route locale

Destinazione	Target	Scopo
Subnet A CIDR	*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
VPC CIDR	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.

Quando elimini una sottorete, il blocco CIDR associato a quella sottorete viene restituito al pool di indirizzi IP disponibili del VPC. Ciò significa che gli indirizzi IP all'interno dell'intervallo CIDR della sottorete possono essere riassegnati ad altre sottoreti o risorse all'interno dello stesso VPC.

È importante notare che l'eliminazione di una sottorete non elimina automaticamente le risorse al suo interno. È necessario innanzitutto terminare tutte EC2 le istanze, eliminare tutte le interfacce di rete e rimuovere tutte le altre risorse associate alla sottorete prima di procedere con l'eliminazione della sottorete.

Eliminazione di una sottorete tramite la console

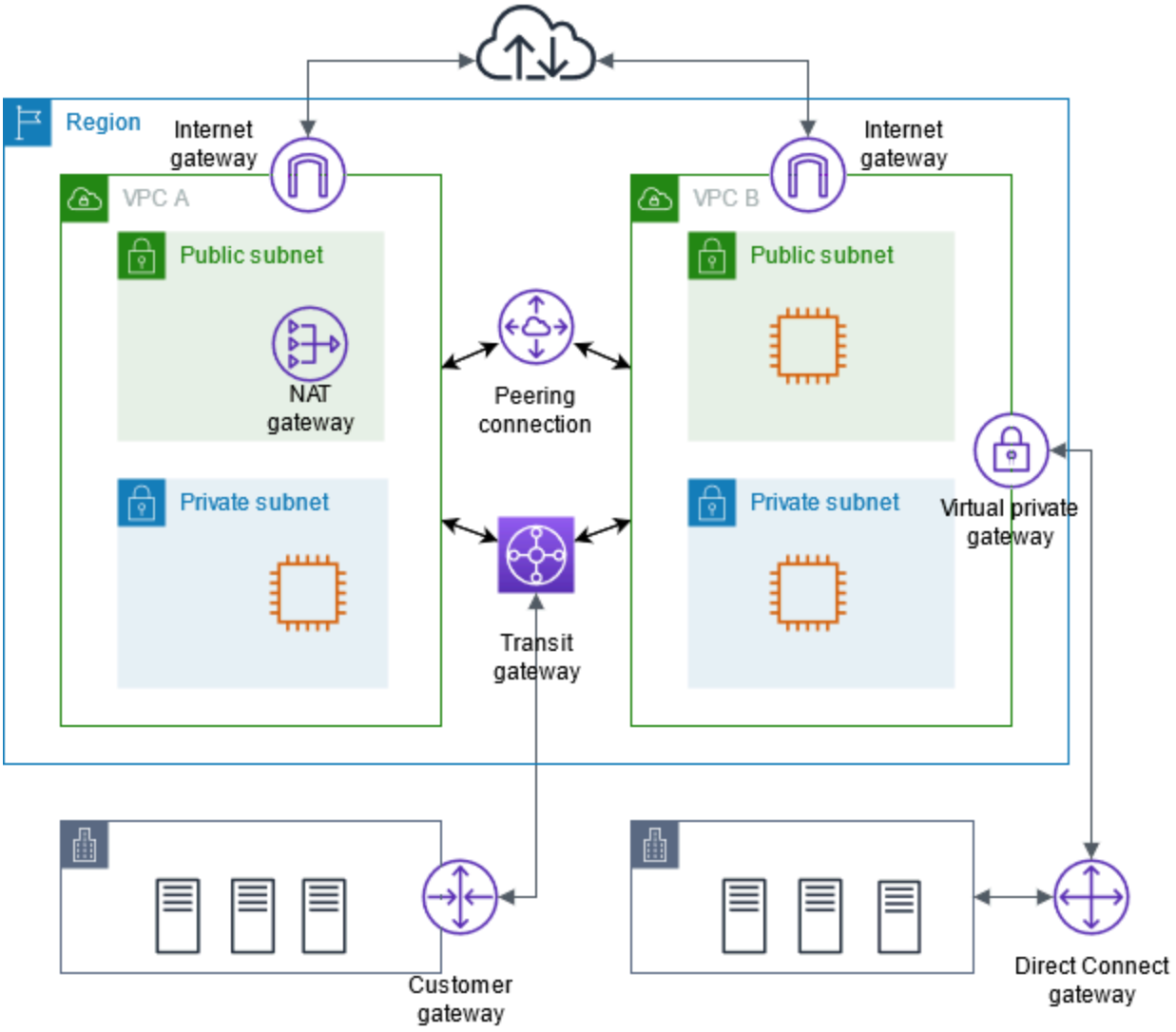
1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Terminare tutte le istanze nella sottorete. Per ulteriori informazioni, consulta Terminare l'istanza nella Amazon EC2 User Guide.
3. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
4. Nel pannello di navigazione, scegli 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).

Per eliminare una sottorete utilizzando il AWS CLI

Usa il comando delete-subnet.

Connetti il tuo VPC ad altre reti

Puoi connettere il tuo cloud privato virtuale (VPC) ad altre reti, come altre VPCs, Internet o la tua rete locale.



Puoi connettere il tuo cloud privato virtuale (VPC) ad altre reti, come altre VPCs, Internet o la tua rete locale.

Il diagramma illustra alcune di queste opzioni di connettività. Il VPC A è connesso a Internet tramite un gateway Internet e l' EC2 istanza nella sottorete privata può connettersi a Internet utilizzando un gateway NAT nella sottorete pubblica. Anche VPC B è connesso a Internet, ma tramite un gateway Internet diretto, che consente all' EC2 istanza nella sottorete pubblica di accedere a Internet.

Tuttavia, VPC A e 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 e il VPC B ha una AWS Direct Connect connessione allo stesso data center. Questa interconnettività consente alle organizzazioni di integrare le proprie risorse cloud con l'infrastruttura on-premises, creando un ambiente cloud ibrido.

La connessione VPCs ad altre reti è un aspetto importante della creazione di un'infrastruttura cloud interna AWS. Offre alle organizzazioni flessibilità e controllo sulle configurazioni di rete, consentendo loro di progettare architetture VPC in linea con i requisiti aziendali e le esigenze di sicurezza. Queste opzioni di connettività facilitano un flusso di dati efficiente tra i vari componenti di un panorama IT distribuito, sia all'interno del cloud che on-premises.

AWS fornisce una gamma di strumenti e funzionalità per abilitare queste connessioni VPC, inclusi gateway Internet, gateway NAT, peering VPC, gateway di transito e. AWS Direct Connect Sfruttando queste funzionalità, le organizzazioni possono creare ambienti cloud sicuri e integrati che si adattano perfettamente all'infrastruttura IT esistente.

È possibile connettere il cloud privato virtuale (VPC) ad altre reti. Ad esempio, altro VPCs, Internet o la rete locale.

Per ulteriori informazioni, consulta Opzioni di connettività di Amazon Virtual Private Cloud.

Indice

- Abilitazione dell'accesso di VPC a Internet tramite gateway Internet
- Abilita il IPv6 traffico in uscita utilizzando un gateway Internet solo in uscita
- Eseguire la connessione a Internet o ad altri VPC utilizzando dispositivi NAT
- Associare gli indirizzi IP elastici alle risorse nel VPC
- Connect il tuo VPC ad altre VPCs reti utilizzando un gateway di transito
- Connetti il tuo VPC a reti remote utilizzando AWS Virtual Private Network
- Connettere i VPC utilizzando il peering VPC

Abilitazione dell'accesso di VPC a Internet tramite 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 IPv4 e gestisce il IPv6 traffico. Non causa rischi di disponibilità o vincoli di larghezza di banda nel traffico di rete.

Un gateway Internet consente alle risorse delle sottoreti pubbliche (come EC2 le istanze) di connettersi a Internet se la risorsa ha un IPv4 indirizzo pubblico o un indirizzo. IPv6 Analogamente, le risorse su Internet possono avviare una connessione alle risorse della sottorete utilizzando l'indirizzo o l'indirizzo pubblico. IPv4 IPv6 Ad esempio, un gateway Internet consente di connettersi a un' EC2istanza 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 IPv4, il gateway Internet esegue anche la traduzione degli indirizzi di rete (NAT). Per ulteriori informazioni, consulta Indirizzi IP e NAT.

> **Note**
>
> Non sono previsti costi per un gateway Internet, ma sono previsti costi per il trasferimento dei dati per i EC2 casi che utilizzano gateway Internet. Per ulteriori informazioni, consulta la pagina dei prezzi di Amazon EC2 On-Demand.

Indice

- Configurazione per l'accesso a Internet
- Aggiunta di un accesso Internet a una sottorete

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.
- Assicurati che le istanze nella tua sottorete abbiano un indirizzo o un IPv4 indirizzo pubblico. IPv6 Per ulteriori informazioni, consulta Indirizzamento IP dell'istanza nella Amazon EC2 User Guide.
- 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.

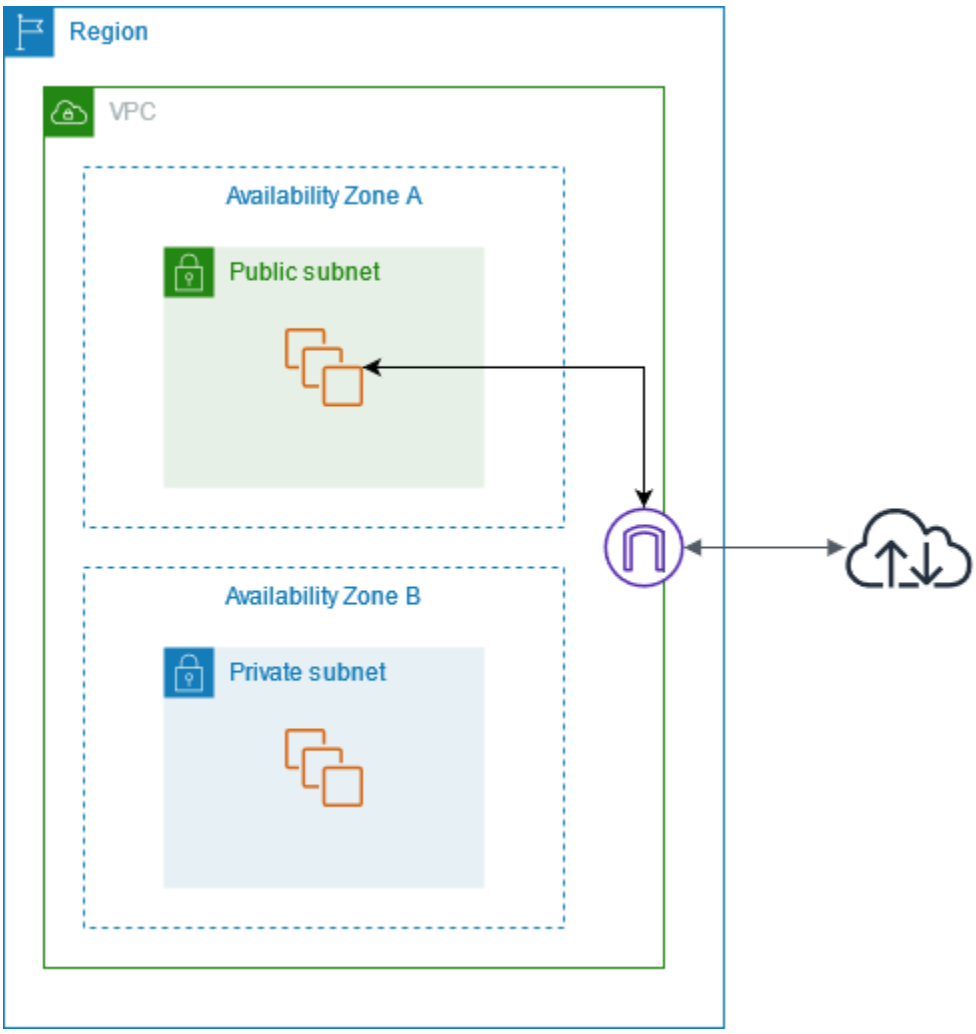
Nella tabella di routing della sottorete pubblica, puoi specificare una route per il gateway Internet verso tutte le destinazioni non esplicitamente note alla tabella delle rotte (`0.0.0.0/0`per IPv4 o `::/0` per IPv6). In alternativa, puoi definire il percorso fino a un intervallo più ristretto di indirizzi IP, ad esempio gli indirizzi pubblici degli endpoint pubblici della tua azienda esterni al tuo VPC o IPv4 gli indirizzi IP elastici di AWS altre EC2 istanze Amazon al di fuori del tuo VPC.

Indirizzi IP e NAT

Per abilitare la comunicazione su Internet per IPv4, l'istanza deve avere un indirizzo pubblico. IPv4 Puoi configurare il tuo VPC per assegnare automaticamente IPv4 indirizzi pubblici alle tue istanze oppure puoi assegnare indirizzi IP elastici alle tue 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 pubblico o sull' IPv4 indirizzo IP elastico dell'istanza e non sul suo indirizzo IP privato. Al contrario, il traffico destinato all' IPv4 indirizzo pubblico o all'indirizzo IP elastico dell'istanza ha l'indirizzo di destinazione tradotto nell' IPv4 indirizzo privato dell'istanza prima che il traffico venga consegnato al VPC.

Per abilitare la comunicazione su Internet IPv6, il VPC e la sottorete devono avere un blocco IPv6 CIDR associato e all'istanza deve essere assegnato un IPv6 indirizzo compreso nell'intervallo della sottorete. IPv6 gli indirizzi sono unici a livello globale e quindi 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 invia tutto il IPv4 traffico collegato 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 hanno indirizzi IP pubblici.



Accesso a Internet predefinito e non predefinito VPCs

La tabella seguente fornisce una panoramica del fatto che il VPC venga fornito automaticamente con i componenti necessari per l'accesso a Internet tramite o. IPv4 IPv6

Componente	VPC predefinito	VPC non predefinito
Internet Gateway	Sì	No
Tabella delle rotte con percorso verso il gateway Internet per il IPv4 traffico (0.0.0.0/0)	Sì	No

Componente	VPC predefinito	VPC non predefinito
Tabella delle rotte con il percorso verso il gateway Internet per il IPv6 traffico (:: /0)	No	No
IPv4 Indirizzo pubblico assegnato automaticamente all'istanza avviata nella sottorete	Sì (sottorete predefinita)	No (sottorete non predefinita)
IPv6 indirizzo assegnato automaticamente all'istanza lanciata nella sottorete	No (sottorete predefinita)	No (sottorete non predefinita)

Per ulteriori informazioni sulle impostazioni predefinite VPCs, vederePredefinito VPCs. Per ulteriori informazioni sulla creazione di un VPC, consulta Crea un VPC.

Aggiunta di un accesso Internet a una sottorete

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

- 1. Creazione di un Internet Gateway
- 2. Collegamento o scollegamento di un gateway Internet da un VPC
- 3. Eliminazione di un Internet Gateway
- Panoramica della riga di comando

1. Creazione di un Internet Gateway

Usa la procedura seguente per creare un gateway Internet.

Creare un gateway Internet

1. Apri la 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.

2. Collegamento o scollegamento di un gateway Internet da un VPC

Per utilizzare un gateway Internet, devi collegarlo a un 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.

Come collegare o scollegare un gateway Internet da un VPC

1. Apri la 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. Per collegarlo, scegli Operazioni, Collega a VPC, seleziona un VPC disponibile e scegli Collega gateway internet.
5. Per scollegarlo, scegli Operazioni, Scollega da VPC e scegli Scollega gateway internet. Quando viene chiesta la conferma, seleziona Detach internet gateway (Scollega gateway Internet).

3. 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. Apri la 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 della riga di comando

È possibile eseguire le attività descritte in questa pagina utilizzando la riga di comando.

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)

Abilita il IPv6 traffico in uscita utilizzando un gateway Internet solo in uscita

Un gateway Internet solo in uscita è un componente VPC a scalabilità orizzontale, ridondante e ad alta disponibilità che consente la comunicazione in uscita IPv6 dalle istanze del tuo VPC a Internet e impedisce a Internet di avviare una connessione con le tue istanze. IPv6

Un gateway Internet solo in uscita può essere utilizzato solo con il traffico. IPv6 Per abilitare la comunicazione Internet solo in uscita IPv4, utilizza invece un gateway NAT. Per ulteriori informazioni, consulta Gateway NAT.

Prezzi

Non è previsto alcun costo per un gateway Internet solo in uscita, ma sono previsti costi per il trasferimento dei dati per le istanze che utilizzano gateway Internet. EC2 Per ulteriori informazioni, consulta la pagina dei prezzi di Amazon EC2 On-Demand.

Indice

- Nozioni di base sull'Internet Gateway egress-only
- Aggiunta di un accesso Internet egress-only a una sottorete

Nozioni di base sull'Internet Gateway egress-only

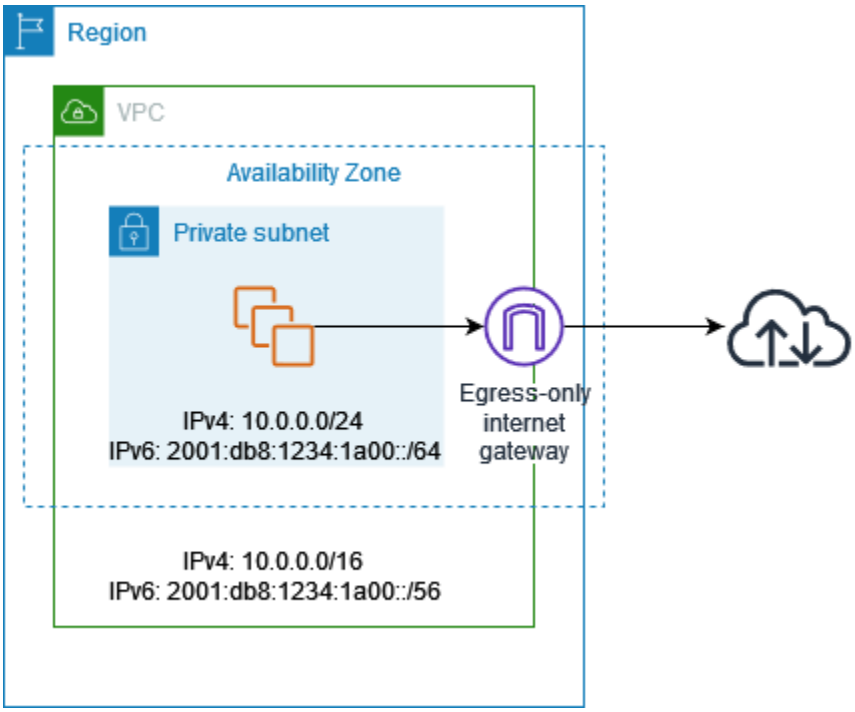
IPv6 gli indirizzi sono unici a livello globale e sono quindi pubblici per impostazione predefinita. Se l'istanza deve essere in grado di accedere a Internet, ma desideri impedire a risorse su Internet di avviare una comunicazione con l'istanza, puoi utilizzare un Internet Gateway egress-only. A tale scopo, crea un gateway Internet per il solo traffico in uscita nel tuo VPC, quindi aggiungi un percorso alla tabella dei percorsi che indirizzi tutto il IPv6 traffico (`::/0`) o un intervallo di IPv6 indirizzi specifico verso il gateway Internet solo in uscita. IPv6 il traffico nella sottorete associata alla tabella delle rotte viene indirizzato al gateway Internet di sola uscita.

Un gateway Internet solo in uscita è stateful: inoltra il traffico dalle istanze della sottorete a Internet o ad altri servizi, quindi invia la risposta alle istanze. AWS

Non è possibile associare un gruppo di sicurezza a un gateway Internet egress-only per controllare il traffico che può raggiungere o lasciare il gateway Internet egress-only. 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 IPv4 sia IPv6 blocchi CIDR che la sottorete IPv4 e blocchi CIDR. IPv6 Il VPC ha un gateway Internet egress-only.



Di seguito è riportata la tabella di routing associata alla sottorete. Esiste un percorso che invia tutto il IPv6 traffico diretto a Internet (:: /0) al gateway Internet di sola uscita.

Destinazione	Target
10.0.0.0/16	Locale
2001:db8:1234:1a00:/64	Locale
::/0	*eigw-id*

Aggiunta di un accesso Internet egress-only a una sottorete

Nelle sezioni seguenti viene descritto come creare un gateway Internet egress-only (in uscita) per la sottorete privata e in che modo configurare il routing per la sottorete.

Attività

- 1. Creazione di un gateway Internet egress-only
- 2. Creazione di una tabella di routing personalizzata
- 3. Eliminazione di un gateway Internet egress-only
- Panoramica della riga di comando

1. 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. Apri la 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. Scegli Create (Crea) .

2. 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. Apri la 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.

3. 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. Apri la 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 della riga di comando

È possibile eseguire le attività descritte in questa pagina utilizzando la riga di comando.

Creazione di un gateway Internet egress-only

- create-egress-only-internet-gateway ()AWS CLI
- 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)

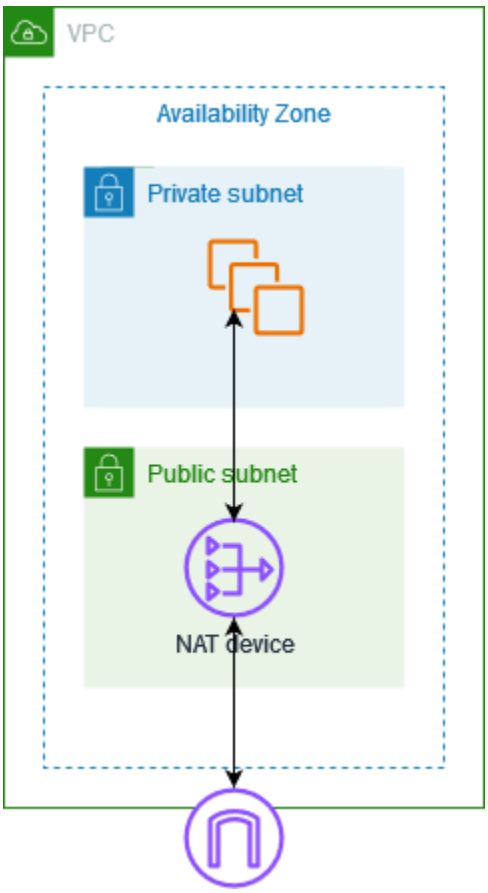
Eliminazione di un gateway Internet egress-only

- delete-egress-only-internet-gateway ()AWS CLI
- Remove-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

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, lo schema 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 fornito da AWS, chiamato gateway NAT oppure creare un tuo dispositivo NAT in un'istanza EC2, detta appunto 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
- Istanze NAT
- Confronto delle istanze NAT e i gateway NAT

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 utilizzare un gateway NAT pubblico per connetterti a un'altra rete VPCs o alla tua 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 in sottoreti private possono connettersi ad altre reti VPCs 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.

Un gateway NAT può essere utilizzato solo con il traffico. IPv4 Per abilitare la comunicazione Internet solo in uscita IPv6, utilizza invece un gateway Internet solo in uscita. Per ulteriori informazioni, consulta Internet Gateway egress-only.

Sia i gateway NAT privati che quelli pubblici mappano l' IPv4 indirizzo privato di origine delle istanze all' IPv4 indirizzo privato del gateway NAT, ma nel caso di un gateway NAT pubblico, il gateway Internet associa quindi l' IPv4 indirizzo 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. Il gateway NAT pubblico utilizzerà il suo EIP come indirizzo IP di origine solo se usato insieme a un gateway Internet nello stesso VPC.
I gateway NAT supportano il traffico con un'unità di trasmissione massima (MTU) di 8.500.
Per ulteriori informazioni, consulta Nozioni di base sul gateway NAT.

Indice

- Nozioni di base sul gateway NAT
- Utilizzo dei gateway NAT
- Casi d'uso di API Gateway
- DNS64 e NAT64
- Monitora i gateway NAT con Amazon CloudWatch
- Risoluzione dei problemi relativi ai gateway NAT
- Prezzi per i gateway NAT

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 nostro traffico. IPv4 IPv6 Per quanto riguarda il IPv6 traffico, il gateway NAT offre prestazioni elevate. NAT64 Utilizzandolo insieme a DNS64 (disponibile sul resolver Route 53), i IPv6 carichi di lavoro in una sottorete di Amazon VPC possono comunicare con le risorse. IPv4 Questi IPv4 servizi possono essere presenti nello stesso VPC (in una sottorete separata) o in un VPC diverso, nell'ambiente locale 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 IPv4 indirizzo può supportare fino a 55.000 connessioni simultanee verso ogni destinazione unica. Una destinazione univoca è identificata da una combinazione unica di indirizzo IP di destinazione, porta di destinazione e protocollo ()TCP/UDP/ICMP. È possibile aumentare questo limite associando fino a 8 IPv4 indirizzi ai gateway NAT (1 IPv4 indirizzo primario e 7 indirizzi secondari IPv4). 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.
- È possibile scegliere l' IPv4 indirizzo privato da assegnare al gateway NAT o farlo assegnare automaticamente dall'intervallo di IPv4 indirizzi della sottorete. L' IPv4 indirizzo privato assegnato persiste finché non si elimina il gateway NAT privato. Non è possibile scollegare l' IPv4 indirizzo privato e non è possibile allegare indirizzi privati aggiuntivi. IPv4
- 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 Controllo del traffico della sottorete con le liste di controllo degli accessi alla rete.
- Un gateway NAT riceve un'interfaccia di rete. È possibile scegliere l' IPv4 indirizzo privato da assegnare all'interfaccia o farlo assegnare automaticamente dall'intervallo di IPv4 indirizzi della sottorete. Puoi visualizzare l'interfaccia di rete per il gateway NAT utilizzando la EC2 console Amazon. 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 puoi instradare traffico a 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 (Direct Connect o Site-to-Site VPN) tramite un gateway privato virtuale. È possibile indirizzare il traffico attraverso un gateway NAT quando il traffico arriva tramite una connessione ibrida (Direct Connect o Site-to-Site VPN) 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:
  - L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto più grande consentito trasferibile attraverso la connessione. Maggiore è la MTU di una connessione, maggiore è la quantità di dati trasferibili in un unico pacchetto.
  - I pacchetti con più di 8.500 byte che arrivano al gateway NAT vengono eliminati (o frammentati, se applicabile).
  - Per evitare la potenziale perdita di pacchetti durante la comunicazione con risorse su Internet utilizzando un gateway NAT pubblico, l'impostazione MTU per le tue EC2 istanze 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 FRAG_NEEDED e pacchetti Packet Too Big (PTB). ICMPv4 ICMPv6
  - I gateway NAT applicano il clamping MSS (Maximum Segment Size) a tutti i pacchetti. Per ulteriori informazioni, consulta RFC879.

Utilizzo dei gateway NAT

Puoi utilizzare la console Amazon VPC per creare e gestire i gateway NAT.

Attività

- Controllo dell'uso dei gateway NAT
- Creazione di un gateway NAT
- Come modificare le associazioni di indirizzi IP secondari
- Tagging di un gateway NAT
- Eliminazione di un gateway NAT
- Panoramica della riga di comando

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.

Creazione di un gateway NAT

Utilizza la procedura seguente per creare un gateway NAT.

Quote correlate

- Non sarai in grado di creare un gateway NAT pubblico se hai esaurito il numero di dati assegnati al tuo account. EIPs Per ulteriori informazioni sulle quote EIP e su come modificarle, consulta Indirizzi IP elastici.
- Puoi assegnare fino a 8 IPv4 indirizzi 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. Apri la 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 EIPs, vedere. 1. Allocare un indirizzo IP elastico

2. (Facoltativo) Scegliete Impostazioni aggiuntive e, in Indirizzo IP privato - opzionale, inserite un IPv4 indirizzo privato per il gateway NAT. Se non inserisci un indirizzo, AWS assegnerà automaticamente un IPv4 indirizzo 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, Metodo di assegnazione IPv4 indirizzi privato, scegli una delle seguenti opzioni:

   - Assegnazione automatica: AWS sceglie l' IPv4 indirizzo privato principale per il gateway NAT. Per Numero di IPv4 indirizzi privati assegnati automaticamente, puoi facoltativamente specificare il numero di IPv4 indirizzi privati secondari per il gateway NAT. AWS sceglie questi indirizzi IP a caso dalla sottorete per il gateway NAT.
   - Personalizzato: per IPv4Indirizzo privato principale, scegli l' IPv4 indirizzo privato principale per il gateway NAT. Per IPv4 gli indirizzi privati secondari, puoi facoltativamente specificare fino a 7 IPv4 indirizzi 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 IPv4 indirizzi secondari che desideri AWS assegnare a questo gateway NAT privato. Puoi scegliere fino a 7 indirizzi. IPv4

> **Note**
>
> IPv4 Gli indirizzi secondari sono facoltativi e devono essere assegnati o allocati quando i carichi di lavoro che utilizzano un gateway NAT superano le 55.000 connessioni simultanee verso una singola destinazione (stesso IP di destinazione, porta e protocollo). IPv4Gli indirizzi secondari aumentano il numero di porte disponibili e quindi aumentano il limite al numero 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 IPv4 Indirizzo privato primario, inserisci un indirizzo privato. IPv4
    2. In IPv4 Indirizzo privato secondario, inserisci fino a 7 IPv4 indirizzi 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 IPv4 indirizzo può supportare fino a 55.000 connessioni simultanee verso ogni destinazione unica. Una destinazione univoca è identificata da una combinazione unica di indirizzo IP di destinazione, porta di destinazione e protocollo ()TCP/UDP/ICMP. È possibile aumentare questo limite associando fino a 8 IPv4 indirizzi ai gateway NAT (1 IPv4 indirizzo primario e 7 indirizzi secondari IPv4). 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.

È possibile utilizzare le CloudWatchmetriche ErrorPortAllocationdel gateway NAT PacketsDropCountper determinare se il gateway NAT genera errori di allocazione delle porte o

elimina pacchetti. Per risolvere questo problema, aggiungi indirizzi secondari IPv4 al tuo gateway NAT.

Considerazioni

- È possibile aggiungere IPv4 indirizzi privati secondari quando si crea un gateway NAT privato o dopo averlo creato utilizzando 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.
- Il gateway NAT può avere fino a 8 IPv4 indirizzi associati (1 IPv4 indirizzo primario e 7 indirizzi secondari IPv4). Puoi assegnare fino a 8 IPv4 indirizzi 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.

Per modificare le associazioni di indirizzi secondari IPv4

1. Apri la 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 desideri modificare le associazioni di IPv4 indirizzi secondari.
4. Scegli Operazioni, quindi scegli Modifica delle associazioni degli indirizzi IP secondari.
5. Se stai modificando le associazioni di IPv4 indirizzi secondari di un gateway NAT privato, in Azione, scegli Assegna nuovi IPv4 indirizzi o Annulla assegnazione indirizzi esistenti. IPv4
   Se stai modificando le associazioni di IPv4 indirizzi secondari di un gateway NAT pubblico, in Azione, scegli Associa nuovi IPv4 indirizzi o Dissocia indirizzi esistenti. IPv4
6. Esegui una di queste operazioni:

   - Se hai scelto di assegnare o associare nuovi IPv4 indirizzi, procedi come segue:
     1. Questo passaggio è obbligatorio. È necessario selezionare un IPv4 indirizzo privato. Scegli il metodo di assegnazione IPv4 dell'indirizzo privato:
        - Assegnazione automatica: sceglie AWS automaticamente un IPv4 indirizzo privato principale e scegli se vuoi assegnare fino AWS a 7 IPv4 indirizzi privati secondari 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' IPv4indirizzo privato principale e fino a 7 IPv4 indirizzi privati secondari da assegnare al gateway NAT.

2. In Elastic IP allocation ID, scegli un EIP da aggiungere come indirizzo secondario. IPv4 Questo passaggio è obbligatorio. È necessario selezionare un EIP insieme a un indirizzo privato. IPv4 Se hai scelto Personalizzato per il metodo di assegnazione degli indirizzi IP privati, devi anche inserire un IPv4 indirizzo 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 confini di rete e EIPs, vedere. 1. Allocare un indirizzo IP elastico

   Al tuo gateway NAT puoi associare fino a 8 indirizzi IP. Se si tratta di un gateway NAT pubblico, esiste un limite di quota predefinito EIPs per regione. Per ulteriori informazioni, consulta Indirizzi IP elastici.

- Se hai scelto di annullare l'assegnazione o annullare l'associazione di nuovi IPv4 indirizzi, completa quanto segue:

  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. Scegli Save changes (Salva 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. Apri la 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. Seleziona 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. Apri la 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 5. Rilascio di un indirizzo IP elastico.

Panoramica della riga di comando

È possibile eseguire le attività descritte in questa pagina utilizzando la riga di comando.

Assegna un IPv4 indirizzo privato a un gateway NAT privato

- assign-private-nat-gateway-indirizzo ()AWS CLI
- Register-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

Associa indirizzi IP elastici (EIPs) e IPv4 indirizzi privati a un gateway NAT pubblico

- associate-nat-gateway-address (AWS CLI)
- Register-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

Creazione di un gateway NAT

- create-nat-gateway (AWS CLI)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)

Eliminazione di un gateway NAT

- delete-nat-gateway (AWS CLI)
- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)

Descrizione di un gateway NAT

- describe-nat-gateways (AWS CLI)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)

Dissocia gli indirizzi IP elastici secondari (EIPs) da un gateway NAT pubblico

- disassociate-nat-gateway-address (AWS CLI)
- Unregister-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

Tagging di un gateway NAT

- create-tags (AWS CLI)

- New-EC2Tag (AWS Tools for Windows PowerShell)

Annulla l'assegnazione di IPv4 indirizzi secondari da un gateway NAT privato

- unassign-private-nat-gateway-indirizzo ()AWS CLI
- Unregister-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

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.

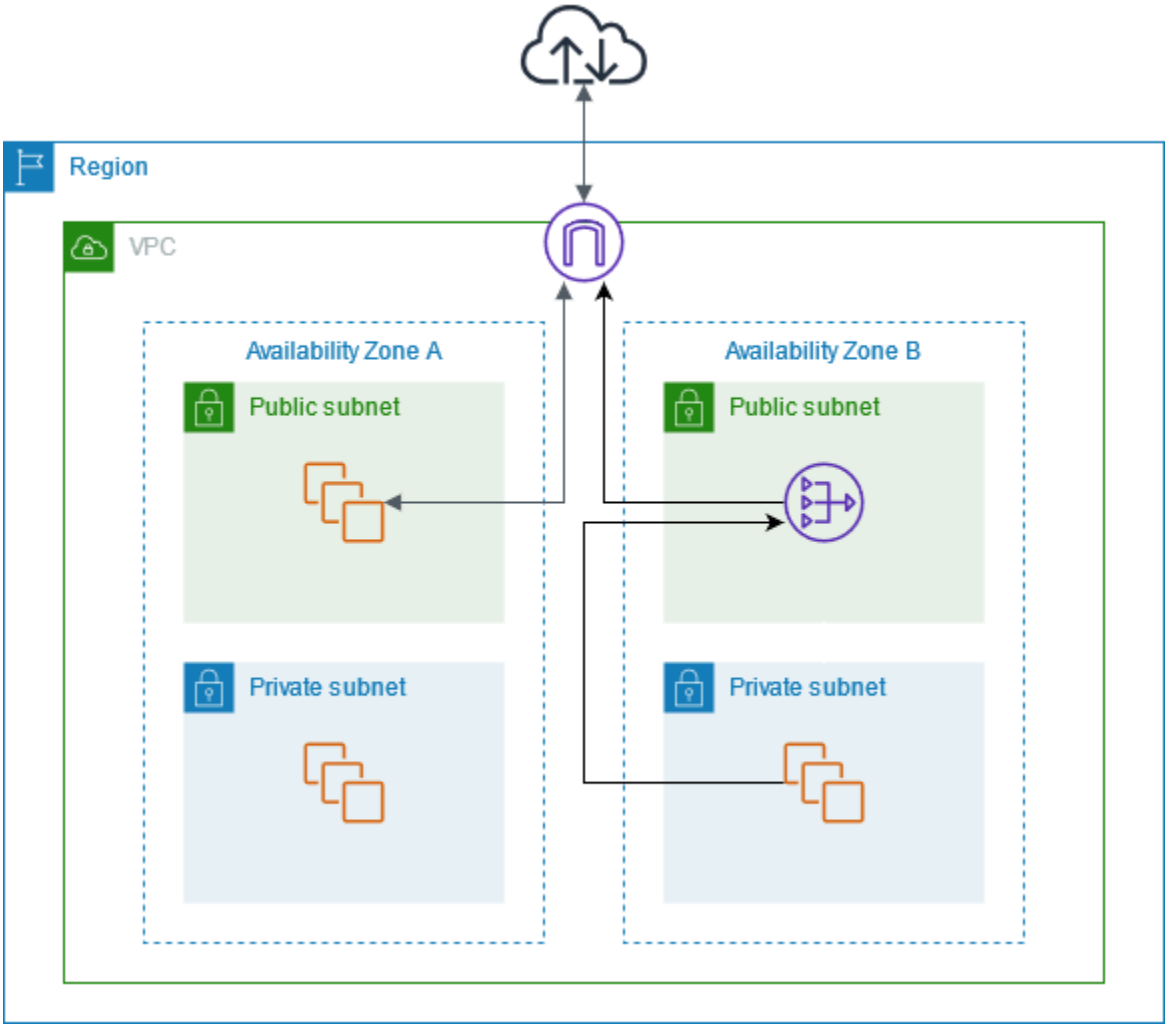
Indice

- Panoramica
- Routing
- Test del gateway NAT pubblico

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. Sia i gateway NAT privati che

quelli pubblici mappano l' IPv4 indirizzo privato di origine delle istanze all' IPv4 indirizzo privato del gateway NAT privato, ma nel caso di un gateway NAT pubblico, il gateway Internet mappa quindi l' IPv4 indirizzo 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
VPC CIDR	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
VPC CIDR	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
VPC CIDR	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
VPC CIDR	locale
0.0.0.0/0	*nat-gateway-id*

Per ulteriori informazioni, consulta the section called “Modificare la tabella di routing di una sottorete”.

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 Convertire la chiave privata utilizzando Pu TTYgen nella Amazon EC2 User Guide.
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, vedi Connect alla tua istanza Linux usando PuTTY. 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 Terminare l'istanza nella Amazon EC2 User Guide.

Accedere alla rete utilizzando gli indirizzi IP consentiti riportati

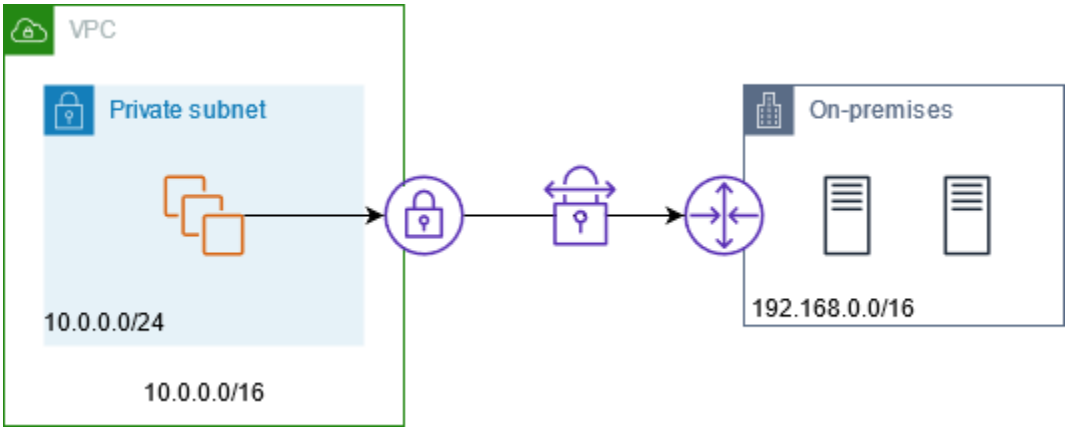
Puoi utilizzare un gateway NAT privato per abilitare la comunicazione dalla tua rete locale VPCs alla tua rete locale utilizzando un pool di indirizzi consentiti. Anziché assegnare a ciascuna istanza un indirizzo IP indipendente dall'intervallo di indirizzi IP consentito, è possibile instradare il traffico dalla sottorete destinata alla rete locale attraverso un gateway NAT privato con un indirizzo IP dall'intervallo di indirizzi IP consentito.

Indice

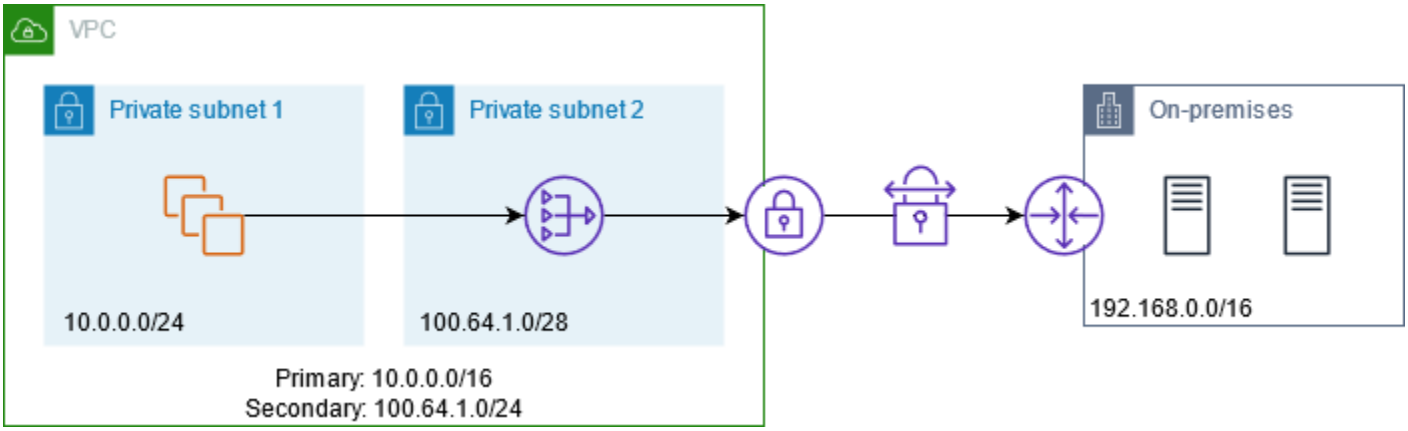
- Panoramica
- Risorse
- Routing

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	local

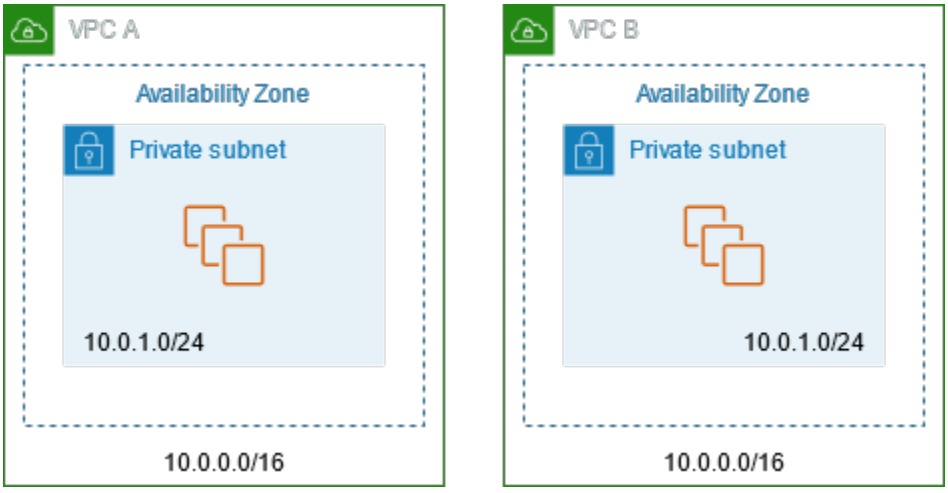
Destinazione	Target
100.64.1.0/24	local
192.168.0.0/16	*nat-gateway-id*

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
10.0.0.0/16	local
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

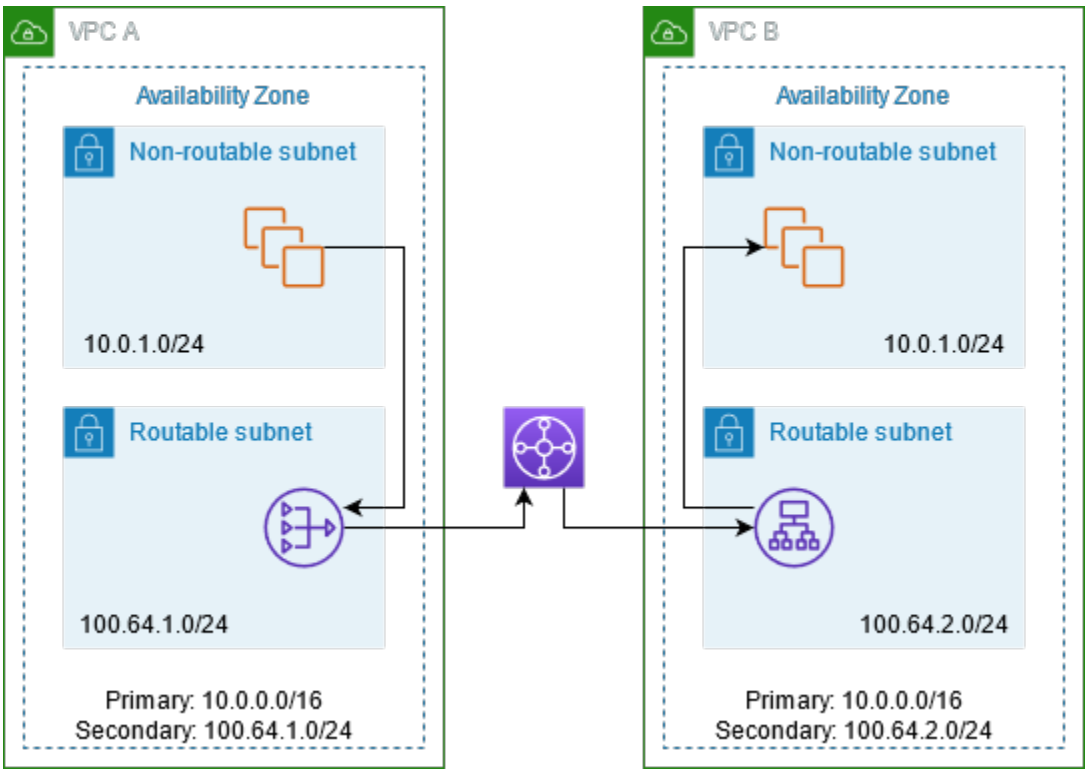
- Panoramica
- Risorse
- Routing

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 le risorse come di seguito:

- Associa gli intervalli di indirizzi IP instradabili assegnati ai rispettivi. VPCs
- 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.
- Crea un gateway di transito per connettere il VPCs. 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
10.0.0.0/16	local
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
10.0.0.0/16	local
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
10.0.0.0/16	local
100.64.2.0/24	local

La seguente è la tabella di instradamento per la sottorete instradabile nel VPC B.

Destinazione	Target
10.0.0.0/16	local
100.64.2.0/24	local

Destinazione	Target
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	*Attachment for VPC A*	Statico
100.64.2.0/24	*Attachment for VPC B*	Statico

DNS64 e NAT64

Un gateway NAT supporta la traduzione degli indirizzi di rete da IPv6 a IPv4, popolarmente nota come. NAT64 NAT64 aiuta IPv6 AWS le tue risorse a comunicare con IPv4 le risorse nello stesso VPC o in un VPC diverso, nella tua rete locale o su Internet. Puoi utilizzarlo NAT64 con DNS64 Amazon Route 53 Resolver o usare il tuo server. DNS64

Indice

- Che cos'è? DNS64
- Che cos'è? NAT64
- Configura e DNS64 NAT64

Che cos'è? DNS64

I tuoi carichi di lavoro « IPv6-only» in esecuzione VPCs possono solo inviare e ricevere pacchetti di IPv6 rete. DNS64In caso contrario, una query DNS per un servizio IPv4 -only produrrà un indirizzo di IPv4 destinazione in risposta e il servizio IPv6 -only non potrà comunicare con esso. Per colmare questa lacuna di comunicazione, è possibile abilitare DNS64 una sottorete, che si applica a tutte le AWS risorse all'interno di quella sottorete. Con DNS64, Amazon Route 53 Resolver cerca il record DNS per il servizio richiesto ed esegue una delle seguenti operazioni:

- Se il record contiene un IPv6 indirizzo, restituisce il record originale e la connessione viene stabilita senza alcuna traduzione. IPv6

- Se non è presente alcun IPv6 indirizzo associato alla destinazione nel record DNS, il Route 53 Resolver ne sintetizza uno anteponendo il `/96` prefisso noto, definito in RFC6 052 ()`64:ff9b::/96`, all'indirizzo nel record. IPv4 Il tuo servizio IPv6 -only invia pacchetti di rete all'indirizzo sintetizzato. IPv6 Dovrai quindi instradare questo traffico attraverso il gateway NAT, che esegue la traduzione necessaria sul traffico per consentire ai servizi della sottorete di accedere ai IPv6 servizi esterni a quella sottorete. IPv4

È possibile abilitare o disabilitare DNS64 su una sottorete modify-subnet-attributeutilizzando la AWS CLI o con la console VPC selezionando una sottorete e scegliendo Azioni > Modifica impostazioni sottorete.

Che cos'è? NAT64

NAT64 consente ai tuoi servizi IPv6 solo in Amazon VPCs di comunicare con servizi IPv4 solo all'interno dello stesso VPC (in diverse sottoreti) o connessi VPCs, nelle tue reti locali o su Internet.

NAT64 è automaticamente disponibile sui gateway NAT esistenti o su tutti i nuovi gateway NAT che crei. 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 funzionare. NAT64

Dopo l'attivazione DNS64, se il servizio IPv6 -only invia pacchetti di rete a un indirizzo sintetizzato IPv6 tramite il gateway NAT, si verifica quanto segue:

- A partire dal `64:ff9b::/96` prefisso, il gateway NAT riconosce che la destinazione originale è IPv4 e traduce i pacchetti sostituendo: IPv6 IPv4
  - Fonte IPv6 con un proprio IP privato che viene tradotto in indirizzo IP elastico dal gateway Internet.
  - Destinazione IPv6 a IPv4 troncando il prefisso. `64:ff9b::/96`
- Il gateway NAT invia i IPv4 pacchetti tradotti alla destinazione tramite il gateway Internet, il gateway privato virtuale o il gateway di transito e avvia una connessione.
- L'host IPv4 -only restituisce i pacchetti di risposta. IPv4 Dopo aver stabilito una connessione, il gateway NAT accetta i IPv4 pacchetti di risposta dagli host esterni.
- I IPv4 pacchetti di risposta sono destinati al gateway NAT, che riceve i pacchetti e NATs li decodifica sostituendo il proprio IP (IP di destinazione) con l' IPv6 indirizzo dell'host e anteponendo l'indirizzo di origine. `64:ff9b::/96` IPv4 Il pacchetto quindi scorre verso l'host seguendo il routing locale.

In questo modo, il gateway NAT consente ai soli carichi di lavoro in una sottorete di comunicare con i servizi IPv6 -only esterni alla sottorete. IPv4

Configura e DNS64 NAT64

Segui i passaggi in questa sezione per configurare DNS64 e NAT64 abilitare la comunicazione con i servizi IPv4 -only.

Indice

- Abilita la comunicazione con IPv4 i soli servizi su Internet con la CLI AWS
- Abilita la comunicazione con i IPv4 soli servizi nel tuo ambiente locale

Abilita la comunicazione con IPv4 i soli servizi su Internet con la CLI AWS

Se disponi di una sottorete con carichi di lavoro IPv6 solo che deve comunicare con servizi IPv4 -only esterni alla sottorete, questo esempio mostra come abilitare questi servizi -only per comunicare con i servizi IPv6 -only su Internet. IPv4

È innanzitutto necessario configurare un gateway NAT in una sottorete pubblica (separata dalla sottorete contenente i carichi di lavoro -only). IPv6 Ad esempio, la sottorete contenente il gateway NAT dovrebbe avere un routing `0.0.0.0/0` che punta al gateway Internet.

Completa questi passaggi per consentire a questi servizi IPv6 -only di connettersi con IPv4 i servizi -only su Internet:

1. Aggiungi le seguenti tre route alla tabella delle rotte della sottorete contenente i carichi di lavoro -only: IPv6

   - IPv4 rotta (se presente) che punta al gateway NAT.
   - Routing `64:ff9b::/96` che punta al gateway NAT. Ciò consentirà di instradare il traffico proveniente dai IPv6 soli carichi di lavoro destinati ai IPv4 soli servizi attraverso il gateway NAT.
   - IPv6 `::/0`percorso che punta al gateway Internet solo in uscita (o al gateway Internet).

   Tieni presente che il puntamento `::/0` al gateway Internet consentirà agli IPv6 host esterni (esterni al VPC) di avviare la connessione. 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. Abilita DNS64 la funzionalità nella sottorete contenente i carichi di lavoro -only. IPv6

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --enable-dns64
```

Ora, le risorse della tua sottorete privata possono stabilire connessioni statiche con entrambi i IPv4 servizi su Internet. IPv6 Configura il tuo gruppo di sicurezza NACLs in modo appropriato per consentire il traffico in uscita e in ingresso al traffico. `64:ff9b::/96`

Abilita la comunicazione con i IPv4 soli servizi nel tuo ambiente locale

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:

- Crei un endpoint in uscita Route 53 Resolver in un VPC e gli assegni gli indirizzi da IPv4 cui desideri che Route 53 Resolver inoltri le query. Per il resolver DNS locale, questi sono gli indirizzi IP da cui provengono le query DNS e, pertanto, dovrebbero 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. È inoltre necessario specificare gli indirizzi dei resolver locali IPv4 .
- Ora che hai configurato un endpoint in uscita Route 53 Resolver, devi DNS64 abilitarlo nella sottorete contenente IPv6 solo i carichi di lavoro e instradare tutti i dati destinati alla rete locale tramite un gateway NAT.

Come funziona per le sole destinazioni nelle reti locali: DNS64 IPv4

1. Assegni un IPv4 indirizzo all'endpoint in uscita Route 53 Resolver nel tuo VPC.

2. La query DNS del tuo IPv6 servizio passa a Route 53 Resolver. IPv6 Route 53 Resolver confronta la query con la regola di inoltro e ottiene un IPv4 indirizzo per il resolver locale.
3. Route 53 Resolver converte il pacchetto di query da IPv4 e lo inoltra all'endpoint IPv6 in uscita. Ogni indirizzo IP dell'endpoint rappresenta un ENI che inoltra la richiesta all'indirizzo locale del resolver DNS. IPv4
4. Il resolver locale invia il pacchetto di risposta attraverso l'endpoint in uscita a IPv4 Route 53 Resolver.
5. Supponendo che la query sia stata effettuata da una sottorete DNS64 abilitata, Route 53 Resolver fa due cose:

    a. Controlla il contenuto del pacchetto di risposta. Se c'è un IPv6 indirizzo nel record, mantiene il contenuto così com'è, ma se contiene solo un record. IPv4 Inoltre, sintetizza un IPv6 record anteponendo l'indirizzo. `64:ff9b::/96` IPv4

    b. Riconfeziona il contenuto e lo invia al servizio nel tuo IPv6 VPC tramite.

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. Queste metriche offrono visibilità sullo stato e sulle prestazioni del tuo gateway NAT, consentendoti di monitorarne attentamente il funzionamento e risolvere rapidamente eventuali problemi.

Le metriche del gateway NAT raccolte da CloudWatch includono punti dati come i byte elaborati, il numero di pacchetti, il conteggio delle connessioni e i tassi di errore. Ciò consente di comprendere a fondo il traffico che scorre attraverso il gateway NAT e di identificare eventuali anomalie o colli di bottiglia. CloudWatch fornisce questi dati metrici a intervalli di 1 minuto, offrendoti una visione granulare del comportamento del tuo gateway NAT. up-to-the-minute

Inoltre, CloudWatch conserva i dati metrici di questo gateway NAT per un periodo prolungato di 15 mesi, consentendoti di analizzare tendenze e modelli nel tempo. È possibile utilizzare questi dati storici per la pianificazione della capacità, l'ottimizzazione delle prestazioni e la comprensione dell'evoluzione a lungo termine dell'utilizzo del gateway NAT.

Per sfruttare queste potenti funzionalità di monitoraggio, puoi creare CloudWatch dashboard e allarmi personalizzati in base alle tue esigenze specifiche. Ad esempio, puoi impostare avvisi che ti

informino ogni volta che il trasferimento di dati in uscita dal gateway NAT supera una certa soglia, consentendoti di affrontare in modo proattivo i potenziali vincoli di larghezza di banda.

Per ulteriori informazioni sui prezzi, consulta la pagina CloudWatch dei prezzi di Amazon.

Indice

- Parametri e dimensioni del gateway NAT
- Visualizza le metriche del gateway CloudWatch NAT
- Crea CloudWatch allarmi per monitorare un gateway NAT

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. Un valore pari a zero indica che non ci sono connessioni attive attraverso il gateway NAT. Unità: numero Statistiche: la statistica più utile è `Max`.
`BytesInFromDestination`	Il numero di byte ricevuti dal gateway NAT e provenienti dalla destinazione. 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. Unità: byte

Parametro	Descrizione
	Statistiche: la statistica più utile è `Sum`.
`BytesInFromSource`	Il numero di byte ricevuti dal gateway NAT e provenienti dai clienti nel tuo VPC. Se il valore per `BytesOutToDestination` è inferiore al valore per `BytesInFromSource`, vi potrebbe essere una perdita di dati durante l'esecuzione del gateway NAT. Unità: byte Statistiche: la statistica più utile è `Sum`.
`BytesOutToDestination`	Il numero di byte inviati per mezzo del gateway NAT verso la destinazione. 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. Unità: byte Statistiche: la statistica più utile è `Sum`.

Parametro	Descrizione
`BytesOutToSource`	Il numero di byte inviati per mezzo del gateway NAT verso i clienti nel tuo VPC. 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. Unità: byte Statistiche: la statistica più utile è `Sum`.
`ConnectionAttemptCount`	In numero di tentativi di connessione attraverso il gateway NAT. 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. Unità: numero Statistiche: la statistica più utile è `Sum`.

Parametro	Descrizione
`ConnectionEstablishedCount`	In numero di connessioni stabilite attraverso il gateway NAT. 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. Unità: numero Statistiche: la statistica più utile è `Sum`.
`ErrorPortAllocation`	Il numero di volte che il gateway NAT potrebbe non allocare una porta di origine. Un valore superiore a zero indica che sono aperte troppe connessioni simultanee sono attraverso il gateway NAT. Unità: numero Statistiche: la statistica più utile è `Sum`.

Parametro	Descrizione
`IdleTimeoutCount`	Numero di connessioni che sono transitate 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. Un valore superiore a zero indica che vi sono connessioni che sono state spostate a uno stato inattivo. Se il valore per `IdleTimeoutCount` aumenta, ciò potrebbe indicare che i clienti dietro al gateway NAT stanno usando connessioni obsolete. Unità: numero Statistiche: la statistica più utile è `Sum`.
`PacketsDropCount`	Il numero di pacchetti consegnati dal gateway NAT. Per calcolare il numero di pacchetti persi come percentuale del traffico complessivo di pacchetti, usa questa formula: `PacketsDropCount/(PacketsInFromSource+PacketsInFromDestination)*100`. Se questo valore supera lo 0,01% del traffico totale sul gateway NAT, potrebbe esserci un problema legato al servizio Amazon VPC. Utilizza la dashboard di stato del servizio AWS per identificare eventuali problemi relativi al servizio che potrebbero causare la perdita di pacchetti da parte dei gateway NAT. Unità: numero Statistiche: la statistica più utile è `Sum`.

Parametro	Descrizione
`PacketsInFromDestination`	Il numero di pacchetti ricevuti dal gateway NAT e provenienti dalla destinazione. 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. Unità: numero Statistiche: la statistica più utile è `Sum`.
`PacketsInFromSource`	Il numero di pacchetti ricevuti dal gateway NAT e provenienti dai clienti nel tuo VPC. Se il valore per `PacketsOutToDestination` è inferiore al valore per `PacketsInFromSource`, vi potrebbe essere una perdita di dati durante l'esecuzione del gateway NAT. Unità: numero Statistiche: la statistica più utile è `Sum`.

Parametro	Descrizione
PacketsOutToDestination	Il numero di pacchetti inviati per mezzo del gateway NAT verso la destinazione. 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. Unità: numero Statistiche: la statistica più utile è Sum.
PacketsOutToSource	Il numero di pacchetti inviati per mezzo del gateway NAT verso i clienti nel tuo VPC. 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. Unità: numero 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. Unità: numero 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). Unità: numero 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 CloudWatch NAT

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. Scegli lo spazio dei nomi delle NATGatewaymetriche.

4. Scegli la dimensione del dei parametri.

Per visualizzare le metriche utilizzando il 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. Scegli lo spazio dei nomi delle NATGatewaymetriche, quindi scegli una dimensione metrica. 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. Scegli Next (Successivo).
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. CloudWatch 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. Scegli lo spazio dei nomi delle NATGatewaymetriche, quindi scegli una dimensione metrica. 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. Scegli Next (Successivo).
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
- Quota gateway NAT
- Quota degli indirizzi IP elastici
- La zona di disponibilità non è supportata
- Il gateway NAT non è più visibile
- Il gateway NAT non risponde a un comando ping
- Le istanze non possono accedere a Internet
- La connessione TCP a una destinazione non va a buon fine
- L'output di tracciamento non visualizza l'indirizzo IP privato del gateway NAT
- Connessione Internet interrotta dopo 350 secondi
- Impossibile stabilire connessione IPsec
- Impossibile avviare più connessioni

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, consultare Aggiunta di un accesso Internet a una sottorete.
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

Errore visualizzato	Causa	Soluzione
		elastico per tale risorsa non è richiesto, puoi annullare l'associazione. In alternativa, alloca un nuovo indirizzo IP elastico nell'account. Per ulteriori informazioni, consulta Iniziare a utilizzare gli 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

Esegui una di queste 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, consulta Creazione di un gateway NAT o Come modificare le associazioni di indirizzi IP secondari.

Prezzi per i gateway NAT

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 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 IPv4 traffico in uscita verso Internet, ma non possono ricevere il traffico in entrata avviato su Internet.

> **Important**
>
> L'AMI NAT è basata sull'ultima versione di Amazon Linux AMI, 2018.03, che ha raggiunto la fine del supporto standard il 31 dicembre 2020 e la fine del supporto alla 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 soddisfano meglio il proprio caso d'uso rispetto ai gateway NAT, è possibile creare la propria AMI NAT da una versione corrente di Amazon Linux come descritto in the section called “3. Creazione di un'AMI NAT”.

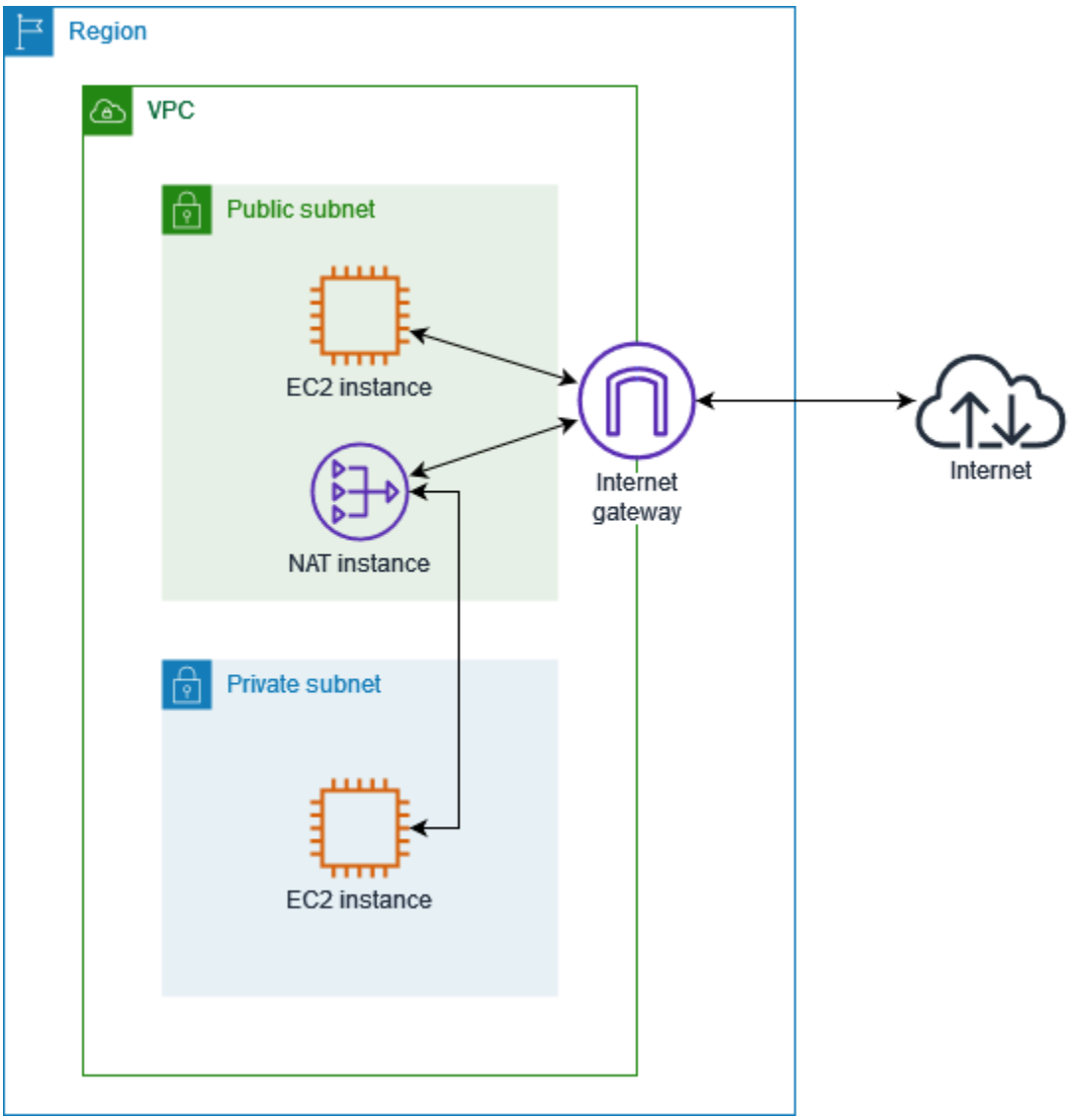
Indice

- Principi di base di un'istanza NAT
- Consentire alle risorse private di comunicare all'esterno del VPC

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 le quote dei EC2 servizi Amazon nel Riferimenti generali di AWS.

Consentire alle risorse private di comunicare all'esterno del VPC

Questa sezione descrive come creare e utilizzare istanze NAT per consentire alle risorse di una sottorete privata di comunicare all'esterno del cloud privato virtuale.

Attività

- 1. Creazione di un VPC per l'istanza NAT

- 2. Creazione di un gruppo di sicurezza per l'istanza NAT
- 3. Creazione di un'AMI NAT
- 4. Avvio di un'istanza NAT
- 5. Disabilitazione dei controlli di origine/destinazione
- 6. Aggiornamento della tabella di routing
- 7. Testa l'istanza NAT

1. 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 la 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.

2. 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 in entrata consigliate.

Crea	Protocollo	Intervallo porte	Commenti
Private subnet CIDR	TCP	80	Consente il traffico HTTP in entrata dai server nella sottorete privata
Private subnet CIDR	TCP	443	Consente il traffico HTTPS in entrata dai server nella sottorete privata
Public IP address range of your network	TCP	22	Consente l'accesso SSH in entrata alle istanze NAT dalla rete (sul gateway Internet).

Di seguito sono riportate le regole in uscita consigliate.

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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello 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.

3. Creazione di un'AMI NAT

Un AMI NAT è configurato per eseguire NAT su un' EC2 istanza. 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' EC2 istanza che esegue AL2 023 o Amazon Linux 2. 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 lo è`eth0`, *`eth0`* sostituiscila 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' EC2 istanza. Per ulteriori informazioni, consulta Creare un'AMI Linux da un'istanza nella Amazon EC2 User Guide.

4. 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 EC2 console Amazon 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 le immagini delle applicazioni e del sistema operativo, seleziona il tuo AMI NAT (scegli Sfoglia altro AMIs, Mio AMIs).
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 5. Disabilitazione dei controlli di origine/destinazione).

10. Aggiorna la tabella di routing per inviare il traffico all'istanza NAT (consulta 6. Aggiornamento della tabella di routing).

5. Disabilitazione dei controlli di origine/destinazione

Ogni EC2 istanza esegue source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. However, a NAT instance must be able to send and receive traffic when the source or destination is not itself. Therefore, you must disable source/destination controlli sull'istanza NAT.

Disabilitazione dei controlli di origine/destinazione

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, seleziona Instances (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. Seleziona 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.

6. 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. Scegli Save changes (Salva modifiche).

Per ulteriori informazioni, consulta Configurare le tabelle di routing.

7. 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
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. Scegli Aggiungi regola. Scegli All 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. Scegli Aggiungi regola. Scegliete Tutto ICMP - IPv4 per Tipo. Scegli Anywhere - 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 EC2 console Amazon 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 tua chiave privata usando Pu TTYgen.

   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 5. Disabilitazione dei controlli di origine/destinazione.
- Controlla che le tabelle di routing siano state correttamente configurate. Per ulteriori informazioni, consulta 6. 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 Terminare l'istanza nella Amazon EC2 User Guide.

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	Gestita 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 le metriche di CloudWatch per il gateway NAT.	Visualizza le metriche di CloudWatch 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. 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 IPv4 indirizzo pubblico statico progettato specificamente per la natura dinamica del cloud computing. Questa funzionalità ti consente di associare un indirizzo IP elastico a qualsiasi istanza o interfaccia di rete all'interno di qualsiasi Virtual Private Cloud (VPC) del tuo account. AWS Sfruttando gli indirizzi IP elastici, puoi sbloccare una serie di vantaggi che semplificano la gestione e la resilienza della tua infrastruttura basata sul cloud.

Uno dei vantaggi principali degli indirizzi IP elastici è la loro capacità di mascherare l'errore di un'istanza. Se un'istanza subisce un'interruzione imprevista o deve essere sostituita, puoi rimappare l'indirizzo IP elastico associato a un'altra istanza all'interno del tuo VPC. Questo processo di failover garantisce che le applicazioni e i servizi mantengano un endpoint pubblico coerente e affidabile, riducendo al minimo il tempo di inattività e offrendo un'esperienza utente superiore.

Inoltre, gli indirizzi IP elastici offrono flessibilità nella gestione delle risorse di rete. È possibile associare e dissociare questi indirizzi in modo programmatico a seconda delle esigenze, in modo da indirizzare il traffico verso istanze diverse in base all'evoluzione dei requisiti aziendali. L'allocazione dinamica degli indirizzi IP pubblici consente di adattarsi ai cambiamenti della domanda, di scalare l'infrastruttura e di implementare architetture innovative senza i vincoli dell'assegnazione statica degli IP.

Oltre a essere utilizzati per il failover delle istanze, gli indirizzi IP elastici possono anche servire come identificatori stabili per le risorse basate sul cloud. Ciò può essere utile quando si configurano servizi esterni, come i record DNS o le regole del firewall, per comunicare con le AWS applicazioni ospitate.

Associando un indirizzo IP pubblico persistente, puoi proteggere in futuro le configurazioni di rete ed evitare di aggiornare i riferimenti esterni quando le istanze sottostanti vengono sostituite o scalate.

Indice

- Concetti e regole degli indirizzi IP elastici
- Iniziare a utilizzare gli indirizzi IP elastici

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 Amazon EC2 User Guide.

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 associ un indirizzo IP elastico all'interfaccia di rete principale dell'istanza, l' IPv4 indirizzo pubblico corrente (se ne aveva uno) viene rilasciato al pool di indirizzi IP pubblico. Se si dissocia l'indirizzo IP elastico, all'interfaccia di rete principale viene assegnato automaticamente un nuovo IPv4 indirizzo 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 non IPv6 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 Rete ACLs.
- 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.
- IPv4 Gli indirizzi pubblici supportano i tag di allocazione dei costi. Se applichi tag a indirizzi IP elastici, puoi utilizzare tali tag per tenere traccia dei costi IPv4 degli indirizzi pubblici. AWS Cost Explorer

  Prima di poter utilizzare i tag come tag di allocazione dei costi, è necessario attivarli. Per ulteriori informazioni, consulta Attivazione dei tag per l'allocazione dei costi definiti dall'utente nella Guida per l'utente di AWS Billing . Dopo aver creato e applicato i tag definiti dall'utente alle risorse, possono essere necessarie fino a 24 ore prima che le chiavi di tag vengano visualizzate nella pagina dei tag di allocazione dei costi per l'attivazione.

  Una volta attivati i tag di allocazione dei costi…
  - Per tutti IPv4 gli indirizzi pubblici (inclusi IPv4 gli indirizzi pubblici assegnati alle EC2 istanze e gli indirizzi IP elastici) associati a un'interfaccia di rete elastica, puoi visualizzare i costi associati IPv4 agli indirizzi pubblici in Cost Explorer selezionando Tipo di utilizzo > Pubblico IPv4 InUseAddress (ore).
  - Se un indirizzo IP elastico con tag non è associato a un ENI o è associato a una risorsa interrotta (come un' EC2 istanza interrotta), viene considerato un indirizzo inattivo IPv4 . È possibile visualizzare i costi associati IPv4 agli indirizzi inattivi in Cost Explorer selezionando Tipo di utilizzo > Pubblico IPv4 IdleAddress (ore).

  Per ulteriori informazioni su Cost Explorer, consulta Analisi dei costi con AWS Cost Explorer nella Guida per l'utente di AWS Billing .

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 .

Per ulteriori informazioni sui prezzi degli indirizzi IP elastici, consulta la sezione IPv4 Indirizzo pubblico nei prezzi di Amazon VPC.

Iniziare a utilizzare gli indirizzi IP elastici

Le sezioni seguenti descrivono come iniziare a utilizzare gli indirizzi IP elastici.

Attività

- 1. Allocare un indirizzo IP elastico
- 2. Associazione di un indirizzo IP elastico
- 3. Annullare l'associazione di un indirizzo IP elastico
- 4. Trasferimento degli indirizzi IP elastici
- 5. Rilascio di un indirizzo IP elastico
- 6. Recupero di un indirizzo IP elastico
- Panoramica della riga di comando

1. 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Elastic IPs.
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 confini di rete è una raccolta di Availability Zones (AZs), 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 da quelli di AZs 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 Local Zones o Wavelength Zones (per ulteriori informazioni, consulta Enable a Local Zone o Enable Wavelength Zones), puoi scegliere un gruppo di confini di rete per Local Zones o Wavelength AZs Zones. Scegliete con attenzione il gruppo di confini di rete, poiché l'EIP e la AWS risorsa a cui è associata devono risiedere nello stesso gruppo di confini di rete. Puoi usare la EC2 console per visualizzare il gruppo di confini di rete in cui si trovano le tue Availability Zones, Local Zones o Wavelength Zones (vedi Local Zones). 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 Local Zones o Wavelength Zones, quando allochi un EIP, il gruppo di confini di rete che rappresenta tutti i confini AZs della regione (ad esempio`us-west-2`) è predefinito e non puoi modificarlo. Ciò significa che l'EIP assegnato a questo gruppo di confine di rete verrà pubblicizzato in tutta la regione in cui ti trovi. AZs

5. Per Public IPv4 address pool scegli una delle seguenti opzioni:

   - Pool di indirizzi IP di Amazon: se desideri che venga assegnato un IPv4 indirizzo dal pool di indirizzi IP di Amazon.
   - Il mio pool di IPv4 indirizzi pubblici: se desideri allocare un IPv4 indirizzo 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 IPv4 indirizzi di proprietà del cliente: se desideri allocare un IPv4 indirizzo da un pool creato dalla tua rete locale da utilizzare con 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.

2. 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Elastic. IPs
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).

3. 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Elastic IPs.
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).

4. Trasferimento degli 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 Account AWS all'altro. Non devi aspettare che i nuovi indirizzi IP elastici vengano inseriti nell'elenco consentito nei tuoi gruppi di sicurezza e. NACLs
- Amministrazione centralizzata della sicurezza: utilizza un account di AWS sicurezza centralizzato per tracciare e trasferire gli indirizzi IP elastici che sono stati controllati per verificarne la conformità alla sicurezza.
- Disaster recovery: utilizza i trasferimenti di indirizzi IP elastici per modificare rapidamente la mappatura dei carichi di lavoro Internet rivolti al pubblico durante IPs 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 describe-address-transfers AWS CLI comando). 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 describe-address-transfers AWS CLI comando) per 14 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 IPv4 indirizzi pubblici 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.

Abilitazione del trasferimento di indirizzi IP elastici

1. Assicurati di utilizzare l' AWS account di origine.
2. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Nel riquadro di navigazione, scegli Elastic IPs.
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 singolo AWS account.
   - Scegli Account multipli se trasferisci gli indirizzi IP elastici su più AWS account.
6. In Transfer account ID, inserisci gli IDs AWS account 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Nel riquadro di navigazione, scegli Elastic IPs.
4. Nell'elenco delle risorse di Elastic IPs, assicurati di avere abilitata la proprietà che mostra la colonna Transfer status.
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 describe-address-transfers AWS CLI comando). 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:

- AddressLimitExceeded: 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 Amazon EC2 User Guide 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 Amazon EC2 User Guide.
- InvalidTransfer. AddressAssociated: Se un indirizzo IP elastico è associato a un ENI o a un' EC2 istanza, 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 Supporto.

Questa procedura deve essere completata dall'account di trasferimento.

Accettazione del trasferimento di un indirizzo IP elastico

1. Assicurati di utilizzare l'account di trasferimento.
2. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Nel riquadro di navigazione, scegli Elastic IPs.
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.

5. 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 anche se non è associato a un'istanza. L'indirizzo IP elastico non deve essere associato a un'istanza o un'interfaccia di rete.

per rilasciare un indirizzo IP elastico

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Elastic IPs.
3. Selezionare l'indirizzo IP elastico e scegliere Actions (Operazioni), Release Elastic IP addresses (Rilascia indirizzi IP elastici).
4. Quando richiesto, selezionare Release (Rilascia).

6. 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 utilizzando l' EC2 API Amazon o uno strumento da 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 della riga di comando

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)

Connect il tuo VPC ad altre VPCs reti utilizzando un gateway di transito

Puoi connettere i tuoi cloud privati virtuali (VPC) e le reti locali utilizzando un gateway di transito, che funge da hub centrale, instradando il traffico tra VPCs connessioni VPN e connessioni. AWS Direct Connect

Uno dei principali vantaggi dell'utilizzo di un gateway di transito è la capacità di centralizzare e semplificare la gestione della connettività tra la VPCs rete aziendale e quella locale. Anziché configurare più collegamenti VPN o Direct Connect, è possibile sfruttare il gateway di transito come unico punto di integrazione, il che aiuta a ridurre la complessità generale e il sovraccarico operativo dell'architettura di rete.

Il prezzo per l'utilizzo di un gateway di transito è basato sul volume di dati trasferiti attraverso il gateway. È prevista una tariffa per GB per i dati trasferiti in entrata e in uscita dal gateway di transito, nonché una tariffa oraria separata per la risorsa gateway di transito stessa. I prezzi specifici possono

variare in base alla AWS regione e sono soggetti a modifiche, quindi è importante fare riferimento alla pagina AWS Transit Gateway dei prezzi corrente per la maggior parte delle up-to-date informazioni. Comprendendo il modello tariffario per i gateway di transito, è possibile pianificare e pianificare meglio i costi correnti associati a questo servizio AWS di rete. In questo modo, e in combinazione con l'efficienza operativa e i vantaggi in termini di connettività, i gateway di transito diventano una scelta convincente per le organizzazioni che desiderano creare soluzioni cloud ibride scalabili e a costi contenuti.

La tabella seguente descrive alcuni casi d'uso comuni per i gateway di transito. Per ulteriori informazioni su ciascun caso d'uso, consulta Esempi di scenari di gateway di transito nella Guida per l'AWS Transit Gateway utente.

Esempio	Utilizzo
Router centralizzato	Configura il tuo gateway di transito come un router centralizzato che collega tutte le tue e VPCs AWS Direct Connect le tue AWS Site-to-Site VPN connessioni.
Isolato VPCs	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.
Isolato VPCs 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 AWS Transit Gateway.

Connetti il tuo VPC a reti remote utilizzando AWS Virtual Private Network

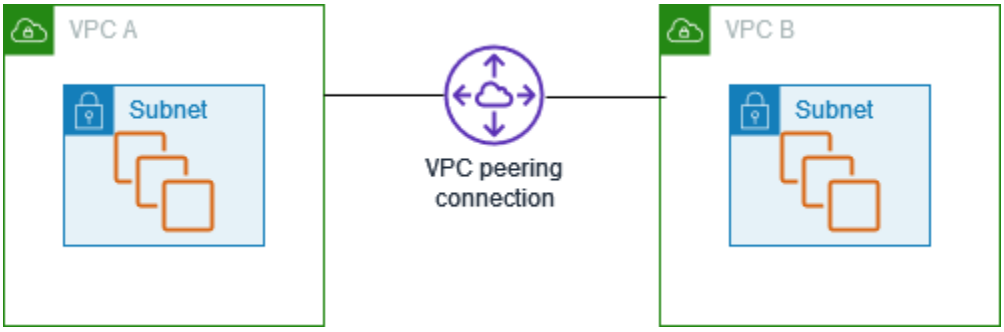
Puoi connettere il tuo VPC a reti e utenti remoti utilizzando le opzioni di connettività VPN seguenti.

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 funzionalità di rete che consente una comunicazione sicura e diretta tra due cloud privati virtuali (VPC) all'interno dell'infrastruttura AWS. Questa connessione privata consente alle risorse dei VPC con peering di interagire tra loro come se facessero parte della stessa rete, eliminando la necessità di attraversare la rete Internet pubblica.



Il processo di creazione di una connessione peering VPC sfrutta l'infrastruttura VPC esistente per stabilire questa connessione, senza la necessità di un gateway, AWS Site-to-Site VPN o un hardware fisico aggiuntivo. Questo design garantisce l'assenza di punti di errore o colli di bottiglia della larghezza di banda.

Uno dei principali vantaggi di una connessione peering VPC è la possibilità di connettere VPC tra account AWS diversi o anche aree AWS diverse. Questa flessibilità consente alle organizzazioni di integrare senza problemi le proprie risorse cloud, indipendentemente dal fatto che si trovino all'interno dello stesso account o distribuite su più account e aree geografiche. La natura privata della connessione garantisce inoltre che tutto il traffico di dati tra i VPC con peering rimanga all'interno della rete AWS, senza mai attraversare la rete Internet pubblica.

I casi d'uso per le connessioni peering VPC sono molteplici. Le organizzazioni possono sfruttare questa funzionalità per consentire una comunicazione sicura tra diversi livelli di un'applicazione (come server Web e server di database), facilitare la condivisione di risorse tra più team o unità aziendali, oppure abilitare persino architetture cloud ibride collegando le reti on-premises ai propri VPC AWS.

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.

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

Puoi utilizzare VPC Flow Logs per acquisire informazioni dettagliate sul traffico in entrata e in uscita dalle interfacce di rete del tuo. VPCs

Amazon CloudWatch Internet Monitor

Puoi utilizzare Internet Monitor per vedere in che modo i problemi di Internet influiscono sulle prestazioni e sulla disponibilità tra le applicazioni ospitate su AWS e gli utenti finali. Puoi anche scoprire, quasi in tempo reale, come migliorare la latenza prevista della tua applicazione passando a utilizzare altri servizi o reindirizzando il traffico verso il tuo carico di lavoro tramite diversi. Regioni AWS Per ulteriori informazioni, consulta Usare Amazon CloudWatch Internet Monitor.

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 funzionalità per copiare il traffico di rete da un'interfaccia di rete di un' EC2 istanza Amazon e inviarlo ad appliance out-of-band di sicurezza e monitoraggio 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 di rete tra due risorse nel VPC. Dopo aver specificato le risorse di origine e di destinazione, Reachability Analyzer hop-by-hop produce i dettagli del percorso virtuale tra di esse 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.

CloudTrail registri

Puoi AWS CloudTrail utilizzarlo per acquisire informazioni dettagliate sulle chiamate effettuate all'API Amazon VPC. Puoi utilizzare CloudTrail i log generati per determinare quali chiamate sono state effettuate, l'indirizzo IP di origine da cui proviene la chiamata, chi ha effettuato la chiamata, quando è stata effettuata la chiamata e così via. Per ulteriori informazioni, consulta la sezione Registrazione delle chiamate EC2 API Amazon AWS CloudTrail nell'Amazon EC2 User Guide.

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. VPCs Per informazioni sui log di flusso per i gateway di transito introdotti nella versione 6, consulta Registrazione del traffico di rete

utilizzando i log di flusso di Transit Gateway nella Guida per l'utente di Amazon VPC Transit Gateway.

Indice

- Nozioni di base sui log di flusso
- Record di log di flusso
- Esempi di record di log di flusso
- Limitazioni del log di flusso
- Prezzi
- Utilizzo dei log di flusso
- Pubblica i log di flusso in Logs CloudWatch
- Pubblicazione di log di flusso su Amazon S3
- Pubblicazione dei log di flusso in 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

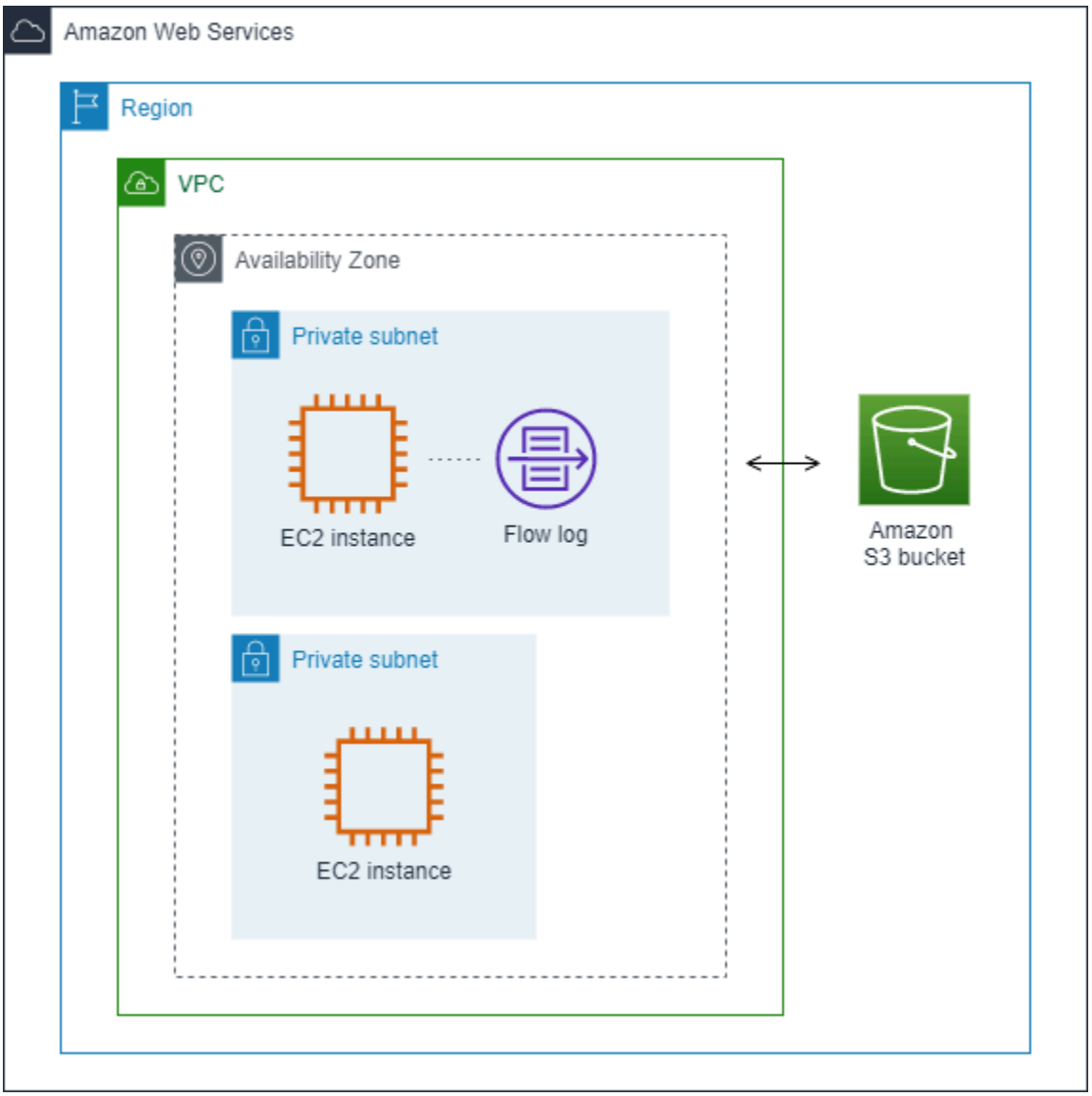
Puoi creare un log di flusso per un VPC, una sottorete o un'interfaccia di rete. Se crei un log di flusso per una sottorete o un VPC, viene monitorata ogni interfaccia di rete nella sottorete o nel VPC.

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.

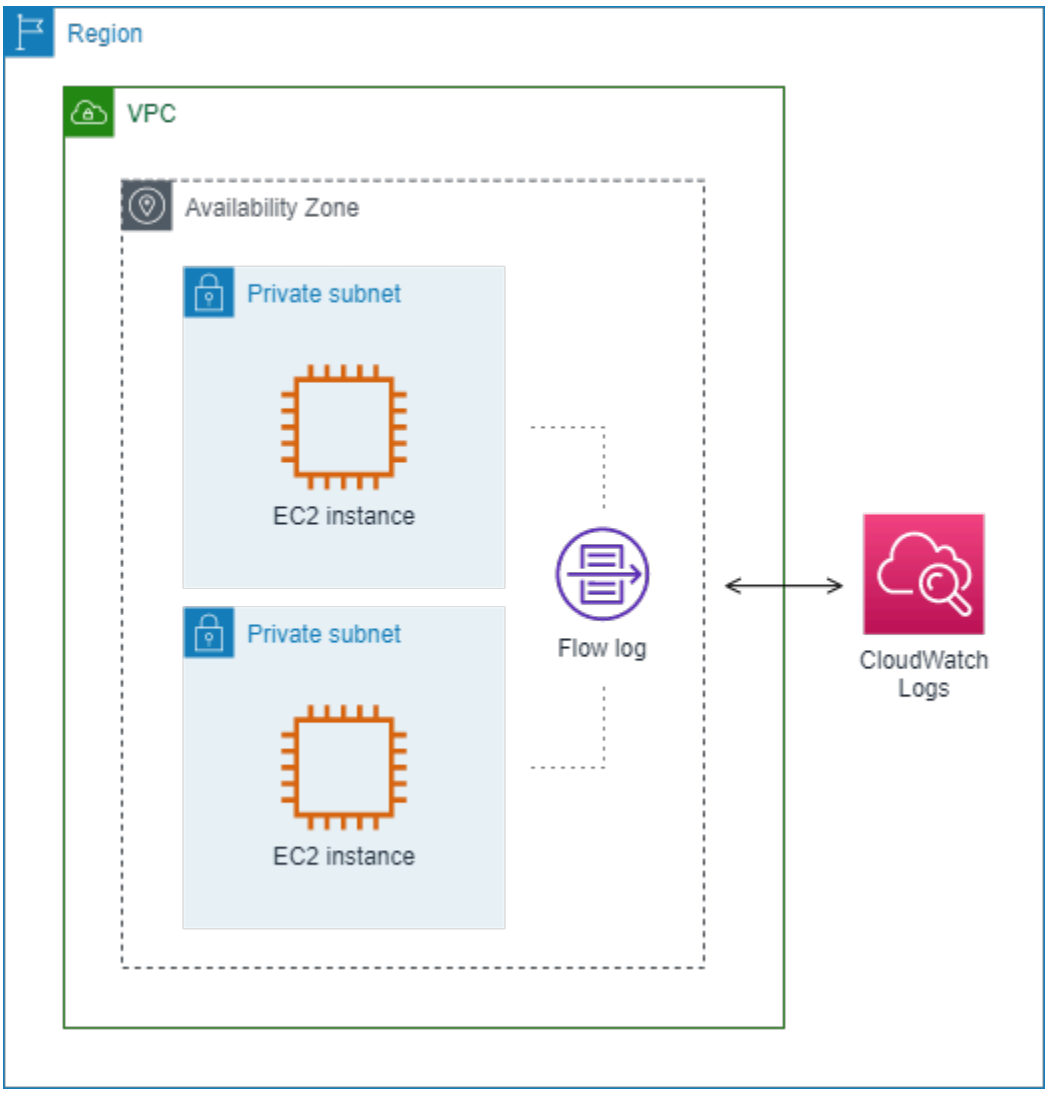
Per creare un log di flusso, occorre specificare:

- 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, crei un log di flusso che acquisisce il traffico accettato per l'interfaccia di rete per una delle EC2 istanze 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 2. 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, devi utilizzare la EC2 console Amazon o l' EC2 API Amazon 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 4. 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
- Formato predefinito
- Formato personalizzato
- Campi disponibili

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 che i dati sono stati acquisiti 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 testo semplice, tutti i campi sono di tipo STRING. Se il formato è Parquet, consulta la tabella per i tipi di dati dei campi.

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. 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 visualizzato unknown per questo campo. Tipo di dati Parquet: STRING	2
interface-id	L'ID dell'interfaccia di rete per la quale il traffico viene registrato. Tipo di dati parquet: STRING	2
srcaddr	Per il traffico in entrata, questo è l'indirizzo IP della fonte di traffico. Per il traffico in uscita, si tratta dell' IPv4 indirizzo privato o dell' IPv6 interfaccia di rete che invia il traffico. Consulta anche pkt-srcaddr. Tipo di dati Parquet: STRING	2
dstaddr	L'indirizzo di destinazione per il traffico in uscita o l' IPv6 indirizzo IPv4 o dell'interfaccia di rete per il traffico in entrata sull'interfaccia di rete. L' IPv4 indirizzo dell'interfaccia di rete è sempre il suo indirizzo privato IPv4 . Consulta anche pkt-dstaddr.	2

Campo	Descrizione	Version
	Tipo di dati Parquet: STRING	
srcport	La porta di origine del traffico. Tipo di dati parquet: INT_32	2
dstport	La porta di destinazione del traffico. 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. Tipo di dati parquet: INT_32	2
packets	Il numero di pacchetti trasferiti durante il flusso. Tipo di dati parquet: INT_64	2
bytes	Il numero di byte trasferiti durante il flusso. 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. Tipo di dati parquet: INT_64	2
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. Tipo di dati parquet: INT_64	2

Campo	Descrizione	Version
action	L'operazione associata al traffico: • ACCEPT — Il traffico è stato accettato. • REJECT — Il traffico è stato respinto. Ad esempio, il traffico non era consentito dai gruppi di sicurezza o dalla rete oppure ACLs i pacchetti sono arrivati dopo la chiusura della connessione. Tipo di dati Parquet: STRING	2
log-status	Lo stato di registrazione del log di flusso: • OK : i dati vengono registrati normalmente nelle destinazioni scelte. • NODATA : non vi è alcun traffico di rete da o per l'interfaccia di rete durante l'intervallo di aggregazione. • 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. Alcuni record del log di flusso sono stati ignorati durante l'intervallo di aggregazione (consulta log-status in Campi disponibili). Ciò può essere causato da un vincolo di AWS capacità interno o da un errore interno. Se utilizzi AWS Cost Explorer per visualizzare i costi dei log di flusso VPC e alcuni log di flusso vengono ignorati durante l'intervallo di aggregazione dei log di flusso, il numero di log di flusso riportato AWS Cost Explorer sarà superiore al numero di log di flusso pubblicati da Amazon VPC. Tipo di dati Parquet: STRING	2
vpc-id	L'ID del VPC che contiene l'interfaccia di rete per cui viene registrato il traffico. 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. 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. Tipo di dati parquet: STRING	3

Campo	Descrizione	Version
tcp-flags	Il valore bitmask per i seguenti flag TCP: • FIN - 1 • SYN - 2 • RST - 4 • SYN-ACK - 18 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 un motivo qualunque 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. 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. Per informazioni generali sui flag TCP (come il significato di flag come FIN, SYN e ACK), consulta Struttura del segmento TCP su Wikipedia. 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. Tipo di dati parquet: STRING	3

Campo	Descrizione	Version
pkt-srcaddr	L'indirizzo IP di origine a livello di pacchetto (originale) del traffico. Utilizzare questo campo con il campo srcaddr per distinguere l'indirizzo 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'indirizzo IP dell'interfaccia di rete del nodo dell'istanza in cui il pod è in esecuzione (per la comunicazione all'interno di un VPC). Tipo di dati parquet: STRING	3
pkt-dstaddr	L'indirizzo IP di destinazione a livello di pacchetto (originale) per il traffico. Utilizzare questo campo con il campo dstaddr per distinguere 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'indirizzo IP dell'interfaccia di rete del nodo dell'istanza in cui il pod è in esecuzione (per la comunicazione all'interno di un VPC). Tipo di dati parquet: STRING	3
region	Regione che contiene l'interfaccia di rete per la quale viene registrato il traffico. 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. 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. 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. Tipo di dati parquet: STRING	4
pkt-src-aws-service	Il nome del sottoinsieme di intervalli di indirizzi IP per il campo pkt-srcaddr campo, se l'indirizzo IP di origine è per un AWS servizio. 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. Tipo di dati parquet: STRING	5
pkt-dst-aws-service	Il nome del sottoinsieme di intervalli di indirizzi IP per il campo 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 . Tipo di dati parquet: STRING	5

Campo	Descrizione	Version
flow-direction	La direzione del flusso rispetto all'interfaccia in cui viene catturato il traffico. I valori possibili sono: ingress | egress. Tipo di dati parquet: STRING	5
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 -. • 1 - Tramite un'altra risorsa nello stesso VPC, comprese le risorse che creano un'interfaccia di rete nel VPC • 2 - Tramite un gateway Internet o un endpoint VPC gateway • 3 - Tramite un gateway privato virtuale • 4 - Tramite una connessione di peering VPC all'interno della regione • 5 - Tramite una connessione di peering VPC tra regioni • 6 - Tramite un gateway locale • 7 — Tramite un endpoint VPC del gateway (solo istanze basate su Nitro) • 8 — Tramite un gateway Internet (solo istanze basate su Nitro) 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 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 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 nel tuo abbonamento, devi essere autorizzato a chiamare ecs: ed ecs:ListClusters . ListContainerInstances 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 nel tuo abbonamento, devi essere autorizzato a chiamare ecs: ListClusters ed ecs:. ListContainerInstances Tipo di dati Parquet: STRING	7
ecs-container-id	ID di runtime Docker del container se il traffico proviene da un'attività ECS in esecuzione. Se nell'attività ECS sono presenti uno o più container, questo sarà l'ID di runtime Docker del primo container. Per includere questo campo nel tuo abbonamento, hai bisogno del permesso di chiamare ecs:. ListClusters Tipo di dati Parquet: STRING	7
ecs-second-container-id	ID di runtime Docker del container se il traffico proviene da un'attività ECS in esecuzione. Se nell'attività ECS sono presenti più container, questo sarà l'ID di runtime Docker del secondo container . Per includere questo campo nel tuo abbonamento, hai bisogno del permesso di chiamare ecs:. ListClusters Tipo di dati Parquet: STRING	7
ecs-service-name	Nome del servizio ECS se il traffico proviene da un'attività ECS in esecuzione e quest'ultima 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, hai bisogno del permesso di chiamare ecs: ListClusters ed ecs:. ListServices 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, hai bisogno del permesso di chiamare ecs: ed ecs: ListClusters ListTaskDefinitions 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, hai bisogno del permesso di chiamare ecs: ListClusters ed ecs:. ListTasks 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, hai bisogno del permesso di chiamare ecs: ListClusters ed ecs:. ListTasks Tipo di dati Parquet: STRING	7
reject-reason	Motivo per cui il traffico è stato respinto. Valori possibili: BPA. Restituisce un “-” per qualsiasi altro motivo di rifiuto. Per ulteriori informazioni su Blocco dell'accesso pubblico (BPA) VPC, consulta Blocca l'accesso pubblico alle sottoreti VPCs e alle sottoreti. Tipo di dati Parquet: STRING	8

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
- Nessun dato e record ignorati

- Regole del gruppo di sicurezza e della lista di controllo accessi di rete
- IPv6 traffico
- Sequenza di flag TCP
- Traffico tramite un gateway NAT
- Traffico tramite un gateway di transito
- Nome del servizio, percorso di traffico e direzione del flusso

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 172.31.16.21 e ID eni-1235b8ca123456789 nell'account 123456789010 è stato 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
```

> **Note**
>
> Alcuni record del log di flusso sono stati ignorati durante l'intervallo di aggregazione (consulta log-status in Campi disponibili). Ciò può essere causato da un limite di AWS capacità interna o da un errore interno. Se utilizzi AWS Cost Explorer per visualizzare i costi dei log di flusso VPC e alcuni log di flusso vengono ignorati durante l'intervallo di aggregazione dei log di flusso, il numero di log di flusso riportato AWS Cost Explorer sarà superiore al numero di log di flusso pubblicati da Amazon VPC.

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. Al contrario, le reti ACLs sono prive di stato, pertanto le risposte al traffico consentito sono soggette alle regole ACL 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 ACLs le reti sono prive di stato, 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.
- A REJECT record 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 l'ACL di rete consente il traffico ICMP in uscita, il log di flusso visualizza due ACCEPT record (uno per il ping originario e uno per il ping di risposta). Se il gruppo di sicurezza nega il traffico ICMP in ingresso, nel registro di flusso viene visualizzato un singolo record REJECT perché al traffico non è stato consentito raggiungere l'istanza.

IPv6 traffico

Di seguito è riportato un esempio di record del log di flusso predefinito. Nell'esempio, era consentito il traffico SSH (porta 22) dall' IPv6 indirizzo 2001:db 8:1234:a 100:8 d6e: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 tcp-flags i campi negli esempi second-to-last di questa sezione sono rappresentati dal valore nel log di flusso. 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 su tcp-flags opzione e una spiegazione di ciascuno dei flag TCP, vedere. 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.

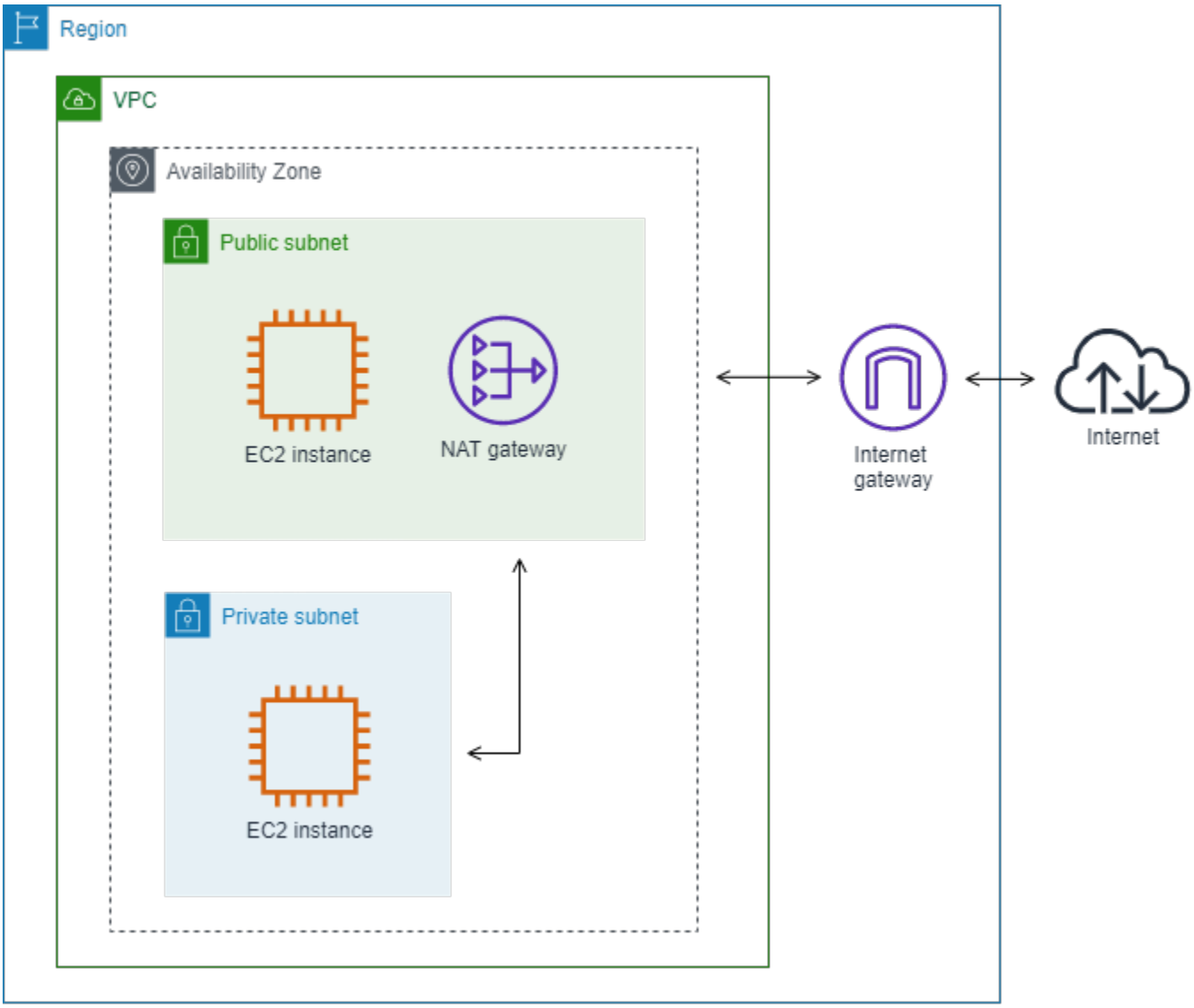
```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 63388 1219 1566848933 1566849113 ACCEPT 1 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 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 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 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.

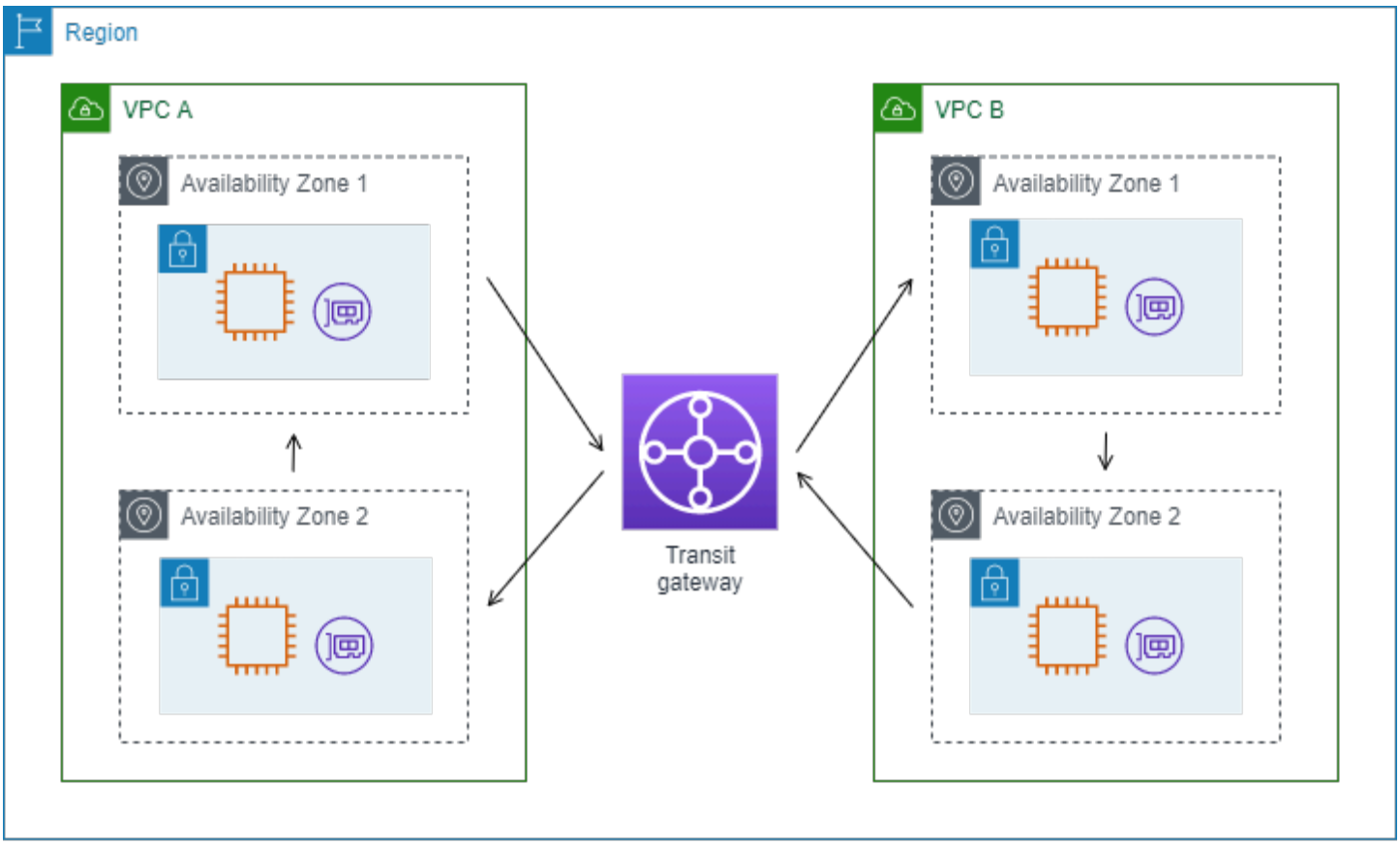
```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

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 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 in 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 dstaddr visualizza l'indirizzo IP privato dell'interfaccia di rete del gateway di transito e il campo pkt-dstaddr visualizza l'indirizzo IP del client in 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' EC2 istanza 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 di ingress e il secondo record ha una direzione di flusso di egress. Per egress record, traffic-path è 8 e indica che il traffico passa attraverso un gateway Internet. Il traffic-path campo non è supportato per ingress il traffico. Quando pkt-srcaddr oppure 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:

- Dopo aver creato un log di flusso, i dati del log di flusso non verranno visualizzati finché non vi sarà traffico attivo per l'interfaccia di rete, la sottorete o il VPC selezionato.
- Non puoi abilitare i log di flusso per quelli VPCs che vengono peerizzati con il tuo VPC a meno che il VPC peer non sia nel tuo account.
- Dopo aver creato un log di flusso, non è possibile modificarne la configurazione o cambiarne il formato del record. 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 ha più IPv4 indirizzi e il traffico viene inviato a un IPv4 indirizzo privato secondario, il log di flusso visualizza l'indirizzo privato IPv4 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' IPv4 indirizzo privato principale nel `dstaddr` campo. Per acquisire l'indirizzo IP di destinazione originale, crea un log di flusso con il campo `pkt-dstaddr`.
- Se il traffico viene inviato da un'interfaccia di rete e l'origine non è uno degli indirizzi IP dell'interfaccia di rete, quando il record di registro riguarda un flusso in uscita, il log di flusso visualizza l' IPv4 indirizzo privato principale nel `srcaddr` campo. Per acquisire l'indirizzo IP di origine originale, crea un log di flusso con il campo `pkt-srcaddr`. Se il record di registro riguarda un flusso di ingresso nell'interfaccia di rete, l'IP privato principale dell'interfaccia di rete non verrà visualizzato nel `srcaddr` campo.
- 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.
- Per i campi `pkt-srcaddr` e `pkt-dstaddr`, se la conservazione dell'indirizzo IP del client è abilitata per il livello intermedio, questo campo può mostrare l'IP del client conservato anziché l'indirizzo IP del livello intermedio.
- Alcuni record del log di flusso sono stati ignorati durante l'intervallo di aggregazione (consulta log-status in Campi disponibili). Ciò può essere causato da un limite di AWS capacità interno o da un errore interno. Se utilizzi AWS Cost Explorer per visualizzare i costi dei log di flusso VPC e alcuni log di flusso vengono ignorati durante l'intervallo di aggregazione dei log di flusso, il numero di

log di flusso riportato AWS Cost Explorer sarà superiore al numero di log di flusso pubblicati da Amazon VPC.

- Se utilizzi Blocco dell'accesso pubblico (BPA) VPC:
  - I log di flusso per BPA VPC non includono i record ignorati.
  - I log di flusso per BPA VPC non includono `bytes` anche se includi il campo `bytes` nel log di flusso.

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 di origine con mirroring. Verrà visualizzato solo il traffico di destinazione 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.
- Traffico ARP (Address Resolution Protocol).

Limitazioni specifiche dei campi ECS disponibili nella versione 7:

- Per creare abbonamenti 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 appartengono al proprietario dell'abbonamento al log di flusso. Ad esempio, se condividi una sottorete (`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 log 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/sottorete, 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, disponi di una sottorete (`subnet-000000`) e crei un abbonamento al log di flusso per questa sottorete con campi ECS

(`fl-00000000`). In `subnet-000000`, avvii un' EC2istanza (`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 sia `i-0000000` che `ECS-Task-1` generano traffico IP, l'abbonamento al log di flusso `fl-00000000` fornirà i log di traffico per entrambe le entità. Tuttavia, solo `ECS-Task-1` disporrà dei metadati ECS effettivi per i campi ECS che hai incluso in logFormat. Per il traffico correlato a `i-0000000`, questi campi avranno il valore di "-".

- `ecs-container-id` e `ecs-second-container-id` vengono ordinati quando il servizio Log di flusso VPC 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 DescribeTask API. Se un container entra nello stato STOPPED mentre l'attività è ancora in esecuzione, potrebbe continuare a essere visualizzato nel log.
- I metadati ECS e i log del traffico IP provengono da due origini diverse. Iniziamo a calcolare il traffico ECS non appena otteniamo tutte le informazioni richieste dalle dipendenze upstream. Dopo aver avviato 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, arrestiamo il calcolo dei campi ECS 1) quando non riceviamo più il traffico IP per l'interfaccia di rete sottostante o riceviamo il traffico IP con un ritardo di più di un giorno e 2) quando riceviamo l'evento ECS che contiene i metadati dell'attività ECS per indicare che l'attività non è più in esecuzione.
- Sono supportate solo le attività ECS avviate in modalità di 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
- Tagging dei flussi di distribuzione nella Guida per gli sviluppatori di Amazon Data Firehose

Utilizzo dei log di flusso

Puoi lavorare con i log di flusso utilizzando console per Amazon e EC2 Amazon VPC.

Attività

- 1. Controllo dell'utilizzo dei log di flusso con IAM
- 2. Creazione di un log di flusso
- 3. Tagging di un log di flusso
- 4. Eliminazione di un log di flusso
- Panoramica della riga di comando

1. Controllo dell'utilizzo dei log di flusso con IAM

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”.

2. Creazione di un log di flusso

Puoi creare log di flusso per le tue sottoreti o le VPCs 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 “Creazione di un log di flusso che viene pubblicato in Amazon Data Firehose”

3. 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 EC2 console Amazon 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.
   - Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel riquadro di navigazione, scegli Your VPCs. Selezionare la casella di controllo relativa al VPC.
   - Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel pannello di navigazione, scegli 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).

4. 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 EC2 console Amazon 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.
   - Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel riquadro di navigazione, scegli Your VPCs. Selezionare la casella di controllo relativa al VPC.
   - Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel pannello di navigazione, scegli 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 della riga di comando

È possibile eseguire le attività descritte in questa pagina utilizzando la riga di comando.

Creazione di un log di flusso

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

Descrizione di un log di flusso

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

Tagging di un log di flusso

- create-tags e delete-tags (AWS CLI)

- New-EC2Tag e Remove-EC2Tag (AWS Tools for Windows PowerShell)

Eliminazione di un log di flusso

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)

Pubblica i log di flusso in Logs CloudWatch

I log di flusso possono pubblicare i dati dei log di flusso direttamente su Amazon CloudWatch. Amazon CloudWatch è un servizio completo di monitoraggio e osservabilità. Raccoglie e tiene traccia di metriche, registri e dati sugli eventi da varie AWS risorse, nonché dalle tue applicazioni e servizi. CloudWatch offre visibilità sull'utilizzo delle risorse, sulle prestazioni delle applicazioni e sullo stato operativo, consentendovi di rilevare e rispondere ai cambiamenti delle prestazioni a livello di sistema e ai potenziali problemi. Con CloudWatch, puoi impostare allarmi, visualizzare log e metriche e reagire automaticamente per raccogliere e ottimizzare le tue risorse cloud. È uno strumento essenziale per garantire l'affidabilità, la disponibilità e le prestazioni dell'infrastruttura e delle applicazioni basate sul cloud.

Quando si pubblica 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
- Crea un log di flusso da pubblicare su Logs CloudWatch
- Visualizza i record dei log di flusso con Logs CloudWatch
- Ricerca dei record dei log di flusso
- Elaborare i record dei log di flusso in CloudWatch Logs

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 riquadro di navigazione, scegli 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. Scegli Next (Successivo).
   d. Immetti un nome per la policy, una descrizione facoltativa e i tag, 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).

Crea un log di flusso da pubblicare su Logs CloudWatch

Puoi creare log di flusso per le tue sottoreti o le VPCs 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`.

Prerequisito

Verifica che il principale IAM che stai utilizzando per effettuare la richiesta disponga delle autorizzazioni per richiamare l'operazione `iam:PassRole`.

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

```
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

Creazione di un flusso di log tramite la console

1. Esegui una di queste operazioni:
   - Apri la EC2 console Amazon 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.
   - Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel riquadro di navigazione, scegli Your VPCs. Selezionare la casella di controllo relativa al VPC.
   - Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel pannello di navigazione, scegli 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 CloudWatch registri.
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. Se inserisci un nome, creiamo il gruppo di log quando è presente traffico da registrare.
7. Per l'accesso al servizio, scegli un ruolo di servizio IAM esistente con le autorizzazioni per pubblicare i log nei CloudWatch registri o scegli di creare un nuovo ruolo di servizio.
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 log.
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-EC2FlowLog (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
```

Visualizza i record dei log di flusso con Logs CloudWatch

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 del log di flusso pubblicati su CloudWatch Logs utilizzando la riga di comando

- get-log-events (AWS CLI)
- Get- CWLLog Event ()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 CloudWatch Logs. 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]
```

Elaborare i record dei log di flusso in CloudWatch Logs

È possibile elaborare 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 dei filtri delle metriche, consulta Creazione di metriche dagli eventi di log utilizzando il filtro nella Amazon CloudWatch Logs 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 del parametro creato e scegli Seleziona parametro.
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).
    - Perché TimeSinceLastActive Whenever is... , 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. Scegli Next (Successivo).
13. Per Notification (Notifica) scegli un argomento SNS esistente oppure Create new topic (Crea nuovo argomento), per crearne uno nuovo. Scegli Next (Successivo).
14. Inserisci un nome e una descrizione per l'allarme, quindi scegli Next (Successivo).
15. Una volta terminata l'anteprima dell'allarme, 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. Amazon S3 (Simple Storage Service) è un servizio di archiviazione di oggetti altamente scalabile e durevole. È stato progettato per archiviare e recuperare qualsiasi quantità di dati, ovunque sul Web. S3 offre durabilità e disponibilità leader del settore, con funzionalità integrate per il controllo delle versioni dei dati, la crittografia e il controllo degli accessi.

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 log di flusso, consulta Create a bucket nella Amazon S3 User Guide.

Per ulteriori informazioni su come semplificare l'inserimento dei log di flusso in VPC, l'elaborazione dei log di flusso e la visualizzazione dei log di flusso, consulta Registrazione centralizzata con nella libreria delle soluzioni. OpenSearch 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

- File di log di flusso
- Autorizzazioni dei bucket Amazon S3 per log di flusso
- Policy di chiave richiesta per l'uso con SSE-KMS
- Autorizzazioni del file di log Amazon S3
- Creazione di un log di flusso che pubblica in Amazon S3
- Visualizzazione dei record dei log di flusso con Amazon S3

File di log di flusso

I log di flusso VPC raccolgono dati sul traffico IP in entrata e in uscita dal VPC in record di log, aggregano questi record in file di log e pubblicano questi ultimi nel bucket Amazon S3 a intervalli di cinque minuti. È possibile pubblicare più file e ogni file di log può contenere alcuni o tutti i record dei log di flusso per il traffico IP registrato nei cinque 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
```

Di seguito è riportato un esempio di file di registro per un log di flusso creato dall'account AWS 123456789012, per una risorsa in us-east-1 Regione, su June 20, 2018 at 16:20 UTC. Il file contiene i record del registro di flusso con un orario di fine compreso tra 16:20:00 e 16:24:59.

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

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:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        }
    ]
}
```

L'ARN specificato *my-s3-arn* dipende dall'utilizzo o meno di 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 al singolo. Account AWS ARNs 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

Oltre alle policy dei bucket richieste, Amazon S3 utilizza le liste di controllo degli accessi ACLs () per gestire l'accesso ai file di registro 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 la panoramica dell'elenco di controllo degli accessi (ACL) nella Guida per l'utente di Amazon S3.

Creazione di un log di flusso che pubblica in Amazon S3

Dopo aver creato e configurato il bucket Amazon S3, puoi creare log di flusso per interfacce di rete, sottoreti e. VPCs

Prerequisito

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": "*"
    }
  ]
}
```

Creazione di un flusso di log tramite la console

1. Esegui una di queste operazioni:
   - Apri la EC2 console Amazon 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.
   - Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel riquadro di navigazione, scegli Your VPCs. Selezionare la casella di controllo relativa al VPC.
   - Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel pannello di navigazione, scegli 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 il nome della risorsa Amazon (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 log.
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 da pubblicare su Amazon S3 utilizzando la riga di comando

Utilizzare uno dei seguenti comandi:

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (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 con Amazon S3

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.

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.

Per visualizzare i record del log di flusso pubblicati in Amazon S3

1. Apri la console Amazon S3 all'indirizzo. 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*/AWSLogs*account_id*/vpcflowlogs///*region*/. *year month day*
4. Seleziona la casella di controllo accanto al nome del file, quindi scegli Download (Scarica).

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.

Pubblicazione dei log di flusso in Amazon Data Firehose

I log di flusso possono pubblicare i loro dati direttamente in Amazon Data Firehose. Amazon Data Firehose è un servizio completamente gestito che raccoglie, trasforma e fornisce flussi di dati in tempo reale in vari AWS archivi di dati e servizi di analisi. Gestisce l'importazione dei dati per conto tuo.

Quando si tratta di log di flusso VPC, Firehose può essere utile. I log di flusso VPC acquisiscono informazioni sul traffico IP verso e dalle interfacce di rete nel VPC. Questi dati possono essere fondamentali per il monitoraggio della sicurezza, l'analisi delle prestazioni e la conformità normativa. Tuttavia, la gestione dell'archiviazione e dell'elaborazione di questo flusso continuo di dati di log può essere un'attività complessa e dispendiosa in termini di risorse.

Integrando Firehose con i log di flusso VPC, puoi distribuire questi dati alla tua destinazione preferita, come Amazon S3, Amazon Redshift o Amazon OpenSearch Service. Firehose scalerà per gestire l'importazione, la trasformazione e la distribuzione dei log di flusso VPC, alleggerendo l'onere operativo. Ciò ti consente di concentrarti sull'analisi dei log e sulla raccolta di informazioni dettagliate, anziché preoccuparti dell'infrastruttura sottostante.

Inoltre, Firehose offre funzionalità come la trasformazione, la compressione e la crittografia dei dati, che possono migliorare l'efficienza e la sicurezza della pipeline di elaborazione dei log di flusso VPC. L'utilizzo di Firehose per i log di flusso VPC può semplificare la gestione dei dati e consentire di ottenere informazioni dettagliate dai dati sul traffico di rete.

Quando si pubblica in Amazon Data Firehose, i dati del log di flusso vengono pubblicati in un flusso di distribuzione Amazon Data Firehose in formato di 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
- Creazione di un log di flusso che viene pubblicato in Amazon Data Firehose

Ruoli IAM per la consegna tra account

Quando si pubblica in Amazon Data Firehouse, è possibile scegliere un flusso di distribuzione che si trova nello stesso account della risorsa da monitorare (l'account di origine) o in un altro account (l'account di destinazione). Per abilitare la distribuzione tra account dei log di flusso ad Amazon Data Firehose, è necessario creare un ruolo IAM nell'account di origine e uno nell'account di destinazione.

Roles

- Ruolo dell'account di origine
- Ruolo dell'account di destinazione

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 crei la tua politica, specifica le VPCs interfacce di rete o le sottoreti che stai 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 riquadro di navigazione, scegli 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. Scegli Next (Successivo).
   d. Immetti un nome per la policy, una descrizione facoltativa e i tag, 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. Scegli Next (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 riquadro di navigazione, scegli 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. Scegli Next (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. Scegli Next (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).

Creazione di un log di flusso che viene pubblicato in Amazon Data Firehose

Puoi creare log di flusso per le tue VPCs sottoreti o le interfacce di rete.

Prerequisiti

- Crea il flusso di distribuzione di 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 che viene pubblicato in Amazon Data Firehose

1. Esegui una di queste operazioni:
   - Apri la EC2 console Amazon 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.
   - Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel riquadro di navigazione, scegli Your VPCs. Selezionare la casella di controllo relativa al VPC.
   - Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Nel pannello di navigazione, scegli 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 nello stesso account: il flusso di distribuzione e la risorsa da monitorare si trovano nello stesso account.
   - Invia ad Amazon Data Firehose in un account diverso: il flusso di distribuzione e la risorsa da monitorare si trovano in account diversi.
6. Per il nome del flusso Amazon Data Firehouse, seleziona il flusso di distribuzione che hai creato.
7. [Solo distribuzione tra account] Per l'accesso al servizio, scegli un ruolo di servizio IAM esistente per la distribuzione tra account che disponga delle autorizzazioni per pubblicare i log o scegli Configura le autorizzazioni per aprire la console IAM e creare un ruolo di servizio.
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 log.
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 la riga di comando

Utilizzare uno dei seguenti comandi:

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (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
```

Come risultato della creazione del log di flusso, è possibile ottenere i dati del log dalla destinazione configurata per il flusso di distribuzione.

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, puoi identificare quali risorse nei tuoi cloud privati virtuali (VPCs) sono le migliori a parlare 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
- CloudFormation Genera il modello utilizzando 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, scegli Your, VPCs quindi seleziona il tuo VPC.
   - Apri la console Amazon VPC. Nel riquadro di navigazione, scegliere Sottoreti e selezionare la sottorete desiderata.
   - Apri la EC2 console Amazon. 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 Crea 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 flow-logs-subscription-idvpcflowlogsathenadatabase< >.
- Un gruppo di lavoro Athena. Il nome del gruppo di lavoro è < >< >< data di inizio >< data di fine >gruppo di lavoro flow-log-subscription-idpartition-load-frequency
- Una tabella Athena partizionata che corrisponde ai record del log di flusso. Il nome della tabella è < >< >< data di inizio >< data di fine >. flow-log-subscription-idpartition-load-frequency
- 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.

CloudFormation Genera il modello utilizzando 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.

Usa 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"
            }
        ]
```

```
    }
}
```

Usa 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.

- VpcFlowLogsAcceptedTraffic— Le connessioni TCP consentite in base ai gruppi di sicurezza e alla rete. ACLs
- VpcFlowLogsAdminPortTraffic— I primi 10 indirizzi IP con il maggior traffico, registrati dalle applicazioni che rispondono alle richieste sulle porte amministrative.
- VpcFlowLogsIPv4Traffico: i byte totali di IPv4 traffico registrati.
- VpcFlowLogsIPv6Traffico: i byte totali di IPv6 traffico registrati.

- VpcFlowLogsRejectedTCPTraffic— Le connessioni TCP che sono state rifiutate in base ai gruppi di sicurezza o alla rete. ACLs
- VpcFlowLogsRejectedTraffic— Il traffico che è stato rifiutato in base ai gruppi di sicurezza o alla rete ACLs.
- VpcFlowLogsSshRdpTraffic— Il traffico SSH e RDP.
- VpcFlowLogsTopTalkers— I 50 indirizzi IP con il maggior traffico registrato.
- VpcFlowLogsTopTalkersPacketLevel— I 50 indirizzi IP a livello di pacchetto con il maggior traffico registrato.
- VpcFlowLogsTopTalkingInstances— Le IDs 50 istanze con il maggior traffico registrato.
- VpcFlowLogsTopTalkingSubnets— La IDs 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
- 'LogDestinationNotFoundException' o 'Accesso negato per LogDestination 'errore
- 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 EC2 console Amazon o nella console Amazon VPC, scegli la scheda Flow Logs per la risorsa pertinente. La tabella dei log di flusso contiene gli eventuali errori nella colonna State (Stato). In alternativa, usa il describe-flow-logscomando e controlla il valore restituito nel `DeliverLogsErrorMessage` campo. 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 le quote CloudWatch di servizio 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 log di flusso e la EC2 console Amazon VPC o Amazon 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.

'LogDestinationNotFoundException' o 'Accesso negato per LogDestination 'errore

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.

CloudWatch metriche per il tuo VPCs

Amazon VPC pubblica i tuoi dati su Amazon. VPCs CloudWatch Puoi recuperare le statistiche relative a te sotto forma di un insieme ordinato di dati di serie temporali, noti VPCs come metriche.

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 Amazon CloudWatch User Guide.

Indice

- Parametri e dimensioni di NAU
- Abilita o disabilita il monitoraggio del NAU
- Esempio di CloudWatch allarme NAU

Parametri e dimensioni di NAU

Utilizzo degli indirizzi di rete (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 della NAU è utile perché se esaurisci le quote NAU o NAU peered per il tuo VPC, non puoi lanciare EC2 nuove istanze o fornire nuove risorse, come Network Load Balancer, endpoint VPC, funzioni Lambda, allegati del gateway di transito e gateway NAT.

Se hai abilitato il monitoraggio dell'utilizzo degli indirizzi di rete per un VPC, Amazon VPC invia ad Amazon i parametri relativi a NAU. 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. Criteri per la creazione di report • Ogni 24 ore. Dimensioni • Nome: `Per-VPC Metrics`, valore: l'ID VPC.

Parametro	Descrizione
`NetworkAddressUsagePeered`	I NAU contano per il VPC e VPCs tutto ciò che lo compone. Criteri per la creazione di report • Ogni 24 ore. Dimensioni • 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. Criteri per la creazione di report • Ogni 24 ore. Dimensioni • Nome: `Service`, valore: `EC2` • Nome: `Type`, valore: `Resource` • Nome: `Resource`, valore: l'ID VPC. • Nome: `Class`, valore: `NetworkAddressUsage`
`ResourceCount`	I NAU contano per il VPC e VPCs tutto ciò che lo compone. Criteri per la creazione di report • Ogni 24 ore.

Parametro	Descrizione
	Dimensioni • Nome: `Service`, valore: `EC2` • Nome: `Type`, valore: `Resource` • Nome: `Resource`, valore: l'ID VPC. • Nome: `Class`, valore: `NetworkAddressUsagePeered`
`ResourceCount`	Una visione combinata dell'utilizzo di NAU in tutto il mondo. VPCs Criteri per la creazione di report • Ogni 24 ore. Dimensioni • Nome: `Service`, valore: `EC2` • Nome: `Type`, valore: `Resource` • Nome: `Resource`, valore: `VPC` • Nome: `Class`, valore: `NetworkAddressUsage`

Parametro	Descrizione
`ResourceCount`	Una visione combinata dell'utilizzo di NAU tra utenti peer. VPCs Criteri per la creazione di report • Ogni 24 ore. Dimensioni • Nome: `Service`, valore: `EC2` • Nome: `Type`, valore: `Resource` • Nome: `Resource`, valore: `VPC` • Nome: `Class`, valore: `NetworkAddressUsagePeered`

Abilita o disabilita il monitoraggio del NAU

Per visualizzare le metriche NAU CloudWatch, devi prima abilitare il monitoraggio su ogni VPC da monitorare.

Abilitazione o disabilitazione del monitoraggio del NAU

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Your. VPCs
3. Seleziona la casella di controllo per il VPC.
4. Seleziona Actions (Operazioni), Edit VPC settings (Modifica impostazioni del VPC).
5. Esegui una di queste 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 CloudWatch allarme NAU

Puoi utilizzare il seguente AWS CLI comando ed esempio `.json` per creare un CloudWatch allarme Amazon e una notifica SNS che tenga traccia dell'utilizzo NAU del VPC con 50.000 come soglia. NAUs 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"
}
```

Gestione delle responsabilità di sicurezza per 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

- Come garantire la protezione dei dati in Amazon Virtual Private Cloud
- Identity and Access Management per Amazon VPC
- Sicurezza dell'infrastruttura in Amazon VPC
- Controlla il traffico verso AWS le tue risorse utilizzando i gruppi di sicurezza
- Controllo del traffico della sottorete con le liste di controllo degli accessi alla rete
- Resilienza in Amazon Virtual Private Cloud
- Convalida della conformità per Amazon Virtual Private Cloud
- Blocca l'accesso pubblico alle sottoreti VPCs e alle sottoreti

- Security best practices for your VPC

Come garantire la 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 Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- 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 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo 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 CLI AWS

SDKs 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.

Come garantire la privacy 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 un 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.
- Liste di controllo degli accessi alla rete (ACL): la rete ACLs consente o nega un traffico specifico in entrata e in uscita a livello di sottorete. Per ulteriori informazioni, consulta Controllo del traffico della sottorete con le liste di controllo degli accessi alla 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' EC2 istanza Amazon. Puoi quindi inviare il traffico ai dispositivi out-of-band di sicurezza e monitoraggio. 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

- Destinatari
- Autenticazione con identità
- Gestione degli accessi tramite le policy
- 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 sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

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)AWS in IAM nella 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, potresti avere un gruppo denominato IAMAdminse concedere a quel 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 Casi d'uso per utenti IAM 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. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). 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 Create a role for a third-party identity provider (federation) 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 Accesso a risorse multi-account in IAM 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 normale che quel 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 inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che 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 operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella 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' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere

credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

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 operazioni 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 sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente 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 sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle 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 operazioni 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.

Elenchi di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

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 del servizio (SCPs): SCPs 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 di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.
- 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 o meno una richiesta quando sono coinvolti più tipi di policy, consulta la 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

- Operazioni
- Risorse
- Chiavi di condizione
- Policy basate sulle risorse di Amazon VPC
- Autorizzazione basata su tag
- Ruoli IAM

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.

Operazioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

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 azioni Amazon VPC, consulta Azioni definite da Amazon EC2 nel Service Authorization Reference.

Risorse

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, 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). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le operazioni 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 VPCs in una regione specifica che appartengono a un account specifico, usa 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 azioni Amazon EC2 API coinvolgono più risorse. Per specificare più risorse in una singola istruzione, separale ARNs con virgole.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Per visualizzare un elenco dei tipi di risorse Amazon VPC e relativi ARNs, consulta Tipi di risorse definiti da Amazon EC2 nel Service Authorization Reference.

Chiavi di condizione

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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. È possibile 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.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile 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 EC2 azioni di Amazon supportano le chiavi `aws:RequestedRegion` e `ec2:Region` condition. 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 delle chiavi di condizione di Amazon VPC, consulta Condition keys for Amazon EC2 nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni 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, devi inoltre 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 Accesso a risorse multi-account in IAM nella Guida per l'utente 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 Concedere l'autorizzazione a taggare le risorse durante la creazione nella Amazon EC2 User Guide.

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 interna all'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. GetFederationToken

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

- Best practice per le policy
- Utilizzo della console Amazon VPC
- 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
- Blocca l'accesso pubblico alle sottoreti e alle VPCs sottoreti
- 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 operazioni 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. È possibile 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 è possibile 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 il Sistema di analisi degli accessi IAM 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 Protezione dell'accesso API 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 abilita la creazione di ruoli VPCs, sottoreti, tabelle di routing 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 i 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 politica concede inoltre ai ruoli il permesso di avviare istanze utilizzando solo AMIs quelle 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/*"
         ]
      }
   ]
}
```

Blocca l'accesso pubblico alle sottoreti e alle VPCs sottoreti

I seguenti esempi di policy concedono ai ruoli l'autorizzazione a utilizzare la funzionalità VPC Block Public Access (BPA) per bloccare l'accesso pubblico alle risorse e alle sottoreti. VPCs

Esempio 1: consenti l'accesso in sola lettura alle impostazioni a livello di account BPA VPC e alle esclusioni BPA VPC.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAReadOnlyAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Esempio 2: consenti l'accesso completo in lettura e scrittura alle impostazioni a livello di account BPA VPC e alle esclusioni BPA VPC.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAFullAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:ModifyVpcBlockPublicAccessOptions",
        "ec2:CreateVpcBlockPublicAccessExclusion",
        "ec2:ModifyVpcBlockPublicAccessExclusion",
        "ec2:DeleteVpcBlockPublicAccessExclusion"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Esempio 3 - Consenti l'accesso a tutti EC2 APIs tranne la modifica delle impostazioni VPC BPA e la creazione di esclusioni.

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

```
  "Statement": [
    {
      "Sid": "EC2FullAccess"
      "Action": [
        "ec2:*",
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "VPCBPAPartialAccess",
      "Action": [
        "ec2:ModifyVpcBlockPublicAccessOptions",
        "ec2:CreateVpcBlockPublicAccessExclusion"
      ],
      "Effect": "Deny",
      "Resource": "*"
    }
  ]
}
```

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 ()AWS PrivateLink
- Peering VPC

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
- Non sono autorizzato a eseguire iam: PassRole

- Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse Amazon VPC

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 i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali policy per consentire alle persone di accedere 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 attraverso Account AWS le 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 di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente 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, consulta Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: Amazon VPCFull Access

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 per questa politica, consulta Amazon VPCFull Access nel AWS Managed Policy Reference.

AWS politica gestita: Amazon VPCRead OnlyAccess

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 per questa politica, consulta Amazon VPCRead OnlyAccess nel AWS Managed Policy Reference.

AWS politica gestita: Amazon VPCCross AccountNetworkInterfaceOperations

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 per questa politica, consulta Amazon VPCCross AccountNetworkInterfaceOperations nel AWS Managed Policy Reference.

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 “VPCFullAccesso Amazon”: aggiornamento a una policy esistente	È stato aggiunto il Associate SecurityGroupVpc, DescribeSecurityGroupVpcAssociationse DisassociateSecurityGroupVp	9 dicembre 2024

Modifica	Descrizione	Data
	c azioni, che consentono di associare, dissociare e visualizzare le associazioni dei gruppi di sicurezza con VPCs.	
the section called “Amazon VPCRead OnlyAccess”: aggiornamento a una policy esistente	Aggiunto il DescribeSecurityGroupVpcAssociations azione, che consente di visualizzare le associazioni dei gruppi di sicurezza con VPCs.	9 dicembre 2024
the section called “VPCFullAccesso Amazon”: aggiornamento a una policy esistente	Aggiunto il GetSecuri tyGroupsForVpc azione, che ti consente di ottenere gruppi di sicurezza utilizzabili nel tuo VPC.	8 febbraio 2024
the section called “Amazon VPCRead OnlyAccess”: aggiornamento a una policy esistente	Aggiunto il GetSecuri tyGroupsForVpc azione, che ti consente di ottenere gruppi di sicurezza utilizzabili nel tuo VPC.	8 febbraio 2024
the section called “Amazon VPCCross AccountNetworkInterfaceOperations”: aggiornamento a una policy esistente	Aggiunto il AssignIpv6Addresses e UnassignIpv6Addresses azioni, che consentono di gestire gli IPv6 indirizzi associati alle interfacce di rete.	25 settembre 2023
the section called “Amazon VPCRead OnlyAccess”: aggiornamento a una policy esistente	Aggiunto il DescribeSecurityGroupRules azione, che consente di visualizzare le regole del gruppo di sicurezza.	2 agosto 2021

Modifica	Descrizione	Data
the section called “VPCFullAccesso Amazon”: aggiornamento a una policy esistente	Aggiunto il DescribeSecurityGroupRules e ModifySecurityGroupRules azioni, che consentono di visualizzare e modificare le regole dei gruppi di sicurezza.	2 agosto 2021
the section called “VPCFullAccesso Amazon”: aggiornamento a una policy esistente	Azioni aggiunte per i gateway degli operatori, i IPv6 pool, i gateway locali e le tabelle di routing dei gateway locali.	23 giugno 2021
the section called “Amazon VPCRead OnlyAccess”: aggiornamento a una policy esistente	Sono state aggiunte azioni per i gateway degli operatori, i IPv6 pool, i gateway locali e le tabelle di routing dei gateway locali.	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 Utilizzalo separatamente VPCs per isolare l'infrastruttura in base al carico di lavoro o all'entità organizzativa.

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

Considera le seguenti opzioni per controllare il traffico di rete verso le risorse del tuo VPC, come EC2 le istanze:

- Utilizza i gruppi di sicurezza come meccanismo principale per controllare l'accesso di rete al tuo. VPCs Se necessario, utilizzate la rete ACLs per fornire un controllo di rete a grana grossa e senza stato. I gruppi di sicurezza sono più versatili della rete ACLs, grazie alla loro capacità di eseguire un filtraggio dei pacchetti basato sullo stato e di creare regole che fanno riferimento ad altri gruppi di sicurezza. La rete ACLs può essere efficace come controllo secondario (ad esempio, per negare un sottoinsieme specifico di traffico) o come guardie di sottorete di alto livello. Inoltre, poiché le reti ACLs si applicano a un'intera sottorete, possono essere utilizzate 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.

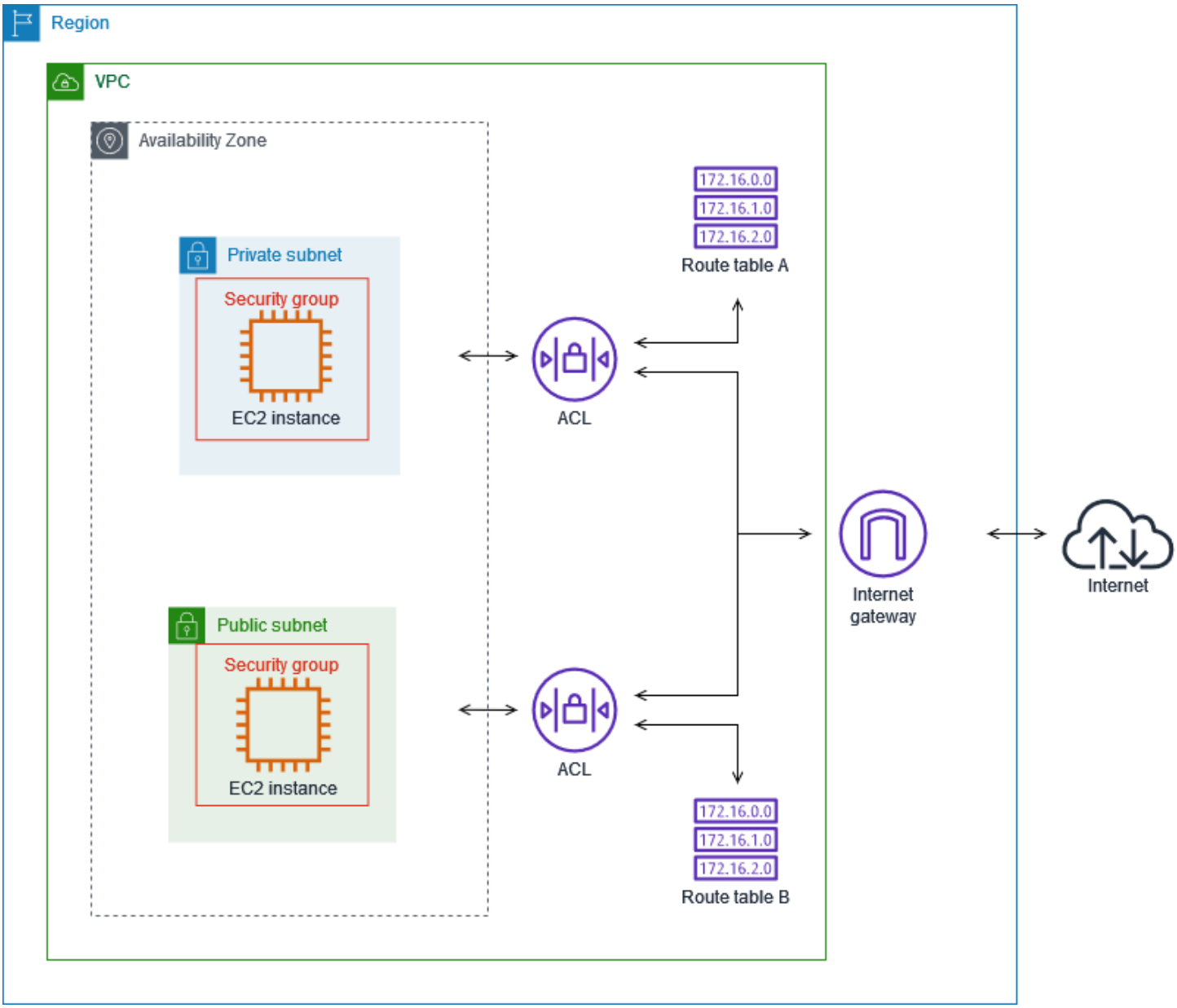
- Prendi in considerazione l'utilizzo di gruppi di sicurezza o interfacce di rete aggiuntivi per controllare e verificare il traffico di gestione delle EC2 istanze Amazon separatamente dal normale traffico delle applicazioni. Pertanto, puoi implementare policy IAM speciali per il controllo delle modifiche, 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 alle tue VPCs. Per ulteriori informazioni, consulta Opzioni di connettività Network-to-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.

Confronta i gruppi di sicurezza e la rete ACLs

La tabella seguente riassume le differenze di base tra i gruppi di sicurezza e la rete ACLs.

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.

Il diagramma seguente illustra i livelli di sicurezza forniti dai gruppi di sicurezza e dalla rete. ACLs 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.



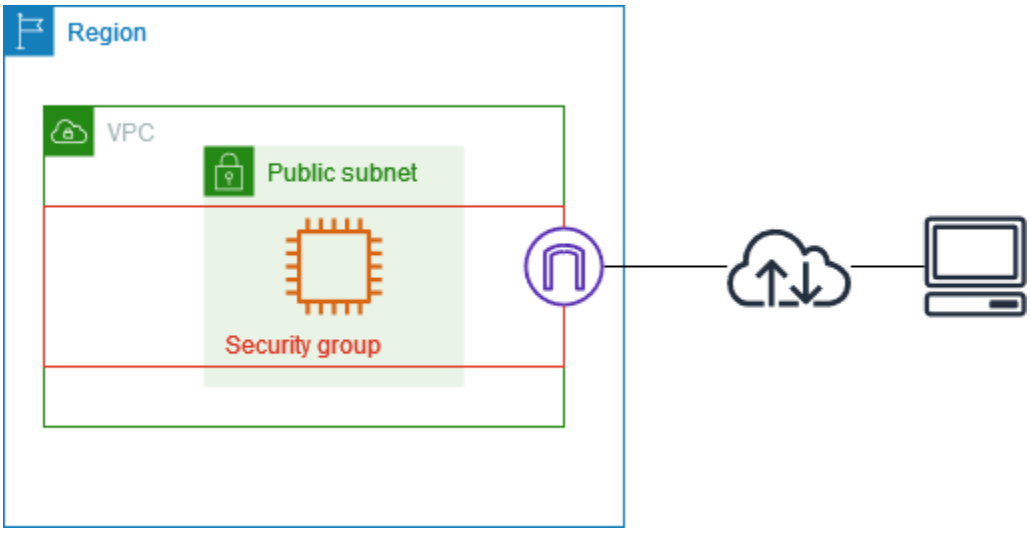
È possibile proteggere le istanze utilizzando solo gruppi di sicurezza. Tuttavia, puoi aggiungere la rete ACLs come ulteriore livello di difesa. Per ulteriori informazioni, consulta Esempio: controllo dell'accesso alle istanze in una sottorete.

Controlla il traffico verso AWS le tue 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' EC2 istanza, quest'ultima controlla il traffico in entrata e in uscita dell'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

- Nozioni di base sui gruppi di sicurezza
- Esempio di gruppo di sicurezza
- Regole del gruppo di sicurezza
- Gruppi di sicurezza predefiniti per i tuoi VPCs

- Creazione di un gruppo di sicurezza per il VPC
- Configurazione delle regole per i gruppi di sicurezza
- Eliminare un gruppo di sicurezza
- Associare gruppi di sicurezza a più gruppi di sicurezza VPCs
- Condividi i gruppi di sicurezza con AWS Organizations

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 EC2 istanze Amazon
  - 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

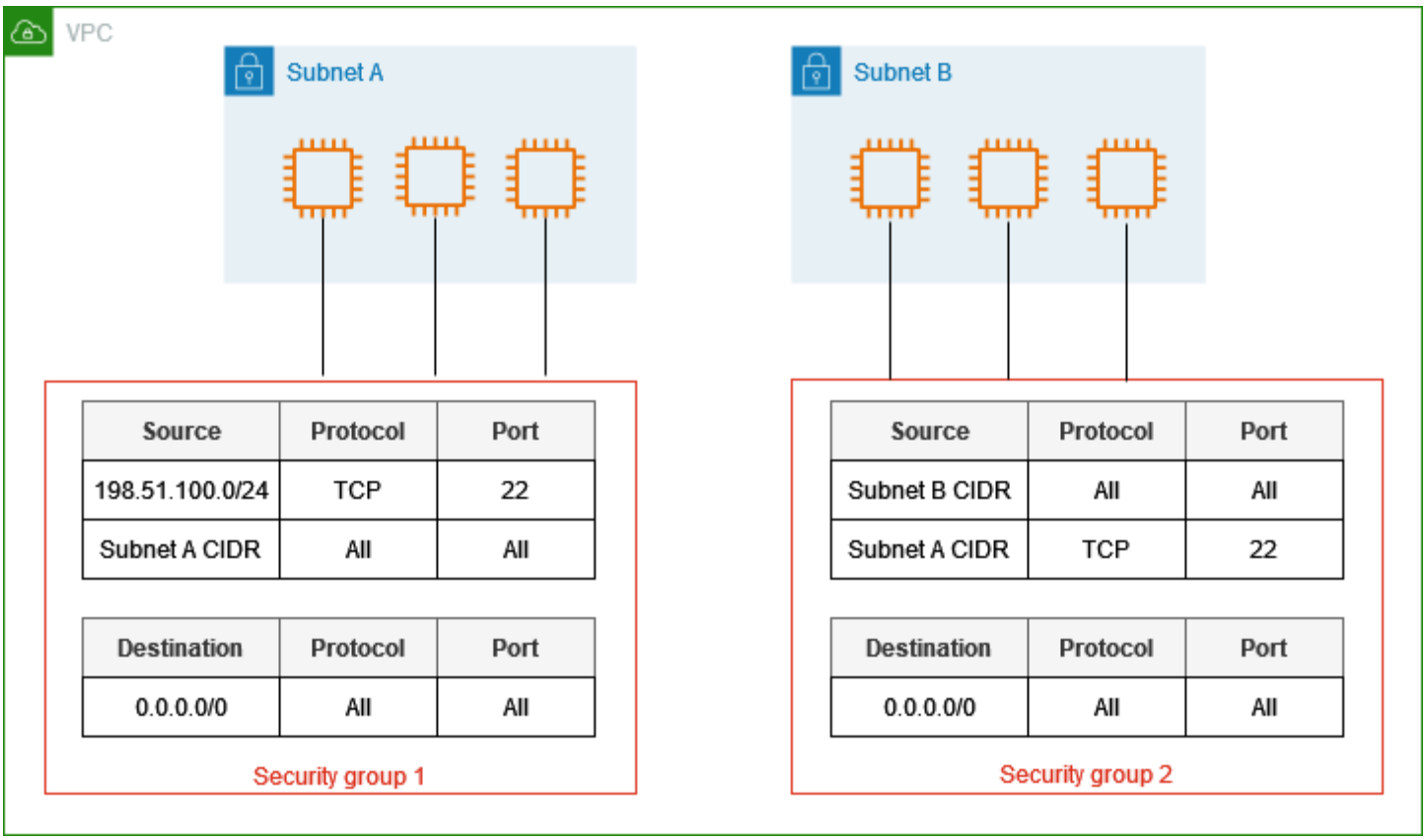
- Autorizza solo specifici principali IAM a creare e modificare gruppi di sicurezza.
- Crea il numero minimo di gruppi di sicurezza di cui hai bisogno per ridurre il rischio di errore. Utilizza ogni gruppo di sicurezza per gestire l'accesso a risorse con funzioni e requisiti di sicurezza simili.
- Quando aggiungi regole in entrata per le porte 22 (SSH) o 3389 (RDP) in modo da poter accedere alle EC2 istanze, autorizza solo intervalli di indirizzi IP specifici. Se specificate 0.0.0.0/0 (IPv4) e: :/ (IPv6), ciò consente a chiunque di accedere alle vostre 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.
- Valuta la possibilità di creare una rete ACLs con regole simili ai tuoi gruppi di sicurezza, per aggiungere un ulteriore livello di sicurezza al tuo VPC. Per ulteriori informazioni sulle differenze tra gruppi di sicurezza e rete ACLs, consultaConfronta i gruppi di sicurezza e la rete ACLs.

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

- Nozioni di base sulle regole dei gruppi di sicurezza
- Componenti di una regola di un gruppo di sicurezza

- Riferimenti dei gruppi di sicurezza
- Dimensioni dei gruppi di sicurezza
- Regole obsolete del gruppo di sicurezza

Nozioni di base sulle regole dei gruppi di sicurezza

Di seguito sono riportate le caratteristiche delle 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. Per istruzioni, consulta Configurazione delle regole per i gruppi 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 Amazon EC2 User Guide.
- 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

Di seguito vengono riportati i componenti delle regole del gruppo di sicurezza in entrata e in uscita:

- 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, usa il tipo 8 per ICMP Echo Request o il tipo 128 per Echo Request. 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 unico indirizzo. IPv4 Devi utilizzare la lunghezza del prefisso `/32`. Ad esempio `203.0.113.1/32`.
  - Un solo IPv6 indirizzo. Devi utilizzare la lunghezza del prefisso `/128`. Ad esempio `2001:db8:1234:1a00::123/128`.
  - Un intervallo di IPv4 indirizzi, in notazione a blocchi CIDR. Ad esempio `203.0.113.0/24`.
  - Una serie di IPv6 indirizzi, in notazione a blocchi 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:

- È possibile fare riferimento a un gruppo di sicurezza nella regola in entrata di un altro gruppo se si verifica una delle seguenti condizioni:
  - I gruppi di sicurezza sono associati allo stesso VPC.
  - Esiste una connessione peering tra i gruppi di sicurezza a VPCs cui sono associati i gruppi di sicurezza.
  - Esiste un gateway di transito tra quelli a VPCs cui sono associati i gruppi di sicurezza.
- È possibile fare riferimento a un gruppo di sicurezza nella regola in entrata se si verifica una delle seguenti condizioni:
  - I gruppi di sicurezza sono associati allo stesso VPC.
  - Esiste una connessione peering tra i gruppi di sicurezza a VPCs cui sono associati i gruppi di sicurezza.
- Nessuna regola del gruppo di sicurezza di riferimento viene aggiunta al gruppo di sicurezza che vi fa riferimento.
- Per quanto riguarda le regole in entrata, le EC2 istanze associate a un gruppo di sicurezza possono ricevere traffico in entrata dagli indirizzi IP privati delle EC2 istanze associate al gruppo di sicurezza di riferimento.
- Per le regole in uscita, le EC2 istanze associate a un gruppo di sicurezza possono inviare traffico in uscita agli indirizzi IP privati delle istanze associate al gruppo di sicurezza di riferimento. EC2

Limitazione

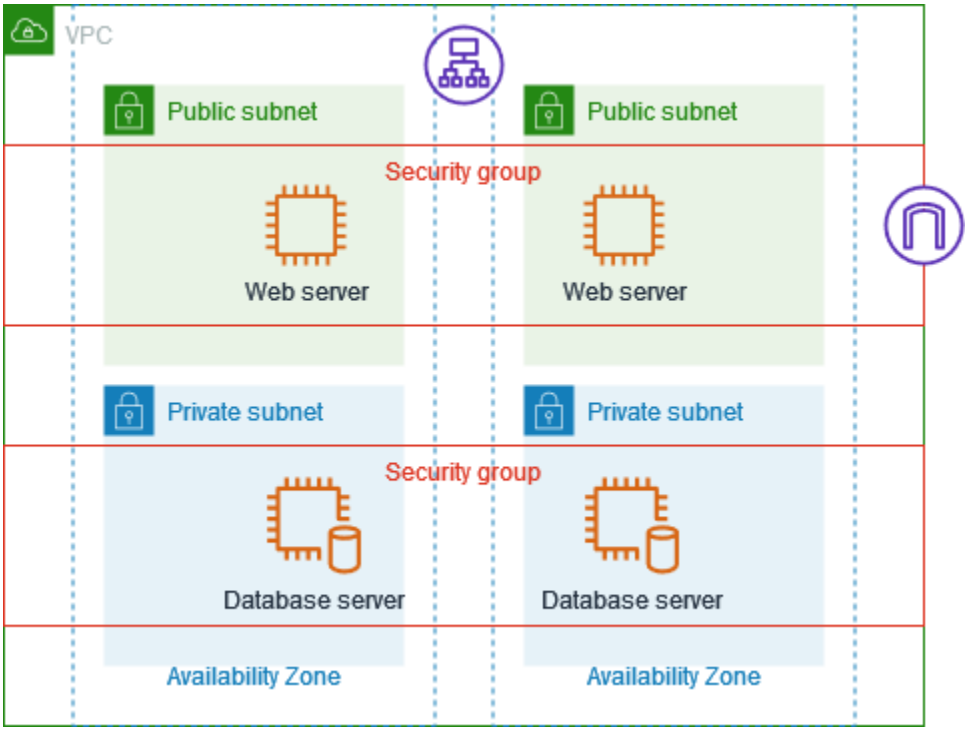
Se le route vengono configurate per inoltrare il traffico tra due istanze in sottoreti diverse attraverso un'appliance middlebox, è necessario assicurarsi che i gruppi di sicurezza per entrambe le istanze

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 prefissi gestiti disponibili AWS”.

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. Per ulteriori informazioni, consulta la sezione relativa all'aggiornamento dei gruppi di sicurezza per fare riferimento ai gruppi di sicurezza in peering nella Guida ad Amazon VPC Peering.

Se disponi di una regola del gruppo di sicurezza che fa riferimento a un gruppo in un VPC in peering o condiviso e il gruppo di sicurezza nel VPC condiviso viene eliminato o la connessione peering VPC viene eliminata, la regola del gruppo viene contrassegnata come obsoleta. Le regole obsolete possono essere Eliminate nello stesso modo delle altre regole del gruppo di sicurezza.

Gruppi di sicurezza predefiniti per i tuoi VPCs

I tuoi valori predefiniti VPCs e quelli VPCs che crei includono un gruppo di sicurezza predefinito. 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 quando avvii un' EC2 istanza, associamo l'istanza al gruppo di sicurezza predefinito per il suo 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

La tabella seguente descrive le regole in entrata predefinite di un gruppo di sicurezza predefinito.

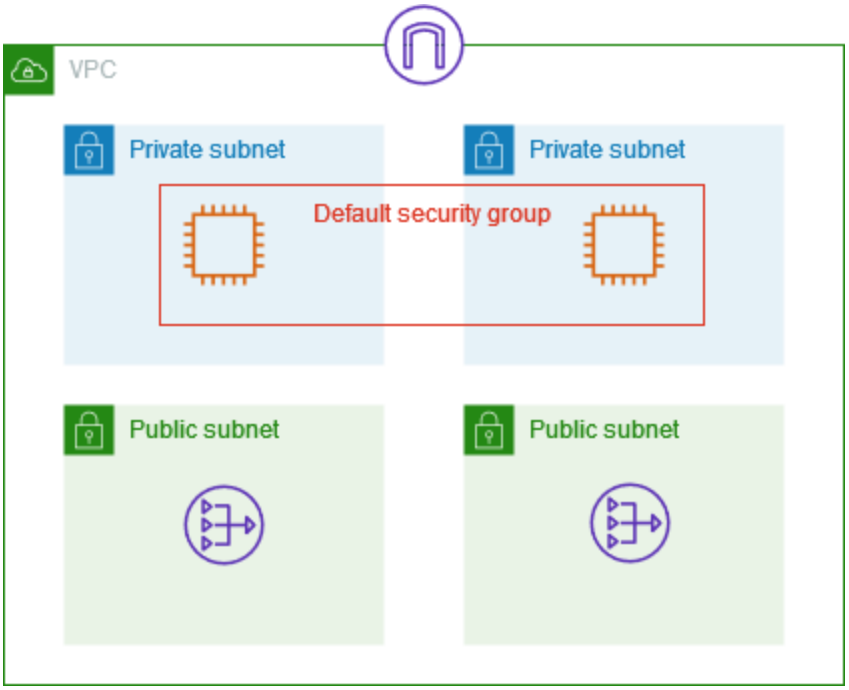
Crea	Protocollo	Intervallo porte	Descrizione
sg-1234567890abcdef0	Tutti	Tutti	Consente il traffico in entrata da tutte le risorse assegnate a questo gruppo di sicurezza. L'origine è l'ID di questo gruppo di sicurezza.

La tabella seguente descrive le regole in uscita predefinite di un gruppo di sicurezza predefinito.

Destinazione	Protocollo	Intervallo porte	Descrizione
0.0.0.0/0	Tutti	Tutti	Consente tutto il traffico in uscita IPv4 .
::/0	Tutti	Tutti	Consente tutto il traffico in uscita IPv6 . Questa regola viene aggiunta solo se al VPC è associato un blocco IPv6 CIDR.

Esempio

Il diagramma seguente mostra un VPC con un gruppo di sicurezza predefinito, un gateway Internet e un gateway NAT. La sicurezza predefinita contiene solo le sue regole predefinite ed è associata a due EC2 istanze in esecuzione nel 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.



Creazione di un gruppo di sicurezza per il VPC

Il cloud privato virtuale (VPC) include un gruppo di sicurezza predefinito. È possibile creare gruppi di sicurezza aggiuntivi. I gruppi di sicurezza possono essere utilizzati solo con le risorse nel VPC per cui vengono creati.

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. È possibile aggiungere regole quando si crea un gruppo di sicurezza o in un secondo momento. Per ulteriori informazioni, consulta Regole del gruppo di sicurezza.

Autorizzazioni richieste

Prima di iniziare, assicurati di disporre delle autorizzazioni richieste. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Gestione dei gruppi di sicurezza
- Gestione delle regole del gruppo di sicurezza

Per creare un gruppo di sicurezza tramite console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello 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. Per VPC, scegli il VPC in cui creare le risorse a cui associare il gruppo di sicurezza.
6. (Facoltativo) Per aggiungere regole in entrata, scegli Regole in entrata. Per ogni regola, scegli Aggiungi regola e specifica il protocollo, la porta e l'origine. Per ulteriori informazioni, consulta Configurazione delle regole per i gruppi di sicurezza.
7. (Facoltativo) Per aggiungere regole in uscita, scegli Regole in uscita. Per ogni regola, scegli Aggiungi regola e specifica il protocollo, la porta e la destinazione.
8. (Facoltativo) Per aggiungere un tag, scegli Add new tag (Aggiungi nuovo tag) e immetti la chiave e il valore del tag.
9. Scegliere Create Security Group (Crea gruppo di sicurezza).

Per creare un gruppo di sicurezza utilizzando il AWS CLI

Utilizza il comando create-security-group.

In alternativa, puoi creare un nuovo gruppo di sicurezza copiandone uno esistente. Quando copi un gruppo di sicurezza, aggiungiamo automaticamente le stesse regole in entrata e in uscita del gruppo di sicurezza originale e utilizziamo lo stesso VPC del gruppo di sicurezza originale. Puoi immettere un nome e una descrizione per il nuovo gruppo di sicurezza. Facoltativamente, puoi scegliere un VPC diverso e modificare le regole in entrata e in uscita secondo le esigenze. Tuttavia, non puoi copiare un gruppo di sicurezza da una Regione a un'altra.

Per creare un gruppo di sicurezza in base a uno esistente

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
3. Selezionare un gruppo di sicurezza.
4. Scegli Operazioni, Copia in un nuovo gruppo di sicurezza.
5. Immettere un nome e una descrizione per il gruppo di sicurezza.
6. (Facoltativo) Scegli un VPC diverso se necessario.
7. (Facoltativo) Aggiungi, rimuovi o modifica le regole del gruppo di sicurezza in base alle esigenze.
8. Scegliere Create Security Group (Crea gruppo di sicurezza).

Configurazione delle regole per i gruppi di sicurezza

Dopo aver creato un gruppo di sicurezza, puoi aggiungere, aggiornare ed eliminare le relative regole. Quando aggiungi, aggiorni o elimini una regola, la modifica viene applicata automaticamente alle risorse associate a quel gruppo.

Autorizzazioni richieste

Prima di iniziare, assicurati di disporre delle autorizzazioni richieste. Per ulteriori informazioni, consulta Gestione delle regole del gruppo di sicurezza.

Origini e destinazioni

È possibile specificare quanto segue come origine per le regole in entrata o come destinazioni per le regole in uscita.

- Personalizzato: un blocco IPv4 CIDR e un blocco IPv6 CIDR, un altro gruppo di sicurezza o un elenco di prefissi.
- Anywhere- IPv4 — Il blocco CIDR 0.0.0.0/0 IPv4 .
- Anywhere- IPv6 — Il blocco CIDR: :/0. IPv6
- Il mio IP: l' IPv4 indirizzo pubblico del computer locale.

> **Warning**
>
> Se scegli Anywhere- IPv4, consenti il traffico proveniente da tutti IPv4 gli indirizzi. Se scegli Anywhere- IPv6, consenti il traffico proveniente da tutti IPv6 gli indirizzi. È consigliabile autorizzare solo gli intervalli di indirizzi IP specifici che richiedono l'accesso alle risorse.

Configurare le regole di un gruppo di sicurezza tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
3. Selezionare il gruppo di sicurezza.
4. Per modificare le regole in entrata, scegli Modifica regole in entrata dalla scheda Azioni o dalla scheda Regole in entrata.

   a. Per aggiungere una regola, scegli Aggiungi regola e immetti il tipo, il protocollo, la porta e l'origine della regola.

      Se il tipo è 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 scegli qualsiasi altro tipo, il protocollo e l'intervallo di porte vengono configurati automaticamente.

   b. Per aggiornare una regola, modificane il protocollo, la descrizione e l'origine in base alle esigenze. Tuttavia, il tipo di origine non può essere modificato. Ad esempio, se l'origine è un blocco IPv4 CIDR, non è possibile specificare un blocco IPv6 CIDR, un elenco di prefissi o un gruppo di sicurezza.

   c. Per eliminare una regola, seleziona il pulsante Elimina corrispondente.
5. Per modificare le regole in uscita, scegli Modifica regole in uscita dalla scheda Azioni o dalla scheda Regole in uscita.

   a. Per aggiungere una regola, scegli Aggiungi regola e immetti il tipo, il protocollo, la porta e la destinazione della regola. Facoltativamente, è possibile inserire una descrizione.

      Se il tipo è 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 scegli qualsiasi altro tipo, il protocollo e l'intervallo di porte vengono configurati automaticamente.

b. Per aggiornare una regola, modificane il protocollo, la descrizione e l'origine in base alle esigenze. Tuttavia, il tipo di origine non può essere modificato. Ad esempio, se l'origine è un blocco IPv4 CIDR, non è possibile specificare un blocco IPv6 CIDR, un elenco di prefissi o un gruppo di sicurezza.

c. Per eliminare una regola, seleziona il pulsante Elimina corrispondente.

6. Scegliere Salva regole.

Per configurare le regole dei gruppi di sicurezza utilizzando il AWS CLI

- Aggiungi: utilizza i authorize-security-group-egresscomandi authorize-security-group-ingressand.
- Rimuovi: utilizza i revoke-security-group-egresscomandi revoke-security-group-ingressand.
- Modifica: utilizza i modify-security-group-rulescomandi update-security-group-rule-descriptions-ingress e -descriptions-egress. update-security-group-rule

Eliminare un gruppo di sicurezza

Quando un gruppo di sicurezza creato non è più necessario, è possibile eliminarlo.

Requisiti

- Il gruppo di sicurezza non può essere associato ad alcuna risorsa.
- Il gruppo di sicurezza non può essere utilizzato come riferimento da una regola di un altro gruppo di sicurezza.
- Il gruppo di sicurezza non può essere utilizzato come gruppo di sicurezza predefinito di un VPC.

Per eliminare un gruppo di sicurezza tramite console

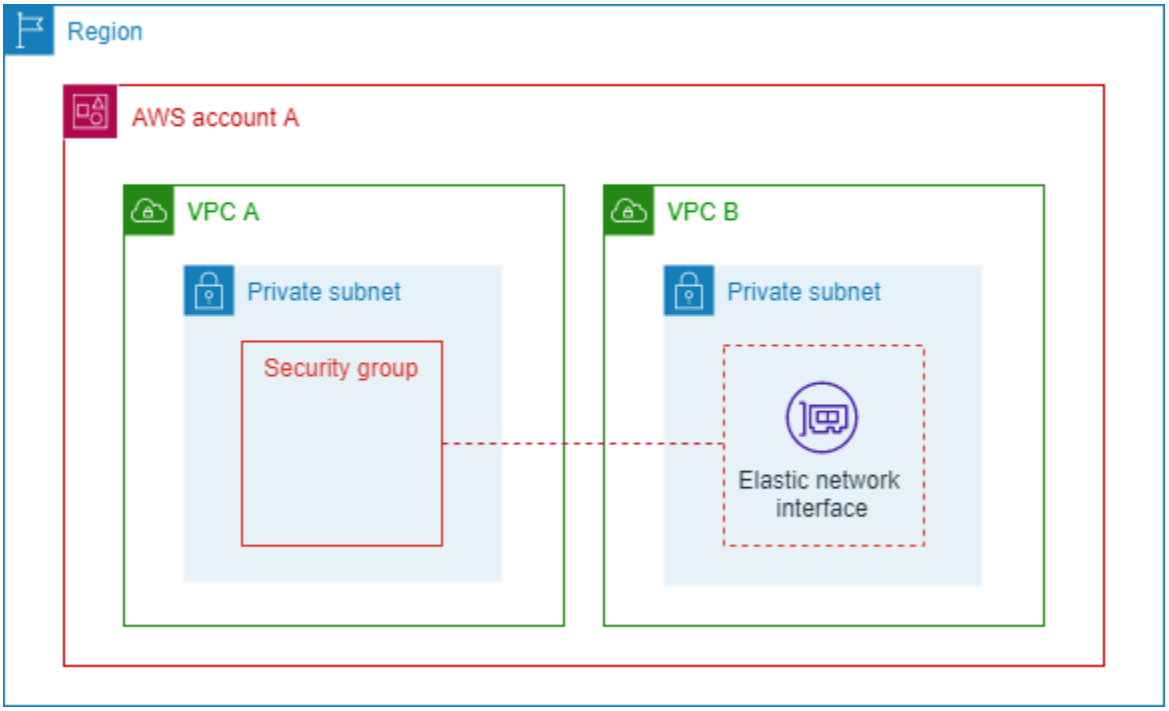
1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
3. Seleziona il gruppo di sicurezza e scegli Operazioni, Elimina gruppi di sicurezza.
4. Se hai selezionato più di un gruppo di sicurezza, ti verrà richiesta la conferma. Se alcuni gruppi di sicurezza non possono essere eliminati, viene visualizzato lo stato di ciascun gruppo di sicurezza, che indica se verrà eliminato. Per confermare l'eliminazione, immetti Elimina.
5. Scegli Elimina.

Per eliminare un gruppo di sicurezza utilizzando AWS CLI

Utilizza il comando delete-security-group.

Associare gruppi di sicurezza a più gruppi di sicurezza VPCs

Se hai carichi di lavoro in esecuzione in più gruppi VPCs che condividono i requisiti di sicurezza di rete, puoi utilizzare la funzionalità Security Group VPC Associations per associare un gruppo di sicurezza a VPCs più gruppi nella stessa regione. Ciò consente di gestire e mantenere i gruppi di sicurezza in un unico posto per più utenti del proprio VPCs account.



Il diagramma precedente mostra l' AWS account A con due al suo VPCs interno. Ciascuno di essi VPCs ha carichi di lavoro in esecuzione in una sottorete privata. In questo caso, i carichi di lavoro nelle sottoreti A e B del VPC condividono gli stessi requisiti di traffico di rete, quindi l'account A può utilizzare la funzionalità Associazioni di VPC e gruppi di sicurezza per associare il gruppo di sicurezza nel VPC A al VPC B. Qualsiasi aggiornamento apportato al gruppo di sicurezza associato viene applicato automaticamente al traffico dei carichi di lavoro nella sottorete B del VPC.

Requisiti della funzionalità Associazioni di VPC e gruppi di sicurezza

- Per associare un gruppo di sicurezza al VPC devi possedere il VPC o avere in condivisione una delle sue sottoreti.
- Il VPC e il gruppo di sicurezza devono trovarsi nella stessa AWS regione.

- Non è possibile associare un gruppo di sicurezza predefinito a un altro VPC o associare un gruppo di sicurezza a un VPC predefinito.
- Sia il proprietario del gruppo di sicurezza che il proprietario del VPC possono visualizzare le associazioni tra VPC e gruppi di sicurezza.

Servizi che supportano questa funzionalità

- Amazon API Gateway (APIs solo REST)
- AWS Auto Scaling
- AWS CloudFormation
- Amazon EC2
- Amazon EFS
- Amazon EKS
- Amazon FSx
- AWS PrivateLink
- Amazon Route 53
- Sistema di bilanciamento del carico elastico
  - Application Load Balancer
  - Network Load Balancer

Associazione di un gruppo di sicurezza a un altro VPC

Questa sezione spiega come utilizzare AWS Management Console e AWS CLI a cui associare un gruppo di sicurezza VPCs.

AWS Management Console

Associare un gruppo di sicurezza a un altro VPC

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Gruppi di sicurezza.
3. Scegli un gruppo di sicurezza per visualizzare i dettagli.
4. Scegli la scheda Associazioni VPC.
5. Scegli Associa VPC.

6. In ID VPC, scegli un VPC da associare al gruppo di sicurezza.
7. Scegli Associa VPC.

Command line

Associare un gruppo di sicurezza a un altro VPC

1. Crea un'associazione VPC con. associate-security-group-vpc
2. Controlla lo stato di un'associazione VPC con describe-security-group-vpc-associations e attendi che lo sia lo stato. `associated`

Il VPC è ora associato al gruppo di sicurezza.

Dopo aver associato il VPC al gruppo di sicurezza, puoi, ad esempio, avviare un'istanza nel VPC e scegliere questo nuovo gruppo di sicurezza o fare riferimento a questo gruppo di sicurezza in una regola del gruppo di sicurezza esistente.

Dissociazione di un gruppo di sicurezza da un altro VPC

Questa sezione spiega come utilizzare AWS Management Console e da cui AWS CLI dissociare un gruppo di sicurezza. VPCs Potresti volerlo fare se il tuo obiettivo è eliminare il gruppo di sicurezza. I gruppi di sicurezza non possono essere eliminati se sono associati. Puoi dissociare un gruppo di sicurezza solo se non ci sono interfacce di rete nel VPC associato che utilizza quel gruppo di sicurezza.

AWS Management Console

Per dissociare un gruppo di sicurezza da un VPC

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Gruppi di sicurezza.
3. Scegli un gruppo di sicurezza per visualizzare i dettagli.
4. Scegli la scheda Associazioni VPC.
5. Scegli Dissocia VPC.
6. In ID VPC, scegli un VPC da dissociare dal gruppo di sicurezza.
7. Scegli Dissocia VPC.

8. Visualizza lo stato della dissociazione nella scheda Associazioni VPC e attendi che lo stato sia `disassociated`.

Command line

Per dissociare un gruppo di sicurezza da un VPC

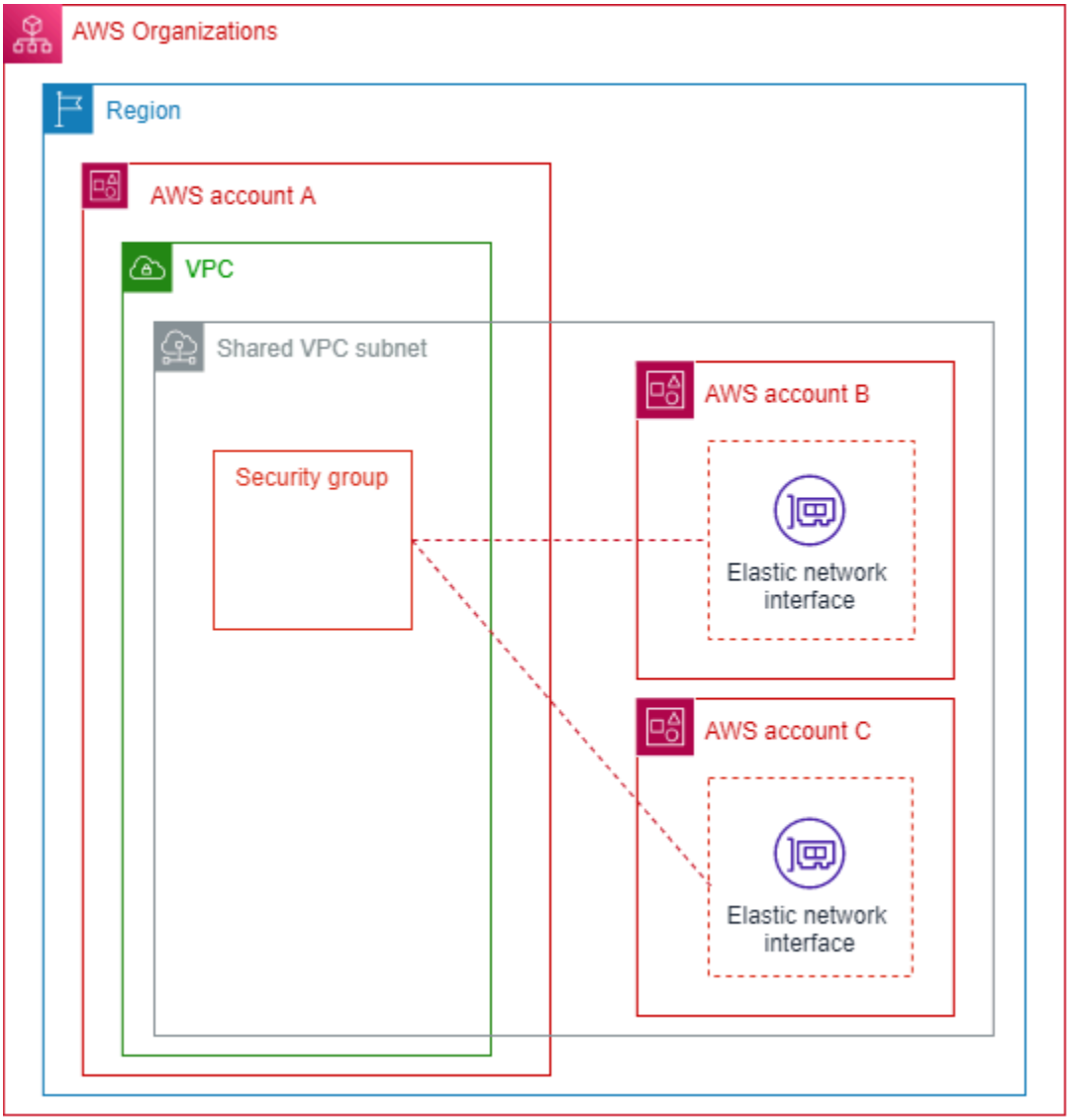
1. Dissocia un'associazione VPC con. disassociate-security-group-vpc
2. Controlla lo stato di una disassociazione VPC con describe-security-group-vpc-associations e attendi che lo sia lo stato. `disassociated`

Il VPC è ora dissociato dal gruppo di sicurezza.

Condividi i gruppi di sicurezza con AWS Organizations

La funzionalità Shared Security Group consente di condividere un gruppo di sicurezza con altri account AWS Organizations all'interno della stessa AWS regione e di rendere il gruppo di sicurezza disponibile per l'utilizzo da parte di tali account.

Il diagramma seguente mostra come utilizzare la funzionalità Shared Security Group per semplificare la gestione dei gruppi di sicurezza tra gli account delle Organizzazioni AWS :



Questo diagramma mostra tre account che fanno parte della stessa organizzazione. L'account A condivide una sottorete VPC con gli account B e C. L'account A condivide il gruppo di sicurezza con gli account B e C utilizzando la funzionalità Gruppo di sicurezza condiviso. Gli account B e C utilizzano quindi quel gruppo di sicurezza quando avviano istanze nella sottorete condivisa. Ciò consente all'account A di gestire il gruppo di sicurezza; qualsiasi aggiornamento al gruppo di sicurezza si applica alle risorse che gli account B e C hanno in esecuzione nella sottorete VPC condivisa.

Requisiti della funzionalità Gruppo di sicurezza condiviso

- Questa funzionalità è disponibile solo per gli account della stessa organizzazione in AWS Organizations. La condivisione delle risorse deve essere abilitata in AWS Organizations.

- L'account che condivide il gruppo di sicurezza deve possedere sia il VPC che il gruppo di sicurezza.
- Non è possibile condividere gruppi di sicurezza predefiniti.
- Non è possibile condividere gruppi di sicurezza che si trovano in un VPC predefinito.
- Gli account dei partecipanti possono creare gruppi di sicurezza in un VPC condiviso, ma non possono condividere tali gruppi di sicurezza.
- È necessario un set minimo di autorizzazioni per consentire a un principale IAM di condividere un gruppo di AWS RAM sicurezza. Utilizza le policy IAM `AmazonEC2FullAccess` e `AWSResourceAccessManagerFullAccess` gestite per assicurarti che i principali IAM dispongano delle autorizzazioni necessarie per condividere e utilizzare gruppi di sicurezza condivisi. Se utilizzi una policy IAM personalizzata, sono necessarie le operazioni `c2:PutResourcePolicy` e `ec2:DeleteResourcePolicy`. Si tratta di operazioni IAM che richiedono solo l'autorizzazione. Se a un principale IAM non sono concesse queste autorizzazioni, si verificherà un errore nel tentativo di condividere il gruppo di sicurezza utilizzando AWS RAM.

Servizi che supportano questa funzionalità

- Amazon API Gateway
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Amazon EMR
- Amazon FSx
- Amazon ElastiCache
- AWS Elastic Beanstalk
- AWS Glue
- Amazon MQ
- Amazon SageMaker AI
- Sistema di bilanciamento del carico elastico
  - Application Load Balancer
  - Network Load Balancer

In che modo questa funzionalità influisce sulle quote esistenti

Si applicano le quote dei gruppi di sicurezza. Per la quota «Gruppi di sicurezza per interfaccia di rete», tuttavia, se un partecipante utilizza sia gruppi di proprietà che gruppi condivisi su un'interfaccia di rete elastica (ENI), si applica la quota minima del proprietario e del partecipante.

Esempio per dimostrare in che modo la quota è influenzata da questa funzionalità:

- Quota dell'account del proprietario: 4 gruppi di sicurezza per interfaccia
- Quota dell'account del partecipante: 5 gruppi di sicurezza per interfaccia
- Il proprietario condivide i gruppi SG-O1, SG-O2, SG-O3, SG-O4, SG-O5 con il partecipante. Il partecipante dispone già di gruppi propri nel VPC: SG-P1, SG-P2, SG-P3, SG-P4, SG-P5.
- Se un partecipante crea una ENI e utilizza solo i gruppi di cui è proprietario, può associare tutti e 5 i gruppi di sicurezza (SG-P1, SG-P2, SG-P3, SG-P4, SG-P5) perché questa è la sua quota.
- Se il partecipante crea una ENI e utilizza dei gruppi condivisi al suo interno, può associare solo fino a 4 gruppi. In questo caso, la quota per tale ENI è la quota minima delle quote del proprietario e del partecipante. Le possibili configurazioni valide sono le seguenti:
  - SG-O1, SG-P1, SG-P2, SG-P3
  - SG-O1, SG-O2, SG-O3, SG-O4

Condivisione di un gruppo di sicurezza

Questa sezione spiega come utilizzare AWS Management Console e condividere un gruppo AWS CLI di sicurezza con altri account dell'organizzazione.

AWS Management Console

Condividere un gruppo di sicurezza

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Gruppi di sicurezza.
3. Scegli un gruppo di sicurezza per visualizzare i dettagli.
4. Scegliere la scheda Sharing (Condivisione) .
5. Scegli Condividi gruppo di sicurezza.
6. Seleziona Crea condivisione risorse. Di conseguenza, si apre la AWS RAM console in cui potrai creare la condivisione di risorse per il gruppo di sicurezza.

7. Aggiungi un Nome per la condivisione della risorsa.
8. In Risorse - facoltativo, scegli Gruppi di sicurezza.
9. Scelta del gruppo di sicurezza. Il gruppo di sicurezza non può essere un gruppo di sicurezza predefinito e non può essere associato al VPC predefinito.
10. Scegli Next (Successivo).
11. Controlla le operazioni che i principali saranno autorizzati a eseguire e scegli Avanti.
12. In Principali - facoltativo, scegli Consenti la condivisione solo all'interno dell'organizzazione.
13. In Principali, seleziona uno dei seguenti tipi di principali e inserisci i numeri appropriati:
    - AWS account: il numero di account di un account dell'organizzazione.
    - Organizzazione: The AWS Organizations ID.
    - Unità organizzativa (UO): l'ID di un'unità organizzativa nell'organizzazione.
    - Ruolo IAM: l'ARN di un ruolo IAM. L'account che ha creato il ruolo deve essere membro della stessa organizzazione dell'account che crea questa condivisione di risorse.
    - Utente IAM: l'ARN di un utente IAM. L'account che ha creato l'utente deve essere membro della stessa organizzazione dell'account che crea questa condivisione di risorse.
    - Principale del servizio: non è possibile condividere un gruppo di sicurezza con un principale del servizio.
14. Scegli Aggiungi.
15. Scegli Next (Successivo).
16. Seleziona Crea condivisione risorse.
17. In Risorse condivise, attendi di visualizzare lo stato di `Associated`. Se si verifica un errore nell'associazione tra i gruppi di sicurezza, il motivo può essere una delle limitazioni sopra elencate. Visualizza i dettagli del gruppo di sicurezza e la scheda Condivisione nella pagina dei dettagli per visualizzare eventuali messaggi relativi al motivo per cui un gruppo di sicurezza potrebbe non essere condivisibile.
18. Torna all'elenco dei gruppi di sicurezza della console VPC.
19. Scegli il gruppo di sicurezza che hai condiviso.
20. Scegliere la scheda Sharing (Condivisione) . La tua AWS RAM risorsa dovrebbe essere visibile lì. In caso contrario, la creazione della condivisione di risorse potrebbe non essere riuscita e potrebbe essere necessario ricrearla.

Command line

Condividere un gruppo di sicurezza

1. È innanzitutto necessario creare una condivisione di risorse per il gruppo di sicurezza con cui si desidera condividere AWS RAM. Per istruzioni su come creare una condivisione di risorse AWS RAM utilizzando il AWS CLI, consulta Creazione di una condivisione di risorse AWS RAM nella Guida per l'AWS RAM utente
2. Per visualizzare le associazioni di condivisione delle risorse create, utilizzare get-resource-share-associations.

Il gruppo di sicurezza è ora condiviso. È possibile selezionare il gruppo di sicurezza quando si avvia un' EC2 istanza in una sottorete condivisa all'interno dello stesso VPC.

Interruzione della condivisione di un gruppo di sicurezza

Questa sezione spiega come utilizzare AWS Management Console e per interrompere la condivisione AWS CLI di un gruppo di sicurezza con altri account dell'organizzazione.

AWS Management Console

Interrompere la condivisione di un gruppo di sicurezza

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Gruppi di sicurezza.
3. Scegli un gruppo di sicurezza per visualizzare i dettagli.
4. Scegliere la scheda Sharing (Condivisione) .
5. Scegli una condivisione di risorse per il gruppo di sicurezza e successivamente Interrompi condivisione.
6. Scegli Sì, interrompi condivisione.

Command line

Interrompere la condivisione di un gruppo di sicurezza

Elimina la condivisione di risorse con delete-resource-share.

Il gruppo di sicurezza non è più condiviso. Una volta che il proprietario interrompe la condivisione di un gruppo di sicurezza, si applicano le regole seguenti:

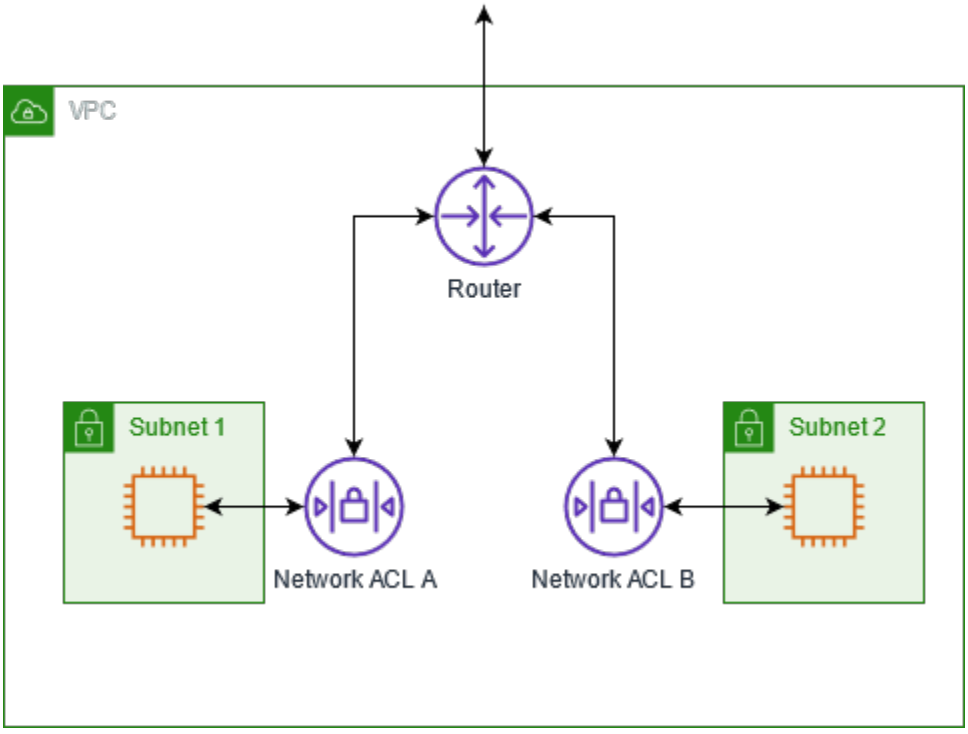
- Il partecipante esistente Elastic Network Interfaces (ENIs) continua a ricevere tutti gli aggiornamenti delle regole dei gruppi di sicurezza apportati ai gruppi di sicurezza non condivisi. L'annullamento della condivisione impedisce solo al partecipante di creare nuove associazioni con il gruppo non condiviso.
- I partecipanti non possono più associare il gruppo di sicurezza non condiviso a nessuno di loro proprietà. ENIs
- I partecipanti possono descrivere ed eliminare i gruppi ENIs di sicurezza ancora associati a gruppi di sicurezza non condivisi.
- Se i partecipanti sono ancora ENIs associati al gruppo di sicurezza non condiviso, il proprietario non può eliminare il gruppo di sicurezza non condiviso. Il proprietario può eliminare il gruppo di sicurezza solo dopo che i partecipanti hanno dissociato (rimosso) il gruppo di sicurezza da tutti i propri. ENIs
- I partecipanti non possono avviare nuove EC2 istanze utilizzando un ENI associato a un gruppo di sicurezza non condiviso.

Controllo del traffico della sottorete con le liste di controllo degli accessi alla 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.

Non ci sono costi aggiuntivi per l'utilizzo della rete ACLs.

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 gruppi di sicurezza e rete ACLs, vedereConfronta i gruppi di sicurezza e la rete ACLs.

Indice

- Informazioni di base sulla lista di controllo accessi di rete
- Regole di liste di controllo accessi di rete
- lista di controllo accessi di rete predefinita
- Rete personalizzata ACLs
- Porte Effimere
- Rilevamento della MTU del percorso
- Lavora con la rete ACLs
- Esempio: controllo dell'accesso alle istanze in una sottorete
- Risoluzione dei problemi di raggiungibilità

Informazioni di base sulla lista di controllo accessi di rete

Di seguito sono riportate le cose di base da sapere sulla rete ACLs:

- Il VPC viene fornito automaticamente con una lista di controllo accessi di rete modificabile. Per impostazione predefinita, consente tutto il traffico in entrata e in uscita e, se applicabile, IPv6 il IPv4 traffico.
- 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.
- NACLs sono stateless, il che significa che 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' EC2 istanza, le risposte vengono automaticamente consentite indipendentemente dalle regole del gruppo di sicurezza in uscita.
- La rete non ACLs può 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.
- La rete non ACLs può bloccare il traffico verso l'Instance Metadata Service (IMDS). Per gestire l'accesso a IMDS, consulta Configurare le opzioni dei metadati dell'istanza nella Amazon EC2 User Guide.
- La rete ACLs non filtra il traffico destinato e proveniente da quanto segue:

- Amazon Domain Name Services (DNS)
- Amazon Dynamic Host Configuration Protocol (DHCP)
- Metadati delle EC2 istanze Amazon
- 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 il numero di rete ACLs per VPC e 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 dall'ACL di rete predefinito o creare una rete aggiuntiva ACLs per il tuo 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 aggiungi una regola utilizzando uno strumento da riga di comando o l' EC2 API Amazon, l'intervallo CIDR viene automaticamente modificato nella sua forma canonica. 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.

La tabella seguente mostra le regole in entrata per un ACL di rete predefinito per un VPC che supporta solo. IPv4

Rule #	Tipo	Protocollo	Intervallo porte	Crea	Consenti/ Nega
100	Tutto il traffico IPv4	Tutti	Tutti	0.0.0.0/0	PERMETTI
*	Tutto IPv4 il traffico	Tutti	Tutti	0.0.0.0/0	DENY

La tabella seguente mostra le regole in uscita per un ACL di rete predefinito per un VPC che supporta solo. IPv4

Rule #	Tipo	Protocollo	Intervallo porte	Destinazione	Consenti/ Nega
100	Tutto il traffico IPv4	Tutti	Tutti	0.0.0.0/0	PERMETTI
*	Tutto IPv4 il traffico	Tutti	Tutti	0.0.0.0/0	DENY

Se crei un VPC con un blocco IPv6 CIDR o se associ un blocco IPv6 CIDR al tuo VPC esistente, aggiungiamo automaticamente regole che consentono a tutto il IPv6 traffico di fluire in entrata e in uscita dalla tua 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.

> **Note**
>
> Se hai modificato le regole in entrata dell'ACL di rete predefinito, non aggiungiamo automaticamente una `ALLOW` regola per il IPv6 traffico in entrata quando associ un IPv6 blocco al tuo VPC. Allo stesso modo, se hai modificato le regole in uscita, non aggiungiamo automaticamente una `ALLOW` regola per il traffico in uscita. IPv6

La tabella seguente mostra le regole in entrata per un ACL di rete predefinito per un VPC che supporta e. IPv4 IPv6

Rule #	Tipo	Protocollo	Intervallo porte	Crea	Consenti/ Nega
100	Tutto il traffico IPv4	Tutti	Tutti	0.0.0.0/0	PERMETTI
101	Tutto IPv6 il traffico	Tutti	Tutti	::/0	ALLOW
*	Tutto il traffico	Tutti	Tutti	0.0.0.0/0	DENY
*	Tutto IPv6 il traffico	Tutti	Tutti	::/0	DENY

La tabella seguente mostra le regole in uscita per un ACL di rete predefinito per un VPC che supporta e. IPv4 IPv6

Rule #	Tipo	Protocollo	Intervallo porte	Destinazione	Consenti/ Nega
100	Tutto il traffico	Tutti	Tutti	0.0.0.0/0	PERMETTI

Rule #	Tipo	Protocollo	Intervallo porte	Destinazione	Consenti/ Nega
101	Tutto il traffico IPv6	Tutti	Tutti	::/0	ALLOW
*	Tutto il traffico	Tutti	Tutti	0.0.0.0/0	DENY
*	Tutto IPv6 il traffico	Tutti	Tutti	::/0	DENY

Rete personalizzata ACLs

L'esempio seguente mostra un ACL di rete personalizzato per un VPC che IPv4 supporta solo. 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.

La tabella seguente mostra le regole in entrata per un ACL di rete personalizzato per un VPC che supporta solo. IPv4

Rule #	Tipo	Protocollo	Intervallo porte	Crea	Consenti/ Nega	Commenti
100	HTTP	TCP	80	0.0.0.0/0	PERMETTI	Consente il traffico HTTP in entrata da

Rule #	Tipo	Protocollo	Intervallo porte	Crea	Consenti/Nega	Commenti
						qualsiasi indirizzo. IPv4
110	HTTPS	TCP	443	0.0.0.0/0	PERMETTI	Consente il traffico HTTPS in entrata da qualsiasi IPv4 indirizzo.
120	SSH	TCP	22	192.0.2.0/24	PERMETTI	Consente il traffico SSH in entrata dall'intervallo di IPv4 indirizzi pubblici della rete domestica (tramite il gateway Internet).
130	RDP	TCP	3389	192.0.2.0/24	PERMETTI	Consente il traffico RDP in entrata verso i server Web dall'intervallo di IPv4 indirizzi pubblici della rete domestica (tramite il gateway Internet).
140	TCP personalizzato	TCP	32768-65535	0.0.0.0/0	PERMETTI	Consente il IPv4 traffico di ritorno in entrata da Internet (ovvero per le richieste che hanno origine nella sottorete). 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	DENY	Nega tutto il IPv4 traffico in entrata che non sia già gestito da una regola precedente (non modificabile).

La tabella seguente mostra le regole in uscita per un ACL di rete personalizzato per un VPC che supporta solo. IPv4

Rule #	Tipo	Protocollo	Intervallo porte	Destinazione	Consenti/Nega	Commenti
100	HTTP	TCP	80	0.0.0.0/0	PERMETTI	Consente il traffico IPv4 HTTP in uscita dalla sottorete a Internet.
110	HTTPS	TCP	443	0.0.0.0/0	PERMETTI	Consente il traffico IPv4 HTTPS in uscita dalla sottorete verso Internet.
120	SSH	TCP	1024-65535	192.0.2.0/24	PERMETTI	Consente il traffico SSH di ritorno in uscita verso l'intervallo di IPv4 indirizzi pubblici della rete domestica (tramite il gateway Internet).
140	TCP personalizzato	TCP	32768-65535	0.0.0.0/0	PERMETTI	Consente IPv4 risposte in uscita ai client su Internet (ad esempio, fornendo

Rule #	Tipo	Protocollo	Intervallo porte	Destinazione	Consenti/Nega	Commenti
						pagine Web agli utenti che visitano i server Web nella sottorete). Questo intervallo è solo un esempio.
*	Tutto il traffico	Tutti	Tutti	0.0.0.0/0	DENY	Nega tutto il IPv4 traffico in uscita non 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.

L'esempio seguente mostra un ACL di rete personalizzato per un VPC a cui è IPv6 associato un blocco CIDR. Questo ACL di rete include regole per tutto il traffico IPv6 HTTP e HTTPS. In questo caso, sono state inserite nuove regole tra le regole esistenti per il IPv4 traffico. Puoi anche aggiungere le regole come regole con numeri più alti dopo le IPv4 regole. IPv4 e IPv6 il traffico sono separati, pertanto nessuna delle regole per il IPv4 traffico si applica al IPv6 traffico.

La tabella seguente mostra le regole in entrata per un ACL di rete personalizzato per un VPC a cui è associato un blocco CIDR. IPv6

Rule #	Tipo	Protocollo	Intervallo porte	Crea	Consenti/Nega	Commenti
100	HTTP	TCP	80	0.0.0.0/0	PERMETTI	Consente il traffico HTTP in entrata da qualsiasi indirizzo. IPv4
105	HTTP	TCP	80	::/0	ALLOW	Consente il traffico HTTP in entrata da qualsiasi IPv6 indirizzo.
110	HTTPS	TCP	443	0.0.0.0/0	PERMETTI	Consente il traffico HTTPS in entrata da qualsiasi IPv4 indirizzo.
115	HTTPS	TCP	443	::/0	ALLOW	Consente il traffico HTTPS in entrata da qualsiasi IPv6 indirizzo.
120	SSH	TCP	22	192.0.2.0/24	PERMETTI	Consente il traffico SSH in entrata dall'intervallo di IPv4 indirizzi pubblici della rete domestica (tramite il gateway Internet).
130	RDP	TCP	3389	192.0.2.0/24	PERMETTI	Consente il traffico RDP in entrata verso i server Web dall'intervallo di IPv4 indirizzi

Rule #	Tipo	Protocollo	Intervallo porte	Crea	Consenti/Nega	Commenti
						pubblici della rete domestica (tramite il gateway Internet).
140	TCP personalizzato	TCP	32768-65535	0.0.0.0/0	PERMETTI	Consente il IPv4 traffico di ritorno in entrata da Internet (ovvero per le richieste che hanno origine nella sottorete). Questo intervallo è solo un esempio.
145	TCP personalizzato	TCP	32768-65535	::/0	ALLOW	Consente il IPv6 traffico di ritorno in entrata da Internet (ovvero, per le richieste che hanno origine nella sottorete). Questo intervallo è solo un esempio.
*	Tutto il traffico	Tutti	Tutti	0.0.0.0/0	DENY	Nega tutto il IPv4 traffico in entrata che non sia già gestito da una regola precedente (non modificabile).

Rule #	Tipo	Protocollo	Intervallo porte	Crea	Consenti/Nega	Commenti
*	Tutto il traffico	Tutti	Tutti	::/0	DENY	Nega tutto il IPv6 traffico in entrata che non sia già gestito da una regola precedente (non modificabile).

La tabella seguente mostra le regole in uscita per un ACL di rete personalizzato per un VPC a cui è associato un blocco CIDR. IPv6

Rule #	Tipo	Protocollo	Intervallo porte	Destinazione	Consenti/Nega	Commenti
100	HTTP	TCP	80	0.0.0.0/0	PERMETTI	Consente il traffico IPv4 HTTP in uscita dalla sottorete a Internet.
105	HTTP	TCP	80	::/0	ALLOW	Consente il traffico IPv6 HTTP in uscita dalla sottorete verso Internet.
110	HTTPS	TCP	443	0.0.0.0/0	PERMETTI	Consente il traffico IPv4 HTTPS in uscita dalla sottorete verso Internet.
115	HTTPS	TCP	443	::/0	ALLOW	Consente il traffico IPv6 HTTPS in uscita dalla sottorete verso Internet.

Rule #	Tipo	Protocollo	Intervallo porte	Destinazione	Consenti/Nega	Commenti
140	TCP personalizzato	TCP	32768-65535	0.0.0.0/0	PERMETTI	Consente IPv4 risposte in uscita ai client su Internet (ad esempio, fornendo pagine Web agli utenti che visitano i server Web nella sottorete). Questo intervallo è solo un esempio.
145	TCP personalizzato	TCP	32768-65535	::/0	ALLOW	Consente IPv6 risposte in uscita ai client su Internet (ad esempio, fornendo pagine Web agli utenti che visitano i server Web nella sottorete). Questo intervallo è solo un esempio.
*	Tutto il traffico	Tutti	Tutti	0.0.0.0/0	DENY	Nega tutto il IPv4 traffico in uscita non già gestito da una regola precedente (non modificabile).
*	Tutto il traffico	Tutti	Tutti	::/0	DENY	Nega tutto il IPv6 traffico in uscita che non sia già gestito da una regola precedente (non modificabile).

ACLs AWS Rete personalizzata e altri servizi

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 ACL di rete consigliate per i sistemi di bilanciamento del carico e le istanze di backend, consulta quanto segue:

- Rete ACLs per il tuo Application Load Balancer
- Rete ACLs per il tuo Network Load Balancer
- Rete ACLs per il tuo Classic Load Balancer

Porte Effimere

La lista di controllo accessi di rete di esempio nella sezione precedente utilizza un intervallo di porte Effimere di 32768-65535. Tuttavia, potresti voler utilizzare un intervallo diverso per la tua rete ACLs a seconda del tipo di client che stai utilizzando o con cui stai comunicando.

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.

Infatti IPv4, quando un host invia un pacchetto più grande dell'MTU dell'host ricevente o più grande dell'MTU di un dispositivo lungo il percorso, l'host o il dispositivo ricevente elimina il pacchetto e quindi restituisce il seguente messaggio ICMP: (Tipo 3, Codice 4). `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` Questo indica all'host trasmittente di dividere il payload in più pacchetti più piccoli e quindi di trasmetterli di nuovo.

Il IPv6 protocollo non supporta la frammentazione della 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 l'unità di trasmissione massima di rete (MTU) per la tua EC2 istanza nella Amazon EC2 User Guide.

Lavora con la rete ACLs

Le seguenti attività mostrano come lavorare con la rete ACLs utilizzando la console Amazon VPC.

Attività

- 1. Determinazione delle associazioni della lista di controllo accessi di rete
- 2. Creazione di una lista di controllo degli accessi di rete
- 3. Aggiunta ed eliminazione di regole
- 4. Associazione di una sottorete a una lista di controllo accessi di rete
- 5. Annullamento dell'associazione di una lista di controllo accessi di rete a una sottorete
- 6. Modifica dell'ACL di rete di una sottorete
- 7. Eliminazione di una lista di controllo accessi di rete
- Panoramica della riga di comando
- Gestione della rete ACLs tramite Firewall Manager

1. 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. La rete ACLs può essere associata a più di una sottorete, quindi puoi anche determinare quali sottoreti sono associate a un ACL di rete.

Per determinare quale lista di controllo accessi di rete è associata a una sottorete

1. Apri la 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Rete. ACLs 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.

2. 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Rete ACLs.
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).

3. 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 ACL di rete definiscono i tipi di traffico di rete che possono entrare o uscire dal tuo VPCs. 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 il tuo. VPCs

Se utilizzi l' EC2 API Amazon o uno strumento da 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Rete ACLs.
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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Rete ACLs, quindi seleziona l'ACL 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).

4. 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Rete ACLs, quindi seleziona l'ACL 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).

5. 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Rete ACLs, quindi seleziona l'ACL 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. Seleziona Salva.

6. 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. Apri la 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).

7. 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. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Rete ACLs.

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 della riga di comando

È possibile eseguire le attività descritte in questa pagina utilizzando la riga di comando.

Creazione di una lista di controllo accessi di rete per il VPC

- create-network-acl (AWS CLI)
- New-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Descrivi una o più delle tue reti ACLs

- 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)

Gestione della rete ACLs tramite Firewall Manager

AWS Firewall Manager semplifica le attività di amministrazione e manutenzione dell'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 delle liste di controllo degli accessi alla rete definite. Firewall Manager è particolarmente utile quando si desidera proteggere l'intera organizzazione o se si aggiungono spesso nuove sottoreti che si desidera proteggere automaticamente da un account 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 definire nella rete ACLs utilizzata nell'organizzazione. È possibile specificare quali account e sottoreti dell'organizzazione rientrano nell'ambito della policy di Firewall Manager. Firewall Manager segnala lo stato di conformità della rete ACLs per le sottoreti incluse nell'ambito ed è possibile configurare Firewall Manager per correggere automaticamente le reti ACLs non conformi e renderle conformi.

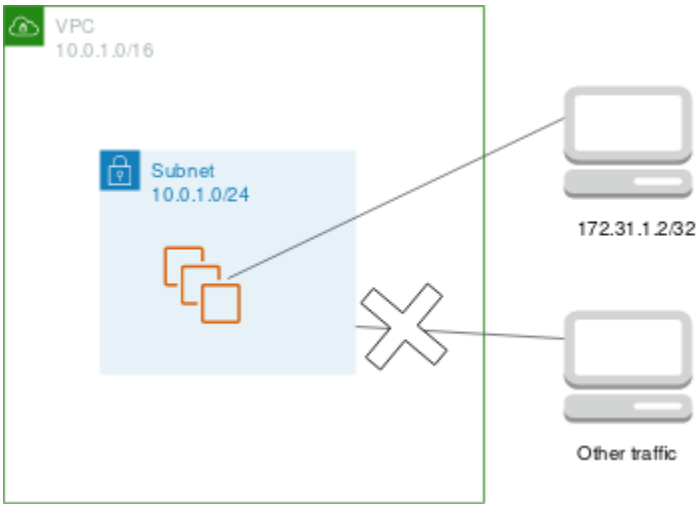
Per ulteriori informazioni sull'utilizzo di Firewall Manager per gestire la rete ACLs, consulta le seguenti risorse nella guida per gli AWS Firewall Manager sviluppatori:

- AWS Firewall Manager prerequisiti
- Guida introduttiva alle AWS Firewall Manager policy ACL della rete Amazon VPC
- Policy delle liste 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.



La tabella che segue mostra le regole in entrata per un gruppo di sicurezza di esempio per le istanze.

Tipo di protocollo	Protocollo	Intervallo porte	Crea	Commenti
Tutto il traffico	Tutti	Tutti	sg-123456 7890abcdef0	Tutte le istanze associate a questo gruppo di sicurezza possono comunicare tra loro.
SSH	TCP	22	172.31.1.2/32	Permette l'accesso SSH in entrata dal computer remoto.

La tabella che segue mostra le regole in uscita per un gruppo di sicurezza di esempio per le istanze. I gruppi di sicurezza sono stateful. Pertanto non è necessaria una regola che consenta le risposte al traffico in entrata.

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.

La tabella che segue mostra le regole in entrata per un'ACL di rete di esempio da associare alle sottoreti per le istanze. Le regole delle liste di controllo accessi di rete si applicano a tutte le istanze nella sottorete.

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.
*	Tutto il traffico	Tutti	Tutti	0.0.0.0/0	RIFIUTA	Nega tutto il traffico in entrata.

La tabella che segue mostra le regole in uscita per un'ACL di rete di esempio da associare alle sottoreti per le istanze. ACLs Le reti sono prive di stato. Pertanto, è necessaria una regola che consenta le risposte al traffico in entrata.

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.

Tipo	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.
SSH	TCP	22	0.0.0.0/0	Permette l'accesso SSH da qualsiasi indirizzo IP.

Risoluzione dei problemi di raggiungibilità

Reachability Analyzer è uno strumento di analisi statica della configurazione. Utilizza questo strumento per analizzare ed eseguire il debug della raggiungibilità di rete tra due risorse nel 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 configurate in modo errato.

Per ulteriori informazioni, consulta la Guida di Reachability Analyzer.

Resilienza in Amazon Virtual Private Cloud

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS 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.

Regioni AWS sono gli elementi costitutivi principali, ognuno dei quali rappresenta una posizione geografica distinta che ospita più zone di disponibilità fisicamente separate e isolate. Queste zone di disponibilità sono collegate attraverso un fabric di rete a bassa latenza, ad alta velocità e altamente ridondante, che consente la comunicazione e il trasferimento di dati senza soluzione di continuità tra esse.

L'architettura delle zone di disponibilità è un elemento chiave di differenziazione, in quanto sono progettate per essere molto più robuste e tolleranti ai guasti rispetto alle tradizionali configurazioni di data center singoli o multipli. Distribuendo le risorse su più zone di disponibilità all'interno di una regione, è possibile progettare applicazioni e database per eseguire automaticamente il failover tra le zone senza alcuna interruzione del servizio. Questo livello di ridondanza e alta disponibilità è un requisito fondamentale per i carichi di lavoro mission critical e consente alle organizzazioni di creare soluzioni resilienti native del cloud.

Inoltre, la scalabilità e la portata globale dell' AWS infrastruttura consentono ai clienti di implementare le proprie applicazioni più vicino agli utenti finali, riducendo la latenza e migliorando l'esperienza utente complessiva. La disponibilità di più Regioni in tutto il mondo consente inoltre un'effettiva sovranità e conformità dei dati, in quanto i clienti possono archiviare ed elaborare i dati entro i confini geografici richiesti dalle loro specifiche esigenze normative e aziendali.

Sfruttando l'infrastruttura AWS globale, le organizzazioni possono progettare i propri ambienti cloud in modo che siano altamente disponibili, tolleranti ai guasti e scalabili, con la flessibilità necessaria per adattarsi ai requisiti mutevoli e alle esigenze aziendali in evoluzione. Questa solida base è un fattore chiave per l'implementazione di successo di applicazioni e servizi moderni basati sul cloud.

Per ulteriori informazioni sulle zone di disponibilità, consulta Global Regioni AWS Infrastructure.AWS

Puoi configurarlo VPCs per soddisfare i requisiti di resilienza per i tuoi 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:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e 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.

Blocca l'accesso pubblico alle sottoreti VPCs e alle sottoreti

VPC Block Public Access (BPA) è una funzionalità di sicurezza centralizzata che consente di impedire in modo autoritario l'accesso pubblico a Internet alle risorse VPC di un intero account AWS , garantendo la conformità ai requisiti di sicurezza e fornendo al contempo flessibilità per eccezioni specifiche e funzionalità di audit.

La funzionalità VPC BPA offre le seguenti modalità:

- Bidirezionale: tutto il traffico da e verso i gateway Internet e i gateway Internet solo in uscita in questa regione (ad eccezione delle sottoreti escluse e delle sottoreti) è bloccato. VPCs
- Solo in ingresso: tutto il traffico Internet verso questa regione (ad eccezione delle sottoreti o delle sottoreti che sono VPCs escluse) è bloccato. VPCs È consentito solo il traffico da e verso i gateway NAT e i gateway Internet egress-only, poiché questi gateway consentono solo di stabilire connessioni in uscita.

Puoi anche creare “esclusioni” in questa funzionalità per il traffico che non desideri bloccare. Un'esclusione è una modalità che può essere applicata a un singolo VPC o a una singola sottorete che lo esenta dalla modalità BPA dell'account e consentirà l'accesso bidirezionale o egress-only.

Le esclusioni possono avere una delle seguenti modalità:

- Bidirezionale: è consentito tutto il traffico Internet da e verso le sottoreti e le sottoreti escluse. VPCs
- Solo in uscita: è consentito il traffico Internet in uscita dalle sottoreti e dalle sottoreti escluse. VPCs Il traffico Internet in entrata verso le sottoreti e le sottoreti escluse è bloccato. VPCs Questo vale solo quando BPA è impostato su Bidirezionale.

Indice

- Nozioni di base su BPA
- Valutazione dell'impatto di BPA e monitoraggio di BPA
- Esempio avanzato

Nozioni di base su BPA

Questa sezione contiene dettagli importanti su VPC BPA, inclusi i servizi che lo supportano e come utilizzarlo.

Indice

- Disponibilità regionale
- AWS impatto e supporto del servizio
- Limitazioni di BPA
- Controllo dell'accesso a VPC BPA con una policy IAM
- Abilitazione della modalità bidirezionale BPA per l'account

- Modifica della modalità VPC BPA in ingress-only
- Creazione ed eliminazione di esclusioni
- Abilitazione di VPC BPA a livello di organizzazione

Disponibilità regionale

VPC BPA è disponibile in tutte le AWS regioni commerciali, comprese le regioni GovCloud della Cina.

In questa guida, troverai anche informazioni sull'utilizzo dello Strumento di analisi degli accessi alla rete e di Reachability Analyzer con VPC BPA. Lo Strumento di analisi degli accessi alla rete e Reachability Analyzer non sono disponibili in tutte le Regioni commerciali. Per informazioni sulla disponibilità regionale dello Strumento di analisi degli accessi alla rete e di Reachability Analyzer, consulta Limitazioni nella Guida dello Strumento di analisi degli accessi alla rete e Considerazioni nella Guida di Reachability Analyzer.

AWS impatto e supporto del servizio

Le risorse e i servizi seguenti supportano VPC BPA e il traffico verso questi servizi e risorse è influenzato da VPC BPA:

- Gateway Internet: tutto il traffico in entrata e in uscita è bloccato.
- Gateway Internet egress-only: tutto il traffico in uscita è bloccato. I gateway Internet egress-only non consentono il traffico in entrata.
- Gateway NAT: tutto il traffico in entrata e in uscita è bloccato. I gateway NAT richiedono un gateway Internet per la connettività Internet.
- Network Load Balancer connesso a Internet: tutto il traffico in entrata e in uscita è bloccato. I Network Load Balancer connessi a Internet richiedono un gateway Internet per la connettività.
- Application Load Balancer connesso a Internet: tutto il traffico in entrata e in uscita è bloccato. Gli Application Load Balancer connessi a Internet richiedono un gateway Internet per la connettività.
- Amazon CloudFront VPC Origins: tutto il traffico in entrata e in uscita è bloccato.
- AWS Global Accelerator: il traffico in entrata verso VPCs è bloccato, indipendentemente dal fatto che la destinazione sia altrimenti accessibile da Internet.
- AWS Wavelength carrier gateway: tutto il traffico in entrata e in uscita è bloccato.

Il traffico relativo alla connettività privata, come il traffico per i seguenti servizi e risorse, non viene bloccato o influenzato da VPC BPA:

- AWS Client VPN
- AWS CloudWAN
- AWS Outposts gateway locale
- AWS Site-to-Site VPN
- Transit Gateway
- Accesso verificato da AWS

> **Important**
>
> Il traffico inviato privatamente dalle risorse del tuo VPC ad altri servizi in esecuzione nel tuo VPC, come EC2 DNS Resolver Amazon OpenSearch Service o, è consentito anche quando BPA è attivo perché non passa attraverso un gateway Internet nel tuo VPC. È possibile che questi servizi effettuino richieste a risorse esterne al VPC per tuo conto, ad esempio per risolvere una query DNS, e possano esporre informazioni sull'attività delle risorse all'interno del VPC se non mitigate da altri controlli di sicurezza.

Limitazioni di BPA

La modalità VPC BPA solo in ingresso non è supportata in Local Zones (LZs), dove i gateway NAT e i gateway Internet solo in uscita non sono consentiti.

Controllo dell'accesso a VPC BPA con una policy IAM

Per esempi di policy IAM che consentono/negano l'accesso alla funzionalità VPC BPA, consulta Blocca l'accesso pubblico alle sottoreti e alle VPCs sottoreti.

Abilitazione della modalità bidirezionale BPA per l'account

La modalità bidirezionale VPC BPA blocca tutto il traffico da e verso i gateway Internet e i gateway Internet solo in uscita in questa regione (ad eccezione delle sottoreti e delle sottoreti escluse). VPCs Per ulteriori informazioni sulle esclusioni, consulta Creazione ed eliminazione di esclusioni.

> **Important**
>
> Ti consigliamo di esaminare attentamente i carichi di lavoro che richiedono l'accesso a Internet prima di abilitare VPC BPA nei tuoi account di produzione.

> **Note**
>
> - Per abilitare VPC BPA sulle sottoreti VPCs e del tuo account, devi possedere le sottoreti and. VPCs
> - Se attualmente condividi sottoreti VPC con altri account, la modalità VPC BPA applicata dal proprietario della sottorete si applica anche al traffico dei partecipanti, ma questi ultimi non possono controllare le impostazioni VPC BPA che influiscono sulla sottorete condivisa.

AWS Management Console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni.
3. Scegli Modifica impostazioni di accesso pubblico.
4. Scegli Attiva il blocco dell'accesso pubblico e Bidirezionale, quindi scegli Salva modifiche.
5. Attendi che lo stato passi su Abilitato. Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato.

La modalità bidirezionale VPC BPA è ora attiva.

AWS CLI

1. Attiva VPC BPA:

   ```
   aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
   ```

   Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato.
2. Visualizza lo stato di VPC BPA:

   ```
   aws ec2 --region us-east-2 describe-vpc-block-public-access-options
   ```

Modifica della modalità VPC BPA in ingress-only

La modalità VPC BPA solo in ingresso blocca tutto il traffico Internet verso questa regione (ad eccezione delle VPCs sottoreti che sono escluse). VPCs È consentito solo il traffico da e verso i gateway NAT e i gateway Internet egress-only, poiché questi gateway consentono solo di stabilire connessioni in uscita.

AWS Management Console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni.
3. Scegli Modifica impostazioni di accesso pubblico.
4. Cambia la direzione impostandola su Solo ingresso.
5. Salva le modifiche e attendi che lo stato venga aggiornato. Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato.

AWS CLI

1. Modifica la direzione del blocco VPC BPA:

   ```
   aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-ingress
   ```

   Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato.
2. Visualizza lo stato di VPC BPA:

   ```
   aws ec2 --region us-east-2 describe-vpc-block-public-access-options
   ```

Creazione ed eliminazione di esclusioni

Un'esclusione VPC BPA è una modalità che può essere applicata a un singolo VPC o a una singola sottorete che lo esenta dalla modalità BPA dell'account e consentirà l'accesso bidirezionale o egress-only. Puoi creare esclusioni BPA per VPCs e sottoreti anche quando BPA non è abilitato sull'account per garantire che non vi siano interruzioni del traffico delle esclusioni quando VPC BPA è attivato. Un'esclusione per un VPC si applica automaticamente a tutte le sottoreti del VPC.

È possibile creare un massimo di 50 esclusioni. Per informazioni su come richiedere un aumento dei limiti, consulta Esclusioni di VPC BPA per account in Quote Amazon VPC.

AWS Management Console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni.
3. Nella scheda Blocca accesso pubblico, in Esclusioni, esegui una delle seguenti operazioni:
   - Per eliminare un'esclusione, seleziona l'esclusione, quindi scegli Azioni > Elimina esclusioni.
   - Per creare un'esclusione, scegli Crea esclusioni e continua con i passaggi successivi.
4. Scegli la direzione del blocco:
   - Bidirezionale: consente tutto il traffico Internet da e verso le sottoreti e le sottoreti escluse VPCs .
   - Solo uscita: consente il traffico Internet in uscita dalle sottoreti escluse e dalle sottoreti. VPCs Blocca il traffico Internet in entrata verso gli esclusi e le sottoreti. VPCs Questa impostazione si applica solo quando BPA è impostato su Bidirezionale.
5. Scegli un VPC o una sottorete.
6. Scegli Crea esclusioni.
7. Attendi che lo Stato dell'esclusione passi su Attivo. Potrebbe essere necessario aggiornare la tabella di esclusione per visualizzare la modifica.

L'esclusione è stata creata.

AWS CLI

1. Modifica la direzione di autorizzazione dell'esclusione:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. L'aggiornamento dello stato dell'esclusione può richiedere del tempo. Per visualizzare lo stato dell'esclusione:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

Abilitazione di VPC BPA a livello di organizzazione

Se utilizzi AWS Organizations per gestire gli account della tua organizzazione, puoi utilizzare una policy dichiarativa di AWS Organizations per applicare il VPC BPA agli account dell'organizzazione. Per ulteriori informazioni sulla policy dichiarativa di VPC BPA, consulta Policy dichiarative supportate nella Guida per l'utente di AWS Organizations.

> **Note**
>
> - Puoi utilizzare la policy dichiarativa di VPC BPA per configurare se le esclusioni sono consentite, ma non puoi creare esclusioni con la policy. Per creare esclusioni, devi comunque crearle nell'account che possiede il VPC. Per ulteriori informazioni sulla creazione di esclusioni di VPC BPA, consulta Creazione ed eliminazione di esclusioni.
> - Se la policy dichiarativa di VPC BPA è abilitata, in Blocca impostazioni di accesso pubblico vedrai Gestito da policy dichiarativa e non potrai modificare le impostazioni di VPC BPA a livello di account.

Valutazione dell'impatto di BPA e monitoraggio di BPA

Questa sezione contiene informazioni su come valutare l'impatto di VPC BPA prima di attivarlo e su come monitorare se il traffico viene bloccato dopo l'attivazione.

Indice

- Valuta l'impatto del BPA con Strumento di analisi degli accessi alla rete
- Monitoraggio dell'impatto di BPA con log di flusso
- Tieni traccia dell'eliminazione delle esclusioni con CloudTrail
- Verifica del blocco della connettività con Reachability Analyzer

Valuta l'impatto del BPA con Strumento di analisi degli accessi alla rete

In questa sezione, visualizzerai le risorse del tuo account che utilizzano un gateway Internet prima di abilitare VPC BPA e bloccare l'accesso. Strumento di analisi degli accessi alla rete Utilizza questa analisi per comprendere l'impatto dell'attivazione di VPC BPA nel tuo account e del blocco del traffico.

> **Note**
>
> - Network Access Analyzer non supporta IPv6, quindi non potrai utilizzarlo per visualizzare il potenziale impatto del BPA sul traffico in uscita del gateway Internet solo in uscita. IPv6
> - Ti vengono addebitati i costi delle analisi eseguite con Strumento di analisi degli accessi alla rete. Per ulteriori informazioni, consulta Prezzi nella Guida di Strumento di analisi degli accessi alla rete .
> - Per informazioni sulla disponibilità regionale dello Strumento di analisi degli accessi alla rete, consulta Limitazioni nella Guida dello Strumento di analisi degli accessi alla rete.

AWS Management Console

1. Apri la console di Network Insights all'indirizzo. AWS https://console.aws.amazon.com/networkinsights/
2. Scegli Strumento di analisi degli accessi alla rete.
3. Scegli Crea ambito di accesso alla rete.
4. Scegli Valuta l'impatto di Blocco dell'accesso pubblico VPC e scegli Avanti.
5. Il modello è già configurato per analizzare il traffico da e verso i gateway Internet del tuo account. Puoi visualizzarlo in Origine e Destinazione.
6. Scegli Next (Successivo).
7. Scegli Crea ambito di accesso alla rete.
8. Scegli l'ambito che hai appena creato e scegli Analizza.
9. Attendi il completamento del processo.
10. Visualizza gli esiti dell'analisi. Ogni riga in Esiti mostra un percorso di rete che un pacchetto può percorrere in una rete da o verso un gateway Internet del tuo account. In questo caso, se attivi VPC BPA e nessuna delle e/o o sottoreti che appaiono in questi risultati è configurata come esclusione BPA, il traffico verso quelle VPCs e le sottoreti sarà limitato. VPCs
11. Analizza ogni risultato per comprendere l'impatto del BPA sulle risorse del tuo. VPCs

L'analisi dell'impatto è completa.

AWS CLI

1. Crea un ambito di accesso alla rete:

```
aws ec2 create-network-insights-access-scope --region us-east-2 --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
```

2. Inizia l'analisi dell'ambito:

```
aws ec2 start-network-insights-access-scope-analysis  --region us-east-2 --
network-insights-access-scope-id nis-id
```

3. Ottieni i risultati dell'analisi:

```
aws ec2 get-network-insights-access-scope-analysis-findings  --region us-east-2
 --network-insights-access-scope-analysis-id nisa-0aa383a1938f94cd1 --max-items
 1
```

   I risultati mostrano il traffico da e verso i gateway Internet in tutto il tuo VPCs account. I risultati sono organizzati come «risultati». "FindingId«:" AnalysisFinding -1" indica che questo è il primo risultato dell'analisi. Tieni presente che esistono diversi esiti e ognuno indica un flusso di traffico che verrà influenzato dall'attivazione di VPC BPA. Il primo risultato mostrerà che il traffico è iniziato da un gateway Internet (» SequenceNumber «: 1), è passato a un NACL (» SequenceNumber «: 2) a un gruppo di sicurezza (» SequenceNumber «: 3) e è terminato in un'istanza (» SequenceNumber «: 4).

4. Analizza i risultati per comprendere l'impatto del BPA sulle risorse del tuo. VPCs

L'analisi dell'impatto è completa.

Monitoraggio dell'impatto di BPA con log di flusso

Log di flusso VPC è una funzionalità che consente di acquisire informazioni sul traffico IP da e verso le interfacce di rete elastiche nel VPC. Puoi utilizzare questa funzionalità per monitorare il traffico bloccato da VPC BPA e impedirgli di raggiungere le interfacce di rete dell'istanza.

Crea un log di flusso per il tuo VPC utilizzando i passaggi in Utilizzo dei log di flusso.

Quando crei il log di flusso, assicurati di utilizzare un formato personalizzato che includa il campo `reject-reason`.

Quando visualizzi i log di flusso, se il traffico verso un ENI viene rifiutato a causa di BPA, viene visualizzato un `reject-reason` di BPA nella voce del log di flusso.

Oltre alle limitazioni standard per i log di flusso VPC, tieni presente le seguenti limitazioni specifiche di VPC BPA:

- I log di flusso per BPA VPC non includono i record ignorati.
- I log di flusso per BPA VPC non includono `bytes` anche se includi il campo `bytes` nel log di flusso.

Tieni traccia dell'eliminazione delle esclusioni con CloudTrail

Questa sezione spiega come monitorare e tenere traccia dell'eliminazione delle esclusioni VPC BPA.
AWS CloudTrail

AWS Management Console

Puoi visualizzare tutte le esclusioni eliminate nella cronologia degli CloudTrail eventi cercando Tipo di risorsa > `AWS::EC2::VPCBlockPublicAccessExclusion` nella console all'indirizzo. AWS CloudTrail https://console.aws.amazon.com/cloudtrailv2/

AWS CLI

Puoi utilizzare il comando `lookup-events` per visualizzare gli eventi relativi all'eliminazione di esclusioni:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

Verifica del blocco della connettività con Reachability Analyzer

VPC Reachability Analyzer può essere utilizzato per valutare se determinati percorsi di rete possono essere raggiunti o meno in base alla configurazione di rete, incluse le impostazioni VPC BPA.

Per informazioni sulla disponibilità regionale di Reachability Analyzer, consulta Considerazioni nella Guida di Reachability Analyzer.

AWS Management Console

1. Apri la console AWS Network Insights all'indirizzohttps://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer.
2. Fai clic su Crea e analizza il percorso.
3. Per Tipo di origine, scegli Gateway Internet e seleziona il gateway Internet per il quale desideri bloccare il traffico dal menu a discesa Origine.
4. Per Tipo di destinazione, scegli Istanze e seleziona l'istanza verso cui desideri bloccare il traffico dal menu a discesa Destinazione.
5. Fai clic su Crea e analizza il percorso.
6. Attendi il completamento del processo. Il processo può richiedere alcuni minuti.
7. Una volta completato, dovresti vedere che lo stato di raggiungibilità è non raggiungibile e che i dettagli del percorso indicano che `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` è la causa di questo problema di raggiungibilità.

AWS CLI

1. Crea un percorso di rete utilizzando l'ID del gateway Internet da cui desideri bloccare il traffico (origine) e l'ID dell'istanza verso cui desideri bloccare il traffico (destinazione):

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
destination instance-id --protocol TCP
```

2. Avvia un'analisi sul percorso di rete:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

3. Richiama i risultati dell'analisi:

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

4. Verifica che `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` sia il `ExplanationCode` della mancanza di raggiungibilità.

Esempio avanzato

Questa sezione contiene un esempio avanzato che ti aiuterà a capire come opera la funzionalità Blocco dell'accesso pubblico VPC in diversi scenari. Ogni scenario si basa sullo scenario precedente, quindi è importante completare i passaggi in ordine.

Important

Non utilizzare questo esempio in un account di produzione. Ti consigliamo di esaminare attentamente i carichi di lavoro che richiedono l'accesso a Internet prima di abilitare VPC BPA nei tuoi account di produzione.

Note

Per comprendere appieno la funzionalità VPC BPA, avrai bisogno di determinate risorse nel tuo account. In questa sezione, forniamo un AWS CloudFormation modello che puoi utilizzare per fornire le risorse necessarie per comprendere appieno come funziona questa funzionalità. Esistono costi associati alle risorse fornite con il CloudFormation modello e alle analisi eseguite con Network Access Analyzer e Reachability Analyzer. Se utilizzi il modello in questa sezione, assicurati di completare i passaggi di pulizia al termine di questo esempio.

Indice

- Implementa il modello CloudFormation
- Visualizza l'impatto di VPC BPA con Strumento di analisi degli accessi alla rete
- Scenario 1: Connessione a istanze senza BPA attivato
- Scenario 2: Attivazione di BPA
- Scenario 3: Modifica della modalità BPA
- Scenario 4: Creazione di un'esclusione
- Scenario 5: modifica della modalità di esclusione
- Scenario 6: Modifica della modalità BPA
- Rimozione

Implementa il modello CloudFormation

Per dimostrare come funziona questa funzionalità, sono necessari un VPC, sottoreti, istanze e altre risorse. Per semplificare il completamento di questa dimostrazione, di seguito abbiamo fornito un AWS CloudFormation modello che puoi utilizzare per aumentare rapidamente le risorse necessarie per gli scenari di questa demo.

> **Note**
>
> Ci sono dei costi associati alle risorse create in questa sezione con il CloudFormation modello, come il costo del gateway NAT e gli indirizzi pubblici IPv4 . Per evitare costi eccessivi, assicurati di completare i passaggi di pulizia per rimuovere tutte le risorse create ai fini di questo esempio.

Il modello crea le seguenti risorse nel tuo account:

- Gateway Internet Egress-only
- Internet Gateway
- Gateway NAT
- Due sottoreti pubbliche
- Una sottorete privata
- Due EC2 istanze con indirizzi pubblici e privati IPv4
- Un' EC2 istanza con un IPv6 indirizzo e un indirizzo privato IPv4
- Un' EC2 istanza con un solo IPv4 indirizzo privato
- Gruppo di sicurezza con traffico SSH e ICMP in entrata consentito e TUTTO il traffico in uscita consentito
- Log di flusso VPC
- Endpoint One EC2 Instance Connect nella sottorete B

Copia il modello seguente e salvalo in un file .yaml.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Creates a VPC with public and private subnets, NAT gateway, and EC2
 instances for VPC BPA.
```

```
Parameters:
  InstanceAMI:
    Description: ID of the Amazone Machine Image (AMI) to use with the instances
 launched by this template
    Type: AWS::EC2::Image::Id
  InstanceType:
    Description: EC2 Instance type to use with the instances launched by this template
    Type: String
    Default: t2.micro

Resources:

  # VPC
  VPCBPA:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsHostnames: true
      EnableDnsSupport: true
      InstanceTenancy: default
      Tags:
        - Key: Name
          Value: VPC BPA

  # VPC IPv6 CIDR
  VPCBPAIpv6CidrBlock:
    Type: AWS::EC2::VPCCidrBlock
    Properties:
      VpcId: !Ref VPCBPA
      AmazonProvidedIpv6CidrBlock: true

  # EC2 Key Pair
  VPCBPAKeyPair:
    Type: AWS::EC2::KeyPair
    Properties:
      KeyName: vpc-bpa-key

  # Internet Gateway
  VPCBPAInternetGateway:
    Type: AWS::EC2::InternetGateway
    Properties:
      Tags:
        - Key: Name
          Value: VPC BPA Internet Gateway
```

```
  VPCBPAInternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      VpcId: !Ref VPCBPA
      InternetGatewayId: !Ref VPCBPAInternetGateway

  # Egress-Only Internet Gateway
  VPCBPAEgressOnlyInternetGateway:
    Type: AWS::EC2::EgressOnlyInternetGateway
    Properties:
      VpcId: !Ref VPCBPA

  # Subnets
  VPCBPAPublicSubnetA:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.1.0/24
      MapPublicIpOnLaunch: true
      Tags:
        - Key: Name
          Value: VPC BPA Public Subnet A

  VPCBPAPublicSubnetB:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.2.0/24
      MapPublicIpOnLaunch: true
      Tags:
        - Key: Name
          Value: VPC BPA Public Subnet B

  VPCBPAPrivateSubnetC:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.3.0/24
      MapPublicIpOnLaunch: false
      Ipv6CidrBlock: !Select [0, !GetAtt VPCBPA.Ipv6CidrBlocks]
      AssignIpv6AddressOnCreation: true
      Tags:
        - Key: Name
```

```
        Value: VPC BPA Private Subnet C

# NAT Gateway
VPCBPANATGateway:
  Type: AWS::EC2::NatGateway
  Properties:
    AllocationId: !GetAtt VPCBPANATGatewayEIP.AllocationId
    SubnetId: !Ref VPCBPAPublicSubnetB
    Tags:
      - Key: Name
        Value: VPC BPA NAT Gateway

VPCBPANATGatewayEIP:
  Type: AWS::EC2::EIP
  Properties:
    Domain: vpc
    Tags:
      - Key: Name
        Value: VPC BPA NAT Gateway EIP

# Route Tables
VPCBPAPublicRouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref VPCBPA
    Tags:
      - Key: Name
        Value: VPC BPA Public Route Table

VPCBPAPublicRoute:
  Type: AWS::EC2::Route
  DependsOn: VPCBPAInternetGatewayAttachment
  Properties:
    RouteTableId: !Ref VPCBPAPublicRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref VPCBPAInternetGateway

VPCBPAPublicSubnetARouteTableAssoc:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    SubnetId: !Ref VPCBPAPublicSubnetA
    RouteTableId: !Ref VPCBPAPublicRouteTable

VPCBPAPublicSubnetBRouteTableAssoc:
```

```
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPublicSubnetB
      RouteTableId: !Ref VPCBPAPublicRouteTable

  VPCBPAPrivateRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Private Route Table

  VPCBPAPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref VPCBPANATGateway

  VPCBPAPrivateSubnetCRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationIpv6CidrBlock: ::/0
      EgressOnlyInternetGatewayId: !Ref VPCBPAEgressOnlyInternetGateway

  VPCBPAPrivateSubnetCRouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPrivateSubnetC
      RouteTableId: !Ref VPCBPAPrivateRouteTable

  # EC2 Instances Security Group
  VPCBPAInstancesSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupName: VPC BPA Instances Security Group
      GroupDescription: Allow SSH and ICMP access
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 22
          ToPort: 22
          CidrIp: 0.0.0.0/0
```

```
      - IpProtocol: icmp
        FromPort: -1
        ToPort: -1
        CidrIp: 0.0.0.0/0
    VpcId: !Ref VPCBPA
    Tags:
      - Key: Name
        Value: VPC BPA Instances Security Group

# EC2 Instances
VPCBPAInstanceA:
  Type: AWS::EC2::Instance
  Properties:
    ImageId: !Ref InstanceAMI
    InstanceType: t2.micro
    KeyName: !Ref VPCBPAKeyPair
    SubnetId: !Ref VPCBPAPublicSubnetA
    SecurityGroupIds:
      - !Ref VPCBPAInstancesSecurityGroup
    Tags:
      - Key: Name
        Value: VPC BPA Instance A

VPCBPAInstanceB:
  Type: AWS::EC2::Instance
  Properties:
    ImageId: !Ref InstanceAMI
    InstanceType: !Ref InstanceType
    KeyName: !Ref VPCBPAKeyPair
    SubnetId: !Ref VPCBPAPublicSubnetB
    SecurityGroupIds:
      - !Ref VPCBPAInstancesSecurityGroup
    Tags:
      - Key: Name
        Value: VPC BPA Instance B

VPCBPAInstanceC:
  Type: AWS::EC2::Instance
  Properties:
    ImageId: !Ref InstanceAMI
    InstanceType: !Ref InstanceType
    KeyName: !Ref VPCBPAKeyPair
    SubnetId: !Ref VPCBPAPrivateSubnetC
    SecurityGroupIds:
```

```
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance C

  VPCBPAInstanceD:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      NetworkInterfaces:
        - DeviceIndex: '0'
          GroupSet:
            - !Ref VPCBPAInstancesSecurityGroup
          SubnetId: !Ref VPCBPAPrivateSubnetC
          Ipv6AddressCount: 1
      Tags:
        - Key: Name
          Value: VPC BPA Instance D

  # Flow Logs IAM Role
  VPCBPAFlowLogRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service: vpc-flow-logs.amazonaws.com
            Action: 'sts:AssumeRole'
      Tags:
        - Key: Name
          Value: VPC BPA Flow Logs Role

  VPCBPAFlowLogPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyName: VPC-BPA-FlowLogsPolicy
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
```

```
            Action:
              - 'logs:CreateLogGroup'
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
              - 'logs:DescribeLogGroups'
              - 'logs:DescribeLogStreams'
            Resource: '*'
      Roles:
        - !Ref VPCBPAFlowLogRole

  # Flow Logs
  VPCBPAFlowLog:
    Type: AWS::EC2::FlowLog
    Properties:
      ResourceId: !Ref VPCBPA
      ResourceType: VPC
      TrafficType: ALL
      LogDestinationType: cloud-watch-logs
      LogGroupName: /aws/vpc-flow-logs/VPC-BPA
      DeliverLogsPermissionArn: !GetAtt VPCBPAFlowLogRole.Arn
      LogFormat: '${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr}
 ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-
status} ${vpc-id} ${subnet-id} ${instance-id} ${tcp-flags} ${type} ${pkt-srcaddr}
 ${pkt-dstaddr} ${region} ${az-id} ${sublocation-type} ${sublocation-id} ${pkt-src-aws-
service} ${pkt-dst-aws-service} ${flow-direction} ${traffic-path} ${reject-reason}'
      Tags:
        - Key: Name
          Value: VPC BPA Flow Logs

  # EC2 Instance Connect Endpoint
  VPCBPAEC2InstanceConnectEndpoint:
    Type: AWS::EC2::InstanceConnectEndpoint
    Properties:
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      SubnetId: !Ref VPCBPAPublicSubnetB

Outputs:
  VPCBPAVPCId:
    Description: A reference to the created VPC
    Value: !Ref VPCBPA
    Export:
      Name: vpc-id
```

```
  VPCBPAPublicSubnetAId:
    Description: The ID of the public subnet A
    Value: !Ref VPCBPAPublicSubnetA

  VPCBPAPublicSubnetANName:
    Description: The name of the public subnet A
    Value: VPC BPA Public Subnet A

  VPCBPAPublicSubnetBId:
    Description: The ID of the public subnet B
    Value: !Ref VPCBPAPublicSubnetB

  VPCBPAPublicSubnetBName:
    Description: The name of the public subnet B
    Value: VPC BPA Public Subnet B

  VPCBPAPrivateSubnetCId:
    Description: The ID of the private subnet C
    Value: !Ref VPCBPAPrivateSubnetC

  VPCBPAPrivateSubnetCName:
    Description: The name of the private subnet C
    Value: VPC BPA Private Subnet C

  VPCBPAInstanceAId:
    Description: The ID of instance A
    Value: !Ref VPCBPAInstanceA

  VPCBPAInstanceBId:
    Description: The ID of instance B
    Value: !Ref VPCBPAInstanceB

  VPCBPAInstanceCId:
    Description: The ID of instance C
    Value: !Ref VPCBPAInstanceC

  VPCBPAInstanceDId:
    Description: The ID of instance D
    Value: !Ref VPCBPAInstanceD
```

AWS Management Console

1. Apri la AWS CloudFormation console all'indirizzo. https://console.aws.amazon.com/cloudformation/
2. Scegli Crea stack e carica il file modello .yaml.
3. Segui i passaggi per avviare il modello. Dovrai inserire un ID immagine e un tipo di istanza (come t2.micro). Dovrai inoltre consentire la creazione CloudFormation di un ruolo IAM per la creazione del log di flusso e l'autorizzazione per l'accesso Amazon CloudWatch.
4. Una volta avviato lo stack, apri la scheda Eventi per visualizzare lo stato di avanzamento e assicurati che lo stack sia completato prima di continuare.

AWS CLI

1. Esegui il seguente comando per creare lo CloudFormation stack:

```
aws cloudformation create-stack --stack-name VPC-BPA-stack --template-body
 file://sampletemplate.yaml --capabilities CAPABILITY_IAM --region us-east-2
```

Output:

```
{
    "StackId": "arn:aws:cloudformation:us-east-2:470889052923:stack/VPC-BPA-
stack/8a7a2cc0-8001-11ef-b196-06386a84b72f"
}
```

2. Visualizza lo stato di avanzamento e assicurati che lo stack sia completato prima di continuare:

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-
east-2
```

Visualizza l'impatto di VPC BPA con Strumento di analisi degli accessi alla rete

In questa sezione, userai Strumento di analisi degli accessi alla rete per visualizzare le risorse del tuo account che utilizzano il gateway Internet. Utilizza questa analisi per comprendere l'impatto dell'attivazione di VPC BPA nel tuo account e del blocco del traffico.

Per informazioni sulla disponibilità regionale dello Strumento di analisi degli accessi alla rete, consulta Limitazioni nella Guida dello Strumento di analisi degli accessi alla rete.

AWS Management Console

1. Apri la console AWS di Network Insights all'indirizzohttps://console.aws.amazon.com/networkinsights/.
2. Scegli Strumento di analisi degli accessi alla rete.
3. Scegli Crea ambito di accesso alla rete.
4. Scegli Valuta l'impatto di Blocco dell'accesso pubblico VPC e scegli Avanti.
5. Il modello è già configurato per analizzare il traffico da e verso i gateway Internet del tuo account. Puoi visualizzarlo in Origine e Destinazione.
6. Scegli Next (Successivo).
7. Scegli Crea ambito di accesso alla rete.
8. Scegli l'ambito che hai appena creato e scegli Analizza.
9. Attendi il completamento del processo.
10. Visualizza gli esiti dell'analisi. Ogni riga in Esiti mostra un percorso di rete che un pacchetto può percorrere in una rete da o verso un gateway Internet del tuo account. In questo caso, se attivi VPC BPA e nessuna delle e/o o sottoreti che appaiono in questi risultati è configurata come esclusione BPA, il traffico verso quelle VPCs e le sottoreti sarà limitato. VPCs
11. Analizza ogni risultato per comprendere l'impatto del BPA sulle risorse del tuo. VPCs

L'analisi dell'impatto è completa.

AWS CLI

1. Crea un ambito di accesso alla rete:

```
aws ec2 create-network-insights-access-scope --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 --region us-east-2
```

Output:

```
{
  "NetworkInsightsAccessScope": {
```

```
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "NetworkInsightsAccessScopeArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope/nis-04cad3c4b3a1d5e3e",
    "CreatedDate": "2024-09-30T15:55:53.171000+00:00",
    "UpdatedDate": "2024-09-30T15:55:53.171000+00:00"
  },
  "NetworkInsightsAccessScopeContent": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "MatchPaths": [
      {
        "Source": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        }
      },
      {
        "Destination": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        }
      }
    ]
  }
}
```

2. Inizia l'analisi dell'ambito:

```
aws ec2 start-network-insights-access-scope-analysis --network-insights-access-
scope-id nis-04cad3c4b3a1d5e3e --region us-east-2
```

Output:

```
{
  "NetworkInsightsAccessScopeAnalysis": {
    "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
```

```
    "NetworkInsightsAccessScopeAnalysisArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope-analysis/
nisa-0aa383a1938f94cd",
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "Status": "running",
    "StartDate": "2024-09-30T15:56:59.109000+00:00",
    "AnalyzedEniCount": 0
  }
}
```

3. Ottieni i risultati dell'analisi:

```
aws ec2 get-network-insights-access-scope-analysis-findings --network-insights-
access-scope-analysis-id nisa-0aa383a1938f94cd1 --region us-east-2 --max-items 1
```

Output:

```
{
  "AnalysisFindings": [
    {
      "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
      "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
      "FindingId": "AnalysisFinding-1",
      "FindingComponents": [
        {
          "SequenceNumber": 1,
          "Component": {
            "Id": "igw-04a5344b4e30486f1",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:internet-gateway/
igw-04a5344b4e30486f1",
            "Name": "VPC BPA Internet Gateway"
          },
          "OutboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ]
          },
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
              {
```

```
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
        },
        {
          "SequenceNumber": 2,
          "AclRule": {
            "Cidr": "0.0.0.0/0",
            "Egress": false,
            "Protocol": "all",
            "RuleAction": "allow",
            "RuleNumber": 100
          },
          "Component": {
            "Id": "acl-06194fc3a4a03040b",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-acl/
acl-06194fc3a4a03040b"
          }
        },
        {
          "SequenceNumber": 3,
          "Component": {
            "Id": "sg-093dde06415d03924",
```

```
            "Arn": "arn:aws:ec2:us-east-2:470889052923:security-group/
sg-093dde06415d03924",
            "Name": "VPC BPA Instances Security Group"
          },
          "SecurityGroupRule": {
            "Cidr": "0.0.0.0/0",
            "Direction": "ingress",
            "PortRange": {
              "From": 22,
              "To": 22
            },
            "Protocol": "tcp"
          }
        },
        {
          "SequenceNumber": 4,
          "AttachedTo": {
            "Id": "i-058db34f9a0997895",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:instance/
i-058db34f9a0997895",
            "Name": "VPC BPA Instance A"
          },
          "Component": {
            "Id": "eni-0fa23f2766f03b286",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-interface/
eni-0fa23f2766f03b286"
          },
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
              {
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
```

```
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
          "Subnet": {
            "Id": "subnet-035d235a762eeed04",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:subnet/
subnet-035d235a762eeed04",
            "Name": "VPC BPA Public Subnet A"
          },
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
        }
      ]
    }
  ],
  "AnalysisStatus": "succeeded",
  "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
  "NextToken":
 "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ=="
}
```


I risultati mostrano il traffico da e verso i gateway Internet in tutto il tuo VPCs account. I risultati sono organizzati come «risultati». "FindingId«:" AnalysisFinding -1" indica che questo è il primo risultato dell'analisi. Tieni presente che esistono diversi esiti e ognuno indica un flusso di traffico che verrà influenzato dall'attivazione di VPC BPA. Il primo risultato mostrerà che il traffico è iniziato da un gateway Internet (» SequenceNumber «: 1), è passato a un NACL (» SequenceNumber «: 2) a un gruppo di sicurezza (» SequenceNumber «: 3) e è terminato in un'istanza (» SequenceNumber «: 4).

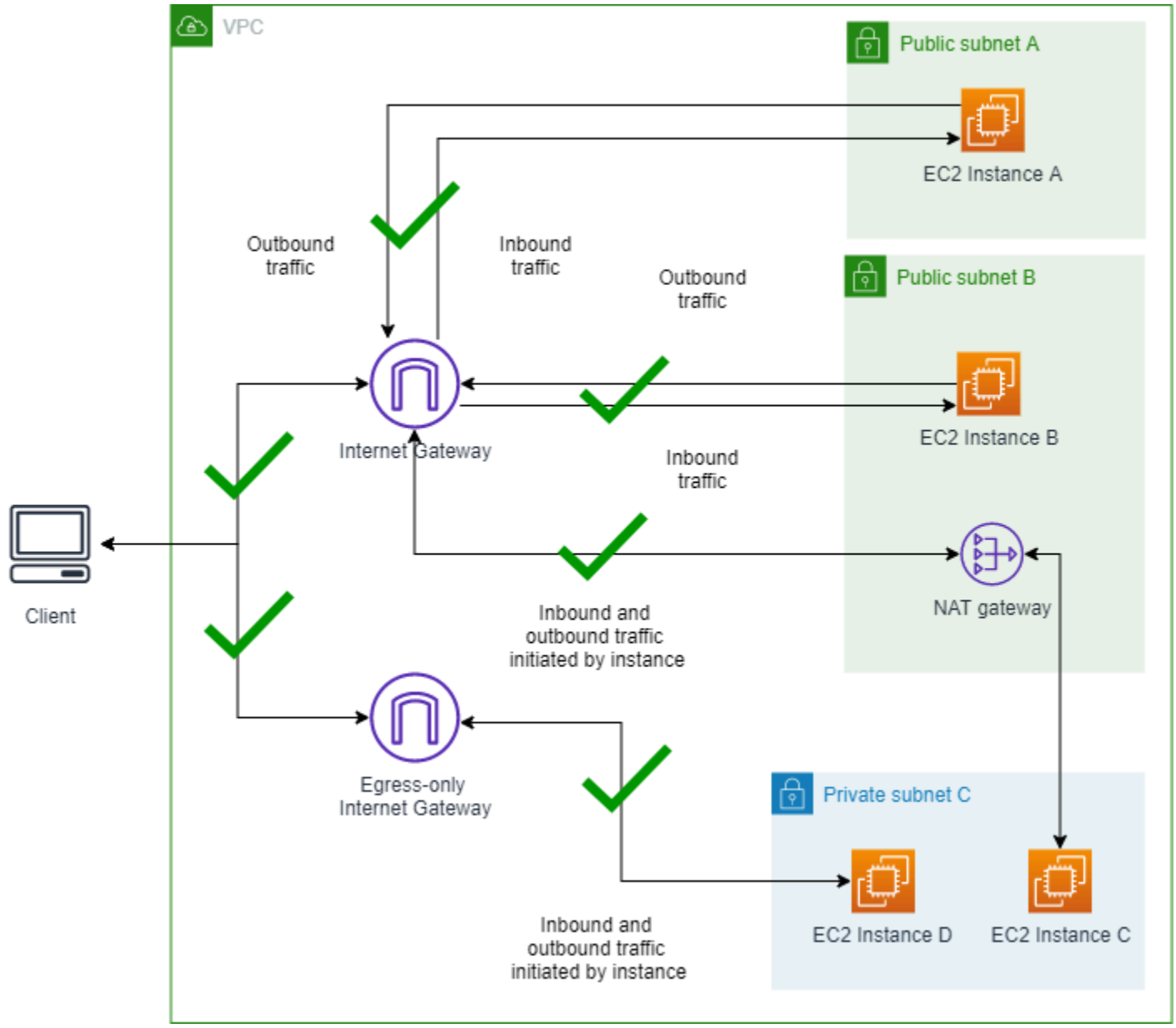
4. Analizza i risultati per comprendere l'impatto del BPA sulle risorse del tuo. VPCs

L'analisi dell'impatto è completa.

Scenario 1: Connessione a istanze senza BPA attivato

In questa sezione, per impostare una linea di base e garantire che, prima di abilitare BPA, tutte le istanze possano essere raggiunte, dovrai connetterti a tutte le istanze e inviare il ping a un indirizzo IP pubblico.

Diagramma di un VPC senza VPC BPA attivato:



1.1 Connessione alle istanze

Completa questa sezione per connetterti alle tue istanze con VPC BPA disattivato per avere la certezza di poterti connettere senza problemi. Tutte le istanze create con questo CloudFormation esempio hanno nomi come «VPC BPA Instance A».

AWS Management Console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Apri i dettagli dell'istanza A.
3. Connettiti all'istanza A utilizzando l'opzione EC2 Instance Connect > Connect using EC2 Instance Connect Endpoint.
4. Scegli Connetti. Una volta stabilita la connessione all'istanza, invia il ping a www.amazon.com per verificare che sia possibile inviare richieste in uscita a Internet.
5. Usa lo stesso metodo utilizzato per connetterti all'istanza A per connetterti a B, C e D. Da ciascuna istanza, esegui il ping a www.amazon.com per verificare di poter inviare le richieste in uscita su Internet.

AWS CLI

1. Esegui il ping dell'istanza A utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

   ```
   ping 18.225.8.244
   ```

   Output:

   ```
   Pinging 18.225.8.244 with 32 bytes of data:

   Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
   Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
   ```

   Nota che il ping riesce correttamente e il traffico non è bloccato.
2. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

   ```
   aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
   east-2 --connection-type eice
   ```

Output:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 18:27:57 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING www-amazon-com.customer.fastly.net (18.65.233.187) 56(84) bytes of data.
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=15 ttl=58 time=2.06 ms
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=16 ttl=58 time=2.26 ms
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

3. Esegui il ping dell'istanza B utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
Reply from 3.18.106.198: bytes=32 time=83ms TTL=110
Reply from 3.18.106.198: bytes=32 time=54ms TTL=110
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

4. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Fri Sep 27 18:12:27 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.55 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.67 ms
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

5. Connetti all'istanza C. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
```

```
Last login: Thu Sep 19 20:31:26 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.75 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.97 ms
64 bytes from server-3-160-24-26.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=3 ttl=248 time=1.08 ms
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

6. Connetti all'istanza D. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output:

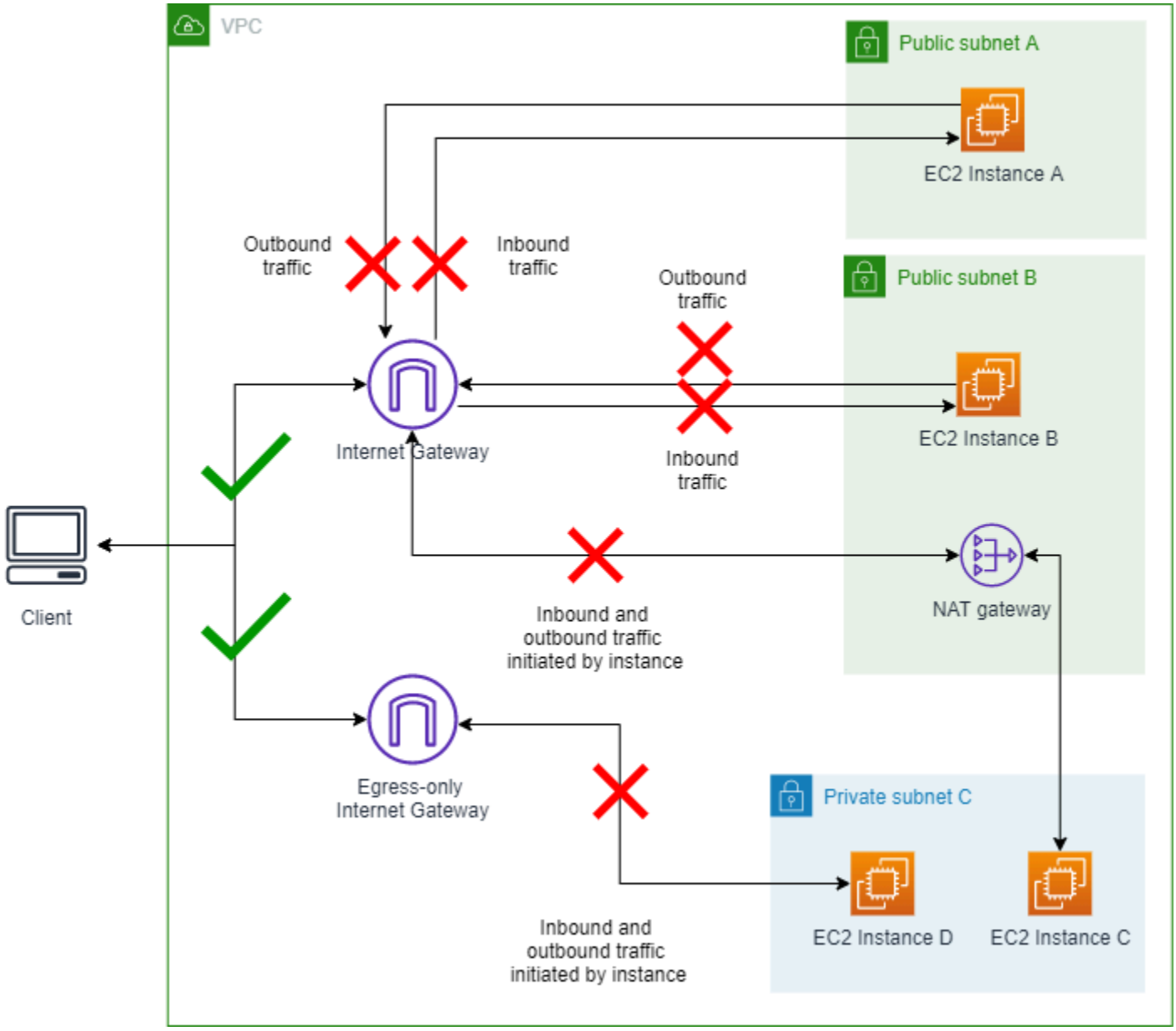
```
The authenticity of host '10.0.3.59 can't be established.
ECDSA key fingerprint is SHA256:c4naBCqbC61/cExDyccEproNU+1HHSpMSzl2J6cOtIZA8g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.59' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ _/
_/m/'
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.19 ms
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.38 ms
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

Scenario 2: Attivazione di BPA

In questa sezione attiverai VPC BPA e bloccherai il traffico da e verso i gateway Internet del tuo account.

Diagramma della modalità bidirezionale VPC BPA attivata:



2.1 Abilitazione della modalità bidirezionale a blocchi VPC BPA

Completa questa sezione per abilitare VPC BPA.

AWS Management Console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni.
3. Scegli Modifica impostazioni di accesso pubblico.
4. Scegli Attiva il blocco dell'accesso pubblico e Bidirezionale, quindi scegli Salva modifiche.
5. Attendi che lo stato passi su Abilitato. Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato.

VPC BPA è ora attivo.

AWS CLI

1. Usa il comando modify-vpc-block-public -access-options per attivare VPC BPA:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-bidirectional
```

Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato.

2. Visualizza lo stato di VPC BPA:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

2.2 Connessione alle istanze

Completa questa sezione per connetterti alle tue istanze.

AWS Management Console

1. Esegui il ping dell' IPv4 indirizzo pubblico dell'istanza A e dell'istanza B come hai fatto nello Scenario 1. Tieni presente che il traffico è bloccato.

2. Connettiti all'istanza A utilizzando l'opzione EC2 Instance Connect > Connect using EC2 Instance Connect Endpoint come hai fatto nello Scenario 1. Assicurati di utilizzare l'opzione endpoint.
3. Scegli Connetti. Dopo aver eseguito la connessione all'istanza, esegui il ping su www.amazon.com. Nota che tutto il traffico in uscita è bloccato.
4. Usa lo stesso metodo che hai usato per connetterti all'istanza A per connetterti alle istanze B, C e D e verifica le richieste in uscita su Internet. Nota che tutto il traffico in uscita è bloccato.

AWS CLI

1. Esegui il ping dell'istanza A utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

```
ping 18.225.8.244
```

Output:

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

Nota che il ping non riesce e il traffico è bloccato.

2. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
```

```
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Nota che il ping non riesce e il traffico è bloccato.

3. Esegui il ping dell'istanza B utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Nota che il ping non riesce e il traffico è bloccato.

4. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Output:

```
The authenticity of host '10.0.2.98' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
```

```
/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Nota che il ping non riesce e il traffico è bloccato.

5. Connetti all'istanza C. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Tue Sep 24 15:17:56 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Nota che il ping non riesce e il traffico è bloccato.

6. Connetti all'istanza D. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ _/
_/m/'
Last login: Fri Sep 27 16:42:01 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:8200:7:49a5:5fd4:b121
 (2600:9000:25f3:8200:7:49a5:5fd4:b121)) 56 data bytes
```

Nota che il ping non riesce e il traffico è bloccato.

2.3 Opzionale: Verifica del blocco della connettività con Reachability Analyzer

VPC Reachability Analyzer può essere utilizzato per comprendere se determinati percorsi di rete possono essere raggiunti o meno in base alla configurazione di rete, incluse le impostazioni VPC BPA. In questo esempio analizzerai lo stesso percorso di rete che è stato tentato in precedenza per confermare che VPC BPA è il motivo del fallimento della connettività.

AWS Management Console

1. Vai alla console Network Insights all'indirizzo https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer.
2. Fai clic su Crea e analizza il percorso.
3. Per Tipo di origine, scegli Gateway Internet e seleziona il gateway Internet etichettato Gateway Internet VPC BPA dal menu a discesa Origine.
4. Per Tipo di destinazione, scegli Istanze e seleziona l'istanza contrassegnata con Istanza VPC BPA A dal menu a discesa Destinazione.
5. Fai clic su Crea e analizza il percorso.
6. Attendi il completamento del processo. Il processo può richiedere alcuni minuti.
7. Una volta completato, dovresti vedere che lo stato di raggiungibilità è non raggiungibile e che i dettagli del percorso indicano che `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` è la causa.

AWS CLI

1. Crea un percorso di rete utilizzando l'ID del gateway Internet denominato Gateway Internet VPC BPA e l'ID dell'istanza etichettata Istanza VPC BPA A:

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
destination instance-id --protocol TCP
```

2. Avvia un'analisi sul percorso di rete:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

3. Richiama i risultati dell'analisi:

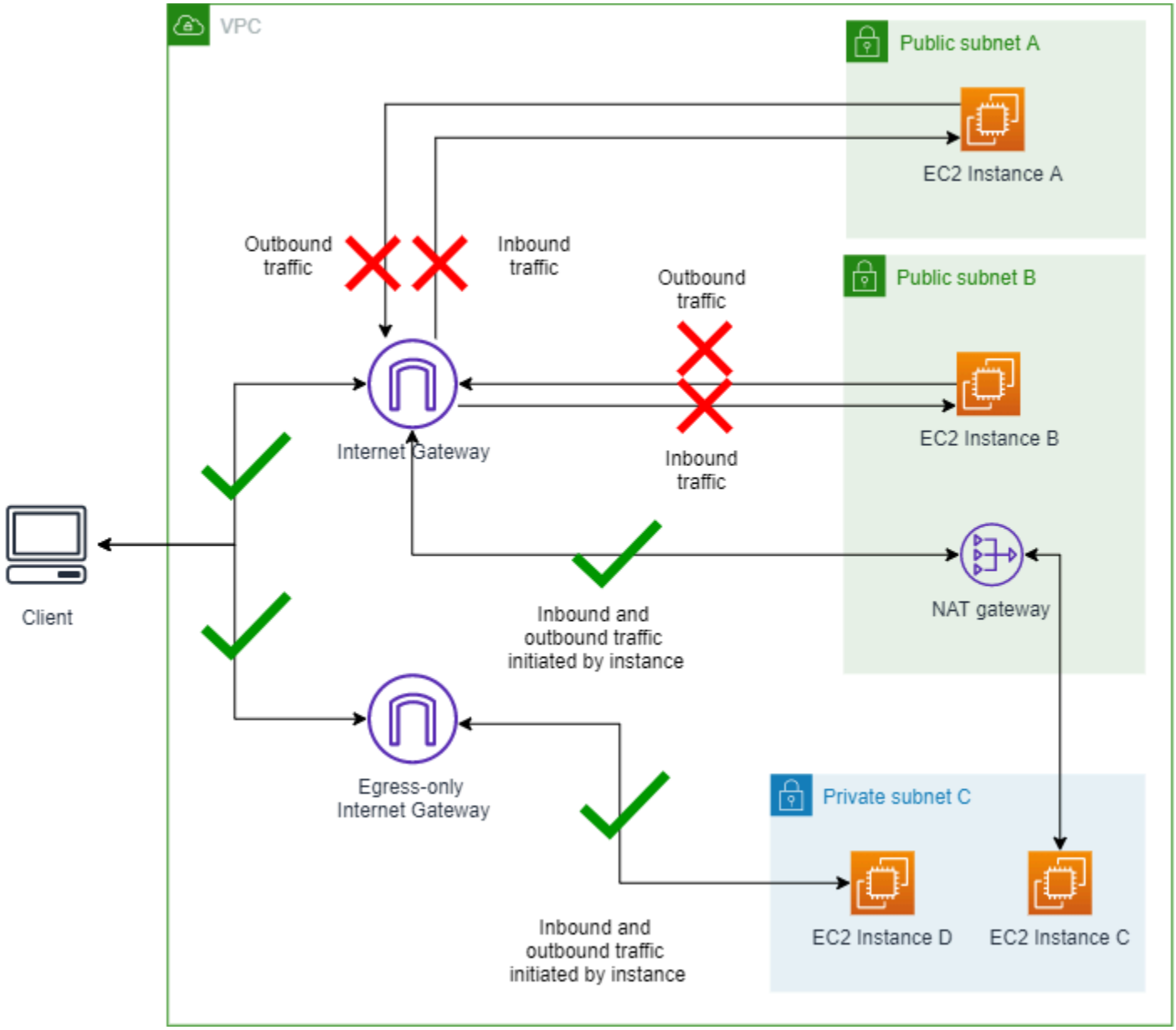
```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

4. Verifica che `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` sia il `ExplanationCode` della mancanza di raggiungibilità.

Scenario 3: Modifica della modalità BPA

In questa sezione cambierai la direzione del traffico VPC BPA e consentirai solo il traffico che utilizza un gateway NAT o un gateway Internet egress-only.

Diagramma della modalità VPC BPA Ingress-only attivata:



3.1 Modifica della modalità in ingress-only

Completa questa sezione per cambiare la modalità.

AWS Management Console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni.
3. Nella scheda Blocca accesso pubblico, scegli Modifica impostazioni di accesso pubblico.

4. Modifica le impostazioni di accesso pubblico nella console VPC e cambia la direzione in Ingress-only.
5. Salva le modifiche e attendi che lo stato venga aggiornato. Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato.

AWS CLI

1. Modifica la modalità VPC BPA:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-ingress
```

   Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato.
2. Visualizza lo stato di VPC BPA:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

3.2 Connessione alle istanze

Completa questa sezione per connetterti alle istanze.

AWS Management Console

1. Esegui il ping dell' IPv4 indirizzo pubblico dell'istanza A e dell'istanza B come hai fatto nello Scenario 1. Tieni presente che il traffico è bloccato.
2. Connettiti alle istanze A e B utilizzando EC2 instance connect come hai fatto nello Scenario 1 e invia il ping a www.amazon.com da esse. Tieni presente che non puoi inviare il ping a un sito pubblico su Internet dall'istanza A o B e che il traffico è bloccato.
3. Connettiti alle istanze C e D utilizzando EC2 instance connect come hai fatto nello Scenario 1 e invia il ping a www.amazon.com da esse. Tieni presente che puoi inviare il ping a un sito pubblico su Internet dall'istanza C o D e che il traffico è consentito.

AWS CLI

1. Esegui il ping dell'istanza A utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

```
ping 18.225.8.244
```

Output:

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

Nota che il ping non riesce e il traffico è bloccato.

2. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Nota che il ping non riesce e il traffico è bloccato.

3. Esegui il ping dell'istanza B utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Nota che il ping non riesce e il traffico è bloccato.

4. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Output:

```
The authenticity of host '10.0.2.98 ' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Nota che il ping non riesce e il traffico è bloccato.

5. Connetti all'istanza C. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

6. Connetti all'istanza D. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 16:48:38 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=14 ttl=58 time=1.47 ms
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=16 ttl=58 time=1.59 ms
```

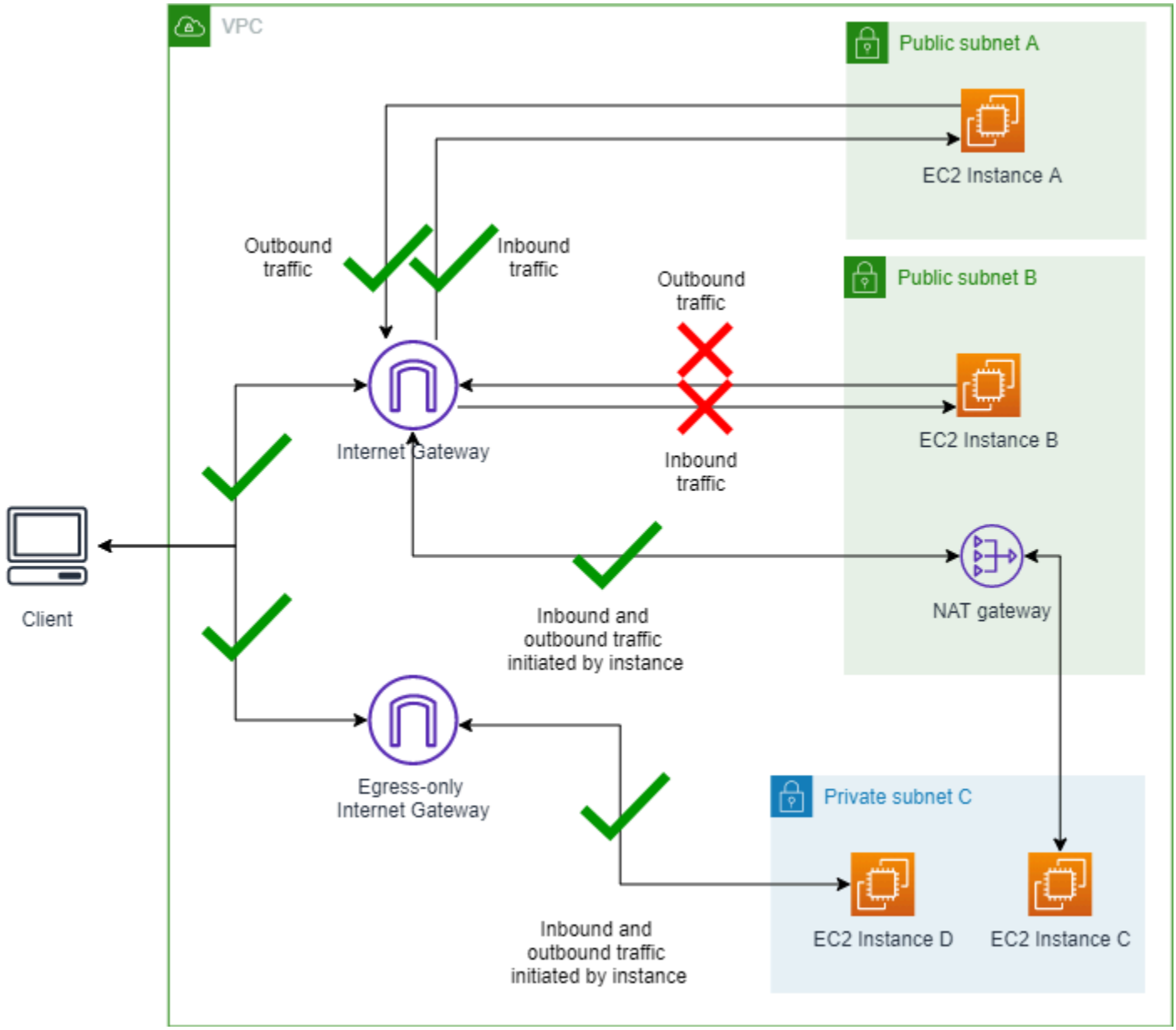
Nota che il ping riesce correttamente e il traffico non è bloccato.

Scenario 4: Creazione di un'esclusione

In questa sezione creerai un'esclusione e bloccherai solo il traffico da e verso la sottorete che non è esclusa da VPC BPA. Un'esclusione VPC BPA è una modalità che può essere applicata a un singolo VPC o a una singola sottorete che lo esenta dalla modalità BPA dell'account e consentirà l'accesso bidirezionale o egress-only. Puoi creare esclusioni BPA per VPCs e sottoreti anche quando BPA non è abilitato sull'account per garantire che non vi siano interruzioni del traffico delle esclusioni quando VPC BPA è attivato.

In questo esempio, creeremo un'esclusione per la sottorete A per mostrare come il traffico verso le esclusioni viene influenzato da VPC BPA.

Diagramma della modalità VPC BPA Ingress-only attivata e dell'esclusione Sottorete A con modalità bidirezionale attivata:



4.1 Creazione di un'esclusione per la sottorete A

Completa questa sezione per creare un'esclusione. Un'esclusione VPC BPA è una modalità che può essere applicata a un singolo VPC o a una singola sottorete che lo esenta dalla modalità BPA dell'account e consentirà l'accesso bidirezionale o egress-only. Puoi creare esclusioni BPA per VPCs e sottoreti anche quando BPA non è abilitato sull'account per garantire che non vi siano interruzioni del traffico delle esclusioni quando VPC BPA è attivato.

AWS Management Console

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

2. Nel riquadro di navigazione a sinistra, scegli Impostazioni.
3. Nella scheda Blocca accesso pubblico, in Esclusioni, scegli Crea esclusioni.
4. Scegli VPC BPA Public Subnet A, assicurati che sia selezionata l'opzione Consenti direzione Bidirezionale e scegli Crea esclusioni.
5. Attendi che lo Stato dell'esclusione passi su Attivo. Potrebbe essere necessario aggiornare la tabella di esclusione per visualizzare la modifica.

L'esclusione è stata creata.

AWS CLI

1. Modifica la direzione di autorizzazione dell'esclusione:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. L'aggiornamento dello stato dell'esclusione può richiedere del tempo. Per visualizzare lo stato dell'esclusione:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

4.2 Connessione alle istanze

Completa questa sezione per connetterti alle istanze.

AWS Management Console

1. Esegui il ping dell' IPv4 indirizzo pubblico dell'istanza A. Tieni presente che il traffico è consentito.
2. Esegui il ping dell' IPv4 indirizzo pubblico dell'istanza B. Tieni presente che il traffico è bloccato.
3. Connettiti all'istanza A utilizzando EC2 instance connect come hai fatto nello Scenario 1 e fai ping su www.amazon.com. Tieni presente che puoi inviare il ping a un sito pubblico su Internet dall'istanza A e che il traffico è consentito.

4. Connettiti all'istanza B utilizzando EC2 instance connect come hai fatto nello Scenario 1 e invia il ping a www.amazon.com da essa. Tieni presente che non puoi inviare il ping a un sito pubblico su Internet dall'istanza B e che il traffico è bloccato.
5. Connettiti alle istanze C e D utilizzando EC2 instance connect come hai fatto nello Scenario 1 e invia il ping a www.amazon.com da esse. Tieni presente che puoi inviare il ping a un sito pubblico su Internet dall'istanza C o D. Il traffico è consentito.

AWS CLI

1. Esegui il ping dell'istanza A utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

```
ping 18.225.8.244
```

Output:

```
Pinging 18.225.8.244 with 32 bytes of data:

Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

2. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
```

```
/m/'
Last login: Fri Sep 27 17:58:12 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.03 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.72 ms
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

3. Esegui il ping dell'istanza B utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Nota che il ping non riesce e il traffico è bloccato.

4. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 18:12:03 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
```

```
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Nota che il ping non riesce e il traffico è bloccato.

5. Connetti all'istanza C. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

6. Connetti all'istanza D. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:00:52 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING
 www.amazon.com(g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologie
 (2600:141f:4000:59a::3bd4)) 56 data bytes
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=1 ttl=48 time=15.9 ms
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=2 ttl=48 time=15.8 ms
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

4.3 Opzionale: verifica della connettività con Reachability Analyzer

Utilizzando lo stesso percorso di rete creato in Reachability Analyzer nello Scenario 2, è possibile eseguire una nuova analisi e confermare che il percorso è raggiungibile ora che è stata creata un'esclusione per la sottorete pubblica A.

Per informazioni sulla disponibilità regionale di Reachability Analyzer, consulta Considerazioni nella Guida di Reachability Analyzer.

AWS Management Console

1. Dal percorso di rete creato in precedenza nella console di Network Insights, fai clic su Esegui nuovamente l'analisi.
2. Attendi il completamento del processo. L'operazione potrebbe richiedere alcuni minuti.
3. Verifica che il percorso sia ora raggiungibile.

AWS CLI

1. Utilizzando l'ID del percorso di rete creato in precedenza, avvia una nuova analisi:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

2. Richiama i risultati dell'analisi:

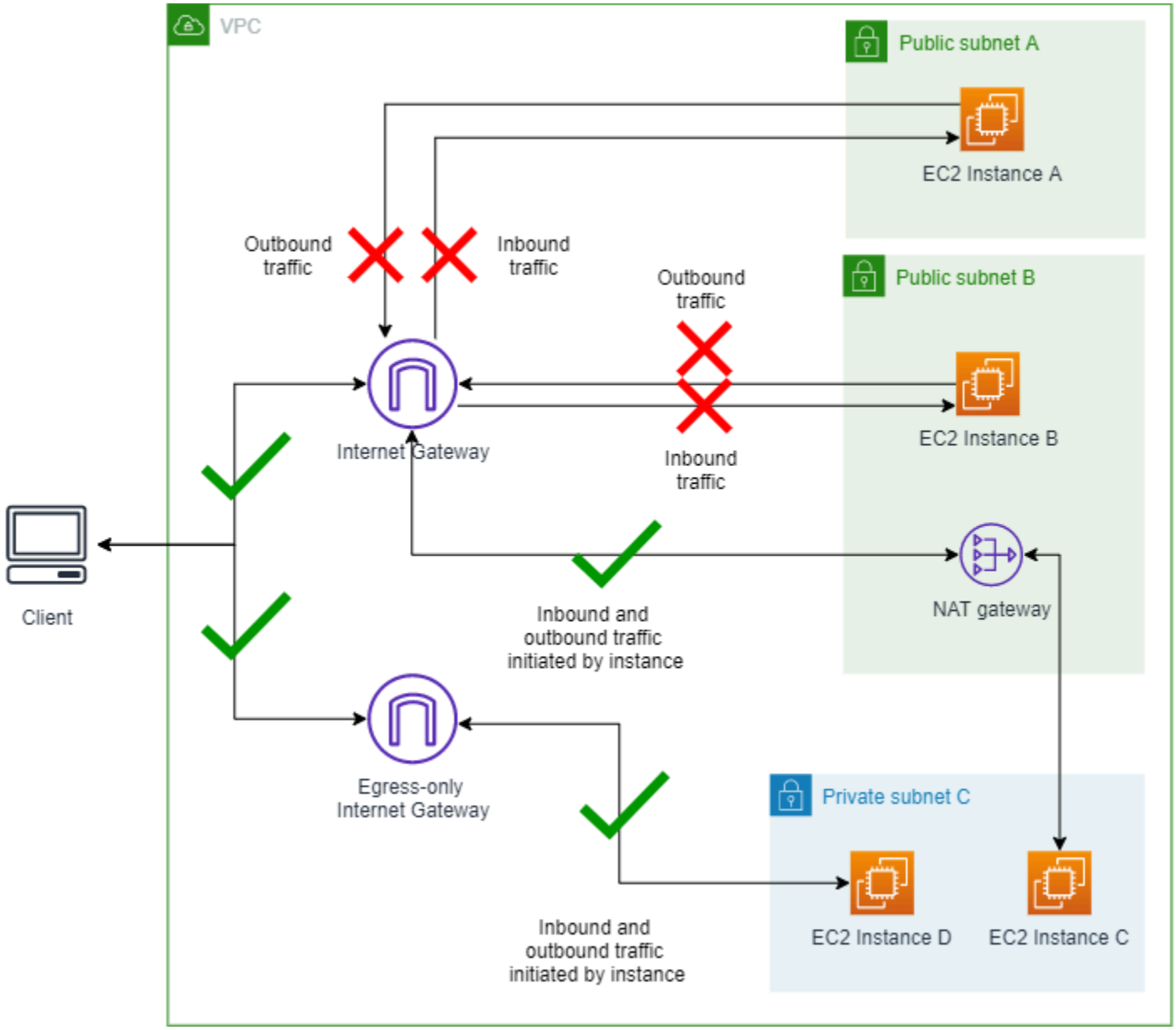
```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

3. Verifica che il codice esplicativo `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` non sia più presente.

Scenario 5: modifica della modalità di esclusione

In questa sezione modificherai la direzione del traffico consentita sull'esclusione per vedere in che modo influisce su VPC BPA. Tieni presente che la modalità egress-only per un'esclusione non è realmente significativa con VPC BPA abilitato nella modalità ingress-only a blocchi. Questo è lo stesso comportamento dello Scenario 3.

Diagramma della modalità VPC BPA Ingress-only attivata e dell'esclusione della sottorete A con modalità egress-only attivata:



5.1 Modifica della direzione di esclusione consentita in egress-only

Completa questa sezione per modificare la direzione di esclusione consentita.

AWS Management Console

1. Modifica l'esclusione creata nello Scenario 4 e modifica la direzione consentita in Egress-only.
2. Scegli Save changes (Salva modifiche).

3. Attendi che lo Stato dell'esclusione passi su Attivo. Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato. Potrebbe essere necessario aggiornare la tabella di esclusione per visualizzare la modifica.

AWS CLI

1. Modifica la direzione di autorizzazione dell'esclusione:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-exclusion --exclusion-
id exclusion-id --internet-gateway-exclusion-mode allow-egress
```

   Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato.
2. L'aggiornamento dello stato dell'esclusione può richiedere del tempo. Per visualizzare lo stato dell'esclusione:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusion
```

5.2 Connessione alle istanze

Completa questa sezione per connetterti alle istanze.

AWS Management Console

1. Esegui il ping dell' IPv4 indirizzo pubblico delle istanze A e B. Tieni presente che il traffico è bloccato.
2. Connettiti all'istanza A e B utilizzando EC2 instance connect come hai fatto nello Scenario 1 e fai ping su www.amazon.com. Tieni presente che non puoi inviare il ping a un sito pubblico su Internet dall'istanza A o B. Il traffico è bloccato.
3. Connettiti alle istanze C e D utilizzando EC2 instance connect come hai fatto nello Scenario 1 e invia il ping a www.amazon.com da esse. Tieni presente che puoi inviare il ping a un sito pubblico su Internet dall'istanza C o D. Il traffico è consentito.

AWS CLI

1. Esegui il ping dell'istanza A utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

```
ping 18.225.8.244
```

Output:

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Nota che il ping non riesce e il traffico è bloccato.

2. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Nota che il ping non riesce e il traffico è bloccato.

3. Esegui il ping dell'istanza B utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
```

```
Request timed out.
```

Nota che il ping non riesce e il traffico è bloccato.

4. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Nota che il ping non riesce e il traffico è bloccato.

5. Connetti all'istanza C. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
```

```
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:00:31 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.51 ms
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.49 ms
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

6. Connetti all'istanza D. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output:

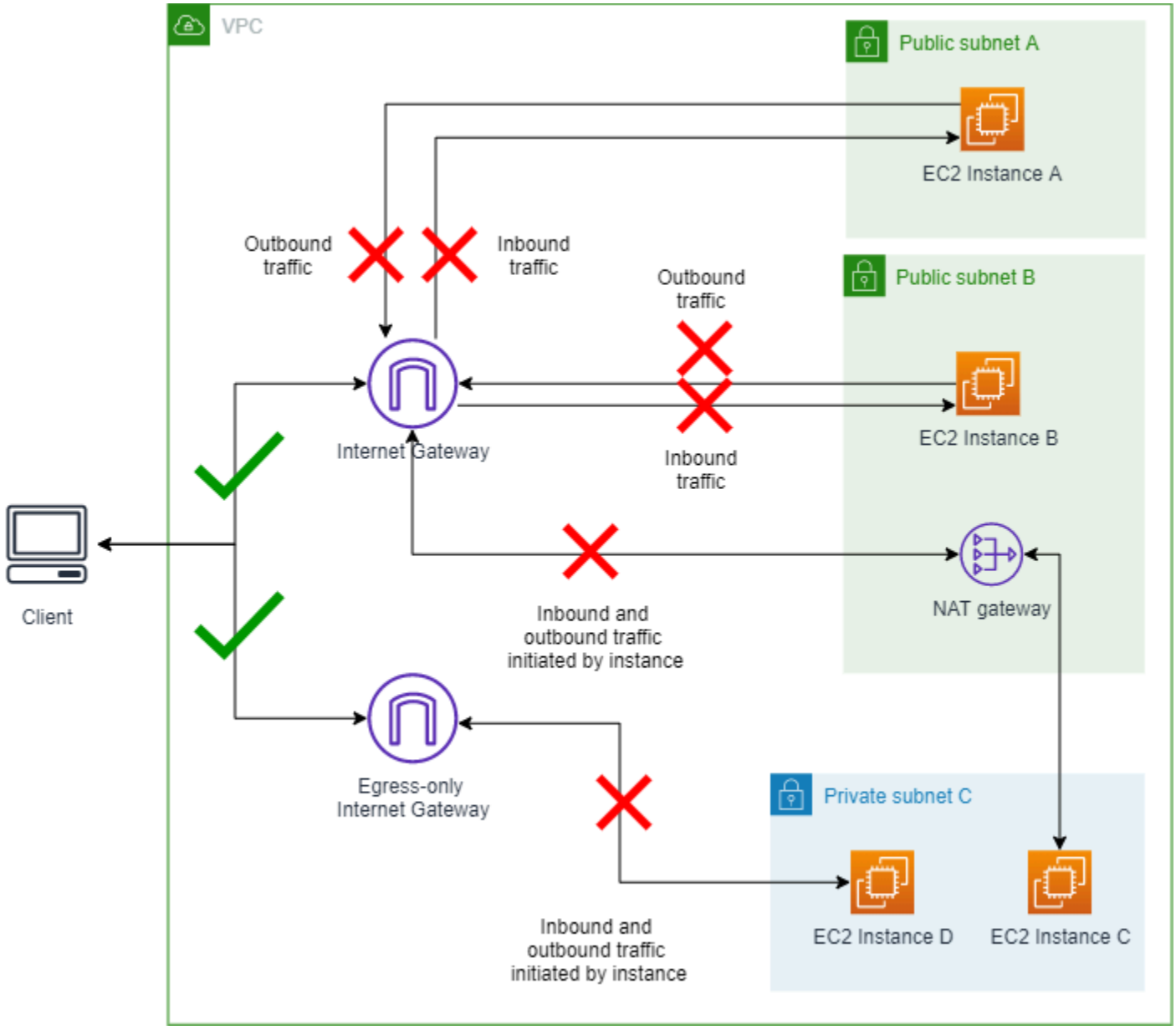
```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:13:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2606:2cc0::374 (2606:2cc0::374)) 56 data bytes
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=1 ttl=58 time=1.21 ms
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=2 ttl=58 time=1.51 ms
```

Nota che il ping riesce correttamente e il traffico non è bloccato.

Scenario 6: Modifica della modalità BPA

In questa sezione modificherai la direzione del blocco VPC BPA per vedere in che modo influisce sul traffico. In questo scenario, VPC BPA abilitato in modalità bidirezionale blocca tutto il traffico proprio come nello Scenario 1. A meno che un'esclusione non abbia accesso a un gateway NAT o gateway Internet egress-only, il traffico viene bloccato.

Diagramma della modalità bidirezionale VPC BPA attivata e dell'esclusione della sottorete A con modalità egress-only attivata:



6.1 Modifica di VPC BPA in modalità bidirezionale

Completa questa sezione per modificare la modalità BPA.

AWS Management Console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni.
3. Scegli Modifica impostazioni di accesso pubblico.
4. Modifica la direzione del blocco in Bidirezionale, quindi scegli Salva modifiche.
5. Attendi che lo stato passi su Abilitato. Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato.

AWS CLI

1. Modifica la direzione del blocco VPC BPA:

   ```
   aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
   ```

   Potrebbero essere necessari alcuni minuti prima che le impostazioni BPA abbiano effetto e lo stato venga aggiornato.
2. Visualizza lo stato di VPC BPA:

   ```
   aws ec2 --region us-east-2 describe-vpc-block-public-access-options
   ```

6.2 Connessione alle istanze

Completa questa sezione per connetterti alle istanze.

AWS Management Console

1. Esegui il ping dell' IPv4 indirizzo pubblico delle istanze A e B. Tieni presente che il traffico è bloccato.
2. Connettiti all'istanza A e B utilizzando EC2 instance connect come hai fatto nello Scenario 1 e fai ping su www.amazon.com. Tieni presente che non puoi inviare il ping a un sito pubblico su Internet dall'istanza A o B. Il traffico è bloccato.

3. Connettiti alle istanze C e D utilizzando EC2 instance connect come hai fatto nello Scenario 1 e invia il ping a www.amazon.com da esse. Tieni presente che non puoi inviare il ping a un sito pubblico su Internet dall'istanza C o D e che il traffico è bloccato.

AWS CLI

1. Esegui il ping dell'istanza A utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

```
ping 18.225.8.244
```

Output:

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Nota che il ping non riesce e il traffico è bloccato.

2. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:17:44 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Nota che il ping non riesce e il traffico è bloccato.

3. Esegui il ping dell'istanza A utilizzando l' IPv4 indirizzo pubblico per controllare il traffico in entrata:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Nota che il ping non riesce e il traffico è bloccato.

4. Usa l' IPv4 indirizzo privato per connetterti e controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Nota che il ping non riesce e il traffico è bloccato.

5. Connetti all'istanza C. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:19:45 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:6200:7:49a5:5fd4:b121
 (2600:9000:25f3:6200:7:49a5:5fd4:b121)) 56 data bytes
```

Nota che il ping non riesce e il traffico è bloccato.

6. Connetti all'istanza D. Poiché non esiste un indirizzo IP pubblico a cui eseguire il ping, usa EC2 Instance Connect per connetterti e quindi esegui il ping di un IP pubblico dall'istanza per controllare il traffico in uscita:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
```

```
Last login: Fri Sep 27 18:20:58 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:b400:7:49a5:5fd4:b121
 (2600:9000:25f3:b400:7:49a5:5fd4:b121)) 56 data bytes
```

Nota che il ping non riesce e il traffico è bloccato.

Rimozione

In questa sezione eliminerai tutte le risorse che hai creato per questo esempio avanzato. È importante ripulire le risorse per evitare costi aggiuntivi eccessivi per le risorse create nel tuo account.

Eliminare le risorse CloudFormation

Completa questa sezione per eliminare le risorse che hai creato con il AWS CloudFormation modello.

AWS Management Console

1. Apri la AWS CloudFormation console all'indirizzohttps://console.aws.amazon.com/cloudformation/.
2. Scegli lo stack VPC BPA.
3. Scegli Elimina.
4. Una volta che inizi a eliminare lo stack, visualizza la scheda Eventi per visualizzare lo stato di avanzamento e assicurarti che lo stack venga eliminato. Potrebbe essere necessario forzare l'eliminazione dello stack per eliminarlo completamente.

AWS CLI

1. Elimina lo CloudFormation stack. Potrebbe essere necessario forzare l'eliminazione dello stack per eliminarlo completamente.

```
aws cloudformation delete-stack --stack-name VPC-BPA-stack --region us-east-2
```

2. Visualizza lo stato di avanzamento e assicurati che lo stack venga eliminato.

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-
east-2
```

Tieni traccia dell'eliminazione delle esclusioni con AWS CloudTrail

Completa questa sezione per tenere traccia dell'eliminazione delle esclusioni con. AWS CloudTrail CloudTrail le voci vengono visualizzate quando si elimina un'esclusione.

AWS Management Console

Puoi visualizzare eventuali esclusioni eliminate nella cronologia degli CloudTrail eventi cercando Tipo di risorsa > AWS:::EC2: VPCBlock PublicAccessExclusion nella AWS CloudTrail console all'indirizzohttps://console.aws.amazon.com/cloudtrailv2/.

AWS CLI

Puoi utilizzare il comando lookup-events per visualizzare gli eventi relativi all'eliminazione di esclusioni:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

L'esempio avanzato è completo.

Security best practices for your 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.
- Utilizza i gruppi di sicurezza per controllare il traffico verso EC2 le istanze nelle sottoreti. Per ulteriori informazioni, consulta Gruppi di sicurezza.
- Usa la rete ACLs per controllare il traffico in entrata e in uscita a livello di sottorete. Per ulteriori informazioni, consulta Controllo del traffico della sottorete con le liste di controllo degli accessi alla 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 Network Access Analyzer per identificare accessi involontari di rete alle risorse del nostro. VPCs 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 le risposte alle domande frequenti relative alla sicurezza dei VPC, consulta Sicurezza e filtraggio in Amazon VPC. FAQs

Utilizzare Amazon VPC con altri Servizi AWS

Amazon Virtual Private Cloud (VPC) è un servizio AWS fondamentale che fornisce un ambiente di rete sicuro e personalizzabile per la tua infrastruttura cloud. Oltre a creare e gestire il tuo VPC, è possibile sfruttare l'integrazione tra VPC e altri servizi AWS per creare soluzioni complete su misura per le tue esigenze specifiche.

Puoi connettere il tuo VPC a vari servizi AWS utilizzando AWS PrivateLink. Ciò consente la connettività privata tra il VPC e i servizi AWS supportati o le applicazioni on-premises, mantenendo il traffico all'interno della rete AWS ed evitando l'esposizione alla rete Internet pubblica ed è particolarmente utile per mantenere rigidi limiti di sicurezza e requisiti di conformità.

Per rafforzare ulteriormente la sicurezza del tuo VPC, puoi usare AWS Network Firewall. Questo servizio firewall gestito ti consente di definire e applicare policy di sicurezza a livello di rete, filtrando il traffico nord-sud ed est-ovest all'interno del tuo VPC. Associando il firewall di rete al tuo VPC, puoi migliorare la tua strategia di difesa e proteggere le tue risorse cloud da accessi non autorizzati o attività dannose.

Inoltre, puoi filtrare il traffico DNS all'interno del tuo VPC utilizzando il firewall DNS Route 53 Resolver. Questa funzionalità consente di creare regole di filtraggio DNS personalizzate per controllare quali domini possono risolvere le risorse VPC, fornendo un ulteriore livello di sicurezza e applicazione della conformità.

Se riscontri problemi di raggiungibilità tra le risorse all'interno del tuo VPC o a esso connesse, puoi sfruttare Reachability Analyzer. Reachability Analyzer esegue test di connettività virtuale, fornendo informazioni dettagliate sul percorso hop-by-hop e identificando eventuali componenti di blocco. Questo strumento di risoluzione dei problemi può aiutarti a identificare e risolvere rapidamente i problemi di connettività di rete.

Integrando questi servizi AWS complementari con il tuo VPC, puoi creare soluzioni cloud potenti, sicure e resilienti che soddisfano i tuoi requisiti aziendali e architetturali univoci.

Indice

- Connect il tuo VPC ai servizi utilizzando AWS PrivateLink
- Filtrare il traffico di rete utilizzando AWS Network Firewall
- Filtrare il traffico DNS utilizzando Route 53 Resolver DNS Firewall
- Risoluzione dei problemi di raggiungibilità con Reachability Analyzer

Connect il tuo VPC ai servizi utilizzando AWS PrivateLink

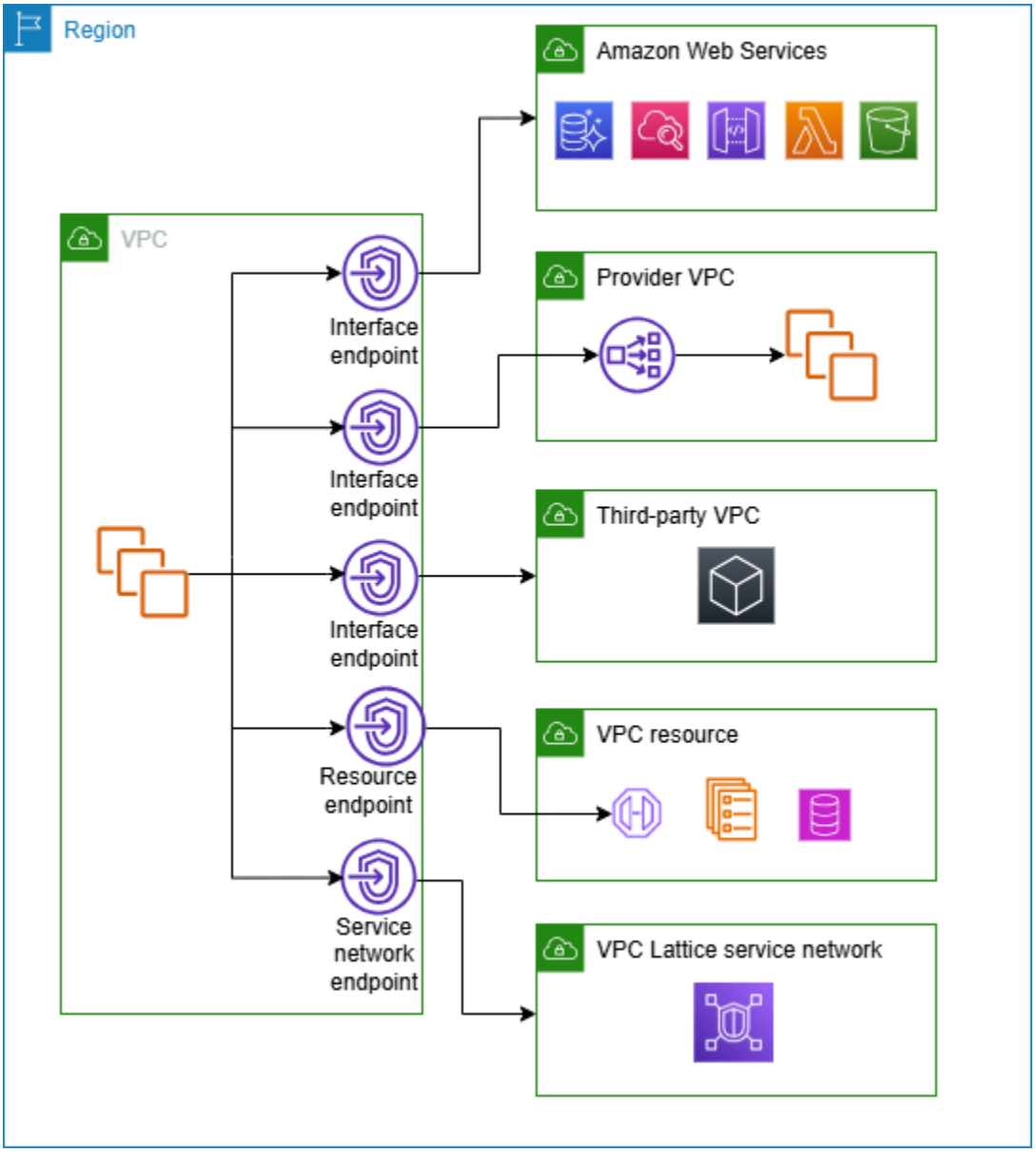
AWS PrivateLink stabilisce una connettività privata tra cloud privati virtuali (VPC) e servizi Servizi AWS supportati, ospitati da Account AWS altri servizi Marketplace AWS supportati e risorse supportate. Non è necessario utilizzare un gateway Internet, un dispositivo NAT, una connessione o AWS Direct Connect una AWS Site-to-Site VPN connessione per comunicare con il servizio o la risorsa.

Per utilizzarlo AWS PrivateLink, crea un endpoint VPC in qualsiasi sottorete da cui è necessario accedere al servizio o alla risorsa. Questo crea interfacce di rete elastiche nelle sottoreti specificate che fungono da punti di ingresso per il traffico destinato al servizio o alla risorsa.

Puoi anche creare il tuo servizio endpoint VPC, basato su AWS PrivateLink e consentire ad altri AWS clienti di accedere al tuo servizio. PrivateLink consente la creazione di endpoint API privati, consentendo alle organizzazioni di esporre i propri servizi in modo sicuro ad altri clienti. AWS Ciò consente alle aziende di monetizzare le proprie funzionalità interne, promuovere ecosistemi collaborativi e mantenere il controllo sull'accesso e sul consumo dei propri servizi.

Uno dei principali vantaggi dell'utilizzo AWS PrivateLink è la possibilità di stabilire una connettività privata e sicura senza la necessità di costrutti di rete tradizionali come gateway Internet, dispositivi NAT o connessioni VPN. Questo aiuta a semplificare l'architettura di rete, ridurre la superficie di attacco e migliorare la sicurezza generale mantenendo il traffico di dati confinato all'interno della rete AWS .

Il diagramma seguente mostra i casi d'uso comuni per. AWS PrivateLink Il VPC dispone di diverse EC2 istanze in una sottorete privata che hanno accesso alle risorse tramite cinque endpoint VPC. Esistono tre endpoint VPC di interfaccia, un endpoint VPC di risorse e un endpoint VPC di rete di servizio.



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. 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 predefini te. Per utilizzare una policy firewall, è necessario associarla a uno o più firewall. 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 comportam ento e nell'utilizzo degli elenchi di controllo degli accessi (ACL) di rete di Amazon VPC. Puoi inoltre definire gruppi di regole stateful per ispeziona re 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. 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 riutilizz abile 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. 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. 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. 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.

Risoluzione dei problemi di raggiungibilità con Reachability Analyzer

Reachability Analyzer è uno strumento di analisi statica della configurazione. Utilizza questo strumento per analizzare ed eseguire il debug della raggiungibilità di rete tra due risorse nel VPC. Reachability Analyzer produce i dettagli hop-by-hop del percorso virtuale tra queste risorse quando sono raggiungibili; in caso contrario ne identifica il componente di blocco.

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

Amazon Virtual Private Cloud (VPC) è un elemento fondamentale all'interno dell' AWS ecosistema, che ti consente di fornire reti virtuali isolate personalizzate in base alle tue esigenze specifiche. Creando e gestendo le tue VPCs, ottieni il pieno controllo dell'ambiente di rete, inclusa la possibilità di definire intervalli di indirizzi IP, sottoreti, tabelle di routing e opzioni di connettività.

Questa sezione contiene tre esempi di configurazioni per i cloud privati virtuali (VPCs), ognuna progettata per soddisfare un diverso set di requisiti:

- VPC per un ambiente di test: questa configurazione spiega come creare un VPC da utilizzare come ambiente di sviluppo o test.
- VPC per server Web e di database: questa configurazione mostra come creare un VPC da utilizzare per un'architettura resiliente in un ambiente di produzione.
- VPC con server in sottoreti private e NAT: in questa configurazione più avanzata, tutte le EC2 istanze vengono fornite all'interno di sottoreti private, con un gateway NAT che facilita l'accesso sicuro a Internet in uscita. Questo è un esempio in cui è necessario limitare la connessione Internet diretta alle risorse pur consentendo le comunicazioni in uscita necessarie.

Fornendo queste configurazioni VPC di esempio, desideriamo illustrare la flessibilità e le opzioni di personalizzazione disponibili durante la progettazione di un ambiente di rete cloud. La configurazione specifica del VPC scelta deve essere basata su architettura dell'applicazione, requisiti di sicurezza e obiettivi aziendali generali. Una pianificazione attenta dell'infrastruttura VPC può aiutarti a creare una rete virtuale solida, scalabile e sicura che supporti la crescita e l'evoluzione dei carichi di lavoro basati sul cloud.

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 connettervi gli uni VPCs agli altri, consulta le configurazioni di peering VPC nella Amazon VPC Peering Guide.

- Per connetterti VPCs alla tua rete, consulta gli scenari Site-to-Site VPN nella Guida per l'utente.AWS Site-to-Site VPN
- Per connettervi gli uni VPCs agli altri e alla vostra rete, consulta Esempi di scenari di gateway di transito nei gateway di transito Amazon VPC.

Risorse aggiuntive

- 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)

Esempio: VPC per un ambiente di test

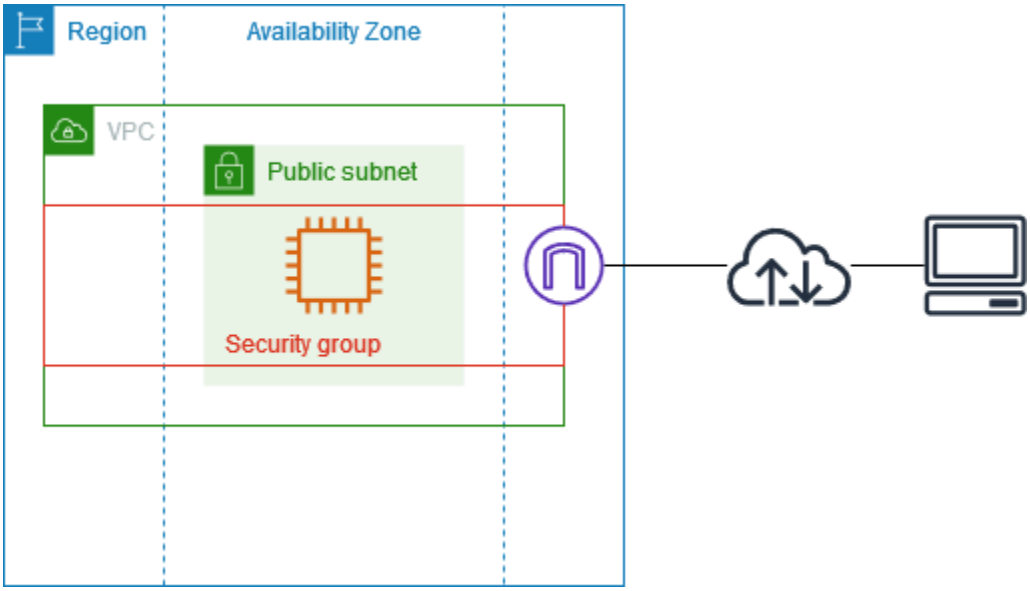
Questo esempio illustra come creare un VPC da utilizzare come ambiente di sviluppo o test. Poiché questo VPC non è destinato all'uso in produzione, non è necessario distribuire i server in più zone di disponibilità. Per contenere i costi e la complessità, è possibile distribuire i server in un'unica zona di disponibilità.

Indice

- Panoramica
- 1. Creazione del VPC
- 2. Distribuzione dell'applicazione
- 3. Test della configurazione
- 4. Eliminazione

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' EC2 istanza 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 della tabella delle rotte con percorsi per entrambi IPv4 e IPv6. Se crei una sottorete IPv4 - only invece di una subnet dual stack, la tabella di routing contiene solo le rotte. IPv4

Destinazione	Target
10.0.0.0/16	local
2001:db8:1234:1a00::/56	locale
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 alcuni esempi di regole in entrata per un gruppo di sicurezza, con regole per entrambi e. IPv4 IPv6 Se si creano sottoreti IPv4 -only anziché sottoreti dual stack, sono necessarie solo le regole per. IPv4

Crea	Protocollo	Intervallo porte	Descrizione
0.0.0.0/0	TCP	80	Consente 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	Consente l'accesso HTTPS in entrata da tutti gli indirizzi IPv4
::/0	TCP	443	Consente l'accesso HTTPS in entrata da tutti gli indirizzi IPv6
Public IPv4 address range of your network	TCP	22	(Facoltativo) Consente l'accesso SSH in entrata dagli indirizzi IPv4 IP della rete
IPv6 address range of your network	TCP	22	(Facoltativo) Consente l'accesso SSH in entrata dagli IPv6 indirizzi IP della rete
Public IPv4 address range of your network	TCP	3389	(Facoltativo) Consente l'accesso RDP in entrata dagli IPv4 indirizzi IP della rete
IPv6 address range of your network	TCP	3389	(Facoltativo) Consente l'accesso RDP in entrata dagli IPv6 indirizzi IP della rete

1. 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. Apri la 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. Configurazione del VPC
    a. Per Name tag auto-generation (Generazione automatica di tag nome), immetti un nome per il VPC.
    b. Per il blocco IPv4 CIDR, puoi mantenere il suggerimento predefinito o, in alternativa, puoi inserire 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 IPv6 indirizzi, scegli blocco CIDR, blocco IPv6 CIDR fornito da Amazon IPv6 .
5. Configurazione delle sottoreti
    a. Per Numero di zone di disponibilità, scegli 1. Puoi mantenere la zona di disponibilità predefinita o, in alternativa, puoi espandere Personalizza AZs 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 Crea VPC.

2. Distribuzione dell'applicazione

Esistono diversi modi per distribuire le EC2 istanze. Per esempio:

- Procedura guidata di EC2 avvio dell'istanza di Amazon
- Amazon EC2 Auto Scaling
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Dopo aver distribuito un' EC2 istanza, puoi connetterti all'istanza, installare il software necessario per l'applicazione e quindi creare un'immagine per utilizzi futuri. Per ulteriori informazioni, consulta Creare un'AMI nella Amazon EC2 User Guide. In alternativa, puoi utilizzare EC2 Image Builder per creare e gestire Amazon Machine Image (AMI).

3. Test della configurazione

Dopo aver completato l'implementazione dell'applicazione, potrai testarla. Se non riesci a connetterti alla tua EC2 istanza o se l'applicazione non è in grado di inviare o ricevere il traffico previsto, puoi utilizzare Reachability Analyzer per aiutarti a 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.

4. Eliminazione

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

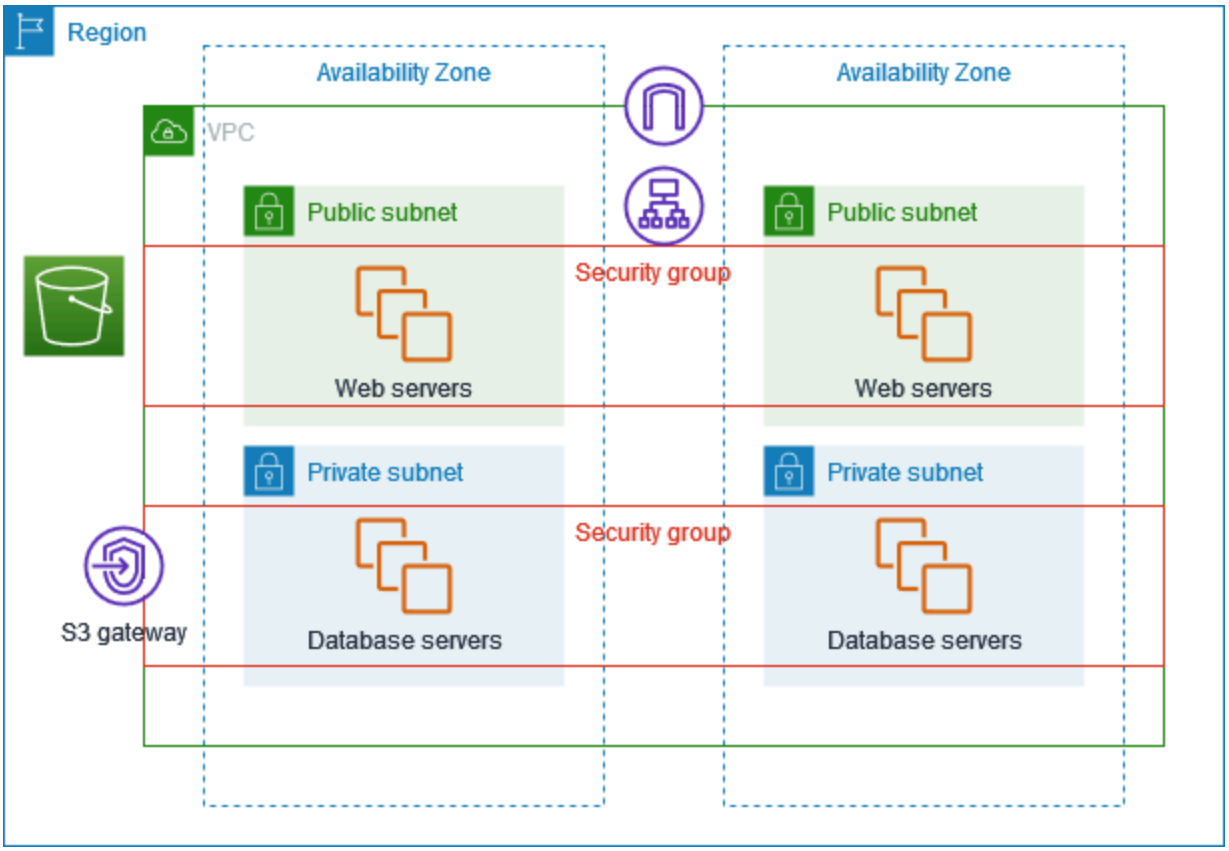
Questo esempio spiega come creare un VPC da utilizzare per un'architettura a due livelli in un ambiente di produzione. Per migliorare la resilienza, implementerai i server in due zone di disponibilità.

Indice

- Panoramica
- 1. Creazione del VPC
- 2. Distribuzione dell'applicazione
- 3. Test della configurazione
- 4. Eliminazione

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
10.0.0.0/16	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
10.0.0.0/16	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.

Crea	Protocollo	Intervallo porte	Descrizione
L'ID del gruppo di sicurezza per il sistema di bilanciamento del carico	TCP	80	Consente l'accesso HTTP in entrata dal sistema di 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

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
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.

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

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 ulteriori informazioni sui gruppi di sicurezza per le istanze di Amazon RDS DB, consulta Controllo dell'accesso con i gruppi di sicurezza nella Guida per l'utente di Amazon RDS.

1. 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. Accedi 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. Configurazione del VPC:
    a. Per creare tag dei nomi per le risorse VPC, mantieni selezionata Generazione automatica dei tag dei nomi altrimenti deselezionala per scegliere autonomamente tag dei nomi 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, consultare 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 che la tenancy del VPC sia `Default`, le istanze EC2 avviate in questo VPC utilizzeranno l'attributo di tenancy specificato all'avvio dell'istanza. Per ulteriori informazioni, consulta Avvio di un'istanza utilizzando parametri definiti nella Guida per l'utente di Amazon EC2. 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. Configurazione delle 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. Puoi mantenere i blocchi CIDR predefiniti per le sottoreti o, in alternativa, espandere Personalizza blocchi CIDR delle sottoreti e inserire un blocco. Per ulteriori informazioni, consultare 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.

2. 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 la pagina Database su AWS: come scegliere.

3. 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.

4. 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, consultare the section called “Eliminazione del VPC”.

Esempio: VPC con server in sottoreti private e NAT

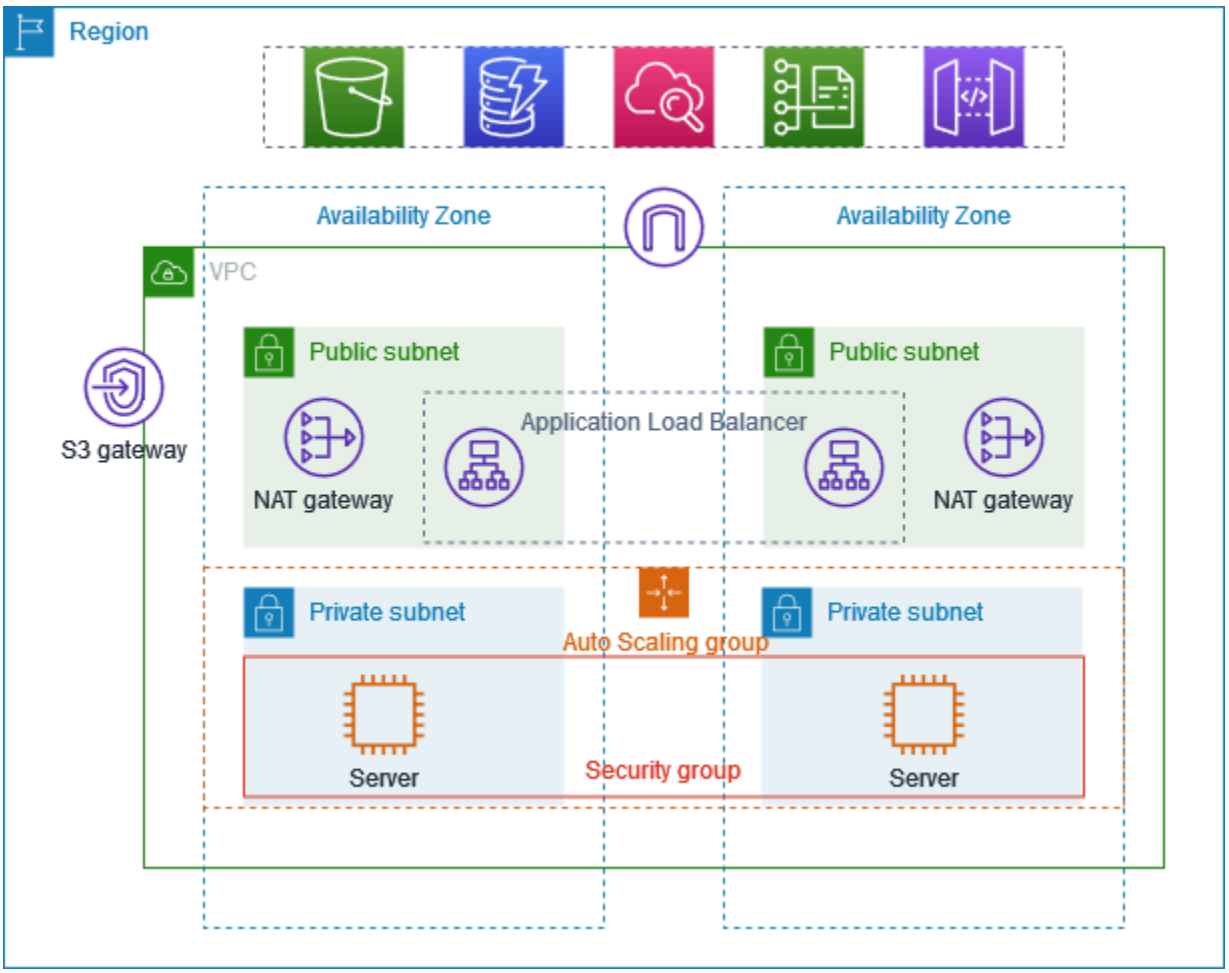
Questo esempio spiega come creare un VPC da utilizzare per i server in un ambiente di produzione. Per migliorare la resilienza, implementerai i server in due zone di disponibilità, utilizzando un gruppo con scalabilità automatica e un Application Load Balancer. Per una maggiore sicurezza, implementerai 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
- 1. Creazione del VPC
- 2. Distribuzione dell'applicazione
- 3. Test della configurazione
- 4. Eliminazione

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.

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

1. 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. Accedi 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. 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, consultare 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 Crea VPC.

2. 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.

3. 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.

4. Eliminazione

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, consultare 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
VPCs per regione	5	Sì	L'aumento di questa quota comporta di pari passo l'aumento della quota relativa agli Internet gateway per Regione. Puoi aumentare questo limite in modo da averne centinaia VPCs per regione.
Sottoreti per VPC	200	Sì	
IPv4 Blocchi CIDR per VPC	5	Sì (fino a 50)	Questo blocco CIDR principale e tutti i blocchi CIDR secondari vengono conteggiati ai fini di questa quota.
IPv6 Blocchi CIDR per VPC	5	Sì (fino a 50)	Il numero di utenti CIDRs che è possibile allocare a un singolo VPC.
Esclusioni di Blocco dell'accesso pubblico VPC per account per regione	50	Sì. Per richiedere un aumento, è necessario aprire	Il numero di esclusioni BPA VPC che puoi creare in un account.

Nome	Predefinita	Adattabile	Commenti
		un caso di aumento del limite di servizio utilizzando AWS Support Center Console.	

DNS

Ogni EC2 istanza può inviare 1024 pacchetti al secondo per interfaccia di rete a Route 53 Resolver (in particolare l'indirizzo .2, ad esempio 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 Account AWS VPCs quota VPCs si applica a utenti individuali e 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 VPCs per regione.

Nome	Predefinita	Adattabile	Commenti
			È possibile collegare un solo Internet gateway egress-only alla volta a un VPC.
Internet gateway per regione	5	Sì	Per aumentare questa quota, aumentare la quota VPCs per regione. 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`.
Quota di indirizzi IP privati per gateway NAT	8	Sì	
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.

Nome	Predefinita	Adattabile	Commenti
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 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.

Rete ACLs

Nome	Predefinita	Adattabile	Commenti
Rete ACLs 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 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 a persone individuali Account AWS VPCs e condivise VPCs. Questo limite viene applicato per zona di disponibilità (AZ). Se, ad esempio, le interfacce di rete sono tre AZs, 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 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 viene applicata separatamente per IPv4 rotte e rotte. IPv6 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 a persone individuali Account AWS VPCs e condivise VPCs. 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. 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. Inoltre, questa quota viene applicata separatamente per IPv4 regole e IPv6 regole. Per un account con la quota predefinita di 60 regole, un gruppo di sicurezza può avere 60 regole in entrata per il IPv4 traffico e 60 regole in entrata per il traffico. IPv6 Per ulteriori informazioni, consulta the section called “Dimensioni dei gruppi di sicurezza”. 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.

Nome	Predefinita	Adattabile	Commenti
Gruppi di sicurezza per interfaccia di rete	5	Sì (fino a 16)	Questa quota moltiplicata per la quota di regole per gruppo di sicurezza non può essere superiore a 1.000.

Condivisione della sottorete VPC

Alle sottoreti VPC condivise 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 condividere le sottoreti in un VPC. Si tratta di una quota VPC e si applica a tutte le sottoreti condivise in un VPC. 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

Utilizzo degli indirizzi di rete

L'utilizzo degli indirizzi di rete (NAU) comprende indirizzi IP, interfacce di rete e CIDRs 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 Utilizzo degli indirizzi di rete.

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 tutte le relative unità peerizzate all'interno della regione. VPCs VPCs che vengono peerizzate tra diverse regioni non contribuiscono a questo numero.

Limitazione EC2 delle API Amazon

Per informazioni sulla limitazione di Amazon, consulta Request EC2 throttling nella Amazon Developer Guide. 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
- Site-to-Site Quote 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
AWS aggiornamento gestito delle politiche	Amazon VPC ha aggiornato il AmazonVPCFullAccess e AmazonVPCReadOnlyAccess politiche gestite.	9 dicembre 2024
Supporto delle policy dichiarative per BPA VPC	Se utilizzi AWS Organizations per gestire gli account della tua organizzazione, puoi utilizzare una politica dichiarativa per applicare il VPC BPA sugli account dell'organizzazione.	1 dicembre 2024
Blocco dell'accesso pubblico (BPA) VPC	VPC Block Public Access (BPA) ti consente di impedire alle risorse VPCs e alle sottoreti di tua proprietà in una regione di raggiungere o essere raggiunte da Internet tramite gateway Internet e gateway Internet solo in uscita.	19 novembre 2024
Gruppi di sicurezza condivisi	Questa funzionalità consente di condividere un gruppo di sicurezza con altri account AWS Organizations.	30 ottobre 2024
Associazioni di VPC e gruppi di sicurezza	Questa funzionalità consente di associare un gruppo di	30 ottobre 2024

	sicurezza VPCs a più gruppi nella stessa regione.	
Gateway NAT (supporto MTU)	I gateway NAT supportan o il traffico con un'unità di trasmissione massima (MTU) di 8.500.	10 settembre 2024
Indirizzamento privato IPv6	Sono state aggiunte informazi oni sull' IPv6 indirizzamento privato. IPv6 Gli indirizzi privati sono disponibili solo in Amazon VPC IP Address Manager.	8 agosto 2024
IPv6 periodo di leasing preferito	Ora puoi scegliere la frequenza con cui un'istanz a in esecuzione a cui è IPv6 assegnata un'istanza deve passare attraverso il rinnovo del DHCPv6 leasing.	20 febbraio 2024
Revisione e miglioramenti della struttura della guida	La struttura della guida è stata rivista e sono stati apportati miglioramenti per perfezionare l'esperienza del cliente relativa alla ricerca di informazioni per scenari specifici.	20 febbraio 2024
AWS aggiornamento gestito delle politiche	Amazon VPC ha aggiornato il AmazonVPCFullAccess e AmazonVPCReadOnlyAccess politiche gestite.	8 febbraio 2024
AWS aggiornamento gestito delle politiche	Amazon VPC ha aggiornat o il AmazonVPCCrossAcco untNetworkInterfaceOperatio ns politica gestita.	25 settembre 2023

EC2-Classic è obsoleto	Con EC2 -Classic, EC2 le istanze venivano eseguite in un'unica rete piatta 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
Aggiungi IPv4 indirizzi secondari ai gateway NAT	È possibile aggiungere IPv4 indirizzi privati secondari ai gateway NAT pubblici e privati. IPv4 Gli indirizzi secondari aumentano il numero di porte disponibili e quindi aumentano il limite al numero di connessio ni simultanee che i carichi di lavoro possono stabilire utilizzando un gateway NAT.	31 gennaio 2023
Allineamento alle best practice IAM	Guida aggiornata per allinears i 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 precedenz a, l'indirizzo IP privato veniva assegnato automaticamente dall'intervallo di indirizzi IP della sottorete.	17 novembre 2022

IPv6 configurazione predefinita del router gateway	Tre IPv6 indirizzi sono ora riservati per l'uso con il 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 in Amazon Data Firehose	È possibile 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
Blocchi IPv6 CIDR multipli	Puoi associare fino a cinque blocchi IPv6 CIDR 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 per IPv6 IPv4	Il gateway NAT supporta la traduzione degli indirizzi di rete da IPv6 a IPv4, popolarmente nota come. NAT64	24 novembre 2021
IPv6-solo sottoreti in VPCs	È possibile creare sottoreti IPv6 -only in cui avviare istanze -only. IPv6 EC2	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
Visione EC2 globale di Amazon	Amazon EC2 Global View ti consente di visualizzare VPCs 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 specifiche per reindirizzare il traffico tra sottoreti all'interno di un VPC (traffico Est-Ovest) a un'appliance middlebox. Puoi impostare la destinazione di un percorso in modo che corrisponda a un intero blocco IPv4 o IPv6 CIDR di una sottorete nel tuo VPC.	30 agosto 2021

Supporto in termini di risorse IDs e 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 comunicazioni private solo in uscita tra o VPCs tra un VPC e la tua rete locale.	10 giugno 2021
Tag alla creazione	È possibile aggiungere tag quando si crea un VPC, opzioni DHCP, gateway Internet, gateway egress-only, 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. CloudWatch	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	Puoi configurare i gruppi di confini di rete per il tuo VPCs . Amazon Virtual Private Cloud Console	22 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 IPv4 CIDR secondari per il tuo VPC	Puoi aggiungere più blocchi IPv4 CIDR 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
IPv6 supporto	Puoi associare un blocco IPv6 CIDR al tuo VPC e IPv6 assegnare indirizzi alle risorse nel tuo 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. Puoi associare i gruppi di sicurezza VPC all'istanza EC2 -Classic, abilitando la comunicazione tra l'istanza EC2 -Classic e le istanze nel tuo VPC utilizzan do 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 risoluzio ne DNS	Puoi modificare le impostazi oni predefinite VPC e disabilit are 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, VPCs in più zone di disponibilità, più VPCs per AWS account e più connessio ni VPN per VPC.	3 agosto 2011
Istanze dedicate	Le istanze dedicate sono EC2 istanze Amazon lanciate all'interno del tuo VPC che eseguono hardware dedicato a un singolo 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.