AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

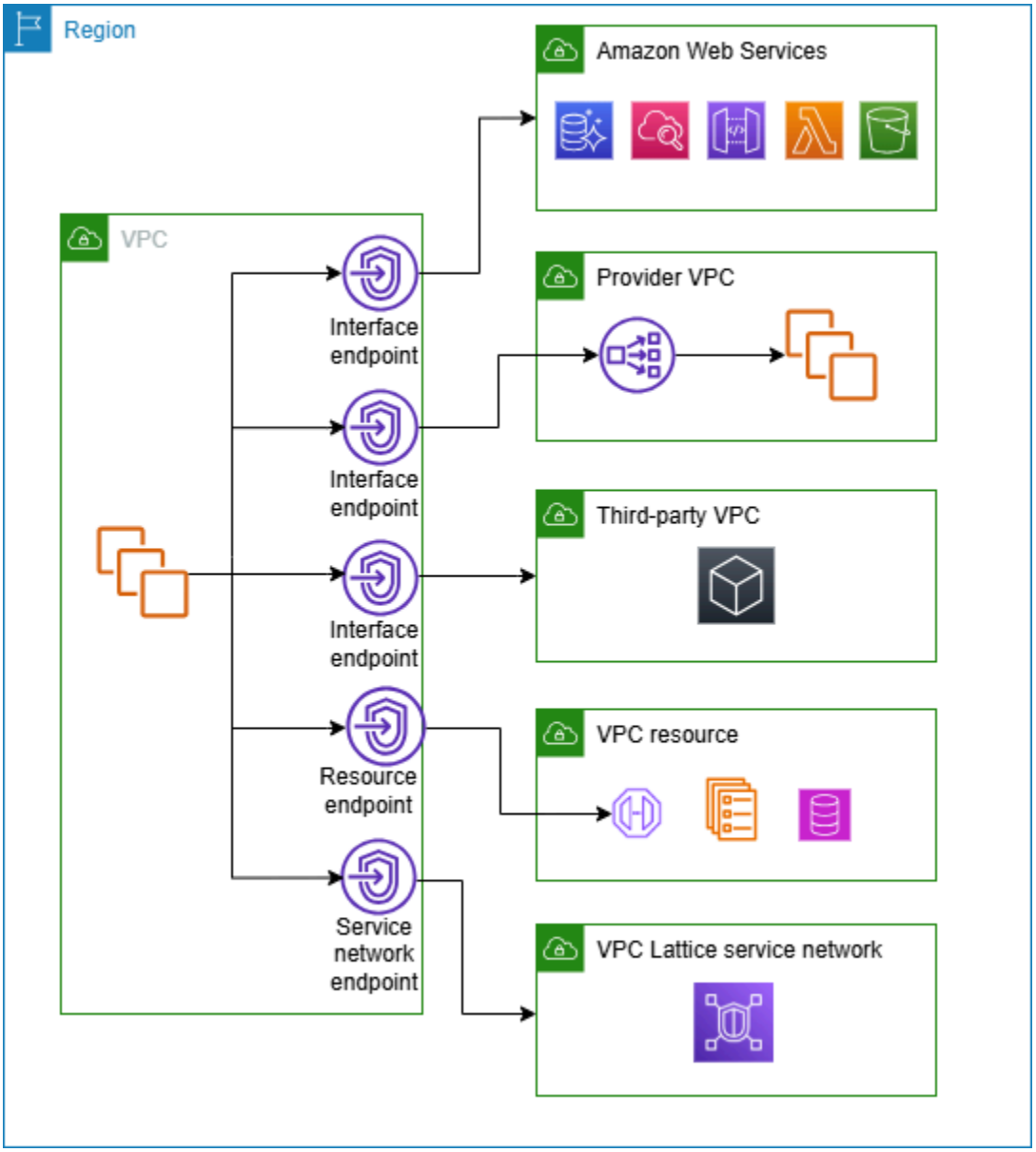
Che cos'è AWS PrivateLink?

AWS PrivateLink è una tecnologia scalabile e altamente disponibile che puoi utilizzare per connettere privatamente il tuo VPC a servizi e risorse come se fossero nel tuo VPC. Non è necessario utilizzare un gateway Internet, un dispositivo NAT, un indirizzo IP pubblico, una connessione o una Direct Connect AWS Site-to-Site VPN connessione per consentire la comunicazione con il servizio o la risorsa dalle sottoreti private. Pertanto, controlli gli endpoint, i siti, i servizi e le risorse API specifici raggiungibili dal tuo VPC.

Casi d'uso

Puoi creare endpoint VPC per connettere i client nel tuo VPC a servizi e risorse che si integrano con. AWS PrivateLink Puoi creare il tuo servizio di endpoint VPC e renderlo disponibile ad altri clienti. AWS Per ulteriori informazioni, consulta the section called “Concetti”.

Nel diagramma seguente, il VPC a sinistra presenta diverse istanze EC2 Amazon in una sottorete privata e cinque endpoint VPC: tre endpoint VPC di interfaccia, un endpoint VPC di risorsa e un endpoint VPC di rete di servizi. Il primo endpoint VPC con interfaccia si connette a un servizio. AWS Il secondo endpoint VPC di interfaccia si connette a un servizio ospitato da un altro AWS account (un servizio endpoint VPC). Il terzo endpoint VPC con interfaccia si connette a un servizio partner del AWS Marketplace. L'endpoint VPC della risorsa si connette a un database. L'endpoint VPC della rete di assistenza si connette a una rete di servizi.



Ulteriori informazioni

- Concetti
- Accesso a Servizi AWS
- Accesso ai prodotti SaaS
- Accesso alle appliance virtuali
- Condividi i tuoi servizi

Utilizza gli endpoint VPC

Puoi creare, accedere e gestire gli endpoint VPC utilizzando uno dei seguenti metodi:

- Console di gestione AWS— Fornisce un'interfaccia web che è possibile utilizzare per accedere alle risorse. AWS PrivateLink Apri la console Amazon VPC e scegli Endpoints o Endpoint Services.
- AWS Command Line Interface (AWS CLI) — Fornisce comandi per un'ampia gamma di, tra Servizi AWS cui. AWS PrivateLink Per ulteriori informazioni sui comandi per AWS PrivateLink, consulta ec2 nella Guida ai AWS CLI comandi.
- CloudFormation: crea modelli che descrivono le tue risorse AWS . I modelli vengono utilizzati per effettuare il provisioning e gestire queste risorse come unità singola. Per ulteriori informazioni, consulta le seguenti risorse AWS PrivateLink :
  - AWS:EC2:: VPCEndpoint
  - AWS:EC2:: VPCEndpoint ConnectionNotification
  - AWS:EC2:: VPCEndpoint Servizio
  - AWS:EC2:: VPCEndpoint ServicePermissions
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS SDKs— Fornisci informazioni specifiche per la linguaAPIs. SDKs Si occupano 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 Strumenti per creare in AWS.
- API di query: forniscono operazioni API di basso livello accessibili tramite richieste HTTPS. L'utilizzo dell'API di query è il modo più diretto di accedere ad Amazon VPC. Tuttavia, richiede che l'applicazione gestisca dettagli di basso livello, come la generazione dell'hash per firmare la richiesta e la gestione degli errori. Per ulteriori informazioni, consulta AWS PrivateLink le azioni nell'Amazon EC2 API Reference.

Prezzi

Per informazioni sul prezzo degli endpoint VPC, consulta Prezzi di AWS PrivateLink.

AWS PrivateLink concetti

È possibile utilizzare Amazon VPC per definire un cloud privato virtuale (VPC), ossia una rete virtuale isolata logicamente. Puoi consentire ai client del tuo VPC di connettersi a destinazioni esterne a quel

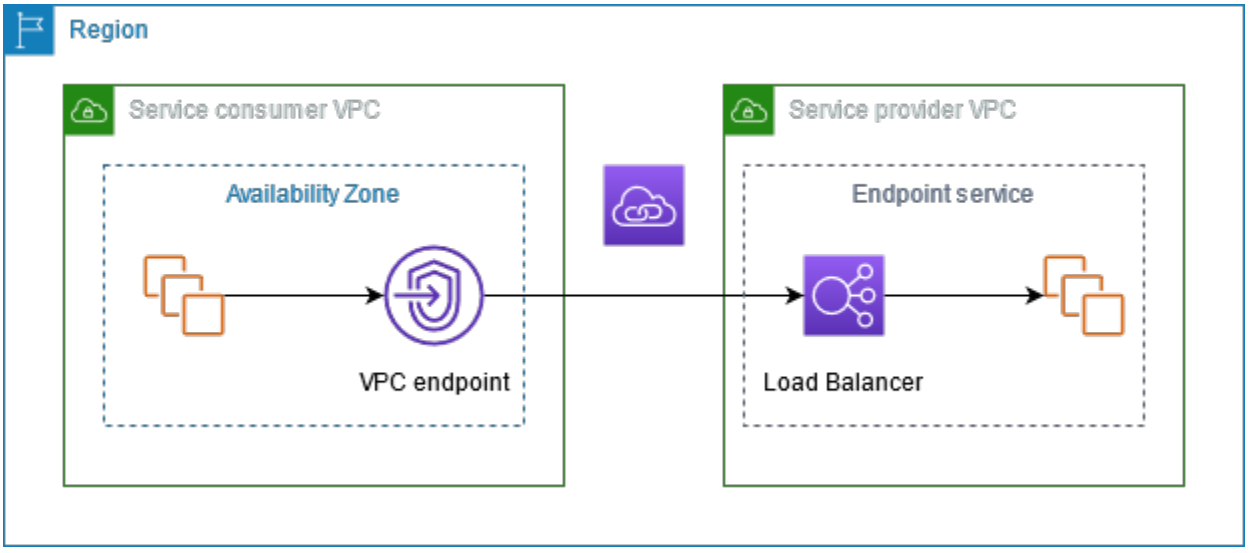
VPC. Ad esempio, puoi aggiungere un gateway Internet al VPC per consentire l'accesso a Internet o aggiungere una connessione VPN per consentire l'accesso alla tua rete on-premise. In alternativa, AWS PrivateLink utilizzalo per consentire ai client del tuo VPC di connettersi a servizi e risorse in altri VPCs utilizzando indirizzi IP privati, come se tali servizi e risorse fossero ospitati direttamente nel tuo VPC.

Di seguito sono riportati alcuni concetti fondamentali da conoscere quando si inizia a utilizzare AWS PrivateLink.

Indice

Diagramma architetturale

Il diagramma seguente fornisce una panoramica di alto livello del funzionamento. AWS PrivateLink I consumatori creano endpoint VPC per connettersi a servizi e risorse endpoint ospitati dai provider.



Fornitori

Comprendi i concetti relativi a un provider.

Fornitore di servizi

Il proprietario di un servizio è il provider di servizi. I fornitori di servizi includono AWS AWS partner e altri Account AWS. I provider di servizi possono ospitare i propri servizi utilizzando AWS risorse, ad esempio EC2 istanze, o utilizzando server locali.

Fornitore di risorse

Il proprietario di una risorsa, ad esempio un database o un' EC2 istanza Amazon, è il fornitore di risorse. I fornitori di risorse includono AWS servizi, AWS partner e altri AWS account. I fornitori di risorse possono ospitare le proprie risorse in sede VPCs o in locale.

Concetti

- Servizi endpoint
- Nomi dei servizi
- Stati del servizio
- Configurazione delle risorse
- Gateway delle risorse

Servizi endpoint

Un provider di servizi crea un servizio endpoint per rendere disponibile un determinato servizio in una regione. Durante la creazione di un servizio endpoint, il provider di servizi deve specificare un load balancer. Il load balancer riceve le richieste dagli utenti del servizio e le instrada al servizio.

Per impostazione predefinita, il servizio endpoint non è disponibile per gli utenti del servizio. È necessario aggiungere autorizzazioni che consentano a AWS destinatari specifici di connettersi al servizio endpoint.

Nomi dei servizi

Ogni servizio endpoint è identificato da un nome del servizio. Un utente del servizio deve specificare tale nome durante la creazione di un endpoint VPC. I consumatori del servizio possono richiedere i nomi dei servizi per. Servizi AWS I provider di servizi devono condividere i nomi dei loro servizi con gli utenti.

Stati del servizio

Di seguito sono riportati i possibili stati per un servizio endpoint:

- In sospeso: il servizio endpoint è in fase di creazione.
- Disponibile: il servizio endpoint è disponibile.
- Fallito: il servizio endpoint non può essere creato.
- Eliminazione: il provider di servizi ha eliminato il servizio endpoint e l'eliminazione è in corso.
- Eliminato: il servizio endpoint viene eliminato.

Configurazione delle risorse

Il provider di risorse crea una configurazione di risorse per condividere una risorsa. Una configurazione di risorse è un oggetto logico che rappresenta una singola risorsa, ad esempio un database, o un gruppo di risorse. Una risorsa può essere un indirizzo IP, una destinazione con nome di dominio o un database Amazon Relational Database Service (Amazon RDS).

Quando si condivide con altri account, il provider di risorse deve condividere la risorsa tramite una condivisione di risorse AWS Resource Access Manager(AWS RAM) per consentire ai AWS principali specifici dell'altro account di connettersi alla risorsa tramite un endpoint VPC di risorse.

Le configurazioni delle risorse possono essere associate a una rete di servizi a cui i principali si connettono tramite un endpoint VPC di rete di servizi.

Gateway delle risorse

Un gateway di risorse è un punto di ingresso in un VPC da cui viene condivisa una risorsa. Il provider crea un gateway di risorse per condividere le risorse dal VPC.

Consumatori di servizi o risorse

L'utente di un servizio o di una risorsa è un consumatore. I consumatori possono accedere ai servizi e alle risorse degli endpoint da loro VPCs o dall'ambiente locale.

Concetti

- Endpoint VPC
- Interfacce di rete dell'endpoint
- Policy di endpoint
- Stati dell'endpoint

Endpoint VPC

Un consumatore crea un endpoint VPC per connettere il proprio VPC a un servizio o una risorsa endpoint. Un consumatore deve specificare il servizio, la risorsa o la rete di servizi dell'endpoint quando crea un endpoint VPC. Esistono diversi tipi di endpoint VPC. È necessario creare il tipo di endpoint VPC richiesto.

- `Interface`- Crea un endpoint di interfaccia per inviare traffico TCP o UDP a un servizio endpoint. Il traffico destinato al servizio endpoint viene risolto utilizzando il DNS.
- `GatewayLoadBalancer`: crea un endpoint Gateway Load Balancer per inviare traffico a un parco istanze di appliance virtuali utilizzando indirizzi IP privati. Puoi instradare il traffico dal tuo VPC all'endpoint Gateway Load Balancer tramite le tabelle di instradamento. Gateway Load Balancer distribuisce il traffico alle appliance virtuali e può scalare in base alla domanda.
- `Resource`- Crea un endpoint di risorse per accedere a una risorsa che è stata condivisa con te e che risiede in un altro VPC. Un endpoint di risorse consente di accedere in modo privato e sicuro a risorse come un database, un' EC2 istanza Amazon, un endpoint applicativo, una destinazione con nome di dominio o un indirizzo IP che può trovarsi in una sottorete privata in un altro VPC o in un ambiente locale. Gli endpoint di risorse non richiedono un sistema di bilanciamento del carico e consentono di accedere direttamente alla risorsa.
- `Service network`- Crea un endpoint di rete di servizi per accedere a una rete di servizi che hai creato o che è stata condivisa con te. È possibile utilizzare un singolo endpoint di rete di servizio per accedere in modo privato e sicuro a più risorse e servizi associati a una rete di servizi.

Esiste un altro tipo di endpoint VPC, `Gateway`, che crea un endpoint gateway per inviare traffico ad Amazon S3 o DynamoDB. Gli endpoint gateway non vengono utilizzati AWS PrivateLink, a differenza degli altri tipi di endpoint VPC. Per ulteriori informazioni, consulta the section called “Endpoint gateway”.

Interfacce di rete dell'endpoint

Un'interfaccia di rete endpoint è un'interfaccia di rete gestita dal richiedente che funge da punto di ingresso per il traffico destinato a un servizio, una risorsa o una rete di servizi endpoint. Per ciascuna sottorete specificata durante la creazione di un endpoint VPC, viene creata un'interfaccia di rete dell'endpoint nella sottorete.

Se un endpoint VPC lo supporta IPv4, le sue interfacce di rete endpoint hanno indirizzi. IPv4
Se un endpoint VPC lo supporta IPv6, le sue interfacce di rete endpoint hanno indirizzi. IPv6 L'

IPv6 indirizzo per un'interfaccia di rete endpoint non è raggiungibile da Internet. Quando descrivi un'interfaccia di rete endpoint con un IPv6 indirizzo, notate che è abilitato. `denyAllIgwTraffic`

Policy di endpoint

Una policy di endpoint VPC è una policy delle risorse IAM che è possibile allegare all'endpoint VPC. Determina quali principali possono utilizzare l'endpoint VPC per accedere al servizio endpoint. La policy di endpoint VPC predefinita consente tutte le azioni di tutti i principali su tutte le risorse dell'endpoint VPC.

Stati dell'endpoint

Quando si crea un endpoint VPC di interfaccia, il servizio endpoint riceve una richiesta di connessione. Il provider di servizi può accettare o rifiutare tale richiesta. Se il fornitore di servizi accetta la richiesta, l'utente del servizio può utilizzare l'endpoint VPC dopo che è entrato nello stato Available.

Di seguito sono riportati i possibili stati per un endpoint VPC:

- PendingAcceptance - La richiesta di connessione è in sospeso. Questo è lo stato iniziale se le richieste vengono accettate manualmente.
- In sospeso: il fornitore di servizi ha accettato la richiesta di connessione. Questo è lo stato iniziale se le richieste vengono accettate automaticamente. L'endpoint VPC torna in questo stato se l'utente del servizio modifica l'endpoint VPC.
- Disponibile: l'endpoint VPC è disponibile per l'uso.
- Rifiutata: il provider di servizi ha rifiutato la richiesta di connessione. Il provider di servizi può rifiutare una connessione anche dopo averla resa disponibile per l'uso.
- Scaduta: la richiesta di connessione è scaduta.
- Fallito: l'endpoint VPC non può essere reso disponibile.
- Eliminazione: l'utente del servizio ha eliminato l'endpoint VPC e l'eliminazione è in corso.
- Eliminato: l'endpoint VPC viene eliminato.

L' AWS PrivateLink API restituisce gli stati possibili utilizzando camel case.

AWS PrivateLink connessioni

Il traffico proveniente dal tuo VPC viene inviato a un servizio o a una risorsa endpoint utilizzando una connessione tra l'endpoint VPC e il servizio o la risorsa endpoint. Il traffico tra un endpoint VPC e un

servizio o una risorsa endpoint rimane all'interno della AWS rete, senza attraversare la rete Internet pubblica.

Un fornitore di servizi aggiunge le autorizzazioni in modo che gli utenti del servizio possano accedere al servizio endpoint. Gli utenti del servizio avviano la connessione e il provider di servizi accetta o rifiuta la richiesta di connessione. Il proprietario di una risorsa o di una rete di servizi condivide una configurazione di risorse o una rete di servizi con i consumatori AWS Resource Access Manager in modo che i consumatori possano accedere alla rete di risorse o servizi.

Con gli endpoint VPC di interfaccia, i consumatori possono utilizzare le policy degli endpoint per controllare quali responsabili IAM possono utilizzare un endpoint VPC per accedere a un servizio o una risorsa endpoint.

Zone ospitate private

Una zona ospitata è un container per i record DNS che definiscono il modo in cui instradare il traffico per un dominio o un sottodominio. Con una zona ospitata pubblica, i record specificano come instradare il traffico su Internet. Con una zona ospitata privata, i record specificano come indirizzare il traffico nella tua. VPCs

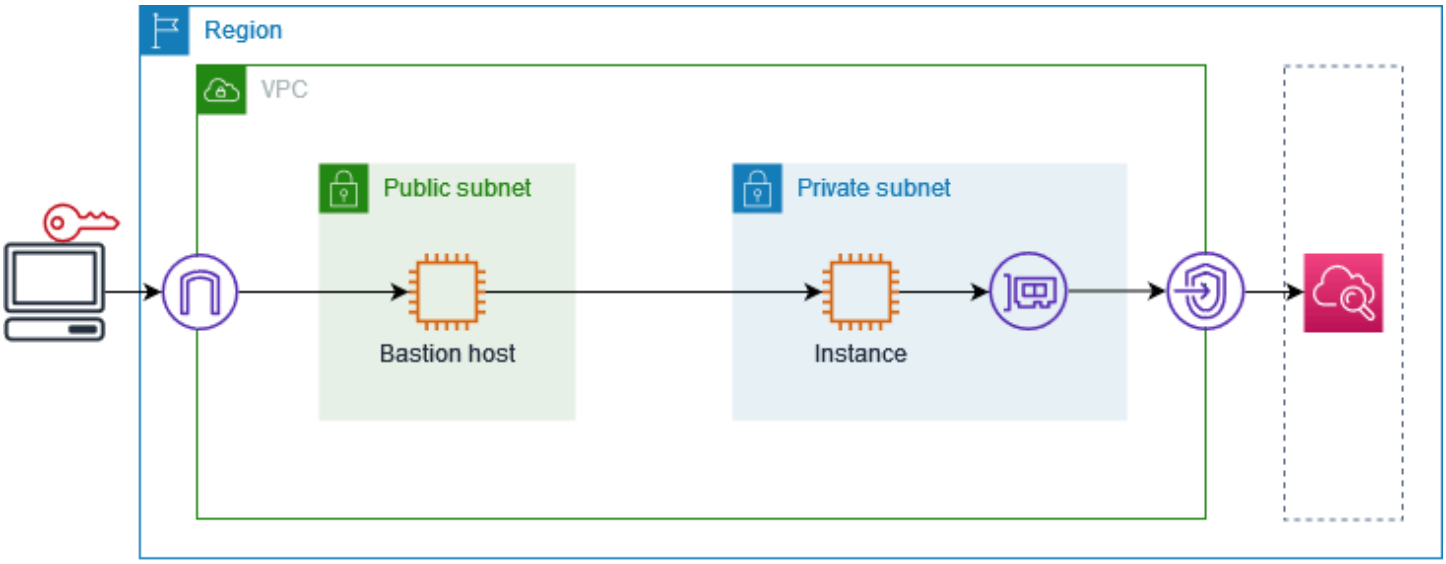
Puoi configurare Amazon Route 53 per instradare il traffico di dominio verso un endpoint VPC. Per ulteriori informazioni, consulta la pagina Routing del traffico a un endpoint VPC utilizzando il proprio nome dominio.

Puoi utilizzare Route 53 per configurare il DNS a orizzonte diviso, in cui utilizzi lo stesso nome di dominio sia per un sito Web pubblico che per un servizio endpoint fornito da. AWS PrivateLink Le richieste DNS per il nome host pubblico provenienti dal VPC dell'utente vengono gestite dagli indirizzi IP privati delle interfacce di rete dell'endpoint, mentre le richieste provenienti da un ambiente esterno al VPC continuano a essere risolte dagli endpoint pubblici. Per ulteriori informazioni, consulta la pagina Meccanismi DNS per instradare il traffico e abilitare il failover per le implementazioni AWS PrivateLink.

Inizia con AWS PrivateLink

Questo tutorial dimostra come inviare una richiesta da un' EC2 istanza in una sottorete privata ad Amazon CloudWatch utilizzando. AWS PrivateLink

Il diagramma seguente fornisce una panoramica di questo scenario. Per connetterti dal tuo computer all'istanza nella sottorete privata, devi prima connetterti a un host bastione in una sottorete pubblica. Sia l'host bastione che l'istanza devono utilizzare la stessa coppia di chiavi. Poiché il file `.pem` per la chiave privata si trova sul computer e non sull'host bastione, utilizzerai l'inoltro delle chiavi SSH. Quindi, puoi connetterti all'istanza dall'host bastione senza specificare il file `.pem` nel comando ssh. Dopo aver configurato un endpoint VPC per CloudWatch, il traffico proveniente dall'istanza a cui è destinato CloudWatch viene risolto nell'interfaccia di rete dell'endpoint e quindi inviato all'utilizzo CloudWatch dell'endpoint VPC.



A scopo di test, puoi utilizzare una singola zona di disponibilità. In produzione, ti consigliamo di utilizzare almeno due zone di disponibilità per assicurare una bassa latenza e una disponibilità elevata.

Attività

- Fase 1: creazione di un VPC con sottoreti
- Fase 2: avvio delle istanze
- Fase 3: Test di CloudWatch accesso
- Fase 4: Creare un endpoint VPC a cui accedere CloudWatch

Fase 1: creazione di un VPC con sottoreti

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.

Fase 2: avvio delle istanze

Utilizzando il VPC creato nella fase precedente, avvia l'host bastione nella sottorete pubblica e l'istanza nella sottorete privata.

Prerequisiti

- Crea una coppia di chiavi utilizzando il formato .pem. Quando avvii sia l'host bastione che l'istanza devi scegliere questa coppia di chiavi.
- Crea un gruppo di sicurezza per l'host bastione che consenta il traffico SSH in entrata dal blocco CIDR per il tuo computer.

- Crea un gruppo di sicurezza per l'istanza che consenta il traffico SSH in entrata dal gruppo di sicurezza per l'host bastione.
- Crea un profilo di istanza IAM e allega la policy. CloudWatchReadOnlyAccess

Per avviare l'host bastione

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Launch Instance (Avvia istanza).
3. Per Name (Nome) immetti un nome per l'host bastione.
4. Mantieni l'immagine e il tipo di istanza predefiniti.
5. In Key pair (Coppia di chiavi), seleziona quella desiderata.
6. In Network settings (Impostazioni di rete) effettua le seguenti operazioni:
    a. In VPC, seleziona il VPC.
    b. In Subnet (Sottorete), seleziona la sottorete pubblica.
    c. Per Auto-assign Public IP (Assegna automaticamente IP pubblico), scegli Enable (Abilita).
    d. Per Firewall, scegli Select existing security group (Seleziona gruppo di sicurezza esistente), quindi scegli il gruppo di sicurezza per l'host bastione.
7. Scegliere Launch Instance (Avvia istanza).

Per avviare l'istanza

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Launch Instance (Avvia istanza).
3. Per Name (Nome), inserisci un nome per l'istanza.
4. Mantieni l'immagine e il tipo di istanza predefiniti.
5. In Key pair (Coppia di chiavi), seleziona quella desiderata.
6. In Network settings (Impostazioni di rete) effettua le seguenti operazioni:
    a. In VPC, seleziona il VPC.
    b. In Subnet (Sottorete), scegli la sottorete privata.
    c. Per Auto-assign Public IP (Assegna automaticamente IP pubblico), scegli Disable (Disabilita).

d. Per Firewall, scegli Select existing security group (Seleziona gruppo di sicurezza esistente), quindi scegli il gruppo di sicurezza per l'istanza.

7. Espandi Advanced details (Dettagli avanzati). Per IAM instance profile (Profilo dell'istanza IAM), scegli il profilo dell'istanza IAM.
8. Scegliere Launch Instance (Avvia istanza).

Fase 3: Test di CloudWatch accesso

Utilizza la procedura seguente per confermare che l'istanza non può accedere CloudWatch. Lo farai utilizzando un AWS CLI comando di sola lettura per. CloudWatch

Per testare l'accesso CloudWatch

1. Dal tuo computer, aggiungi la key pair all'agente SSH usando il seguente comando, dove *key.pem* è il nome del tuo file.pem.

```
ssh-add ./key.pem
```

   Se ricevi un messaggio di errore che indica che le autorizzazioni per la coppia di chiavi sono troppo aperte, esegui il comando seguente e quindi riprova il comando precedente.

```
chmod 400 ./key.pem
```

2. Connettiti all'host bastione dal computer. Devi specificare l'opzione `-A`, il nome utente dell'istanza (ad esempio `ec2-user`) e l'indirizzo IP pubblico dell'host bastione.

```
ssh -A ec2-user@bastion-public-ip-address
```

3. Connettiti all'istanza dall'host bastione. È necessario specificare il nome utente dell'istanza (ad esempio `ec2-user`) e l'indirizzo IP privato dell'istanza.

```
ssh ec2-user@instance-private-ip-address
```

4. Esegui il comando CloudWatch list-metrics sull'istanza come segue. Per l'opzione `--region`, specifica la regione in cui hai creato il VPC.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

5. Dopo alcuni minuti, il comando scade. Ciò dimostra che non è possibile accedere CloudWatch dall'istanza con la configurazione VPC corrente.

```
Connect timeout on endpoint URL: https://monitoring.us-east-1.amazonaws.com/
```

6. Mantieni la connessione all'istanza. Dopo aver creato l'endpoint VPC, prova di nuovo questo comando list-metrics.

Fase 4: Creare un endpoint VPC a cui accedere CloudWatch

Utilizzare la procedura seguente per creare un endpoint VPC a cui connettersi. CloudWatch

Prerequisito

Crea un gruppo di sicurezza per l'endpoint VPC che consenta il traffico di. CloudWatch Ad esempio, aggiungi una regola che consenta il traffico HTTPS dal blocco CIDR del VPC.

Per creare un endpoint VPC per CloudWatch

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Per Name tag (Tag nome) immetti un nome per l'endpoint.
5. Per Service category (Categoria servizio), scegli Servizi AWS.
6. Per Assistenza, seleziona com.amazonaws. ***region***.monitoraggio.
7. In VPC, seleziona il tuo VPC.
8. In Subnets (Sottoreti), seleziona la zona di disponibilità e quindi seleziona la sottorete privata.
9. In Security group (Gruppo di sicurezza), seleziona il gruppo di sicurezza per l'endpoint VPC.
10. Per Policy, seleziona Full access (Accesso completo) per consentire tutte le operazioni da parte di tutti i principali su tutte le risorse dell'endpoint VPC.
11. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
12. Seleziona Crea endpoint. Lo stato iniziale è Pending (In sospeso). Prima di passare alla fase successiva, attendi che lo stato sia Available (Disponibile). Ciò può richiedere alcuni minuti.

Fase 5: test dell'endpoint VPC

Verifica che l'endpoint VPC stia inviando richieste dalla tua istanza a. CloudWatch

Per testare l'endpoint VPC

Eseguire il seguente comando sull'istanza. Per l'opzione `--region`, specifica la regione in cui hai creato l'endpoint VPC.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

Se ricevi una risposta, anche se con risultati vuoti, sei connesso all' CloudWatch utilizzo. AWS PrivateLink

Se ricevi un `UnauthorizedOperation` errore, assicurati che l'istanza abbia un ruolo IAM che consenta l'accesso a CloudWatch.

Se la richiesta scade, verifica quanto segue:

- Il gruppo di sicurezza per l'endpoint consente al CloudWatch traffico di.
- L'opzione `--region` specifica la regione in cui è stato creato l'endpoint VPC.

Fase 6: pulizia

Se non hai più bisogno dell'host bastione e dell'istanza creati per questo tutorial, puoi terminarli.

Per terminare le istanze

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Instance state (Stato istanza), Terminate instance (Termina istanza).
4. Quando viene richiesta la conferma, seleziona Terminate (Termina).

Se un endpoint VPC non è più necessario, puoi eliminarlo.

Per eliminare l'endpoint VPC

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

2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint VPC.
4. Seleziona Actions (Operazioni), Delete VPC endpoints (Eliminazione di endpoint VPC).
5. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Accesso tramite Servizi AWSAWS PrivateLink

Si accede e Servizio AWS si utilizza un endpoint. Gli endpoint del servizio predefiniti sono interfacce pubbliche, quindi è necessario aggiungere un gateway Internet al VPC in modo che il traffico possa passare dal VPC al Servizio AWS. Se questa configurazione non soddisfa i tuoi requisiti di sicurezza di rete, puoi usarla AWS PrivateLink per connettere i tuoi VPC Servizi AWS come se fossero nel tuo VPC, senza l'uso di un gateway Internet.

Puoi accedere privatamente agli endpoint Servizi AWS che si integrano con AWS PrivateLink l'utilizzo di VPC. Puoi creare e gestire tutti i livelli dello stack di applicazioni senza utilizzare un gateway Internet.

Prezzi

Ti viene fatturata ogni ora di provisioning dell'endpoint VPC di interfaccia in ciascuna zona di disponibilità. Ti viene inoltre addebitato un importo per GB di dati elaborati. Per ulteriori informazioni, consultare AWS PrivateLink Prezzi.

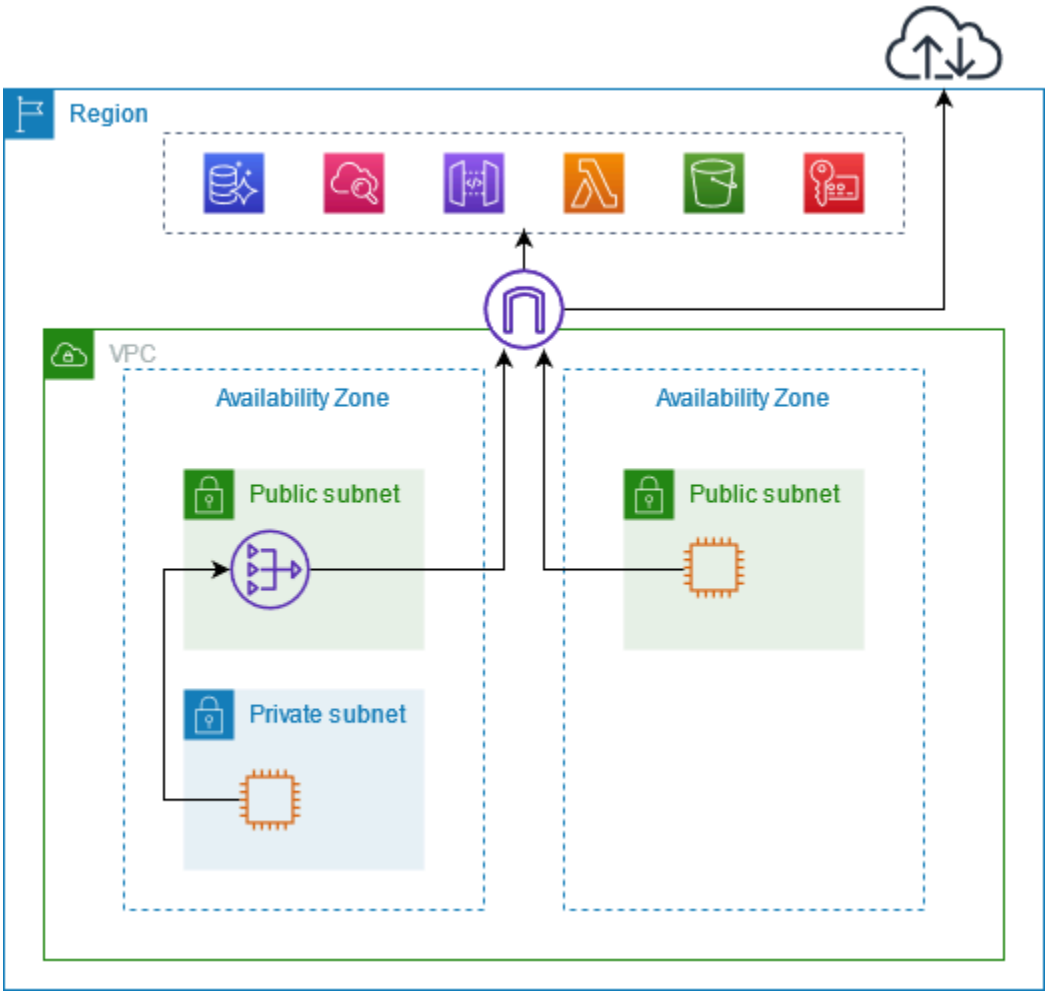
Indice

Panoramica

Puoi accedere Servizi AWS tramite i loro endpoint di servizio pubblico o connetterti agli utenti supportati Servizi AWS . AWS PrivateLink Questa panoramica mette a confronto i due metodi.

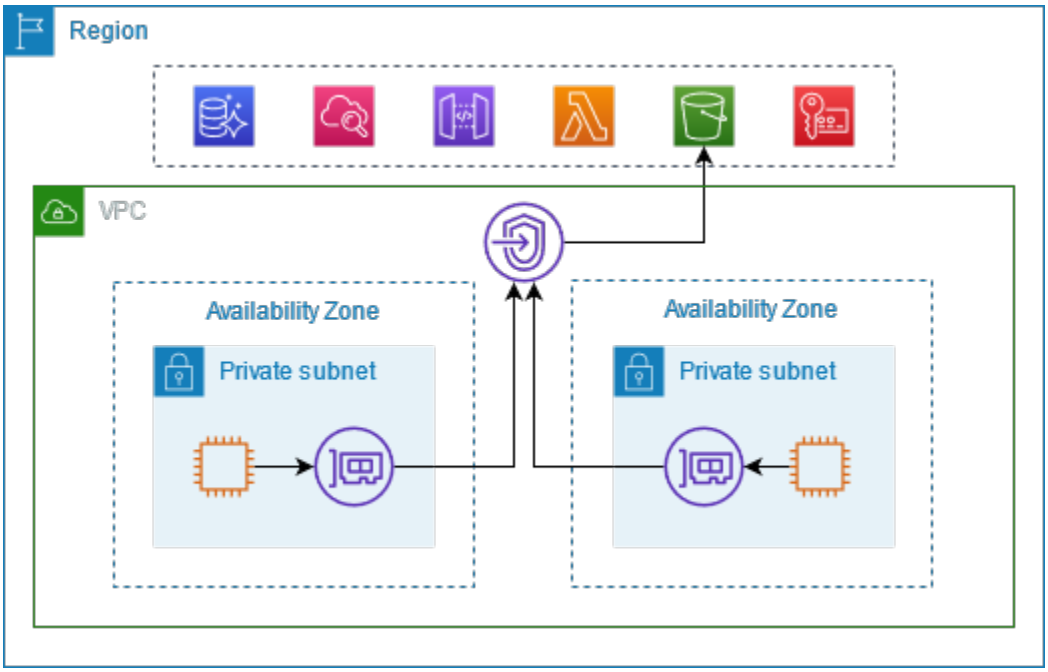
Accesso tramite endpoint del servizio pubblico

Il diagramma seguente mostra come le istanze accedono Servizi AWS tramite gli endpoint del servizio pubblico. Il traffico Servizio AWS da e verso un'istanza in una sottorete pubblica viene indirizzato al gateway Internet per il VPC e quindi a. Servizio AWS Il traffico verso un Servizio AWS da un'istanza presente in una sottorete privata viene instradato a un gateway NAT, poi al gateway Internet del VPC e infine ad Servizio AWS. Sebbene questo traffico attraversi il gateway Internet, non esce dalla rete. AWS



Connect tramite AWS PrivateLink

Il diagramma seguente mostra come le istanze accedono tramite Servizi AWS . AWS PrivateLink Innanzitutto, crei un endpoint VPC di interfaccia, che stabilisce connessioni tra le sottoreti del tuo VPC e un'interfaccia di rete che utilizza. Servizio AWS Il traffico destinato a Servizio AWS viene risolto negli indirizzi IP privati delle interfacce di rete degli endpoint utilizzando DNS e quindi inviato Servizio AWS utilizzando la connessione tra l'endpoint VPC e il. Servizio AWS



Servizi AWS accetta automaticamente le richieste di connessione. Il servizio non può avviare richieste alle risorse tramite l'endpoint VPC.

Hostname DNS

La maggior parte Servizi AWS offre endpoint regionali pubblici, che hanno la seguente sintassi.

```
protocol://service_code.region_code.amazonaws.com
```

Ad esempio, l'endpoint pubblico per Amazon CloudWatch in us-east-2 è il seguente.

```
https://monitoring.us-east-2.amazonaws.com
```

Con AWS PrivateLink, invii traffico al servizio utilizzando endpoint privati. Quando crei un endpoint VPC di interfaccia, creiamo nomi DNS regionali e zonali che puoi usare per comunicare con il tuo VPC. Servizio AWS

Il nome DNS regionale per l'endpoint VPC dell'interfaccia presenta la sintassi seguente:

```
endpoint_id.service_id.region.vpce.amazonaws.com
```

I nomi DNS zonali sono caratterizzati dalla sintassi seguente:

```
endpoint_id-az_name.service_id.region.vpce.amazonaws.com
```

Quando crei un endpoint VPC di interfaccia per un Servizio AWS, puoi abilitare il DNS privato. Con il DNS privato, puoi continuare a effettuare richieste a un servizio utilizzando il nome DNS per il relativo endpoint pubblico, sfruttando al contempo la connettività privata tramite l'endpoint VPC dell'interfaccia. Per ulteriori informazioni, consulta the section called “Risoluzione DNS”.

Il describe-vpc-endpointscomando seguente visualizza le voci DNS per un endpoint di interfaccia.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-id vpce-099deb00b40f00e22 --query
 VpcEndpoints[*].DnsEntries
```

Di seguito è riportato un esempio di output per un endpoint di interfaccia per Amazon CloudWatch con nomi DNS privati abilitati. La prima voce è costituita dall'endpoint regionale privato. Le tre voci successive sono gli endpoint zonali privati. L'ultima voce rappresenta la zona ospitata privata nascosta, che risolve le richieste dell'endpoint pubblico agli indirizzi IP privati delle interfacce di rete dell'endpoint.

```
[
    [
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2c.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2a.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
```

```
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2b.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "monitoring.us-east-2.amazonaws.com",
            "HostedZoneId": "Z06320943MMOWYG6MAVL9"
        }
    ]
]
```

Risoluzione DNS

I record DNS creati per l'endpoint VPC dell'interfaccia sono pubblici. Pertanto, questi nomi DNS sono risolvibili pubblicamente. Le richieste DNS provenienti dall'esterno del VPC, tuttavia, continuano a restituire gli indirizzi IP privati delle interfacce di rete dell'endpoint. Di conseguenza, non è possibile utilizzare questi indirizzi IP per accedere al servizio endpoint, a meno che non si abbia accesso al VPC.

DNS privato

Se abiliti il DNS privato per il tuo endpoint VPC di interfaccia e il tuo VPC ha sia i nomi host DNS che la risoluzione DNS abilitati, creiamo per te una zona ospitata privata nascosta e gestita. AWS La zona ospitata contiene un set di record per il nome DNS predefinito per il servizio che si risolve negli indirizzi IP privati delle interfacce di rete dell'endpoint nel VPC. Pertanto, se disponi di applicazioni esistenti che inviano richieste a un endpoint regionale pubblico, tali richieste ora passano attraverso le interfacce di rete degli endpoint, senza che sia necessario apportare modifiche a tali applicazioni. Servizio AWS

Ti consigliamo di abilitare nomi host DNS privati per gli endpoint VPC per Servizi AWS. Ciò garantisce che le richieste che utilizzano gli endpoint del servizio pubblico, come le richieste effettuate tramite un AWS SDK, vengano risolte sull'endpoint VPC.

Amazon fornisce un server DNS per il tuo VPC chiamato il Route 53 Resolver. Il Route 53 Resolver risolve automaticamente i nomi di dominio VPC locali e i record in zone ospitate private. Tuttavia, non puoi utilizzare il Route 53 Resolver dall'esterno del tuo VPC. Se desideri accedere al tuo

endpoint VPC dalla rete on-premise, puoi utilizzare gli endpoint del Route 53 Resolver e le regole del resolver. Per ulteriori informazioni, consulta Integrazione con and. AWS Transit GatewayAWS PrivateLinkAmazon Route 53 Resolver

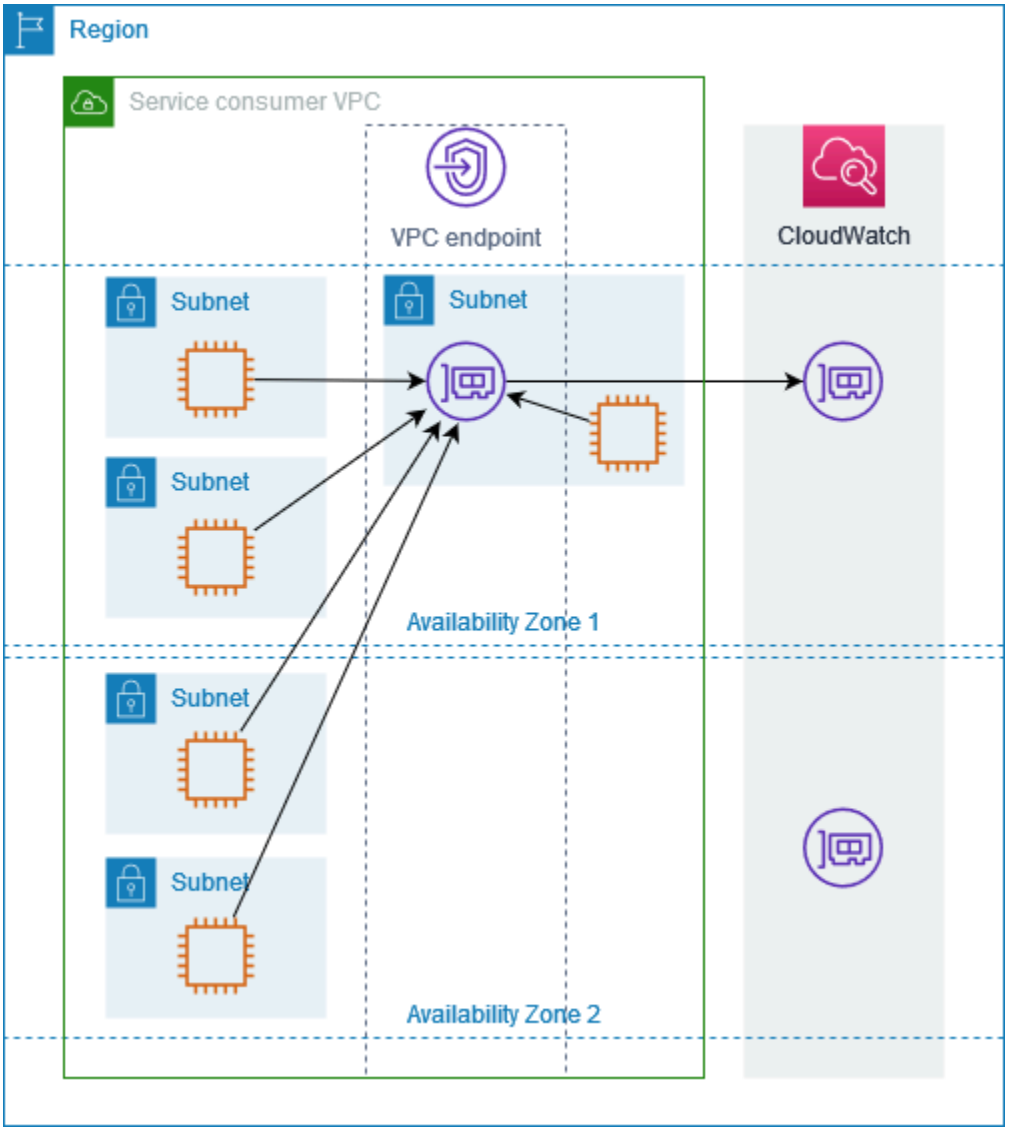
Sottoreti e zone di disponibilità

Puoi configurare l'endpoint VPC con una sottorete per zona di disponibilità. Nella sottorete, viene creata un'interfaccia di rete dell'endpoint per l'endpoint VPC. Vengono assegnati indirizzi IP a ogni interfaccia di rete dell'endpoint dalla relativa sottorete, in base al tipo di indirizzo IP dell'endpoint VPC. Gli indirizzi IP di un'interfaccia di rete dell'endpoint non cambieranno durante la durata del relativo endpoint VPC.

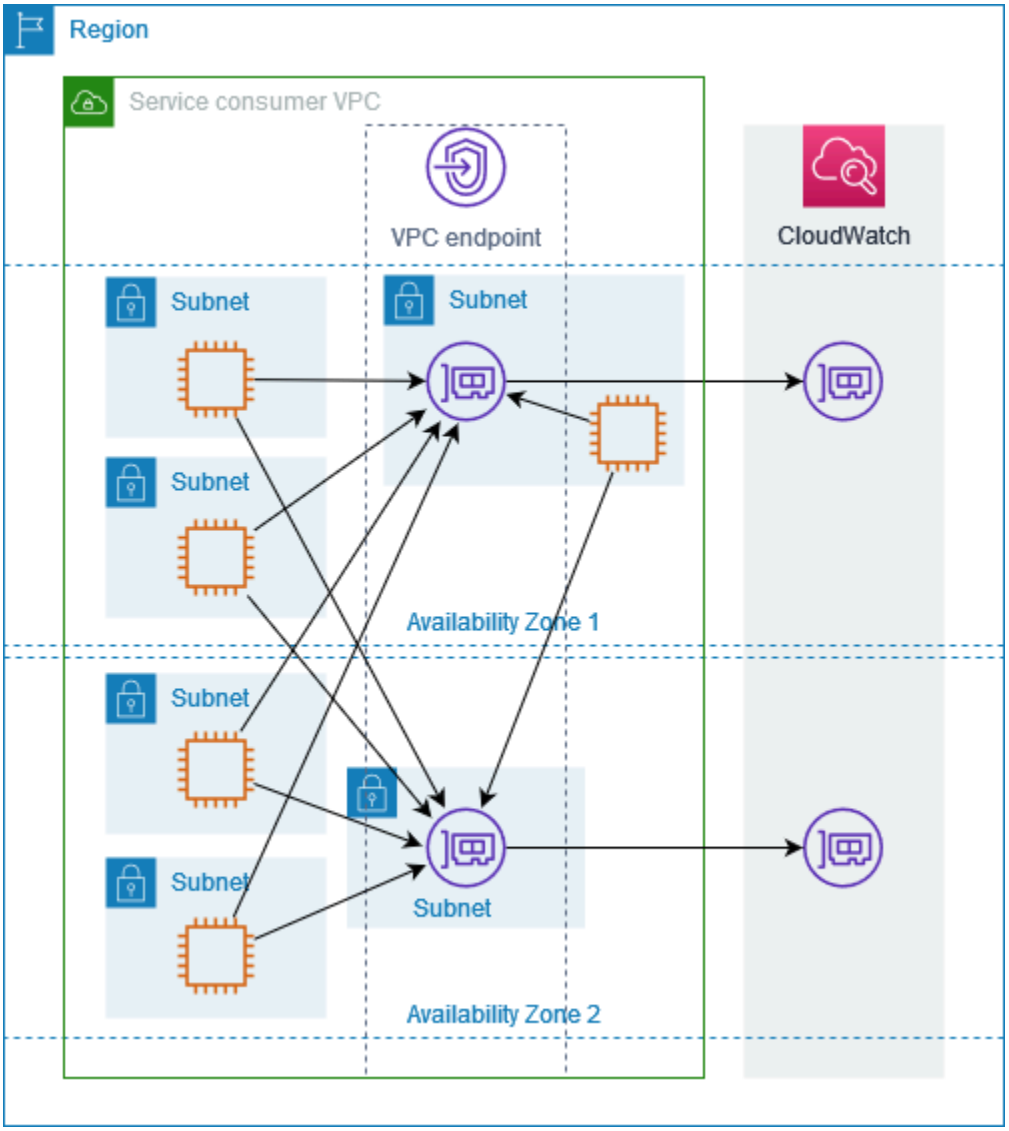
In un ambiente di produzione, per un'elevata disponibilità e resilienza, consigliamo quanto segue:

- Configura almeno due zone di disponibilità per endpoint VPC e distribuisci AWS le risorse che devono accedervi Servizio AWS in queste zone di disponibilità.
- Configura i nomi DNS privati per l'endpoint VPC.
- Accedi a Servizio AWS utilizzando il suo nome DNS regionale, noto anche come endpoint pubblico.

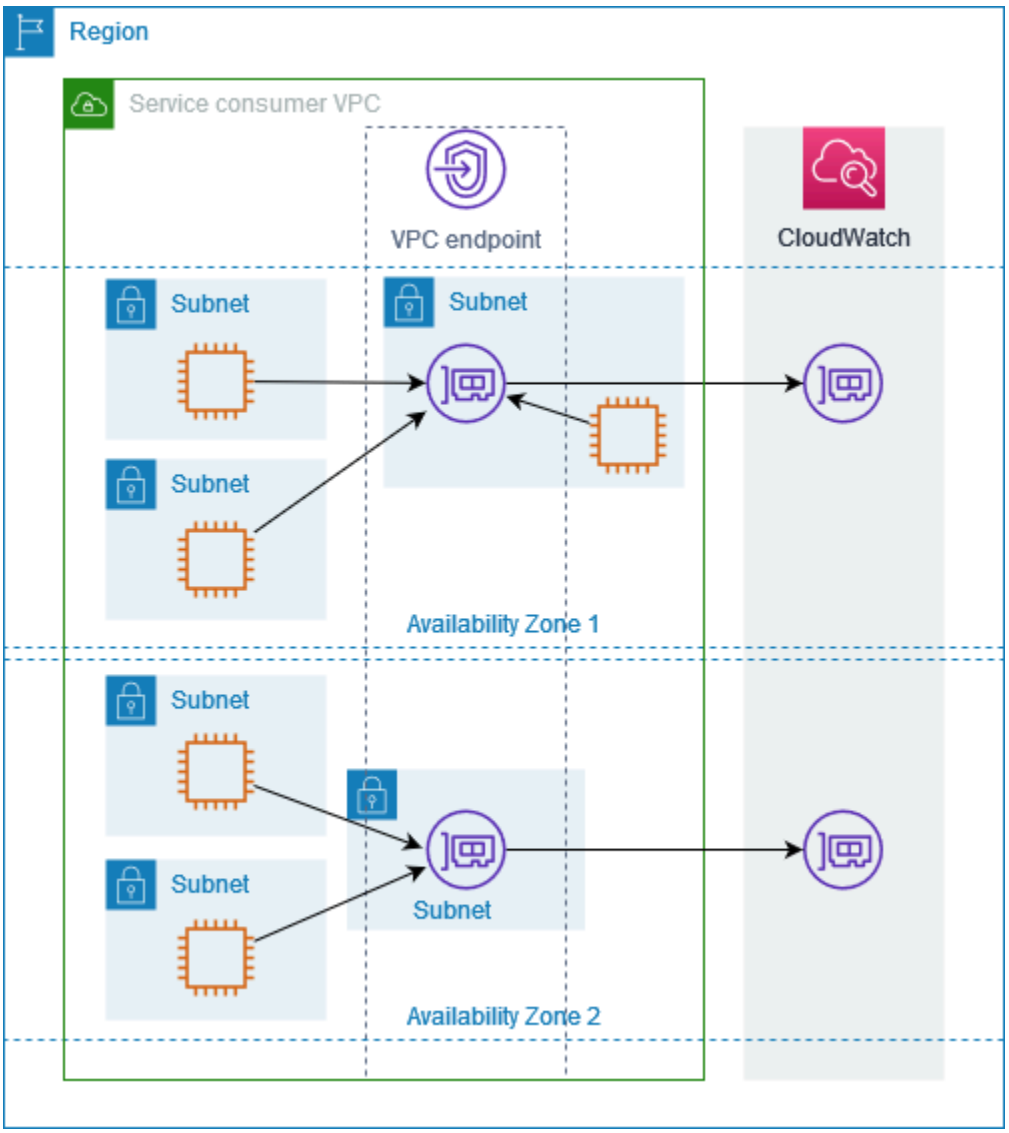
Il diagramma seguente mostra un endpoint VPC per CloudWatch Amazon con un'interfaccia di rete endpoint in un'unica zona di disponibilità. Quando una risorsa in qualsiasi sottorete del VPC accede ad CloudWatch Amazon utilizzando il suo endpoint pubblico, risolviamo il traffico all'indirizzo IP dell'interfaccia di rete dell'endpoint. Include il traffico proveniente da sottoreti in altre zone di disponibilità. Tuttavia, se la Zona di disponibilità 1 è compromessa, le risorse nella Zona di disponibilità 2 perdono l'accesso ad Amazon CloudWatch.



Il diagramma seguente mostra un endpoint VPC per CloudWatch Amazon con interfacce di rete endpoint in due zone di disponibilità. Quando una risorsa in qualsiasi sottorete del VPC accede ad CloudWatch Amazon utilizzando il suo endpoint pubblico, selezioniamo un'interfaccia di rete endpoint sana, utilizzando l'algoritmo round robin per alternarle. Quindi trasferiamo il traffico verso l'indirizzo IP dell'interfaccia di rete dell'endpoint selezionata.



Se è più adatto al tuo caso d'uso, puoi inviare traffico al Servizio AWS dalle tue risorse utilizzando l'interfaccia di rete dell'endpoint nella stessa zona di disponibilità. A tale scopo, utilizza l'endpoint zonale privato o l'indirizzo IP dell'interfaccia di rete dell'endpoint.



Tipi di indirizzi IP

Servizi AWS possono supportare IPv6 tramite i propri endpoint privati anche se non lo fanno tramite i propri endpoint pubblici. IPv6 Gli endpoint che lo supportano IPv6 possono rispondere alle query DNS con record AAAA.

Requisiti da abilitare per un endpoint di interfaccia IPv6

- Servizio AWS Deve rendere disponibili i propri endpoint di servizio su. IPv6 Per ulteriori informazioni, consulta the section called “Visualizza IPv6 il supporto”.
- Il tipo di indirizzo IP di un endpoint dell'interfaccia deve essere compatibile con le sottoreti dell'endpoint dell'interfaccia, come descritto di seguito:

- IPv4— Assegna IPv4 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate hanno intervalli di indirizzi. IPv4
- IPv6— Assegna IPv6 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono solo sottoreti. IPv6
- Dualstack: assegna entrambi IPv4 gli indirizzi alle interfacce di rete degli endpoint. IPv6 Questa opzione è supportata solo se tutte le sottoreti selezionate hanno entrambi gli intervalli di indirizzi. IPv4 IPv6

Se l'interfaccia è supportata da un endpoint VPC IPv4, le interfacce di rete degli endpoint dispongono di indirizzi. IPv4 Se l'interfaccia è supportata da un endpoint VPC IPv6, le interfacce di rete degli endpoint dispongono di indirizzi. IPv6 L' IPv6 indirizzo per un'interfaccia di rete endpoint non è raggiungibile da Internet. Se descrivi un'interfaccia di rete endpoint con un IPv6 indirizzo, nota che è abilitata. `denyAllIgwTraffic`

Tipo di IP del record DNS

A seconda del tipo di indirizzo IP, quando si chiama un endpoint VPC, il AWS servizio può restituire record A, record AAAA o entrambi i record A e AAAA. È possibile personalizzare i tipi di record restituiti dal AWS servizio modificando il tipo IP del record DNS. La tabella seguente mostra i tipi di IP dei record DNS supportati e i tipi di record restituiti:

Tipo IP di record DNS	Tipi di record restituiti
IPv4	A
IPv6	AAAA
Dualstack	A e AAAA

Per impostazione predefinita, il tipo di record DNS è lo stesso del tipo di indirizzo IP. È possibile scegliere un tipo di IP di record DNS diverso, ma è necessario utilizzare un tipo di indirizzo IP compatibile per il servizio endpoint. La tabella seguente mostra il tipo IP di record DNS supportato per ogni tipo di indirizzo IP per gli endpoint di interfaccia:

Tipo di indirizzo IP	Tipi di IP di record DNS supportati
IPv4	IPv4
IPv6	IPv6
Dualstack	Dualstack*,, definito dal servizio IPv4 IPv6

* Rappresenta il tipo IP di record DNS predefinito.

Un tipo IP di record DNS definito dal servizio restituisce i record DNS in base all'endpoint del servizio chiamato. Se utilizzi un tipo di IP di record DNS definito dal servizio, assicurati che il servizio sia in grado di gestire chiamate variabili dagli endpoint del servizio. Per visualizzare i record DNS supportati dall'endpoint di interfaccia, consulta i nomi DNS del tuo endpoint VPC in, o use. Console di gestione AWSDescribeVpcEndpoints

Il comportamento del tipo IP del record DNS è diverso per gli endpoint gateway. Per ulteriori informazioni, consulta Tipo di IP del record DNS per gli endpoint del gateway.

Servizi AWS che si integrano con AWS PrivateLink

Quanto segue si Servizi AWS integra con AWS PrivateLink. Puoi creare un endpoint VPC per connetterti a questi servizi in privato, come se fossero in esecuzione nel tuo VPC.

Scegli il link nella Servizio AWScolonna per visualizzare la documentazione relativa ai servizi che si integrano con AWS PrivateLink. La colonna Service name contiene il nome del servizio specificato quando si crea l'endpoint VPC di interfaccia o indica che il servizio gestisce l'endpoint.

Servizio AWS	Nome servizio
Gestione dell'account AWS	com.amazonaws. *region*.account
Gateway Amazon API	com.amazonaws. *region*.execute-api
	com.amazonaws. *region*. un gateway API
AWS AppConfig	com.amazonaws. *region*.app config
	com.amazonaws. *region*.appconfig-fips

Servizio AWS	Nome servizio
com.amazonaws. *region*.appconfigdata	
com.amazonaws. *region*.appconfigdata-fips	
AWS App Mesh	com.amazonaws. *region*.app mesh
	com.amazonaws. *region*. appmesh-envoy-management
AWS App Runner	com.amazonaws. *region*.app runner
Servizi AWS App Runner	com.amazonaws. *region*.apprunner.richieste
Application Auto Scaling	com.amazonaws. *region*.scalabilità automatica delle applicazioni
AWS Application Discovery Service	com.amazonaws. *region*.scoperta
	com.amazonaws. *region*.scoperta dell'arsenale
AWS Servizio di migrazione delle applicazioni	com.amazonaws. *region*.mgn
WorkSpaces Applicazioni Amazon	com.amazonaws. *region*.appstream. api
	com.amazonaws. *region*.appstream. streaming
AWS AppSync	com.amazonaws. *region*.appsync-api
Amazon Athena	com.amazonaws. *region*.atena
AWS Audit Manager	com.amazonaws. *region*. gestore di audit
Amazon Aurora	com.amazonaws. *region*.rds
	com.amazonaws. *region*.rds-fips
Amazon Aurora DSQL	com.amazonaws. *region*.dsql

Servizio AWS	Nome servizio
AWS Auto Scaling	com.amazonaws. *region*.piani di scalabilità automatica
AWS Scambio di dati B2B	com.amazonaws. *region*.b2bi
AWS Backup	com.amazonaws. *region*.backup
	com.amazonaws. *region*.gateway di backup
AWS Batch	com.amazonaws. *region*.batch
Amazon Bedrock	com.amazonaws. *region*.substrato roccioso
	com.amazonaws. *region*.agente bedrock
	com.amazonaws. *region*. bedrock-agent-runtime
	com.amazonaws. *region*. bedrock-data-automation
	com.amazonaws. *region*. bedrock-data-automation-fips
	com.amazonaws. *region*. bedrock-data-automation-runtime
	com.amazonaws. *region*. bedrock-data-automation-runtime-fips
	com.amazonaws. *region*.bedrock-runtime
Gestione dei costi e fatturazione AWS	com.amazonaws. *region*.fatturazione
	com.amazonaws. *region*.livello gratuito
	com.amazonaws. *region*.tassa
AWS Billing Conductor	com.amazonaws. *region*. addetto alla fatturazione
Amazon Braket	com.amazonaws. *region*.staffa
AWS Certificate Manager	com.amazonaws.it. *region*.cam

Servizio AWS	Nome servizio
	com.amazonaws. *region*.acm-fips
AWS Clean Rooms	com.amazonaws. *region*. camere pulite
	com.amazonaws. *region*.camere pulite - fips
AWS Camere pulite ML	com.amazonaws. *region*.camere pulite - ml
AWS Cloud Control API	com.amazonaws. *region*.cloudcontrol api
	com.amazonaws. *region*.cloudcontrolapi-fips
Directory del cloud Amazon	com.amazonaws. *region*.directory cloud
AWS CloudFormation	com.amazonaws. *region*. formazione di nuvole
	com.amazonaws. *region*.cloudformation-fips
AWS CloudHSM	com.amazonaws. *region*.cloudhsmv2
AWS Cloud Map	com.amazonaws. *region*.servicediscovery
	com.amazonaws. *region*.servicediscovery-fips
	com.amazonaws. *region*.data-service discovery
	com.amazonaws. *region*. data-servicediscovery-fips
AWS CloudTrail	com.amazonaws. *region*.cloudtrail
AWS WAN nel cloud	com.amazonaws. *region*. gestore di rete
Amazon CloudWatch	com.amazonaws. *region*.segnali applicativi
	com.amazonaws. *region*. approfondimenti sulle applicazioni
	com.amazonaws. *region*. monitor internet
	com.amazonaws. *region*.internetmonitor-fips

Servizio AWS	Nome servizio
	com.amazonaws. *region*.monitoraggio
	com.amazonaws. *region*. monitor del flusso di rete
	com.amazonaws. *region*.report di monitoraggio del flusso di rete
	com.amazonaws. *region*.monitor di rete
	com.amazonaws. *region*.observabilityadmin
	com.amazonaws. *region*.rum
	com.amazonaws. *region*.rum-dataplane
	com.amazonaws. *region*.sintetici
	com.amazonaws. *region*.synthetics-fips
	com.amazonaws. *region*.oam
CloudWatch Registri Amazon	com.amazonaws.it. *region*.registri
AWS CodeArtifact	com.amazonaws. *region*.codeartifact.api
	com.amazonaws. *region*.codeartifact.repository
AWS CodeBuild	com.amazonaws. *region*.codebuild
	com.amazonaws. *region*.codebuild-fips
AWS CodeCommit	com.amazonaws. *region*.codecommit
	com.amazonaws. *region*.codecommit-fips
	com.amazonaws. *region*.git-codecommit
	com.amazonaws. *region*. git-codecommit-fips
AWS CodeConnections	com.amazonaws. *region*.codeconnections.api

Servizio AWS	Nome servizio
	com.amazonaws. *region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws. *region*.codedeploy
	com.amazonaws. *region*. codedeploy-commands-secure
	com.amazonaws. *region*.codedeploy-fips
Amazon CodeGuru Profiler	com.amazonaws. *region*.codeguru-profiler
CodeGuru Revisore Amazon	com.amazonaws. *region*.codeguru-revisore
AWS CodePipeline	com.amazonaws. *region*.codepipeline
Amazon Comprehend	com.amazonaws. *region*. comprendere
Amazon Comprehend Medical	com.amazonaws. *region*. comprende la medicina
AWS Compute Optimizer	com.amazonaws. *region*.ottimizzatore per computer
AWS Config	com.amazonaws. *region*.config
	com.amazonaws.it. *region*.config-fips
Amazon Connect	com.amazonaws. *region*.app - integrazioni
	com.amazonaws. *region*.casi
	com.amazonaws. *region*campagne.connect
	com.amazonaws. *region*.profilo
	com.amazonaws. *region*.voiceid
	com.amazonaws. *region*.saggezza
AWS Connector Service	com.amazonaws. *region*.connettore aws
Catalogo di controllo AWS	com.amazonaws. *region*.control catalog

Servizio AWS	Nome servizio
AWS Cost Explorer	com.amazonaws. *region*.ce
Centrale ottimizzazione costi AWS	com.amazonaws. *region*. cost-optimization-hub
AWS Control Tower	com.amazonaws. *region*. torre di controllo
	com.amazonaws. *region*.controltower-fips
AWS Data Exchange	com.amazonaws. *region*. scambio di dati
Esportazioni di dati AWS	aws.api. *region*. bcm-data-exports
	com.amazonaws. *region*. bcm-pricing-calculator
Amazon Data Firehose	com.amazonaws. *region*.kinesis-firehose
Amazon Data Lifecycle Manager	com.amazonaws. *region*.dlm
	com.amazonaws. *region*.dlm-fips
AWS Database Migration Service	com.amazonaws. *region*.dms
	com.amazonaws. *region*.dms-fips
AWS DataSync	com.amazonaws. *region*.datasync
Amazon DataZone	com.amazonaws. *region*.zona dati
	com.amazonaws. *region*.datazone-fips
AWS Deadline Cloud	com.amazonaws. *region*.deadline.gestione
	com.amazonaws. *region*.deadline.schedulazione
Amazon Detective	com.amazonaws. *region*.investigatore
	com.amazonaws. *region*.detective-fips
Amazon DevOps Guru	com.amazonaws. *region*.devops-guru

Servizio AWS	Nome servizio
AWS Direct Connect	com.amazonaws. *region*. connessione diretta
	com.amazonaws. *region*.directconnect-fips
AWS Directory Service	com.amazonaws. *region*.ds
	com.amazonaws. *region*.ds-dati
	com.amazonaws. *region*. ds-data-fips
Amazon DocumentDB	com.amazonaws. *region*.rds
Amazon DynamoDB	com.amazonaws.it. *region*.dinamodb
	com.amazonaws. *region*.dynamodb-fips
	com.amazonaws. *region*.dynamodb-stream
Amazon EBS diretto APIs	com.amazonaws. *region*.ebs
	com.amazonaws. *region*.ebs-fips
Amazon EC2	com.amazonaws. *region*.ec2
	com.amazonaws. *region*.ec2-fips
Amazon EC2 Auto Scaling	com.amazonaws. *region*.scalabilità automatica
	com.amazonaws. *region*.autoscaling-fips
EC2 Image Builder	com.amazonaws. *region*.generatore di immagini
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
Amazon ECS	com.amazonaws. *region*.ecs
	com.amazonaws.it. *region*.agente ecs

Servizio AWS	Nome servizio
	com.amazonaws. *region*.ecs-telemetria
Amazon EKS	com.amazonaws. *region*.eks
	com.amazonaws. *region*.eks-auth
	com.amazonaws. *region*.eks-fips
	com.amazonaws. *region*.eks-proxy
AWS Elastic Beanstalk	com.amazonaws. *region*. elasticbeanstalk
	com.amazonaws. *region*. elasticbeanstalk-health
AWS Elastic Disaster Recovery	com.amazonaws. *region*.drs
Amazon Elastic File System	com.amazonaws. *region*.filesystem elastico
	com.amazonaws. *region*.elasticfilesystem-fips
Elastic Load Balancing	com.amazonaws. *region*. bilanciamento elastico del carico
VMware Servizio Amazon Elastic	com.amazonaws. *region*.evs
	com.amazonaws. *region*.evs-fips
Amazon ElastiCache	com.amazonaws. *region*. dolore elastico
	com.amazonaws. *region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws. *region*.mediaconnect
AWS Elemental MediaConvert	com.amazonaws. *region*.mediaconvert
	com.amazonaws. *region*.mediaconvert-fips
Amazon EMR	com.amazonaws. *region*. elasticmapreduce
	com.amazonaws. *region*. elasticmapreduce-fips

Servizio AWS	Nome servizio
Amazon EMR su EKS	com.amazonaws. *region*.emr-container
Amazon EMR Serverless	com.amazonaws. *region*.emr senza server
	com.amazonaws. *region*. emr-serverless-services.livido
	com.amazonaws. *region*.emr-serverless.dashboard
Amazon EMR WAL	com.amazonaws. *region*.emrwal.prod
AWS Messaggistica sociale per utenti finali	com.amazonaws. *region*.messaggistica sociale
	com.amazonaws. *region*. social-messaging-fips
AWS Entity Resolution	com.amazonaws. *region*.risoluzione dell'entità
	com.amazonaws. *region*.entityresolution-fips
Amazon EventBridge	com.amazonaws. *region*.eventi
	com.amazonaws. *region*.eventi-fips
	com.amazonaws. *region*.tubi
	com.amazonaws.it. *region*.pipes-dati
	com.amazonaws. *region*.pipes-fips
	com.amazonaws. *region*.schemi
Amazon EventBridge Scheduler	com.amazonaws.it. *region*.scheduler
AWS Fault Injection Service	com.amazonaws. *region*.fis
	com.amazonaws. *region*.fis-fips
Amazon FinSpace	com.amazonaws. *region*.finspace
	com.amazonaws. *region*.finspace-api

Servizio AWS	Nome servizio
AWS Firewall Manager	com.amazonaws. *region*.fms
	com.amazonaws. *region*.fms-fips
Amazon Forecast	com.amazonaws. *region*.previsione
	com.amazonaws. *region*.query di previsione
	com.amazonaws. *region*.forecast-fips
	com.amazonaws. *region*. forecastquery-fips
Amazon Fraud Detector	com.amazonaws. *region*.rilevatore di frodi
Amazon FSx	com.amazonaws. *region*.fsx
	com.amazonaws. *region*.fsx-fips
GameLift Server Amazon	com.amazonaws.it. *region*.gamelift
Amazon GameLift Stream	com.amazonaws. *region*.gameliftstream
Reti globali AWS per gateway di transito	com.amazonaws. *region*. gestore di rete
AWS Glue	com.amazonaws. *region*.colla
	com.amazonaws. *region*.colla. dashboard
AWS Glue DataBrew	com.amazonaws. *region*.databrew
	com.amazonaws. *region*.databrew-fips
Grafana gestito da Amazon	com.amazonaws. *region*.grafana
	com.amazonaws. *region*.grafana - spazio di lavoro
AWS Ground Station	com.amazonaws. *region*. stazione di terra
	com.amazonaws. *region*.groundstation-fips

Servizio AWS	Nome servizio
Amazon GuardDuty	com.amazonaws. *region*.servizio di guardia
	com.amazonaws. *region*.guardduty-data
	com.amazonaws. *region*. guardduty-data-fips
	com.amazonaws. *region*.guardduty-fips
AWS HealthImaging	com.amazonaws. *region*. dicom-medical-imaging
	com.amazonaws. *region*.diagnostica per immagini
	com.amazonaws. *region*. runtime-medical-imaging
AWS HealthLake	com.amazonaws. *region*.salutelake
AWS HealthOmics	com.amazonaws. *region*.analisi-omics
	com.amazonaws. *region*. analytics-omics-fips
	com.amazonaws. *region*. control-storage-omics
	com.amazonaws. *region*. control-storage-omics-fips
	com.amazonaws. *region*.storage-omics
	com.amazonaws. *region*.tag-omics
	com.amazonaws. *region*. tags-omics-fips
	com.amazonaws. *region*.workflows-omics
	com.amazonaws. *region*. workflows-omics-fips
AWS Identity and Access Management (IAM)	com.amazonaws.iam
Sistema di analisi degli accessi IAM	com.amazonaws.it. *region*.analizzatore di accesso
	com.amazonaws. *region*. access-analyzer-fips

Servizio AWS	Nome servizio
Centro identità IAM	com.amazonaws. *region*. negozio di identità
IAM Roles Anywhere	com.amazonaws. *region*. ruoli ovunque
	com.amazonaws. *region*.rolesanywhere-fips
Amazon Inspector	com.amazonaws. *region*.ispettore 2
	com.amazonaws. *region*.ispector 2 fips
	com.amazonaws. *region*.inspector-scan
	com.amazonaws. *region*. inspector-scan-fips
Amazon Interactive Video Service	com.amazonaws. *region*.ivs.contribuisci
AWS IoT Core	com.amazonaws. *region*.iot.api
	com.amazonaws. *region*.iot-fips.api
	com.amazonaws. *region*.iot.dati
	com.amazonaws. *region*.iot.credenziali
AWS IoT Device Management tunneling sicuro	com.amazonaws. *region*.iot.tunneling.api
	com.amazonaws. *region*.iot-fips.tunneling.api
	com.amazonaws. *region*.iot.tunneling.data
	com.amazonaws. *region*.iot-fips.tunneling.data
AWS IoT Core Device Advisor	com.amazonaws. *region*.deviceadvisor.iot
Integrazioni gestite per AWS IoT Device Management	com.amazonaws. *region*.iotmanagedintegrations.api
	com.amazonaws. *region*.integrazioni gestite iot-fips.api
AWS IoT Core per LoRaWAN	com.amazonaws. *region*.iotwireless.api

Servizio AWS	Nome servizio
	com.amazonaws. *region*.lorawan.coppe
	com.amazonaws. *region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws. *region*. IoT per quanto riguarda la flotta
AWS IoT Greengrass	com.amazonaws. *region*. erba verde
AWS IoT RoboRunner	com.amazonaws. *region*. iotrobo runner
AWS IoT SiteWise	com.amazonaws. *region*.iotsitewise.api
	com.amazonaws. *region*.iotsitewise.data
AWS IoT TwinMaker	com.amazonaws. *region*.iottwinmaker.api
	com.amazonaws. *region*.iottwinmaker.data
Amazon Kendra	com.amazonaws. *region*.kendra
	aws.api. *region*.classifica kendra
AWS Key Management Service	com.amazonaws. *region*.kms
	com.amazonaws. *region*.kms-fips
Amazon Keyspaces (per Apache Cassandra)	com.amazonaws. *region*.cassandra
	com.amazonaws. *region*.cassandra-fips
Flusso di dati Amazon Kinesis	com.amazonaws. *region*.kinesis-stream
	com.amazonaws. *region*. kinesis-streams-fips
AWS Lake Formation	com.amazonaws. *region*. formazione di laghi
AWS Lambda	com.amazonaws. *region*.lambda
AWS Launch Wizard	com.amazonaws.it. *region*.launchwizard

Servizio AWS	Nome servizio
Amazon Lex	com.amazonaws. *region*.modelli-v2-lex
	com.amazonaws. *region*.runtime-v2-lex
AWS License Manager	com.amazonaws. *region*.gestore delle licenze
	com.amazonaws. *region*. license-manager-fips
	com.amazonaws. *region*. license-manager-linux-subscriptions
	com.amazonaws. *region*. license-manager-linux-subscriptions-fips
	com.amazonaws. *region*. license-manager-user-subscriptions
	com.amazonaws. *region*. license-manager-user-subscriptions-fips
Amazon Lightsail	com.amazonaws. *region*.vela leggera
Servizio di posizione Amazon	com.amazonaws. *region*.geo.maps
	com.amazonaws. *region*.geo.places
	com.amazonaws. *region*.geo.routes
	com.amazonaws. *region*.geo.geofencing
	com.amazonaws. *region*.geo.tracking
	com.amazonaws. *region*.geo.metadati
Amazon Lookout per le apparecchiature	com.amazonaws. *region*. attrezzatura lookout
Amazon Lookout per le metriche	com.amazonaws. *region*.lookoutmetrics

Servizio AWS	Nome servizio
Amazon Lookout per Vision	com.amazonaws. *region*. lookout vision
Amazon Macie	com.amazonaws. *region*.macie 2
	com.amazonaws. *region*.macie2-fips
Modernizzazione del mainframe AWS	com.amazonaws. *region*.app test
	com.amazonaws. *region*.m2
Blockchain gestita da Amazon	com.amazonaws. *region*. query blockchain gestita
	com.amazonaws. *region*.blockchain gestita.bitcoin.mainnet
	com.amazonaws. *region*.blockchain gestita.bitcoin.testnet
AWS Marketplace Metering Service	com.amazonaws. *region*.mercato di misurazione
Amazon Managed Service per Prometheus	com.amazonaws. *region*.app
	com.amazonaws. *region*.aps-workspaces
Amazon Managed Streaming per Apache Kafka (MSK)	com.amazonaws. *region*.kafka
	com.amazonaws. *region*.kafka-fips
Flussi di lavoro gestiti da Amazon per Apache Airflow	com.amazonaws. *region*.airflow.api
	com.amazonaws. *region*.airflow.api-fips
	com.amazonaws. *region*.airflow.env
	com.amazonaws. *region*.airflow.env-fips
	com.amazonaws. *region*.airflow.ops
Amazon Route 53	com.amazonaws.route53

Servizio AWS	Nome servizio
Console di gestione AWS	com.amazonaws. *region*.console
	com.amazonaws. *region*. accedi
Amazon MemoryDB	com.amazonaws. *region*.memory-db
	com.amazonaws. *region*.memorydb-fips
Orchestratore dell'Hub di migrazione AWS	com.amazonaws. *region*.migrationhub-orchestrator
AWS Migration Hub Refactor Spaces	com.amazonaws. *region*.refactor-spaces
Suggerimenti sulla strategia di Migration Hub	com.amazonaws. *region*.migrationhub - strategia
Amazon MQ	com.amazonaws. *region*.mq
	com.amazonaws. *region*.mq-fips
Analisi di Amazon Neptune	com.amazonaws. *region*.neptune-graph
	com.amazonaws. *region*. neptune-graph-data
	com.amazonaws. *region*. neptune-graph-fips
AWS Network Firewall	com.amazonaws. *region*.firewall di rete
	com.amazonaws. *region*. network-firewall-fips
OpenSearch Servizio Amazon	Questi endpoint sono gestiti dai servizi
AWS Organizations	com.amazonaws. *region*.organizzazioni
	com.amazonaws. *region*.organizzazioni-fips
AWS Outposts	com.amazonaws. *region*. avamposti
AWS Panorama	com.amazonaws. *region*.panorama

Servizio AWS	Nome servizio
AWS Crittografia dei pagamenti	com.amazonaws. *region*.payment-cryptography.controlplane
	com.amazonaws. *region*.crittografia-pagamento.dataplane
AWS PC	com.amazonaws. *region*.pz
	com.amazonaws. *region*.pcs-fips
Amazon Personalize	com.amazonaws. *region*.personalizzare
	com.amazonaws. *region*.personalizza gli eventi
	com.amazonaws. *region*.personalize-runtime
Amazon Pinpoint	com.amazonaws. *region*.puntino
	com.amazonaws. *region*. pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws. *region*.polly
	com.amazonaws. *region*.polly-fips
Listino prezzi AWS	com.amazonaws. *region*.prezzi. api
AWS Autorità di certificazione privata	com.amazonaws. *region*.acm-pca
	com.amazonaws. *region*. acm-pca-fips
	com.amazonaws. *region*. pca-connector-ad
	com.amazonaws. *region*. pca-connector-scep
AWS Proton	com.amazonaws. *region*.protone
Amazon Q Business	aws.api. *region*.qbusiness
Amazon Q Developer	com.amazonaws. *region*.codewhisperer

Servizio AWS	Nome servizio
	com.amazonaws. *region*q.
	com.amazonaws. *region*.app
Abbonamenti utenti Amazon Q	com.amazonaws. *region*.service.user-subscriptions
Quick Suite	com.amazonaws. *region*.quicksight - sito web
Amazon RDS	com.amazonaws. *region*.rds
	com.amazonaws. *region*.rds-fips
API dati di Amazon RDS	com.amazonaws. *region*.rds-dati
Approfondimenti sulle prestazioni di Amazon RDS	com.amazonaws. *region*.pi
	com.amazonaws. *region*.pi-fips
AWS Re:Post privato	com.amazonaws. *region*.repostspace
Cestino di riciclaggio	com.amazonaws. *region*.rbin
Amazon Redshift	com.amazonaws. *region*. spostamento rosso
	com.amazonaws. *region*.redshift-fips
	com.amazonaws. *region*.redshift-senza server
	com.amazonaws. *region*. redshift-serverless-fips
API dati di Amazon Redshift	com.amazonaws. *region*.redshift-dati
	com.amazonaws. *region*. redshift-data-fips
Amazon Rekognition	com.amazonaws. *region*.riconoscimento
	com.amazonaws. *region*.recognition-fips
	com.amazonaws. *region*.riconoscimento in streaming

Servizio AWS	Nome servizio
	com.amazonaws. *region*. streaming-rekognition-fips
AWS Resource Access Manager	com.amazonaws. *region*.ram
	com.amazonaws. *region*.ram-fips
Esploratore di risorse AWS	com.amazonaws. *region*.resource-explorer-2
	com.amazonaws. *region*.resource-explorer-2-fips
AWS Resource Groups	com.amazonaws. *region*.gruppi-risorse
	com.amazonaws. *region*. resource-groups-fips
AWS Resource Groups Tagging API	com.amazonaws. *region*.etichettatura
Amazon S3	com.amazonaws. *region*.s3
	com.amazonaws. *region*.s3 tabelle
Punti di accesso multi-Regione di Amazon S3	com.amazonaws.s3-global.accesspoint
Amazon S3 su Outposts	com.amazonaws. *region*.s3 - avamposti
Amazon SageMaker AI	aws.sagemaker. *region*. esperimenti
	aws.sagemaker. *region*.taccuino
	aws.sagemaker. *region*.app per i partner
	aws.sagemaker. *region*.studio
	com.amazonaws. *region*. sagemaker-data-science-assistant
	com.amazonaws. *region*.sagemaker.api
	com.amazonaws. *region*.sagemaker.api-fips

Servizio AWS	Nome servizio
	com.amazonaws. *region*.sagemaker.featurestore-runtime
	com.amazonaws. *region*.saggista. featurestore-runtime-fips
	com.amazonaws. *region*.sagemaker.metrics
	com.amazonaws. *region*.sagemaker.runtime
	com.amazonaws. *region*.sagemaker.runtime-fips
Savings Plans	com.amazonaws.savingsplans
Gestione dei segreti AWS	com.amazonaws. *region*. gestore dei segreti
AWS Security Hub CSPM	com.amazonaws. *region*.hub di sicurezza
	com.amazonaws. *region*.securityhub-fips
Amazon Security Lake	com.amazonaws. *region*. lago di sicurezza
	com.amazonaws. *region*.security lake-fips
AWS Security Token Service	com.amazonaws. *region*.sts
	com.amazonaws.it. *region*.sts-fips
AWS Serverless Application Repository	com.amazonaws. *region*.repository senza server
Service Catalog	com.amazonaws. *region*.catalogo dei servizi
	com.amazonaws. *region*.servicecatalog-app
Service Quotas (Quote di Servizio)	com.amazonaws. *region*. quote di servizio
Amazon SES	com.amazonaws. *region*.email-smtp

Servizio AWS	Nome servizio
	com.amazonaws. *region*.gestore di posta
	com.amazonaws. *region*. mail-manager-fips
	com.amazonaws. *region*. mail-manager-smtp.auth.fips
	com.amazonaws. *region*. mail-manager-smtp.apri.fips
AWS SimSpace Weaver	com.amazonaws. *region*.simspaceweaver
AWS Snowball Edge Device Management	com.amazonaws. *region*. snow-device-management
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
	com.amazonaws. *region*.sqs-fips
Amazon SWF	com.amazonaws. *region*.swf
	com.amazonaws. *region*.swf-fips
AWS Step Functions	com.amazonaws. *region*.stati
	com.amazonaws. *region*.sync-stati
Gateway di archiviazione AWS	com.amazonaws.it. *region*.gateway di archiviazione
Catena di approvvigionamento di AWS	com.amazonaws. *region*.scn
AWS Systems Manager	com.amazonaws.it. *region*messaggi.ec2
	com.amazonaws. *region*.ssm
	com.amazonaws. *region*.ssm-contatti
	com.amazonaws. *region*.ssm-incidenti

Servizio AWS	Nome servizio
	com.amazonaws. *region*. ssm-incidents-fips
	com.amazonaws. *region*.ssm - configurazione rapida
	com.amazonaws. *region*messaggi.ssm
AWS Systems Manager per SAP	com.amazonaws. *region*.ssm-sap
	com.amazonaws. *region*. ssm-sap-fips
AWS Costruttore di reti di telecomunicazioni	com.amazonaws. *region*.tnb
Amazon Textract	com.amazonaws. *region*.tr estrarre
	com.amazonaws. *region*.textract-fips
Amazon Timestream	com.amazonaws. *region*.timestream.ingest- *cell*
	com.amazonaws. *region*.timestream.query- *cell*
Amazon Timestream per InfluxDB	com.amazonaws. *region*.timestream-influxdb
	com.amazonaws. *region*. timestream-influxdb-fips
Amazon Transcribe	com.amazonaws. *region*.trascrivere
	com.amazonaws. *region*. trascrivi lo streaming
	com.amazonaws. *region*. transcribestreaming-fips
Amazon Transcribe Medical	com.amazonaws. *region*.trascrivere
	com.amazonaws. *region*. trascrivi lo streaming
AWS Transfer for SFTP	com.amazonaws. *region*.trasferimento
	com.amazonaws. *region*.trasferisce.server
AWS Transform	com.amazonaws. *region*.trasformare

Servizio AWS	Nome servizio
Amazon Translate	com.amazonaws. *region*.tradurre
AWS Trusted Advisor	com.amazonaws. *region*. consulente affidabile
Notifiche all'utente AWS	com.amazonaws. *region*.notifiche
	com.amazonaws. *region*.notificazioni-contatti
Autorizzazioni verificate da Amazon	com.amazonaws. *region*. autorizzazioni verificate
	com.amazonaws. *region*.permessi verificati-fips
Amazon VPC Lattice	com.amazonaws. *region*.vpc-reticolo
AWS WAFV2	com.amazonaws. *region*.waf v2
	com.amazonaws. *region*.wafv2-fips
AWS Well-Architected Tool	com.amazonaws. *region*. ben architettato
Amazon WorkMail	com.amazonaws. *region*.posta di lavoro
	com.amazonaws. *region*.flusso di messaggi di posta elettronica di lavoro
Amazon WorkSpaces	com.amazonaws. *region*.spazi di lavoro
Browser WorkSpaces sicuro Amazon	com.amazonaws. *region*.workspaces-web
	com.amazonaws. *region*. workspaces-web-fips
WorkSpaces streaming	com.amazonaws. *region*.highlander
Amazon WorkSpaces Thin Client	com.amazonaws. *region*.thinclient.api
AWS X-Ray	com.amazonaws. *region*.raggi x
Servizio gestito da Amazon per Apache Flink	com.amazonaws.it. *region*.kinesis analytics
	com.amazonaws. *region*.kinesisanalytics-fips

Visualizzazione dei nomi del Servizio AWS disponibili

È possibile utilizzare il describe-vpc-endpoint-servicescomando per visualizzare i nomi dei servizi che supportano gli endpoint VPC.

L'esempio seguente visualizza gli endpoint dell'interfaccia Servizi AWS che supportano nella regione specificata. L'opzione `--query` limita l'output ai nomi dei servizi.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query ServiceNames
```

Di seguito è riportato un output di esempio. L'output completo non viene visualizzato.

```
[
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.emr-service-cell01",
    "aws.api.us-east-1.freetier",
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    . . .
     "com.amazonaws.us-east-1.xray"
]
```

Visualizzazione delle informazioni su un servizio

Dopo aver ottenuto il nome del servizio, è possibile utilizzare il describe-vpc-endpoint-servicescomando per visualizzare informazioni dettagliate su ciascun servizio endpoint.

L'esempio seguente mostra informazioni sull'endpoint CloudWatch dell'interfaccia Amazon nella regione specificata.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.monitoring" \
  --region us-east-1
```

Di seguito è riportato un output di esempio. `VpcEndpointPolicySupported` indica se le politiche degli endpoint sono supportate. `SupportedIpAddressTypes` indica quali tipi di indirizzi IP sono supportati.

```
{
    "ServiceDetails": [
        {
            "ServiceName": "com.amazonaws.us-east-1.monitoring",
            "ServiceId": "vpce-svc-0fc975f3e7e5beba4",
            "ServiceType": [
                {
                    "ServiceType": "Interface"
                }
            ],
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
                "us-east-1c",
                "us-east-1d",
                "us-east-1e",
                "us-east-1f"
            ],
            "Owner": "amazon",
            "BaseEndpointDnsNames": [
                "monitoring.us-east-1.vpce.amazonaws.com"
            ],
            "PrivateDnsName": "monitoring.us-east-1.amazonaws.com",
            "PrivateDnsNames": [
                {
                    "PrivateDnsName": "monitoring.us-east-1.amazonaws.com"
                },
                {
                    "PrivateDnsName": "monitoring.us-east-1.api.aws"
                },
                {
                    "PrivateDnsName": "monitoring-fips.us-east-1.amazonaws.com"
                },
                {
                    "PrivateDnsName": "monitoring-fips.us-east-1.api.aws"
                }           ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": [],
            "PrivateDnsNameVerificationState": "verified",
            "SupportedIpAddressTypes": [
                "ipv6",
```

```
                "ipv4"
            ]
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.monitoring"
    ]
}
```

Visualizza il supporto della politica dell'endpoint

Per verificare se un servizio supporta le policy degli endpoint, chiama il describe-vpc-endpoint-servicescomando e verifica il valore di. `VpcEndpointPolicySupported` I valori possibili sono `true` e `false`.

L'esempio seguente verifica se il servizio specificato supporta le policy di endpoint nella regione specificata. L'opzione `--query` limita l'output al valore di `VpcEndpointPolicySupported`.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.s3" \
  --region us-east-1 \
  --query ServiceDetails[*].VpcEndpointPolicySupported \
  --output text
```

Di seguito è riportato un output di esempio.

```
True
```

L'esempio seguente elenca quelli Servizi AWS che supportano le policy degli endpoint nella regione specificata. L'opzione `--query` limita l'output ai nomi dei servizi. Per eseguire questo comando utilizzando il prompt dei comandi di Windows, rimuovi le virgolette singole dalla stringa di query e modifica il carattere di continuazione della riga da \ a ^.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`true`].ServiceName'
```

Di seguito è riportato un output di esempio. L'output completo non viene visualizzato.

```
[
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.emr-service-cell01",
    "aws.api.us-east-1.freetier",
    "aws.api.us-east-1.kendra-ranking",
    . . .
    "com.amazonaws.us-east-1.xray"
]
```

L'esempio seguente elenca quelli Servizi AWS che non supportano le policy degli endpoint nella regione specificata. L'opzione `--query` limita l'output ai nomi dei servizi. Per eseguire questo comando utilizzando il prompt dei comandi di Windows, rimuovi le virgolette singole dalla stringa di query e modifica il carattere di continuazione della riga da \ a ^.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`false`].ServiceName'
```

Di seguito è riportato un output di esempio. L'output completo non viene visualizzato.

```
[
    "com.amazonaws.us-east-1.appmesh-envoy-management",
    "com.amazonaws.us-east-1.apprunner.requests",
    "com.amazonaws.us-east-1.appstream.api",
    "com.amazonaws.us-east-1.appstream.streaming",
    "com.amazonaws.us-east-1.awsconnector",
    . . .
    "com.amazonaws.us-east-1.transfer.server"
]
```

Visualizza IPv6 il supporto

Per visualizzare IPv6 il supporto per AWS i servizi, consulta AWS i servizi che supportano IPv6.
È inoltre possibile utilizzare il describe-vpc-endpoint-servicescomando seguente per visualizzare i Servizi AWS file a cui è possibile accedere IPv6 nella regione specificata. L'opzione `--query` limita l'output ai nomi dei servizi.

```
aws ec2 describe-vpc-endpoint-services \
```

```
  --filters Name=supported-ip-address-types,Values=ipv6 Name=owner,Values=amazon
 Name=service-type,Values=Interface \
  --region us-east-1 \
  --query ServiceNames
```

Di seguito è riportato un output di esempio. L'output completo non viene visualizzato.

```
[
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.freetier",
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "aws.api.us-east-1.resource-explorer-2",
    "aws.api.us-east-1.resource-explorer-2-fips",
    "aws.sagemaker.us-east-1.experiments",
    "aws.sagemaker.us-east-1.partner-app",
    "com.amazonaws.iam",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    . . .
    "com.amazonaws.us-east-1.xray"
]
```

Attivata per più regioni Servizi AWS

Quanto segue si Servizi AWS integra con cross Region. AWS PrivateLink Puoi creare un endpoint di interfaccia per connetterti a questi servizi in un'altra AWS regione, in privato, come se fossero in esecuzione nel tuo VPC.

Scegli il link nella Servizio AWScolonna per vedere la documentazione del servizio. La colonna Service name contiene il nome del servizio specificato al momento della creazione dell'endpoint di interfaccia.

Servizio AWS	Nome servizio
Amazon S3	com.amazonaws. *region*.s3
AWS Identity and Access Management (IAM)	com.amazonaws.iam

Servizio AWS	Nome servizio
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
AWS Key Management Service	com.amazonaws. *region*.kms
	com.amazonaws. *region*.kms-fips
Amazon ECS	com.amazonaws. *region*.ecs
AWS Lambda	com.amazonaws. *region*.lambda
Amazon Data Firehose	com.amazonaws.it. *region*.kinesis-firehose
Servizio gestito da Amazon per Apache Flink	com.amazonaws. *region*.kinesis analytics
	com.amazonaws. *region*.kinesisanalytics-fips
Amazon Route 53	com.amazonaws.route53

Visualizzazione dei nomi del Servizio AWS disponibili

È possibile utilizzare il comando per visualizzare i servizi abilitati per più regioni. describe-vpc-endpoint-services

L'esempio seguente mostra Servizi AWS che un utente della `us-east-1` regione può accedere, tramite gli endpoint dell'interfaccia, alla regione di servizio specificata (`us-west-2`). L'opzione `--query` limita l'output ai nomi dei servizi.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --service-region us-west-2 \
  --query ServiceNames
```

Di seguito è riportato un output di esempio. L'output completo non viene visualizzato.

```
[
```

```
    "com.amazonaws.us-west-2.ecr.api",
    "com.amazonaws.us-west-2.ecr.dkr",
    "com.amazonaws.us-west-2.ecs",
    "com.amazonaws.us-west-2.ecs-fips",
    ...
    "com.amazonaws.us-west-2.s3"
]
```

> **Note**
>
> È necessario utilizzare DNS regionali. Il DNS zonale non è supportato quando si accede da un'altra Servizi AWS regione. Per ulteriori informazioni, consulta Visualizza e aggiorna gli attributi DNS nella Amazon VPC User Guide.

Autorizzazioni e considerazioni

- Per impostazione predefinita, le entità IAM non dispongono dell'autorizzazione per accedere a un sito Servizio AWS in un'altra regione. Per concedere le autorizzazioni necessarie per l'accesso tra diverse regioni, un amministratore IAM può creare policy IAM che consentano l'azione di `vpce:AllowMultiRegion` sola autorizzazione.
- Assicurati che la tua Service Control Policy (SCP) non neghi le azioni basate solo sulle autorizzazioni. `vpce:AllowMultiRegion` Per utilizzare la funzionalità AWS PrivateLink di connettività interregionale di cui disponete, sia la vostra politica di identità che il vostro SCP devono consentire questa azione.
- Per controllare le regioni che un'entità IAM può specificare come regione di servizio durante la creazione di un endpoint VPC, utilizza la `ec2:VpceServiceRegion` chiave condition.
- Un consumatore di servizi deve aderire a una regione con attivazione prima di selezionarla come regione di servizio per un endpoint. Ove possibile, consigliamo agli utenti del servizio di accedere a un servizio utilizzando la connettività interregionale anziché la connettività interregionale. La connettività intraregionale offre una latenza inferiore e costi inferiori.
- Puoi utilizzare la nuova chiave di condizione `aws:SourceVpcArn` globale di IAM per proteggere da quali regioni Account AWS e risorse è possibile VPCs accedere alle tue risorse. Questa chiave aiuta a implementare la residenza dei dati e il controllo degli accessi basato sulla regione.
- Per un'elevata disponibilità, crea un endpoint di interfaccia abilitato per più regioni in almeno due zone di disponibilità. In questo caso, i fornitori e i consumatori non sono tenuti a utilizzare le stesse zone di disponibilità.

- Grazie all'accesso interregionale, AWS PrivateLink gestisce il failover tra le zone di disponibilità sia nelle aree di servizio che in quelle di consumo. Non gestisce il failover tra le regioni.
- L'accesso interregionale non è supportato per le seguenti zone di disponibilità:`use1-az3`,`usw1-az2`, `apne1-az3apne2-az2`, `eapne2-az4`.
- È possibile utilizzarlo AWS Fault Injection Service per simulare eventi regionali e modellare scenari di errore per endpoint di interfaccia abilitati a livello regionale e interregionale. Per ulteriori informazioni, consulta la documentazione.AWS FIS

Crea un endpoint di interfaccia verso un'altra Servizio AWS regione

Per creare un endpoint di interfaccia utilizzando la Console, consulta la sezione Creare un endpoint VPC.

Nella CLI, puoi utilizzare il create-vpc-endpointcomando per creare un endpoint VPC in una Servizio AWS regione diversa. L'esempio seguente crea un endpoint di interfaccia verso Amazon S3 `us-west-2` da un ingresso VPC. `us-east-1`

```
aws ec2 create-vpc-endpoint \
  --vpc-id vpc-id \
  --service-name com.amazonaws.us-west-2.s3 \
  --vpc-endpoint-type Interface \
  --subnet-ids subnet-id-1 subnet-id-2 \
  --region us-east-1 \
  --service-region us-west-2
```

Accedere e Servizio AWS utilizzare un endpoint VPC di interfaccia

È possibile creare un endpoint VPC di interfaccia per connettersi ai servizi forniti AWS PrivateLink, inclusi molti. Servizi AWS Per una panoramica, consulta the section called “Concetti” e Accesso a Servizi AWS.

Per ogni sottorete specificata dal VPC, creiamo un'interfaccia di rete dell'endpoint nella sottorete e le assegniamo un indirizzo IP privato dall'intervallo di indirizzi della sottorete. Un'interfaccia di rete dell'endpoint è un'interfaccia di rete gestita dal richiedente. Puoi visualizzarla nel tuo Account AWS, ma non puoi gestirla autonomamente.

Ti viene addebitato l'utilizzo orario e le spese di elaborazione dati. Per ulteriori informazioni, consulta prezzi degli endpoint di interfaccia.

Indice

Prerequisiti

- Implementa le risorse che accederanno Servizio AWS al tuo VPC.
- Per utilizzare i DNS privati, devi abilitare i nomi host DNS e la risoluzione DNS per il VPC. Per ulteriori informazioni, consulta la sezione Visualizzazione e aggiornamento degli attributi DNS nella Guida per l'utente di Amazon VPC.
- IPv6 Per abilitare un endpoint di interfaccia, è Servizio AWS necessario supportare l'accesso tramite. IPv6 Per ulteriori informazioni, consulta the section called “Tipi di indirizzi IP”.
- Crea un gruppo di sicurezza per l'interfaccia di rete degli endpoint che consenta il traffico previsto dalle risorse del tuo VPC. Ad esempio, per garantire che AWS CLI possa inviare richieste HTTPS a Servizio AWS, il gruppo di sicurezza deve consentire il traffico HTTPS in entrata.
- Se le tue risorse si trovano in una sottorete con un ACL di rete, verifica che l'ACL di rete consenta il traffico tra le risorse del tuo VPC e le interfacce di rete degli endpoint.
- Le tue risorse sono soggette a quote. AWS PrivateLink Per ulteriori informazioni, consulta AWS PrivateLink quote.

Creare un endpoint VPC

Utilizza la procedura seguente per creare un endpoint VPC dell'interfaccia in grado di connettersi a un Servizio AWS.

Per creare un endpoint di interfaccia per un Servizio AWS

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.

4. Per Tipo, scegli AWS servizi.
5. (Facoltativo) Se crei un endpoint Servizio AWS in un'altra regione, seleziona la casella di controllo Abilita endpoint interregionale, quindi seleziona l'area del servizio dal menu a discesa.
6. Per Service name (Nome servizio), seleziona il servizio. Per ulteriori informazioni, consulta the section called “Servizi integrati”.
7. Per VPC, seleziona il VPC da cui accederai al Servizio AWS.
8. Se nel passaggio 5 hai selezionato il nome del servizio per Amazon S3 e desideri configurare il supporto DNS privato, seleziona Impostazioni aggiuntive, Abilita nome DNS. Quando si effettua questa selezione, viene automaticamente selezionata anche l'opzione Abilita il DNS privato solo per l'endpoint in entrata. Puoi configurare il DNS privato con un endpoint del resolver in entrata solo per gli endpoint di interfaccia per Amazon S3. Se non disponi di un endpoint gateway per Amazon S3 e selezioni Abilita il DNS privato solo per l'endpoint in entrata, riceverai un errore quando tenterai il passaggio finale di questa procedura.

   Se nel passaggio 5 hai selezionato il nome del servizio per qualsiasi servizio diverso da Amazon S3, Impostazioni aggiuntive, Abilita nome DNS sarà già selezionato. Ti consigliamo di mantenere l'impostazione predefinita. Ciò garantisce che le richieste che utilizzano gli endpoint del servizio pubblico, come le richieste effettuate tramite un AWS SDK, vengano risolte sull'endpoint VPC.
9. Per le sottoreti, seleziona le sottoreti in cui creare interfacce di rete endpoint. È possibile selezionare una sottorete per zona di disponibilità. Non è possibile selezionare più sottoreti dalla stessa zona di disponibilità. Per ulteriori informazioni, consulta the section called “Sottoreti e zone di disponibilità”.

   Per impostazione predefinita, selezioniamo gli indirizzi IP dagli intervalli di indirizzi IP della sottorete e li assegniamo alle interfacce di rete degli endpoint. Per scegliere tu stesso gli indirizzi IP, seleziona Designare indirizzi IP. Tieni presente che i primi quattro indirizzi IP e l'ultimo indirizzo IP in un blocco CIDR di sottorete sono riservati all'uso interno, quindi non puoi specificarli per le interfacce di rete degli endpoint.
10. Per IP address type (Tipo di indirizzo IP), seleziona una delle opzioni seguenti:

    - IPv4— Assegna IPv4 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate hanno intervalli di IPv4 indirizzi e il servizio accetta le richieste. IPv4
    - IPv6— Assegna IPv6 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono IPv6 solo sottoreti e il servizio accetta le richieste. IPv6

- Dualstack: assegna entrambi IPv4 gli indirizzi e alle interfacce di rete degli endpoint. IPv6 Questa opzione è supportata solo se tutte le sottoreti selezionate hanno entrambi intervalli di IPv6 indirizzi IPv4 e il servizio accetta entrambe le richieste. IPv4 IPv6

11. Per Security groups (Gruppi di sicurezza), seleziona i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint. Per impostazione predefinita, per il VPC viene associato il gruppo di sicurezza predefinito.
12. Per Policy, per consentire tutte le operazioni da parte di tutti i principali su tutte le risorse sull'endpoint dell'interfaccia, seleziona Accesso completo. Per limitare l'accesso, seleziona Personalizzato e inserisci una policy. Questa opzione è disponibile solo se il servizio supporta le policy dell'endpoint VPC. Per ulteriori informazioni, consulta Policy di endpoint.
13. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
14. Seleziona Crea endpoint.

Per creare un endpoint dell'interfaccia mediante la riga di comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Sottoreti condivise

Non puoi creare, descrivere, modificare o eliminare gli endpoint VPC nelle sottoreti condivise con te. Tuttavia, puoi utilizzare gli endpoint VPC in sottoreti condivise con te.

ICMP

Gli endpoint dell'interfaccia non rispondono alle ping richieste. È possibile utilizzare invece nmap i comandi nc or.

Configurazione di un endpoint dell'interfaccia

Dopo aver creato un endpoint VPC dell'interfaccia, è possibile aggiornarne la configurazione.

Processi

- Aggiunta o rimozione di sottoreti

- Associazione dei gruppi di sicurezza
- Modifica della policy di endpoint VPC
- Abilitazione dei nomi DNS privati
- Gestione dei tag

Aggiunta o rimozione di sottoreti

Per l'endpoint dell'interfaccia, puoi scegliere una sottorete per zona di disponibilità. Quando si aggiunge una sottorete, al suo interno viene creata un'interfaccia di rete dell'endpoint e le si assegna un indirizzo IP privato dall'intervallo di indirizzi IP della sottorete. Durante la rimozione di una sottorete, si elimina anche la relativa interfaccia di rete dell'endpoint. Per ulteriori informazioni, consulta the section called “Sottoreti e zone di disponibilità”.

Per modificare le sottoreti utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint dell'interfaccia.
4. Seleziona Actions (Operazioni), Manage Subnets (Gestisci sottoreti).
5. Seleziona o deseleziona le Zone di disponibilità in base alle esigenze. Per ogni Zona di disponibilità, seleziona una sottorete. Per impostazione predefinita, selezioniamo gli indirizzi IP dagli intervalli di indirizzi IP della sottorete e li assegniamo alle interfacce di rete degli endpoint. Per scegliere gli indirizzi IP per un'interfaccia di rete endpoint, seleziona Designate IP address e inserisci un IPv4 indirizzo dall'intervallo di indirizzi di sottorete. Se il servizio endpoint lo supporta IPv6, puoi anche inserire un IPv6 indirizzo dall'intervallo di indirizzi di sottorete.

   Se si specifica un indirizzo IP per una sottorete che dispone già di un'interfaccia di rete endpoint per l'endpoint VPC, sostituiamo l'interfaccia di rete degli endpoint con una nuova. Questo processo disconnette temporaneamente la sottorete e l'endpoint VPC.
6. Scegli Modify subnets (Modifica sottoreti).

Per modificare le sottoreti utilizzando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Strumenti per Windows) PowerShell

Associazione dei gruppi di sicurezza

Puoi modificare i gruppi di sicurezza associati alle interfacce di rete per l'endpoint dell'interfaccia. Le regole del gruppo di sicurezza controllano il traffico consentito verso l'interfaccia di rete dell'endpoint dalle risorse nel VPC.

Per modificare i gruppi di sicurezza utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint dell'interfaccia.
4. Selezionare Actions (Operazioni), Manage security groups (Gestisci gruppi di sicurezza).
5. Seleziona o deseleziona i gruppi di sicurezza in base alle esigenze.
6. Scegli Modify security groups (Modifica i gruppi di sicurezza).

Per modificare i gruppi di sicurezza utilizzando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Modifica della policy di endpoint VPC

Se Servizio AWS supporta le policy degli endpoint, è possibile modificare le policy degli endpoint per l'endpoint. Dopo avere aggiornato l'endpoint, possono essere necessari alcuni minuti prima che le modifiche diventino effettive. Per ulteriori informazioni, consulta Policy di endpoint.

Per modificare la policy di endpoint usando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint dell'interfaccia.
4. Scegli Actions (Operazioni), Manage policy (Gestisci policy).
5. Scegli Full Access (Accesso completo) per consentire l'accesso completo al servizio oppure scegli Custom (Personalizzato) e specifica una policy personalizzata.
6. Scegli Save (Salva).

Per modificare la policy di endpoint utilizzando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Strumenti per Windows) PowerShell

Abilitazione dei nomi DNS privati

Ti consigliamo di abilitare nomi host DNS privati per gli endpoint VPC per Servizi AWS. Ciò garantisce che le richieste che utilizzano gli endpoint del servizio pubblico, come le richieste effettuate tramite un AWS SDK, vengano risolte sull'endpoint VPC.

Per utilizzare i nomi DNS privati, devi abilitare i nomi host DNS e la risoluzione DNS per il VPC. Quando si abilitano i nomi DNS privati, potrebbero essere necessari alcuni minuti prima che gli indirizzi IP privati diventino disponibili. I record DNS creati durante l'abilitazione dei nomi DNS privati sono privati. Pertanto, il nome DNS privato non è risolvibile pubblicamente.

Per modificare l'opzione relativa ai nomi DNS privati utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint dell'interfaccia.
4. Scegli Actions (Operazioni), Modify Private DNS names (Modifica nomi DNS privati).
5. Seleziona o deseleziona Enable for this endpoint (Abilita per questo endpoint) in base alle esigenze.
6. Se il servizio è Amazon S3, selezionando Abilita per questo endpoint nel passaggio precedente si seleziona anche Abilita il DNS privato solo per l'endpoint in entrata. Se preferisci la funzionalità DNS privato standard, deseleziona Abilita il DNS privato solo per l'endpoint in entrata. Se non disponi di un endpoint gateway per Amazon S3 in aggiunta a un endpoint di interfaccia per Amazon S3 e selezioni Abilita il DNS privato solo per l'endpoint in entrata, riceverai un errore quando salverai le modifiche nel passaggio successivo. Per ulteriori informazioni, consulta the section called “DNS privato”.
7. Scegli Salva modifiche.

Per modificare l'opzione dei nomi DNS privati utilizzando la riga di comando

- modify-vpc-endpoint (AWS CLI)

- Edit-EC2VpcEndpoint(Strumenti per Windows) PowerShell

Gestione dei tag

Puoi contrassegnare l'endpoint dell'interfaccia per identificarlo o classificarlo più facilmente in base alle esigenze dell'organizzazione.

Per gestire i tag utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint dell'interfaccia.
4. Scegliere Actions (Operazioni), Manage tags (Gestisci tag).
5. Per ogni tag da aggiungere, seleziona Add new tag (Aggiungi nuovo tag) e immetti la chiave e il valore per il tag.
6. Per rimuovere un tag, scegli Remove (Rimuovi) a destra della chiave e del valore del tag.
7. Scegli Save (Salva).

Per gestire i tag utilizzando la riga di comando

- create-tags e delete-tags (AWS CLI)
- New-EC2Tage Remove-EC2Tag(Strumenti per Windows PowerShell)

Ricezione di avvisi per gli eventi relativi all'endpoint dell'interfaccia

Puoi creare una notifica per ricevere avvisi per eventi specifici relativi all'endpoint dell'interfaccia. Ad esempio, puoi ricevere un'e-mail nel momento in cui una richiesta di connessione viene accettata o rifiutata.

Processi

- Creare una notifica SNS
- Aggiungere una policy di accesso
- Aggiungere una policy della chiave

Creare una notifica SNS

Usa la procedura seguente per creare un argomento Amazon SNS per le notifiche e iscriverti all'argomento.

Per creare una notifica per un endpoint dell'interfaccia utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint dell'interfaccia.
4. Nella scheda Notifications (Notifiche), scegli Create notification (Crea notifica).
5. Per Notification ARN, scegli Amazon Resource Name (ARN) per l'argomento SNS che hai creato.
6. Per iscriverti a un evento, selezionalo da Events (Eventi).
   - Connect (Connetti): l'utente del servizio ha creato l'endpoint dell'interfaccia. Questa operazione invia una richiesta di connessione al provider di servizi.
   - Accept (Accetta): il provider di servizi ha accettato la richiesta di connessione.
   - Reject (Rifiuta): il provider di servizi ha rifiutato la richiesta di connessione.
   - Delete (Elimina): l'utente del servizio ha eliminato l'endpoint dell'interfaccia.
7. Selezionare Create Notification (Crea notifica).

Per creare una notifica per l'endpoint dell'interfaccia utilizzando la riga di comando

- create-vpc-endpoint-connection-notifica ()AWS CLI
- New-EC2VpcEndpointConnectionNotification(Strumenti per Windows PowerShell)

Aggiungere una policy di accesso

Aggiungi una policy di accesso all'argomento Amazon SNS che AWS PrivateLink consenta di pubblicare notifiche per tuo conto, come le seguenti. Per ulteriori informazioni, consulta Come modifico la policy di accesso dell'argomento di Amazon SNS? Utilizza le chiavi di condizione globali `aws:SourceArn` e `aws:SourceAccount` per evitare il problema del "confused deputy".

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

Aggiungere una policy della chiave

Se utilizzi argomenti SNS crittografati, la politica delle risorse per la chiave KMS deve essere affidabile per AWS PrivateLink chiamare AWS KMS le operazioni dell'API. Di seguito è riportato un esempio di policy della chiave.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
```

```
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

Eliminazione di un endpoint dell'interfaccia

Quando un endpoint VPC non è più necessario, è possibile eliminarlo. L'eliminazione di un endpoint dell'interfaccia elimina anche le interfacce di rete dell'endpoint.

Per eliminare un endpoint dell'interfaccia tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint dell'interfaccia.
4. Seleziona Actions (Operazioni), Delete VPC endpoints (Eliminazione di endpoint VPC).
5. Quando viene richiesta la conferma, immetti **delete**.
6. Scegli Elimina.

Per eliminare un endpoint dell'interfaccia tramite la riga di comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Endpoint gateway

Gli endpoint VPC gateway offrono una connettività affidabile ad Amazon S3 e DynamoDB senza richiedere un gateway Internet o un dispositivo NAT per il VPC. Gli endpoint gateway non vengono utilizzati AWS PrivateLink, a differenza di altri tipi di endpoint VPC.

Amazon S3 e DynamoDB supportano sia gli endpoint gateway che gli endpoint di interfaccia. Per un confronto tra le opzioni, consulta quanto segue:

- Tipi di endpoint VPC per Amazon S3
- Tipi di endpoint VPC per Amazon DynamoDB

Prezzi

L'utilizzo di endpoint gateway non comporta costi supplementari.

Indice

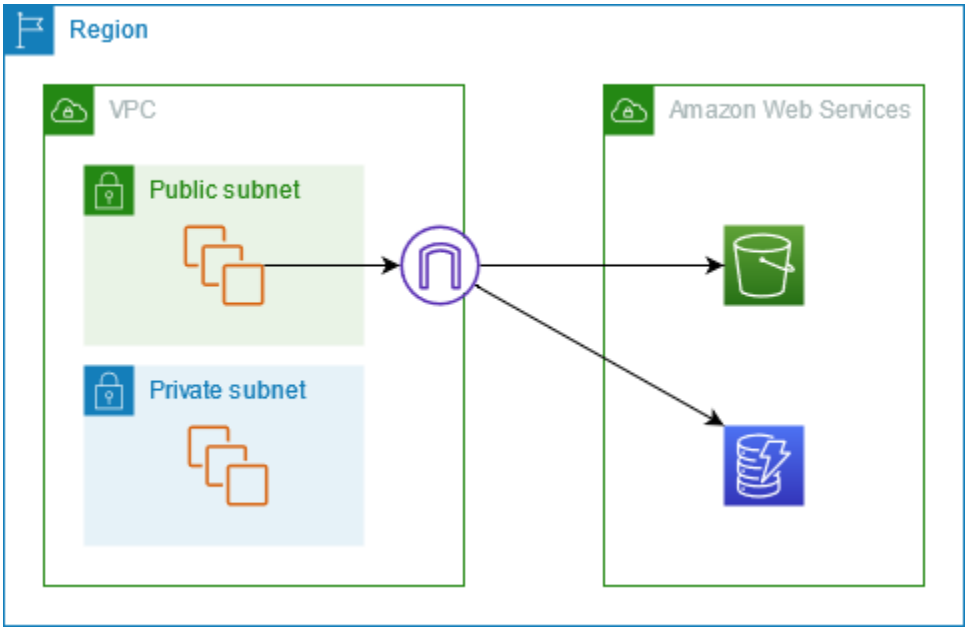
Panoramica

Puoi accedere ad Amazon S3 e DynamoDB tramite gli endpoint di servizio pubblico o tramite gli endpoint gateway. Questa panoramica mette a confronto i due metodi.

Accesso tramite un gateway Internet

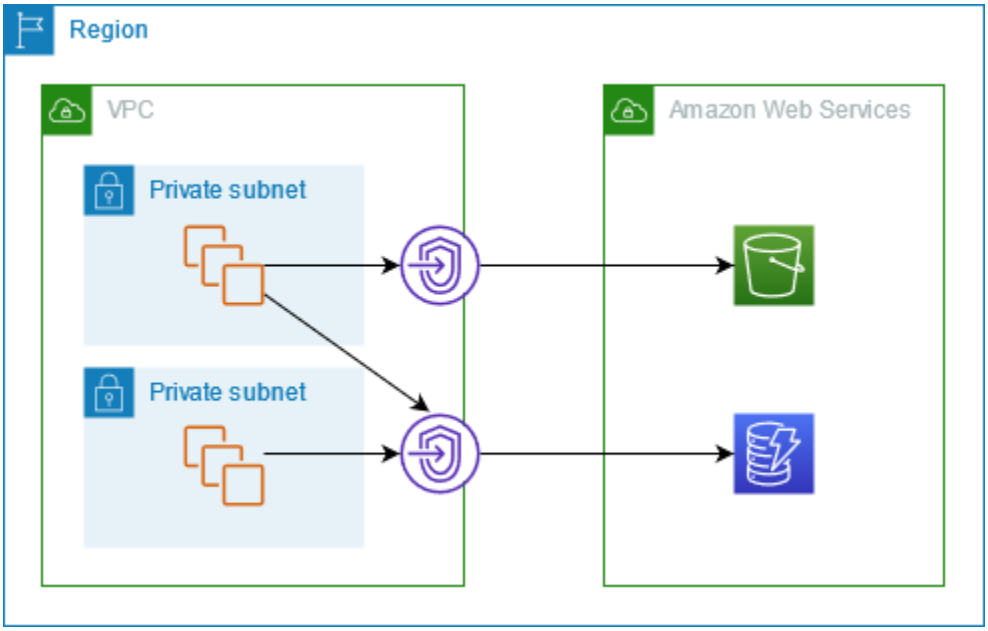
Il diagramma seguente mostra il modo in cui le istanze accedono ad Amazon S3 e DynamoDB tramite i loro endpoint di servizio pubblico. Il traffico verso Amazon S3 o DynamoDB da un'istanza presente in una sottorete pubblica viene instradato al gateway Internet del VPC e successivamente

al servizio. Le istanze presenti in una sottorete privata non possono inviare traffico ad Amazon S3 o DynamoDB, perché per definizione le sottoreti private non hanno route verso un gateway Internet. Per abilitare le istanze nella sottorete privata per inviare il traffico ad Amazon S3 o DynamoDB, è necessario aggiungere un dispositivo NAT alla sottorete pubblica e instradare il traffico nella sottorete privata al dispositivo NAT. Sebbene il traffico verso Amazon S3 o DynamoDB attraversi il gateway Internet, non esce dalla rete. AWS



Accesso tramite un endpoint gateway

Il diagramma seguente mostra il modo in cui le istanze accedono ad Amazon S3 e DynamoDB tramite un endpoint gateway. Il traffico in transito dal VPC ad Amazon S3 o a DynamoDB viene instradato verso l'endpoint gateway. Ogni tabella di instradamento della sottorete deve disporre di una route che invia il traffico destinato al servizio all'endpoint gateway utilizzando l'elenco di prefissi del servizio. Per maggiori informazioni, consulta Elenchi di prefissi gestiti da AWS nella Guida dell'utente di Amazon VPC.



Routing

Quando crei un endpoint gateway, seleziona le tabelle di instradamento del VPC per le sottoreti abilitate. La route seguente viene aggiunta automaticamente a ogni tabella di instradamento selezionata. La destinazione è un elenco di prefissi per il servizio di proprietà di AWS e la destinazione è l'endpoint del gateway.

Destinazione	Target
prefix_list_id	*gateway_endpoint_id*

Considerazioni

- Puoi esaminare le route dell'endpoint che aggiungiamo alla tabella di instradamento, ma non puoi modificarle o eliminarle. Per aggiungere una route dell'endpoint a una tabella di instradamento, associala all'endpoint gateway. La route dell'endpoint viene eliminata quando si dissocia la tabella di instradamento dall'endpoint gateway o quando si rimuove l'endpoint gateway.
- Tutte le istanze nelle sottoreti associate a una tabella di instradamento, a sua volta associata a un endpoint gateway, utilizzano automaticamente l'endpoint gateway per accedere al servizio. Le istanze presenti nelle sottoreti non associate a queste tabelle di instradamento utilizzano l'endpoint del servizio pubblico, non l'endpoint gateway.

- Una tabella di instradamento può presentare sia una route dell'endpoint verso Amazon S3 sia una route dell'endpoint verso DynamoDB. È possibile avere route dell'endpoint che fanno riferimento allo stesso servizio (Amazon S3 o DynamoDB) in più tabelle di instradamento. Tuttavia, non è possibile avere più route dell'endpoint per lo stesso servizio (Amazon S3 o DynamoDB) in una singola tabella di instradamento.
- La route più specifica che corrisponde al traffico viene utilizzata per determinare come istradare il traffico (corrispondenza prefisso più lungo). Per le tabelle di instradamento con una route dell'endpoint, questo significa che:
  - Se disponi di una route che invia tutto il traffico Internet (0.0.0.0/0) a un gateway Internet, la route dell'endpoint ha la precedenza per il traffico destinato al servizio (Amazon S3 o DynamoDB) nella regione corrente. Il traffico destinato a un altro utente Servizio AWS utilizza il gateway Internet.
  - Il traffico destinato al servizio (Amazon S3 o DynamoDB) in una regione diversa viene indirizzato verso il gateway Internet perché gli elenchi di prefissi sono specifici per una regione.
  - Se disponi di una route che specifica l'intervallo esatto di indirizzi IP per il servizio (Amazon S3 o DynamoDB) nella stessa regione, tale route ha la precedenza sulla route dell'endpoint.

Sicurezza

Quando le istanze accedono ad Amazon S3 o DynamoDB tramite un endpoint gateway, accedono al servizio tramite il relativo endpoint pubblico. I gruppi di sicurezza per queste istanze devono consentire il traffico dal servizio. Di seguito è riportato un esempio di una regola di uscita. Fa riferimento all'ID dell'elenco dei prefissi del servizio.

Destinazione	Protocollo	Intervallo porte
prefix_list_id	TCP	443

La rete ACLs per le sottoreti per questi casi deve inoltre consentire il traffico da e verso il servizio. Di seguito è riportato un esempio di una regola di uscita. Non è possibile fare riferimento agli elenchi di prefissi nelle regole ACL di rete, ma è possibile ottenere gli intervalli di indirizzi IP per il servizio dal relativo elenco di prefissi.

Destinazione	Protocollo	Intervallo porte
service_cidr_block_1	TCP	443
service_cidr_block_2	TCP	443
service_cidr_block_3	TCP	443

Tipo di indirizzo IP

Il tipo di indirizzo IP determina quale elenco di prefissi è associato alla tabella di routing.

Requisiti da abilitare IPv6 per un endpoint gateway

- Il tipo di indirizzo IP di un endpoint gateway deve essere compatibile con le sottoreti dell'endpoint gateway, come descritto di seguito:
  - IPv4— Aggiungere l'elenco dei IPv4 prefissi del servizio alla tabella delle rotte.
  - IPv6— Aggiungi l'elenco dei IPv6 prefissi del servizio alla tabella dei percorsi. Questa opzione è supportata solo se tutte le sottoreti selezionate sono IPv6 solo sottoreti.
  - Dualstack: aggiungi l'elenco dei IPv4 prefissi del servizio alla tabella delle rotte e aggiungi l'elenco dei prefissi del servizio alla tabella delle rotte. IPv6 Questa opzione è supportata solo se tutte le sottoreti selezionate hanno entrambi gli intervalli di indirizzi. IPv4 IPv6

Tipo IP del record DNS

Per impostazione predefinita, un endpoint gateway restituisce i record DNS in base all'endpoint del servizio chiamato. Se crei il tuo endpoint gateway utilizzando l'endpoint del IPv4 servizio, ad esempio Amazon S3 restituisce i record A ai tuoi clienti e tutte le sottoreti nella tabella di routing vengono utilizzati. `s3.us-east-2.amazonaws.com` IPv4

Al contrario, se crei il tuo endpoint gateway utilizzando l'endpoint del servizio dualstack, ad esempio, Amazon `s3.dualstack.us-east-2.amazonaws.com` S3 restituisce i record A e AAAA ai tuoi client e le sottoreti nella tua tabella di routing utilizzano e. IPv4 IPv6

> **Note**
>
> Per i directory bucket, o S3 Express One Zone, gli endpoint gateway per il piano dati sarebbero e rispettivamente. `s3express-use2-az1.us-east-2.amazonaws.com` `s3express-use2-az1.dualstack.us-east-2.amazonaws.com`

Il tipo di IP del record DNS influisce sul modo in cui il traffico viene indirizzato ai client. Se crei un endpoint gateway utilizzando l'endpoint del IPv4 servizio e poi chiami l'endpoint del servizio dualstack, il traffico che utilizza i record AAAA non verrà instradato attraverso l'endpoint del gateway. Il traffico verrà interrotto o indirizzato su un percorso compatibile, se presente. IPv6 Se utilizzi un tipo di IP di record DNS definito dal servizio, assicurati che il servizio sia in grado di gestire chiamate variabili da più endpoint di servizio.

Invece dell'impostazione predefinita del tipo di IP del record DNS definita dal servizio, puoi personalizzare il tipo IP del record DNS per scegliere quali record vengono restituiti per un endpoint specifico. La tabella seguente mostra i tipi di IP di record DNS supportati e i tipi di record restituiti:

Tipo IP di record DNS	Tipi di record restituiti
IPv4	A
IPv6	AAAA
Dualstack	A e AAAA
definito dal servizio	I record dipendono dall'endpoint del servizio

Per scegliere un tipo di IP di record DNS, è necessario utilizzare un tipo di indirizzo IP compatibile per il servizio endpoint. La tabella seguente mostra il tipo IP di record DNS supportato per ogni tipo di indirizzo IP per gli endpoint del gateway:

Tipo di indirizzo IP	Tipi di IP di record DNS supportati
IPv4	IPv4, definito dal servizio*
IPv6	IPv6, definito dal servizio*

Tipo di indirizzo IP	Tipi di IP di record DNS supportati
Dualstack	IPv4, IPv6 Dualstack, definito dal servizio*

* Rappresenta il tipo IP di record DNS predefinito.

> **Note**
>
> Per utilizzare tipi di IP di record DNS diversi da quelli definiti dal servizio per l'endpoint Gateway, è necessario consentire `enableDnsSupport` e attributi `enableDnsHostnames` nelle impostazioni VPC.

Non è possibile modificare il tipo IP del record DNS per un endpoint gateway DynamoDB. DynamoDB supporta solo il tipo IP di record DNS definito dal servizio.

Il comportamento del tipo IP del record DNS è diverso per gli endpoint dell'interfaccia. Per ulteriori informazioni, consulta Tipo di IP del record DNS per gli endpoint di interfaccia.

Endpoint gateway per Amazon S3

Puoi accedere ad Amazon S3 dal tuo VPC utilizzando gli endpoint VPC del gateway. Dopo aver creato l'endpoint gateway, puoi aggiungerlo come destinazione nella tabella di instradamento per il traffico in transito dal VPC ad Amazon S3.

L'utilizzo di endpoint gateway non comporta costi supplementari.

Amazon S3 supporta sia gli endpoint gateway che gli endpoint di interfaccia. Con un endpoint gateway, puoi accedere ad Amazon S3 dal tuo VPC senza richiedere un gateway Internet o un dispositivo NAT per il tuo VPC e senza costi aggiuntivi. Tuttavia, gli endpoint gateway non consentono l'accesso da reti locali, da reti peer-to-peer VPCs in altre AWS regioni o tramite un gateway di transito. Per questi casi, è necessario utilizzare un endpoint di interfaccia, disponibile a un costo aggiuntivo. Per ulteriori informazioni, consulta Tipi di endpoint VPC per Amazon S3 nella Guida per l'utente di Amazon S3.

Indice

- DNS privato
- Creare un endpoint gateway
- Controllo dell'accesso tramite le policy di bucket
- Associazione delle tabelle di instradamento
- Modifica della policy di endpoint VPC
- Eliminazione di un endpoint gateway

Considerazioni

- Un endpoint gateway è disponibile solo nella regione in cui è stato creato. Assicurati di creare l'endpoint gateway nella stessa regione dei bucket S3.
- Se utilizzi i server Amazon DNS, devi abilitare i nomi host DNS e la risoluzione DNS per il VPC. In alternativa, se utilizzi un server DNS, assicurati che le richieste destinate ad Amazon S3 vengano risolte correttamente negli indirizzi IP gestiti da AWS.
- Le regole per i gruppi di sicurezza per le istanze che accedono ad Amazon S3 tramite l'endpoint gateway devono consentire il traffico da e verso Amazon S3. Puoi fare riferimento all'ID dell'elenco dei prefissi per Amazon S3 nelle regole del gruppo di sicurezza.
- L'ACL di rete per la sottorete per le istanze che accedono ad Amazon S3 tramite l'endpoint gateway devono consentire il traffico da e verso Amazon S3. Non è possibile fare riferimento agli elenchi di prefissi nelle regole ACL di rete, ma è possibile ottenere gli intervalli di indirizzi IP per Amazon S3 dal relativo elenco di prefissi.
- Verifica se stai utilizzando un bucket S3 Servizio AWS che richiede l'accesso a un bucket S3. Ad esempio, un servizio potrebbe richiedere l'accesso a bucket che contengono file di registro o potrebbe richiedere il download di driver o agenti per le tue istanze. EC2 In tal caso, assicurati che la policy dell'endpoint consenta alla risorsa Servizio AWS o alla risorsa di accedere a questi bucket utilizzando l'azione. `s3:GetObject`
- Non è possibile utilizzare la condizione `aws:SourceIp` in una policy di identità o in una policy di bucket per le richieste ad Amazon S3 che attraversano un endpoint VPC. Utilizza invece la condizione `aws:VpcSourceIp`. In alternativa, puoi utilizzare le tabelle di routing per controllare quali EC2 istanze possono accedere ad Amazon S3 tramite l'endpoint VPC.
- La fonte IPv4 o IPv6 gli indirizzi delle istanze nelle sottoreti interessate ricevuti da Amazon S3 passano da indirizzi pubblici a indirizzi privati nel tuo VPC. Un endpoint cambia i percorsi di rete E disconnette le connessioni TCP aperte. Le connessioni precedenti che utilizzavano indirizzi pubblici non vengono ripristinate. Ti consigliamo di non eseguire attività critiche quando crei o modifichi un

endpoint; oppure di verificare che il software utilizzato sia in grado di riconnettersi automaticamente ad Amazon S3 dopo l'interruzione della connessione.

- Le connessioni endpoint non possono essere Estese all'esterno di un VPC. Le risorse sull'altro lato di una connessione VPN, di una connessione peering VPC, di un gateway di transito o di una Direct Connect connessione nel tuo VPC non possono utilizzare un endpoint gateway per comunicare con Amazon S3.
- Il tuo account ha una quota predefinita, ma modificabile, di 20 endpoint gateway per regione. Esiste inoltre un limite di 255 endpoint gateway per VPC.

DNS privato

Puoi configurare un DNS privato per ottimizzare i costi quando crei sia un endpoint gateway che un endpoint di interfaccia per Amazon S3.

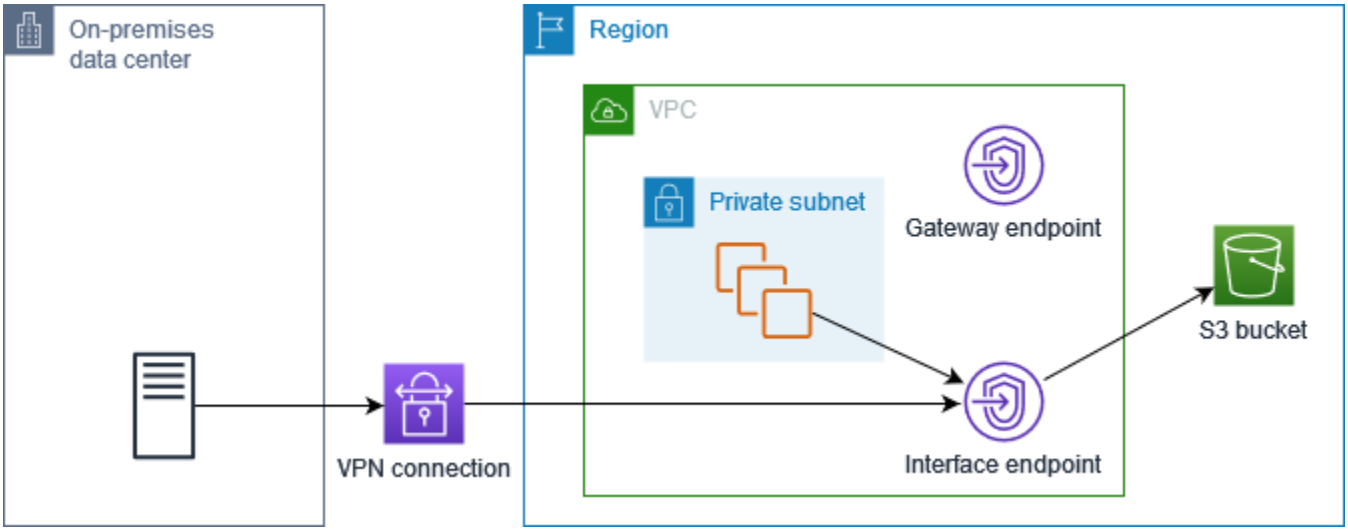
Risolutore Route 53

Amazon fornisce un server DNS chiamato il Route 53 Resolver per il tuo VPC. Il Route 53 Resolver risolve automaticamente i nomi di dominio VPC locali e i record in zone ospitate private. Tuttavia, non puoi utilizzare il Route 53 Resolver dall'esterno del tuo VPC. Route 53 fornisce gli endpoint e le regole del resolver in modo da poter utilizzare il Route 53 Resolver dall'esterno del VPC. Un endpoint del resolver in entrata inoltra le query DNS dalla rete on-premise al Route 53 Resolver. Un endpoint del resolver in uscita inoltra le query DNS dal Resolver Route 53 alla rete on-premise.

Quando configuri l'endpoint di interfaccia per Amazon S3 per utilizzare il DNS privato solo per l'endpoint del resolver in entrata, creiamo un endpoint del resolver in entrata. L'endpoint del resolver in entrata risolve le query DNS verso Amazon S3 dagli indirizzi IP on-premise a quelli privati dell'endpoint di interfaccia. Aggiungiamo anche i record ALIAS per il Resolver Route 53 alla zona ospitata pubblica per Amazon S3, in modo che le query DNS provenienti dal tuo VPC vengano risolte verso gli indirizzi IP pubblici di Amazon S3, che indirizzano il traffico verso l'endpoint del gateway.

DNS privato

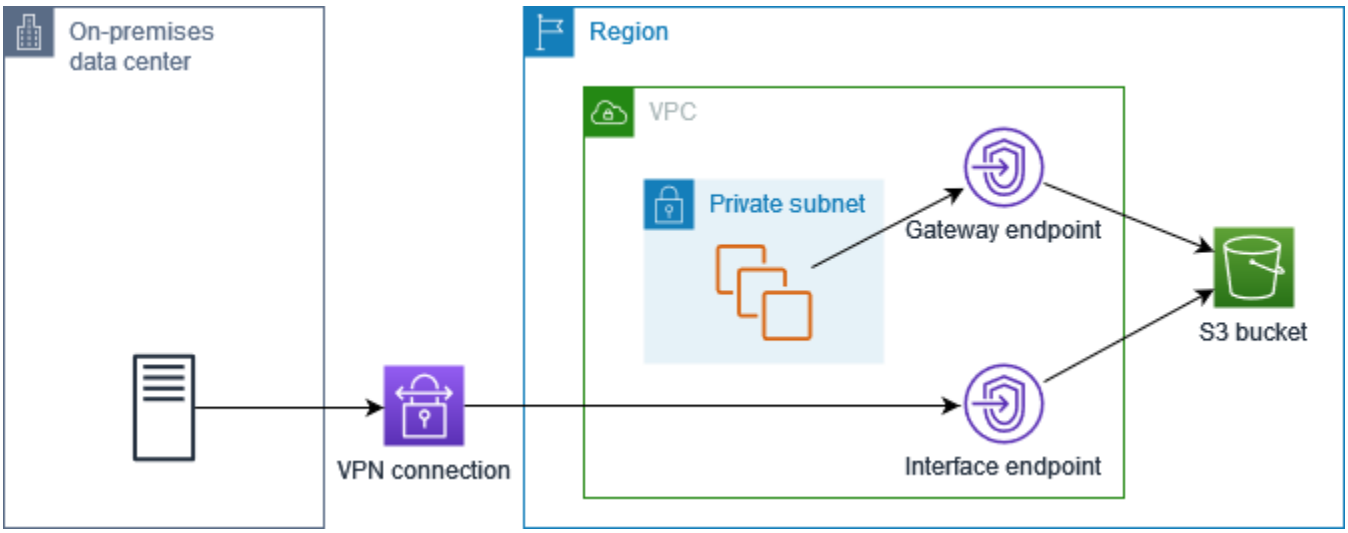
Se configuri il DNS privato per l'endpoint di interfaccia per Amazon S3 ma non configuri il DNS privato solo per l'endpoint del resolver in entrata, le richieste provenienti sia dalla rete on-premise che dal VPC utilizzano l'endpoint di interfaccia per accedere ad Amazon S3. Pertanto, paghi per utilizzare l'endpoint dell'interfaccia per il traffico proveniente dal VPC, anziché utilizzare l'endpoint gateway senza costi aggiuntivi.



DNS privato solo per l'endpoint del resolver in entrata

Se configuri il DNS privato solo per l'endpoint del resolver in entrata, le richieste provenienti dalla rete on-premise utilizzano l'endpoint di interfaccia per accedere ad Amazon S3 e le richiese provenienti dal tuo VPC utilizzano l'endpoint del gateway per accedere ad Amazon S3. Pertanto, ottimizzi i costi, perché paghi per utilizzare l'endpoint dell'interfaccia solo per il traffico che non può utilizzare l'endpoint del gateway.

Per configurarlo, il tipo di IP del record DNS dell'endpoint del gateway deve corrispondere o essere l'endpoint dell'interfaccia. `service-defined` AWS PrivateLink non supporta nessun'altra combinazione. Per ulteriori informazioni, consulta the section called “Tipo IP del record DNS”.



Configura il DNS privato

Puoi configurare il DNS privato per un endpoint di interfaccia per Amazon S3 quando lo crei o dopo averlo creato. Per ulteriori informazioni, vedere the section called “Creare un endpoint VPC” (configurazione durante la creazione) o the section called “Abilitazione dei nomi DNS privati” (configurazione dopo la creazione).

Creare un endpoint gateway

Utilizza la procedura seguente per creare un endpoint gateway che si connette ad Amazon S3.

Per creare un endpoint gateway tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Per Service category (Categoria servizio), scegli Servizi AWS.
5. Per i servizi, aggiungi il filtro Type = Gateway.

   Se i tuoi dati Amazon S3 sono archiviati in bucket generici, seleziona com.amazonaws.*region*.s3.

   Se i dati di Amazon S3 sono archiviati in bucket di directory, seleziona com.amazonaws.*region*.s3 express.
6. In VPC, seleziona un VPC in cui creare l'endpoint.
7. Per IP address type (Tipo di indirizzo IP), seleziona una delle opzioni seguenti:

   - IPv4— Assegna IPv4 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate hanno intervalli di IPv4 indirizzi e il servizio accetta le richieste. IPv4
   - IPv6— Assegna IPv6 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono IPv6 solo sottoreti e il servizio accetta le richieste. IPv6
   - Dualstack: assegna entrambi IPv4 gli indirizzi e alle interfacce di rete degli endpoint. IPv6 Questa opzione è supportata solo se tutte le sottoreti selezionate hanno entrambi intervalli di IPv6 indirizzi IPv4 e il servizio accetta entrambe le richieste. IPv4 IPv6
8. In Route tables (Tabelle di instradamento), seleziona le tabelle di instradamento che devono essere utilizzate dall'endpoint. Viene aggiunta automaticamente una route che indirizza il traffico destinato per il servizio all'interfaccia di rete dell'endpoint.

9. Per Policy, seleziona Full access (Accesso completo) per consentire tutte le operazioni da parte di tutti i principali su tutte le risorse dell'endpoint VPC. In caso contrario, seleziona Custom (Personalizza) per allegare una policy dell'endpoint VPC in grado di verificare le autorizzazioni di cui dispongono i principali per eseguire operazioni sulle risorse dell'endpoint VPC.
10. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
11. Seleziona Crea endpoint.

Per creare un endpoint gateway utilizzando la riga di comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Strumenti per Windows) PowerShell

Controllo dell'accesso tramite le policy di bucket

È possibile utilizzare le policy dei bucket per controllare l'accesso ai bucket da endpoint specifici VPCs, intervalli di indirizzi IP e. Account AWS Questi esempi presuppongono che vi siano anche dichiarazioni di policy che consentono l'accesso richiesto per i casi d'uso.

Example Esempio: limitazione dell'accesso a uno specifico endpoint

Puoi creare una policy di bucket che limita l'accesso a un endpoint specifico utilizzando la chiave di condizione aws:sourceVpce. La policy seguente nega l'accesso al bucket specificato utilizzando le azioni specificate a meno che non si utilizzi l'endpoint gateway specificato. Tieni presente che questa policy blocca l'accesso al bucket specificato utilizzando le azioni specificate tramite Console di gestione AWS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPCE",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
```

```
                "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example Esempio: limitazione dell'accesso a uno specifico VPC

Puoi creare una policy sui bucket che limiti l'accesso a elementi specifici utilizzando la chiave di condizione VPCs AWS:SourceVPC. Questa operazione è utile se si dispone di più endpoint configurati nello stesso VPC. La policy seguente nega l'accesso al bucket specificato utilizzando le azioni specificate a meno che non si utilizzi il VPC specificato. Tieni presente che questa policy blocca l'accesso al bucket specificato utilizzando le azioni specificate tramite Console di gestione AWS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-111bbb22"
        }
      }
    }
  ]
}
```

Example Esempio: limitazione dell'accesso a un intervallo di indirizzi IP specifici

Puoi creare una policy che limiti l'accesso a intervalli di indirizzi IP specifici utilizzando la chiave aws:condition. VpcSourceIp La policy seguente nega l'accesso al bucket specificato utilizzando le azioni specificate a meno che non si utilizzi l'indirizzo IP specificato. Tieni presente che questa policy blocca l'accesso al bucket specificato utilizzando le azioni specificate tramite Console di gestione AWS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC-CIDR",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
    }
  ]
}
```

Example Esempio: limita l'accesso ai bucket in uno specifico Account AWS

Puoi creare una policy che limita l'accesso ai bucket S3 in un Account AWS specifico utilizzando la chiave di condizione `s3:ResourceAccount`. La policy seguente nega l'accesso ai bucket S3 utilizzando le azioni specificate a meno che non appartengano a Account AWS specificato.

JSON

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

```
      "Sid": "Allow-access-to-bucket-in-specific-account",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:GetObject", "s3:PutObject", "s3:DeleteObject"],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

Associazione delle tabelle di instradamento

Puoi modificare le tabelle di instradamento associate all'endpoint gateway. Quando associ una tabella di instradamento, viene aggiunta automaticamente una route che indirizza il traffico destinato per il servizio all'interfaccia di rete dell'endpoint. Quando dissoci una tabella di instradamento, la route dell'endpoint viene rimossa automaticamente.

Per associare le tabelle di instradamento utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint gateway.
4. Selezionare Actions (Operazioni), Manage route tables (Gestisci tabelle di routing).
5. Seleziona o deseleziona le tabelle di instradamento in base alle esigenze.
6. Scegli Modify route tables (Modifica le tabelle di routing).

Per associare le tabelle di instradamento utilizzando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Modifica della policy di endpoint VPC

Puoi modificare la policy di endpoint per un endpoint gateway, che controlla l'accesso ad Amazon S3 dal VPC, tramite l'endpoint. Dopo avere aggiornato l'endpoint, possono essere necessari alcuni minuti prima che le modifiche diventino effettive. La policy predefinita consente l'accesso completo. Per ulteriori informazioni, consulta Policy di endpoint.

Per modificare la policy di endpoint usando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint gateway.
4. Scegli Actions (Operazioni), Manage policy (Gestisci policy).
5. Scegli Full Access (Accesso completo) per consentire l'accesso completo al servizio oppure scegli Custom (Personalizzato) e specifica una policy personalizzata.
6. Scegli Save (Salva).

Di seguito sono riportati esempi di policy dell'endpoint per accedere ad Amazon S3.

Example Esempio: limitazione dell'accesso a uno specifico bucket

Puoi creare una policy che limita l'accesso solo a specifici bucket S3. Ciò è utile se Servizi AWS nel tuo VPC ne hai altri che utilizzano bucket S3.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-bucket",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
         "s3:ListBucket",
         "s3:GetObject",
         "s3:PutObject"
      ],
      "Resource": [
```

```
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
      ]
    }
  ]
}
```

Example Esempio: limitazione dell'accesso a un ruolo IAM specifico

Puoi creare una policy che limita l'accesso a un ruolo IAM specifico. Devi utilizzare `aws:PrincipalArn` per concedere l'accesso a un principale.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-IAM-role",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
        }
      }
    }
  ]
}
```

Example Esempio: limitazione dell'accesso agli utenti in un account specifico

Puoi creare una policy che limita l'accesso a un account specifico.

JSON

```
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-callers-from-specific-account",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```

Eliminazione di un endpoint gateway

Quando un endpoint gateway non è più necessario, è possibile eliminarlo. L'eliminazione di un endpoint gateway comporta la rimozione della route dell'endpoint dalle tabelle di instradamento della sottorete.

Non è possibile eliminare un endpoint gateway se è abilitato il DNS privato.

Per eliminare un endpoint gateway usando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint gateway.
4. Seleziona Actions (Operazioni), Delete VPC endpoints (Eliminazione di endpoint VPC).
5. Quando viene richiesta la conferma, immetti **`delete`**.
6. Scegli Elimina.

Per eliminare un endpoint gateway usando la riga di comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Strumenti per Windows) PowerShell

Endpoint gateway per Amazon DynamoDB

Puoi accedere ad Amazon DynamoDB dal tuo VPC utilizzando gli endpoint VPC del gateway. Dopo aver creato l'endpoint gateway, puoi aggiungerlo come destinazione nella tabella di instradamento per il traffico in transito dal VPC a DynamoDB.

L'utilizzo di endpoint gateway non comporta costi supplementari.

DynamoDB supporta sia gli endpoint gateway che gli endpoint di interfaccia. Con un endpoint gateway, puoi accedere a DynamoDB dal tuo VPC, senza richiedere un gateway Internet o un dispositivo NAT per il tuo VPC e senza costi aggiuntivi. Tuttavia, gli endpoint gateway non consentono l'accesso da reti locali, da reti peer-to-peer VPCs in altre regioni o tramite un gateway di transito. AWS Per questi casi, è necessario utilizzare un endpoint di interfaccia, disponibile a un costo aggiuntivo. Per ulteriori informazioni, consulta Tipi di endpoint VPC per DynamoDB nella Amazon DynamoDB Developer Guide.

Indice

Considerazioni

- Un endpoint gateway è disponibile solo nella regione in cui è stato creato. Assicurati di creare l'endpoint gateway nella stessa regione delle tabelle DynamoDB.
- Se utilizzi i server Amazon DNS, devi abilitare i nomi host DNS e la risoluzione DNS per il VPC. In alternativa, se utilizzi un server DNS, assicurati che le richieste destinate a DynamoDB vengano risolte correttamente negli indirizzi IP gestiti da AWS.
- Le regole per i gruppi di sicurezza per le istanze che accedono a DynamoDB tramite l'endpoint gateway devono consentire il traffico da e verso DynamoDB. Puoi fare riferimento all'ID dell'elenco dei prefissi per DynamoDB nelle regole del gruppo di sicurezza.
- L'ACL di rete per la sottorete per le istanze che accedono a DynamoDB tramite l'endpoint gateway devono consentire il traffico da e verso DynamoDB. Non è possibile fare riferimento agli elenchi di

prefissi nelle regole ACL di rete, ma è possibile ottenere gli intervalli di indirizzi IP per DynamoDB dal relativo elenco di prefissi.

- Se si utilizza AWS CloudTrail per registrare le operazioni DynamoDB, i file di registro contengono gli indirizzi IP privati delle istanze EC2 nel VPC del service consumer e l'ID dell'endpoint gateway per tutte le richieste eseguite tramite l'endpoint.
- Gli endpoint del gateway supportano solo il traffico. IPv4
- IPv4 Gli indirizzi di origine delle istanze nelle sottoreti interessate cambiano da IPv4 indirizzi pubblici a IPv4 indirizzi privati del tuo VPC. Un endpoint cambia le route di rete e disconnette le connessioni TCP aperte. Le connessioni precedenti che utilizzavano IPv4 indirizzi pubblici non vengono ripristinate. Ti consigliamo di non eseguire attività critiche quando crei o modifichi un endpoint gateway. In alternativa, verifica che il software utilizzato sia in grado di riconnettersi automaticamente a DynamoDB in caso di interruzione della connessione.
- Le connessioni endpoint non possono essere Estese all'esterno di un VPC. Le risorse sull'altro lato di una connessione VPN, di una connessione peering VPC, di un gateway di transito o di una Direct Connect connessione nel tuo VPC non possono utilizzare un endpoint gateway per comunicare con DynamoDB.
- Il tuo account ha una quota predefinita, ma modificabile, di 20 endpoint gateway per regione. Esiste inoltre un limite di 255 endpoint gateway per VPC.

Creare un endpoint gateway

Utilizza la procedura seguente per creare un endpoint gateway che si connette a DynamoDB.

Per creare un endpoint gateway tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Per Service category (Categoria servizio), scegli Servizi AWS.
5. Per Servizi, aggiungi il filtro Type = Gateway e seleziona com.amazonaws. *region*.dynamodb.
6. In VPC, seleziona un VPC in cui creare l'endpoint.
7. In Route tables (Tabelle di instradamento), seleziona le tabelle di instradamento che devono essere utilizzate dall'endpoint. Viene aggiunta automaticamente una route che indirizza il traffico destinato per il servizio all'interfaccia di rete dell'endpoint.

8. Per Policy, seleziona Full access (Accesso completo) per consentire tutte le operazioni da parte di tutti i principali su tutte le risorse dell'endpoint VPC. In caso contrario, seleziona Custom (Personalizza) per allegare una policy dell'endpoint VPC in grado di verificare le autorizzazioni di cui dispongono i principali per eseguire operazioni sulle risorse dell'endpoint VPC.
9. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
10. Seleziona Crea endpoint.

Per creare un endpoint gateway utilizzando la riga di comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Strumenti per Windows) PowerShell

Controllo dell'accesso utilizzando le policy IAM

Puoi creare policy IAM per controllare quali principali IAM possono accedere alle tabelle DynamoDB utilizzando un endpoint VPC specifico.

Example Esempio: limitazione dell'accesso a uno specifico endpoint

Puoi creare una policy che limita l'accesso a un endpoint VPC specifico utilizzando la chiave di condizione aws:sourceVpce. La policy seguente nega l'accesso alle tabelle DynamoDB nell'account a meno che non si utilizzi l'endpoint VPC specificato. Questo esempio presuppone che vi sia anche una dichiarazione di policy che consente l'accesso richiesto per i casi d'uso.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-endpoint",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:us-east-1:111111111111:table/*",
         "Condition": {
            "StringNotEquals" : {
               "aws:sourceVpce": "vpce-11aa22bb"
```

```
            }
         }
      }
   ]
}
```

Example Esempio: concessione dell'accesso da un ruolo IAM specifico

Puoi creare una policy che consente l'accesso utilizzando un ruolo IAM specifico. La policy seguente concede l'accesso al ruolo IAM specificato.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-IAM-role",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "ArnEquals": {
               "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
            }
         }
      }
   ]
}
```

Example Esempio: concessione dell'accesso da un account specifico

Puoi creare una policy che consente l'accesso solo da un account specifico. La policy seguente concede l'accesso agli utenti nell'account specificato.

JSON

```
{
```

```
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-account",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "aws:PrincipalAccount": "111122223333"
            }
         }
      }
   ]
}
```

Associazione delle tabelle di instradamento

Puoi modificare le tabelle di instradamento associate all'endpoint gateway. Quando associ una tabella di instradamento, viene aggiunta automaticamente una route che indirizza il traffico destinato per il servizio all'interfaccia di rete dell'endpoint. Quando dissoci una tabella di instradamento, la route dell'endpoint viene rimossa automaticamente.

Per associare le tabelle di instradamento utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint gateway.
4. Selezionare Actions (Operazioni), Manage route tables (Gestisci tabelle di routing).
5. Seleziona o deseleziona le tabelle di instradamento in base alle esigenze.
6. Scegli Modify route tables (Modifica le tabelle di routing).

Per associare le tabelle di instradamento utilizzando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Modifica della policy di endpoint VPC

Puoi modificare la policy di endpoint per un endpoint gateway, che controlla l'accesso a DynamoDB dal VPC, tramite l'endpoint. Dopo avere aggiornato l'endpoint, possono essere necessari alcuni minuti prima che le modifiche diventino effettive. La policy predefinita consente l'accesso completo. Per ulteriori informazioni, consulta Policy di endpoint.

Per modificare la policy di endpoint usando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint gateway.
4. Scegli Actions (Operazioni), Manage policy (Gestisci policy).
5. Scegli Full Access (Accesso completo) per consentire l'accesso completo al servizio oppure scegli Custom (Personalizzato) e specifica una policy personalizzata.
6. Scegli Save (Salva).

Per modificare un endpoint gateway usando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Di seguito sono riportati esempi di policy dell'endpoint per accedere a DynamoDB.

Example Esempio: concessione dell'accesso in sola lettura

Puoi creare una policy che concede l'accesso in sola lettura. La policy seguente concede l'autorizzazione per elencare e descrivere le tabelle DynamoDB.

```
{
  "Statement": [
    {
      "Sid": "ReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:ListTables"
```

```
      ],
      "Resource": "*"
    }
  ]
}
```

Example Esempio: limitare l'accesso a una tabella specifica

È possibile creare una policy che limita l'accesso a una tabella DynamoDB specifica. La policy seguente consente l'accesso alla tabella DynamoDB specificata.

```
{
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-table",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Resource": "arn:aws:dynamodb:region:123456789012:table/table_name"
    }
  ]
}
```

Eliminazione di un endpoint gateway

Quando un endpoint gateway non è più necessario, è possibile eliminarlo. L'eliminazione di un endpoint gateway comporta la rimozione della route dell'endpoint dalle tabelle di instradamento della sottorete.

Per eliminare un endpoint gateway usando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint gateway.

4. Seleziona Actions (Operazioni), Delete VPC endpoints (Eliminazione di endpoint VPC).
5. Quando viene richiesta la conferma, immetti **`delete`**.
6. Scegli Elimina.

Per eliminare un endpoint gateway usando la riga di comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Accedi ai prodotti SaaS tramite AWS PrivateLink

Utilizzando AWS PrivateLink, puoi accedere ai prodotti SaaS in privato, come se fossero in esecuzione nel tuo VPC.

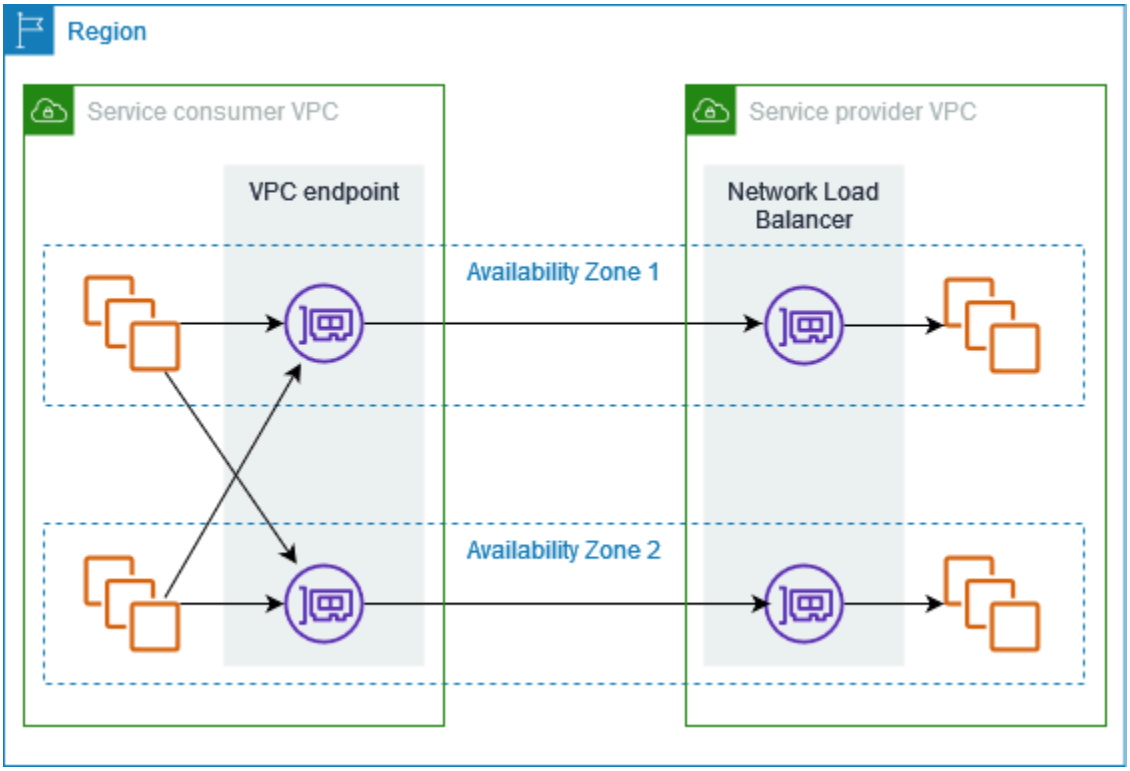
Indice

Panoramica

Puoi scoprire, acquistare ed effettuare il provisioning di prodotti SaaS con tecnologia Through. AWS PrivateLink Marketplace AWS Per ulteriori informazioni, consulta Accedere alle applicazioni SaaS in modo sicuro e privato. AWS PrivateLink

Puoi anche trovare prodotti SaaS forniti AWS PrivateLink da AWS Partners. Per ulteriori informazioni, consulta Partner AWS PrivateLink.

Il diagramma seguente mostra come utilizzare gli endpoint VPC per connetterti ai prodotti SaaS. Il provider di servizi crea un servizio endpoint e garantisce ai propri clienti l'accesso al servizio endpoint. L'utente del servizio crea un endpoint VPC dell'interfaccia che stabilisce le connessioni tra una o più sottoreti nel VPC e il servizio endpoint.



Creazione di un endpoint di interfaccia

Utilizza la procedura seguente per creare un endpoint VPC dell'interfaccia in grado di connettersi al prodotto SaaS.

Requisito

Iscriversi al servizio.

Per creare un endpoint di interfaccia a un servizio partener

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Se hai acquistato il servizio da Marketplace AWS, procedi come segue:
    a. Per Tipo, scegli Marketplace AWS i servizi.
    b. Seleziona il servizio.
5. Se ti sei abbonato a un servizio con la designazione AWS Service Ready, procedi come segue:

   a. Per Tipo, scegli i servizi partner PrivateLink Ready.
   b. Inserisci il nome del servizio, quindi scegli Verifica servizio.
6. Per VPC, seleziona il VPC da cui accederai al prodotto.
7. Per Subnet, seleziona le sottoreti in cui creare interfacce di rete endpoint.
8. Per Security groups (Gruppi di sicurezza), seleziona i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint. Le regole del gruppo di sicurezza devono consentire il traffico tra le risorse nel VPC e le interfacce di rete dell'endpoint.
9. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
10. Seleziona Crea endpoint.

Per configurare un endpoint di interfaccia

Per ulteriori informazioni sulla configurazione dell'endpoint di interfaccia, consulta the section called “Configurazione di un endpoint dell'interfaccia”.

Accedi alle appliance virtuali tramite AWS PrivateLink

Puoi utilizzare un Gateway Load Balancer per distribuire il traffico a una flotta di appliance virtuali di rete. Le appliance possono essere utilizzate per ispezioni di sicurezza, conformità, controlli delle policy e altri servizi di rete. Quando crei un servizio endpoint VPC, specifica il Gateway Load Balancer. Gli altri principali AWS possono accedere al servizio endpoint creando un Endpoint Gateway Load Balancer.

Prezzi

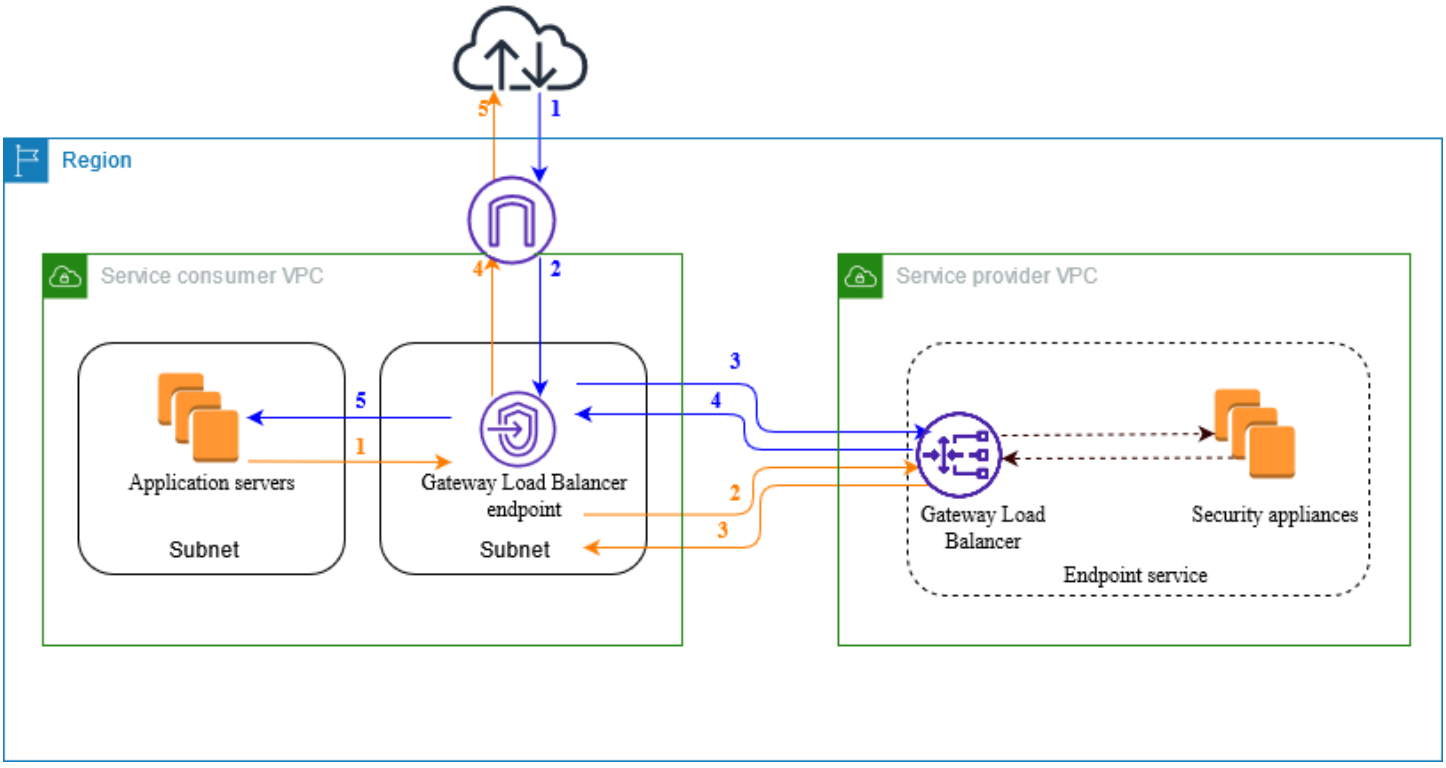
La fatturazione viene calcolata per ogni ora di provisioning dell'endpoint Gateway Load Balancer in ciascuna zona di disponibilità. Ti viene inoltre addebitato un importo per GB di dati elaborati. Per ulteriori informazioni, consultare AWS PrivateLink Prezzi.

Indice

Per ulteriori informazioni, consultare Bilanciatori del carico del gateway.

Panoramica

Il diagramma seguente mostra in che modo i server delle applicazioni accedono alle appliance di sicurezza tramite. AWS PrivateLink I server dell'applicazione vengono eseguiti in una sottorete del VPC dell'utente del servizio. Crea un endpoint Gateway Load Balancer in un'altra sottorete dello stesso VPC. Tutto il traffico che entra nel VPC dell'utente del servizio attraverso il gateway Internet viene innanzitutto instradato all'endpoint Gateway Load Balancer per l'ispezione e poi instradato alla sottorete di destinazione. Analogamente, tutto il traffico che esce dai server dell'applicazione viene instradato sull'endpoint Gateway Load Balancer per l'ispezione prima di essere instradato nuovamente attraverso il gateway Internet.



Traffico in transito da Internet ai server dell'applicazione (frecce blu):

1. Il traffico entra nel VPC dell'utente del servizio attraverso il gateway Internet.
2. Il traffico viene inviato all'endpoint Gateway Load Balancer in base alla configurazione della tabella di instradamento.
3. Il traffico viene inviato al Gateway Load Balancer per l'ispezione tramite l'appliance di sicurezza.
4. Il traffico viene inviato nuovamente all'endpoint Gateway Load Balancer dopo l'ispezione.
5. Il traffico viene inviato ai server dell'applicazione in base alla configurazione della tabella di instradamento.

Traffico in transito dai server dell'applicazione a Internet (frecce arancioni):

1. Il traffico viene inviato all'endpoint Gateway Load Balancer in base alla configurazione della tabella di instradamento.
2. Il traffico viene inviato al Gateway Load Balancer per l'ispezione tramite l'appliance di sicurezza.
3. Il traffico viene inviato nuovamente all'endpoint Gateway Load Balancer dopo l'ispezione.
4. Il traffico viene inviato al gateway Internet in base alla configurazione della tabella di instradamento.

5. Il traffico viene reindirizzato a Internet.

Tipi di indirizzi IP

I provider di servizi possono rendere disponibili i propri endpoint di servizio ai consumatori di servizi tramite o entrambi i dispositivi IPv4 IPv6 IPv6, anche se IPv4 le proprie appliance di sicurezza supportano solo il supporto. IPv4 Se abiliti il supporto dualstack, i consumatori esistenti possono continuare a utilizzarlo per accedere IPv4 al tuo servizio e i nuovi consumatori possono scegliere di utilizzare IPv6 per accedere al tuo servizio.

Se un endpoint Gateway Load Balancer supporta IPv4, le interfacce di rete degli endpoint dispongono di indirizzi. IPv4 Se un endpoint Gateway Load Balancer supporta IPv6, le interfacce di rete degli endpoint dispongono di indirizzi. IPv6 L' IPv6 indirizzo per un'interfaccia di rete endpoint non è raggiungibile da Internet. Se descrivi un'interfaccia di rete endpoint con un IPv6 indirizzo, nota che è abilitata. `denyAllIgwTraffic`

Requisiti per l'attivazione IPv6 di un servizio endpoint

- Il VPC e le sottoreti per il servizio endpoint devono avere blocchi CIDR associati. IPv6
- Il Gateway Load Balancer per il servizio endpoint deve utilizzare il tipo di indirizzo IP dualstack. Le appliance di sicurezza non devono supportare il traffico. IPv6

Requisiti per l'abilitazione IPv6 di un endpoint Gateway Load Balancer

- Il servizio endpoint deve avere un tipo di indirizzo IP che includa il supporto. IPv6
- Il tipo di indirizzo IP di un endpoint Gateway Load Balancer deve essere compatibile con la sottorete dell'endpoint Gateway Load Balancer, come descritto di seguito:
  - IPv4— Assegna IPv4 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate hanno intervalli di indirizzi. IPv4
  - IPv6— Assegna IPv6 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono solo sottoreti. IPv6
  - Dualstack: assegna entrambi IPv4 gli indirizzi alle interfacce di rete degli endpoint. IPv6 Questa opzione è supportata solo se tutte le sottoreti selezionate hanno entrambi gli intervalli di indirizzi. IPv4 IPv6
- Le tabelle di routing per le sottoreti nel VPC del consumatore di servizi devono instradare il IPv6 traffico e la rete ACLs per queste sottoreti deve consentire il traffico. IPv6

Routing

Per instradare il traffico al servizio endpoint, specifica l'endpoint Gateway Load Balancer come destinazione nelle tabelle di instradamento, utilizzando il relativo ID. Partendo dal diagramma precedente, aggiungi le route alle tabelle di instradamento, come descritto di seguito. Quando si utilizza un endpoint Gateway Load Balancer come destinazione, non è possibile specificare un elenco di prefissi come destinazione. In queste tabelle, sono inclusi i IPv6 percorsi per una configurazione dualstack.

Tabella di instradamento per il gateway Internet

Questa tabella di instradamento deve disporre di una route che invia il traffico destinato ai server dell'applicazione all'endpoint Gateway Load Balancer.

Destinazione	Target
VPC IPv4 CIDR	Locale
VPC IPv6 CIDR	Locale
Application subnet IPv4 CIDR	*vpc-endpoint-id*
Application subnet IPv6 CIDR	*vpc-endpoint-id*

Tabella di instradamento per la sottorete con i server dell'applicazione

Questa tabella di instradamento deve disporre di una route che invia tutto il traffico dai server dell'applicazione all'endpoint Gateway Load Balancer.

Destinazione	Target
VPC IPv4 CIDR	Locale
VPC IPv6 CIDR	Locale
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Tabella di instradamento per la sottorete con l'endpoint Gateway Load Balancer

Questa tabella di instradamento deve indirizzare il traffico restituito dall'ispezione alla destinazione finale. Per il traffico proveniente da Internet, la route locale invia il traffico ai server dell'applicazione. Per il traffico proveniente dai server dell'applicazione, aggiungi una route che invii tutto il traffico al gateway Internet.

Destinazione	Target
VPC IPv4 CIDR	Locale
VPC IPv6 CIDR	Locale
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

Creazione di un sistema di ispezione come servizio endpoint Gateway Load Balancer

È possibile creare il proprio servizio basato su AWS PrivateLink, noto come servizio endpoint. Tu sei il fornitore di servizi e AWS i principali responsabili che creano connessioni al tuo servizio sono i consumatori del servizio.

I servizi endpoint richiedono un Network Load Balancer o un Gateway Load Balancer. In questo caso, creerai un servizio endpoint utilizzando un Gateway Load Balancer. Per ulteriori informazioni sulla creazione di un servizio endpoint tramite un Network Load Balancer, consulta la pagina Creazione di un servizio endpoint.

Indice

Considerazioni

- Un servizio endpoint è disponibile nella regione in cui è stato creato.
- Quando gli utenti del servizio recuperano le informazioni relative a un servizio endpoint, possono visualizzare solo le zone di disponibilità in comune con il provider di servizi. Se il provider di servizi e l'utente si trovano in account diversi, un nome della zona di disponibilità, ad esempio `us-east-1a`, potrebbe essere mappato a una zona di disponibilità fisica diversa in ciascun Account AWS. Puoi utilizzare AZ IDs per identificare in modo coerente le zone di disponibilità per il tuo servizio. Per ulteriori informazioni, consulta AZ IDs nella Amazon EC2 User Guide.
- Le tue AWS PrivateLink risorse sono soggette a quote. Per ulteriori informazioni, consulta AWS PrivateLink quote.

Prerequisiti

- Creare un VPC del provider di servizi con almeno due sottoreti nella zona di disponibilità in cui il servizio deve essere disponibile. Una sottorete è destinata alle istanze dell'appliance di sicurezza e l'altra al Gateway Load Balancer.
- Creare un Gateway Load Balancer nel VPC del provider di servizi. Se prevedi di abilitare il IPv6 supporto sul tuo servizio endpoint, devi abilitare il supporto dualstack sul tuo Gateway Load Balancer. Per ulteriori informazioni, consulta Nozioni di base su Gateway Load Balancer.
- Avviare le appliance di sicurezza nel VPC del provider di servizi e registrale con un gruppo di destinazione del load balancer.

Creazione del servizio endpoint

Utilizza la procedura seguente per creare un servizio endpoint utilizzando un Gateway Load Balancer.

Per creare un servizio endpoint tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Scegli Create Endpoint Service (Crea servizio endpoint).
4. Per Load balancer type (Tipo di load balancer), scegli Gateway.
5. In Available load balancers (Load balancer disponibili), seleziona il Gateway Load Balancer.

6. In Require acceptance for endpoint (Richiedi accettazione per l'endpoint), seleziona Acceptance required (Accettazione richiesta) per richiedere l'accettazione manuale delle richieste di connessione al servizio endpoint. In caso contrario, queste vengono accettate automaticamente.
7. Per Supported IP address types (Tipi di indirizzo IP supportati), esegui una delle operazioni seguenti:
   - Seleziona IPv4: abilita il servizio endpoint ad accettare le richieste. IPv4
   - Seleziona IPv6: abilita il servizio endpoint ad accettare IPv6 le richieste.
   - Seleziona IPv4e IPv6: abilita il servizio endpoint ad accettare entrambe IPv4 le IPv6 richieste.
8. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
9. Scegli Create (Crea).

Per creare un servizio endpoint utilizzando la riga di comando

- create-vpc-endpoint-service-configurazione ()AWS CLI
- New-EC2VpcEndpointServiceConfiguration(Strumenti per Windows PowerShell)

Rendere disponibile il servizio endpoint

Per mettere a disposizione i propri servizi agli utenti, i provider devono eseguire le operazioni seguenti.

- Aggiungere le autorizzazioni che consentono a ciascun utente del servizio di connettersi al servizio endpoint. Per ulteriori informazioni, consulta the section called “Gestione delle autorizzazioni”.
- Fornire all'utente del servizio il nome del servizio e le zone di disponibilità supportate in modo che possa creare un endpoint dell'interfaccia per connettersi al servizio. Per ulteriori informazioni, consultare la procedura seguente.
- Accettare la richiesta di connessione all'endpoint inviata dall'utente del servizio. Per ulteriori informazioni, consulta the section called “Accettare o rifiutare le richieste di connessione”.

AWS i responsabili possono connettersi al servizio endpoint in modo privato creando un endpoint Gateway Load Balancer. Per ulteriori informazioni, consulta Crea un endpoint Gateway Load Balancer.

Accesso a un sistema di ispezione utilizzando un endpoint Gateway Load Balancer

Puoi creare un endpoint del sistema di bilanciamento del carico del gateway per connetterti ai servizi dell'endpoint basati su AWS PrivateLink.

Per ogni sottorete specificata dal VPC, creiamo un'interfaccia di rete dell'endpoint nella sottorete e le assegniamo un indirizzo IP privato dall'intervallo di indirizzi della sottorete. Un'interfaccia di rete per endpoint è un'interfaccia di rete gestita dal richiedente; puoi visualizzarla nel tuo dispositivo Account AWS, ma non puoi gestirla tu stesso.

Ti viene addebitato l'utilizzo orario e le spese di elaborazione dati. Per ulteriori informazioni, consulta Prezzi dell'endpoint Gateway Load Balancer.

Indice

Considerazioni

- Puoi selezionare una sola zona di disponibilità nel VPC dell'utente del servizio. Non puoi modificare questa sottorete in un secondo momento. Per utilizzare un endpoint Gateway Load Balancer in una sottorete diversa, dovrai creare un nuovo endpoint Gateway Load Balancer.
- Puoi creare un solo endpoint Gateway Load Balancer per zona di disponibilità per un servizio, selezionando la zona di disponibilità supportata da Gateway Load Balancer. Se il provider di servizi e l'utente si trovano in account diversi, un nome della zona di disponibilità, ad esempio `us-east-1a`, potrebbe essere mappato a una zona di disponibilità fisica diversa in ciascun Account AWS. Puoi utilizzare AZ IDs per identificare in modo coerente le zone di disponibilità per il tuo servizio. Per ulteriori informazioni, consulta AZ IDs nella Amazon EC2 User Guide.

- Prima di poter utilizzare il servizio endpoint, il provider di servizi deve accettare le richieste di connessione. I servizi non possono avviare richieste alle risorse nel VPC tramite l'endpoint VPC. L'endpoint restituisce solo il traffico avviato dalle risorse nel VPC.
- Ogni endpoint Gateway Load Balancer può supportare una larghezza di banda massima di 10 Gpbs per zona di disponibilità e aumenta automaticamente fino a 100 Gbps.
- Se un servizio endpoint è associato a più Gateway Load Balancer, per una zona di disponibilità specifica un endpoint Gateway Load Balancer stabilirà una connessione con un solo load balancer.
- Per mantenere il traffico all'interno della stessa zona di disponibilità, è consigliabile creare un endpoint Gateway Load Balancer in ogni zona di disponibilità a cui verrà inviato il traffico.
- La conservazione dell'IP del client del Network Load Balancer non è supportata quando il traffico viene instradato attraverso un endpoint di load balancer del gateway, anche se la destinazione si trova nello stesso VPC del Network Load Balancer.
- Se i server delle applicazioni e l'endpoint Gateway Load Balancer si trovano nella stessa sottorete, le regole NACL vengono valutate per il traffico dai server delle applicazioni all'endpoint Gateway Load Balancer.
- Se si utilizza un Gateway Load Balancer con un gateway Internet di sola uscita, il traffico viene interrotto. IPv6 Utilizza invece un gateway Internet e le regole del firewall in entrata.
- Le tue AWS PrivateLink risorse sono soggette a quote. Per ulteriori informazioni, consulta AWS PrivateLink quote.

Prerequisiti

- Creare un VPC dell'utente del servizio con almeno due sottoreti nella zona di disponibilità da cui accederai al servizio. Una sottorete è destinata ai server dell'applicazione e l'altra all'endpoint Gateway Load Balancer.
- Per verificare quali zone di disponibilità sono supportate dal servizio endpoint, descrivi il servizio endpoint utilizzando la console o il comando. describe-vpc-endpoint-services
- Se le risorse si trovano in una sottorete con un ACL di rete, verifica che l'ACL di rete consenta il traffico tra le interfacce di rete dell'endpoint e le risorse nel VPC.

Creare l'endpoint

Utilizza la procedura seguente per creare un endpoint Gateway Load Balancer che si connette al servizio endpoint per il sistema di ispezione.

Per creare un endpoint Gateway Load Balancer utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Per Tipo, scegli i servizi Endpoint che utilizzano e. NLBs GWLBs
5. In Service name (Nome servizio), specifica il nome del servizio, quindi seleziona Verify service (Verifica servizio).
6. Per VPC, seleziona il VPC da cui accederai al servizio endpoint.
7. Per le sottoreti, seleziona una sottorete in cui creare un'interfaccia di rete endpoint.
8. Per IP address type (Tipo di indirizzo IP), seleziona una delle opzioni seguenti:
   - IPv4— Assegna IPv4 indirizzi all'interfaccia di rete degli endpoint. Questa opzione è supportata solo se la sottorete selezionata ha un IPv4 intervallo di indirizzi.
   - IPv6— Assegna IPv6 indirizzi all'interfaccia di rete dell'endpoint. Questa opzione è supportata solo se la sottorete selezionata è un' IPv6 unica sottorete.
   - Dualstack: assegna entrambi IPv6 gli indirizzi all'interfaccia di rete dell' IPv4 endpoint. Questa opzione è supportata solo se la sottorete selezionata include entrambi gli intervalli di indirizzi. IPv4 IPv6
9. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
10. Seleziona Crea endpoint. Lo stato iniziale è `pending acceptance`.

Per creare un endpoint Gateway Load Balancer utilizzando la riga di comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Configurazione del routing

Utilizza la procedura seguente per configurare le tabelle di instradamento per il VPC dell'utente del servizio. Ciò consente alle appliance di sicurezza di eseguire ispezioni per il traffico in entrata destinato ai server dell'applicazione. Per ulteriori informazioni, consulta the section called “Routing”.

Per configurare l'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).
3. Seleziona la tabella di instradamento per il gateway Internet ed esegui le operazioni seguenti:
   a. Selezionare Actions (Operazioni), Edit routes (Modifica route).
   b. Se lo supporti IPv4, scegli Aggiungi percorso. Per Destinazione, inserisci il blocco IPv4 CIDR della sottorete per i server delle applicazioni. Per Target, seleziona l'endpoint VPC.
   c. Se lo supporti IPv6, scegli Aggiungi percorso. Per Destinazione, inserisci il blocco IPv6 CIDR della sottorete per i server delle applicazioni. Per Target, seleziona l'endpoint VPC.
   d. Scegli Save changes (Salva modifiche).
4. Seleziona la tabella di instradamento per la sottorete con i server dell'applicazione ed esegui le operazioni seguenti:
   a. Selezionare Actions (Operazioni), Edit routes (Modifica route).
   b. Se lo supporti IPv4, scegli Aggiungi percorso. In Destination (Destinazione), immettere **`0.0.0.0/0`**. Per Target, seleziona l'endpoint VPC.
   c. Se supporti IPv6, scegli Aggiungi percorso. In Destination (Destinazione), immettere **`::/0`**. Per Target, seleziona l'endpoint VPC.
   d. Scegli Save changes (Salva modifiche).
5. Seleziona la tabella di instradamento per la sottorete con l'endpoint Gateway Load Balancer ed esegui le operazioni seguenti:
   a. Selezionare Actions (Operazioni), Edit routes (Modifica route).
   b. Se supporti IPv4, scegli Aggiungi percorso. In Destination (Destinazione), immettere **`0.0.0.0/0`**. Per Target, seleziona il gateway Internet.
   c. Se supporti IPv6, scegli Aggiungi percorso. In Destination (Destinazione), immettere **`::/0`**. Per Target, seleziona il gateway Internet.
   d. Scegli Save changes (Salva modifiche).

Per configurare l'instradamento utilizzando la riga di comando

- create-route (AWS CLI)
- New-EC2Route(Strumenti per Windows PowerShell)

Gestisci tag

Puoi contrassegnare l'endpoint Gateway Load Balancer per identificarlo o classificarlo più facilmente in base alle esigenze dell'organizzazione.

Per gestire i tag utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint dell'interfaccia.
4. Scegliere Actions (Operazioni), Manage tags (Gestisci tag).
5. Per ogni tag da aggiungere, seleziona Add new tag (Aggiungi nuovo tag) e immetti la chiave e il valore per il tag.
6. Per rimuovere un tag, scegli Remove (Rimuovi) a destra della chiave e del valore del tag.
7. Scegli Save (Salva).

Per gestire i tag utilizzando la riga di comando

- create-tags e delete-tags (AWS CLI)
- New-EC2Tage Remove-EC2Tag(Strumenti per Windows PowerShell)

Eliminazione di un endpoint Gateway Load Balancer

Quando un endpoint non è più necessario, è possibile eliminarlo. L'eliminazione di un endpoint Gateway Load Balancer comporta anche l'eliminazione delle interfacce di rete dell'endpoint. Un endpoint Gateway Load Balancer non può essere eliminato se nelle tabelle di instradamento sono presenti route che puntano all'endpoint.

Per eliminare un endpoint Gateway Load Balancer

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Endpoints (Endpoint) e selezionare l'endpoint.
3. Selezionare Actions (Operazioni), Delete Endpoint (Elimina endpoint).
4. Nella schermata di conferma, selezionare Yes, Delete (Sì, elimina).

Per eliminare un endpoint Gateway Load Balancer

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (AWS Tools for Windows PowerShell)

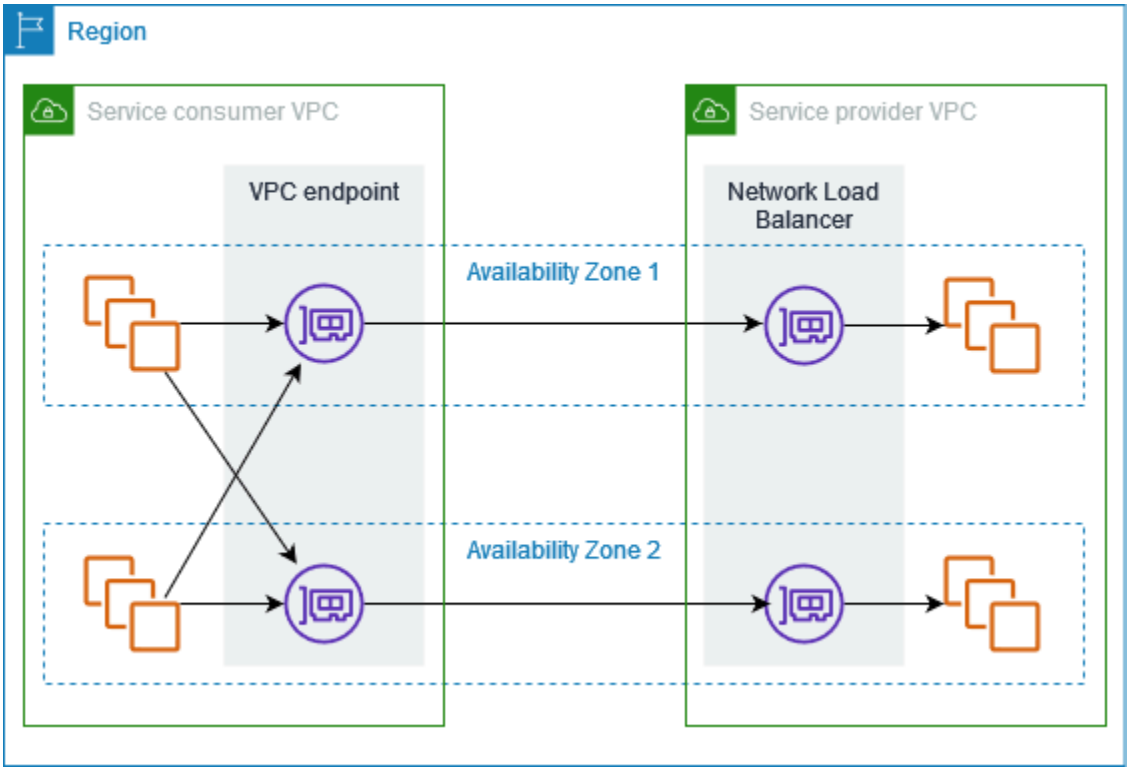
Condividi i tuoi servizi tramite AWS PrivateLink

Puoi ospitare il tuo servizio AWS PrivateLink personalizzato, noto come servizio endpoint, e condividerlo con altri AWS clienti.

Indice

Panoramica

Il diagramma seguente mostra come condividi il servizio ospitato AWS con altri AWS clienti e come questi clienti si connettono al tuo servizio. In qualità di provider di servizi, crea un Network Load Balancer nel tuo VPC come front-end del servizio. Seleziona quindi il load balancer durante la configurazione del servizio endpoint VPC. Concedi l'autorizzazione a principali AWS specifici in modo che possano connettersi al servizio. In qualità di utente del servizio, il consumatore crea un endpoint VPC dell'interfaccia che stabilisce connessioni tra le sottoreti selezionate dal proprio VPC e il servizio endpoint. Il load balancer riceve le richieste dagli utenti del servizio e le instrada alle destinazioni che lo ospitano.



Per una bassa latenza e una disponibilità elevata, consigliamo di rendere il servizio disponibile in almeno due zone di disponibilità.

Hostname DNS

Quando un provider di servizi crea un servizio endpoint VPC, AWS genera un nome host DNS specifico dell'endpoint per il servizio. Questi nomi sono caratterizzati dalla sintassi seguente:

```
endpoint_service_id.region.vpce.amazonaws.com
```

Di seguito è riportato un esempio di un nome host DNS per un servizio endpoint VPC nella regione us-est-2:

```
vpce-svc-071afff70666e61e0.us-east-2.vpce.amazonaws.com
```

Quando un utente del servizio crea un endpoint VPC dell'interfaccia, vengono generati i nomi DNS regionali e zonali che l'utente può utilizzare per comunicare con il servizio endpoint. I nomi regionali sono caratterizzati dalla sintassi seguente:

```
endpoint_id.endpoint_service_id.service_region.vpce.amazonaws.com
```

I nomi zonali sono caratterizzati dalla sintassi seguente:

```
endpoint_id-endpoint_zone.endpoint_service_id.service_region.vpce.amazonaws.com
```

DNS privato

Un provider di servizi può inoltre associare un nome DNS privato al proprio servizio endpoint, in modo che gli utenti del servizio possano continuare ad accedere al servizio utilizzando il nome DNS esistente. Se un provider di servizi associa un nome DNS privato al servizio endpoint, gli utenti del servizio possono abilitare i nomi DNS privati per gli endpoint di interfaccia. Se un provider di servizi non abilita il DNS privato, gli utenti del servizio potrebbero dover aggiornare le proprie applicazioni per utilizzare il nome DNS pubblico del servizio endpoint VPC. Per ulteriori informazioni, consulta Gestione dei nomi DNS.

Sottoreti e zone di disponibilità

Il servizio endpoint è disponibile nelle zone di disponibilità abilitate per il Network Load Balancer. Per un'elevata disponibilità e resilienza, ti consigliamo di abilitare il sistema di bilanciamento del carico in almeno due zone di disponibilità, distribuire EC2 le istanze in ciascuna zona abilitata e registrare queste istanze con il gruppo target del sistema di bilanciamento del carico.

Puoi abilitare il bilanciamento del carico tra zone come alternativa all'hosting del servizio endpoint in più zone di disponibilità. Tuttavia, i consumatori perderanno l'accesso al servizio endpoint da entrambe le zone in caso di guasto della zona che ospita il servizio endpoint. Tieni inoltre presente che quando abiliti il bilanciamento del carico tra zone per un Network Load Balancer EC2 , vengono applicati i costi di trasferimento dei dati.

Il consumatore può creare endpoint VPC di interfaccia nelle zone di disponibilità in cui è disponibile il servizio endpoint. Creiamo un'interfaccia di rete endpoint in ogni sottorete che il consumatore configura per l'endpoint VPC. Vengono assegnati indirizzi IP a ogni interfaccia di rete dell'endpoint dalla relativa sottorete, in base al tipo di indirizzo IP dell'endpoint VPC. Quando una richiesta utilizza l'endpoint regionale per il servizio endpoint VPC, selezioniamo un'interfaccia di rete endpoint sana, utilizzando l'algoritmo round robin per alternare le interfacce di rete in diverse zone di disponibilità. Quindi trasferiamo il traffico verso l'indirizzo IP dell'interfaccia di rete dell'endpoint selezionata.

Il consumatore può utilizzare gli endpoint zonali per l'endpoint VPC se per il suo caso d'uso è preferibile mantenere il traffico nella stessa zona di disponibilità.

Accesso a più regioni

Un provider di servizi può ospitare un servizio in una regione e renderlo disponibile in una serie di regioni supportate. Un consumatore di servizi seleziona una regione di servizio durante la creazione di un endpoint.

Permissions

- Per impostazione predefinita, le entità IAM non sono autorizzate a rendere disponibile un servizio endpoint in più regioni o ad accedere a un servizio endpoint in più regioni. Per concedere le autorizzazioni necessarie per l'accesso tra più regioni, un amministratore IAM può creare policy IAM che consentano l'azione solo in base alle autorizzazioni. `vpce:AllowMultiRegion`
- Per controllare le regioni che un'entità IAM può specificare come regione supportata durante la creazione di un servizio endpoint, utilizza la chiave condition. `ec2:VpceSupportedRegion`
- Per controllare le regioni che un'entità IAM può specificare come regione di servizio durante la creazione di un endpoint VPC, utilizza la `ec2:VpceServiceRegion` chiave condition.

Considerazioni

- Un provider di servizi deve aderire a una regione con consenso esplicito prima di aggiungerla come regione supportata per un servizio endpoint.
- Il servizio endpoint deve essere accessibile dalla regione ospitante. Non è possibile rimuovere la regione host dal set di regioni supportate. Per motivi di ridondanza, puoi distribuire il servizio endpoint in più regioni e abilitare l'accesso interregionale per ogni servizio endpoint.
- Un consumatore di servizi deve aderire a una regione opzionale prima di selezionarla come regione di servizio per un endpoint. Ove possibile, consigliamo agli utenti del servizio di accedere a un servizio utilizzando la connettività interregionale anziché la connettività interregionale. La connettività intraregionale offre una latenza inferiore e costi inferiori.
- Se un fornitore di servizi rimuove una regione dal set di regioni supportate, gli utenti del servizio non possono selezionare tale regione come regione di servizio quando creano nuovi endpoint. Tieni presente che ciò non influisce sull'accesso al servizio endpoint dagli endpoint esistenti che utilizzano questa regione come regione del servizio.
- Per un'elevata disponibilità, i provider devono utilizzare almeno due zone di disponibilità. L'accesso tra regioni non richiede che fornitori e consumatori utilizzino le stesse zone di disponibilità.
- L'accesso tra regioni non è supportato per le seguenti zone di disponibilità:`use1-az3`,, `usw1-az2` `apne1-az3apne2-az2`, e. `apne2-az4`

- Con l'accesso interregionale, AWS PrivateLink gestisce il failover tra zone di disponibilità. Non gestisce il failover tra regioni.
- L'accesso tra regioni non è supportato per i Network Load Balancer con un valore personalizzato configurato per il timeout di inattività TCP.
- L'accesso tra regioni non è supportato con la frammentazione UDP.
- L'accesso tra regioni è supportato solo per i servizi tramite cui condividi. AWS PrivateLink

Tipi di indirizzi IP

I provider di servizi possono rendere disponibili i propri endpoint di servizio agli utenti del servizio tramite o entrambi IPv4 e IPv4 IPv6 IPv6, anche se i loro server di backend supportano solo il supporto. IPv4 Se abiliti il supporto dualstack, i consumatori esistenti possono continuare a utilizzarlo per accedere IPv4 al tuo servizio e i nuovi consumatori possono scegliere di utilizzare IPv6 per accedere al tuo servizio.

Se l'interfaccia è supportata da un endpoint VPC IPv4, le interfacce di rete degli endpoint dispongono di indirizzi. IPv4 Se l'interfaccia è supportata da un endpoint VPC IPv6, le interfacce di rete degli endpoint dispongono di indirizzi. IPv6 L' IPv6 indirizzo per un'interfaccia di rete endpoint non è raggiungibile da Internet. Se descrivi un'interfaccia di rete endpoint con un IPv6 indirizzo, nota che è abilitata. `denyAllIgwTraffic`

Requisiti per l'attivazione IPv6 di un servizio endpoint

- Il VPC e le sottoreti per il servizio endpoint devono avere blocchi CIDR associati. IPv6
- Tutti i Network Load Balancer per il servizio endpoint devono utilizzare il tipo di indirizzo IP dualstack. Non è necessario che gli obiettivi supportino il traffico. IPv6 Se il servizio elabora gli indirizzi IP di origine dall'intestazione del protocollo proxy versione 2, deve elaborare IPv6 gli indirizzi.

Requisiti da abilitare IPv6 per un endpoint di interfaccia

- Il servizio endpoint deve supportare IPv6 le richieste.
- Il tipo di indirizzo IP di un endpoint dell'interfaccia deve essere compatibile con le sottoreti dell'endpoint dell'interfaccia, come descritto di seguito:
  - IPv4— Assegna IPv4 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate hanno intervalli di indirizzi. IPv4

- IPv6— Assegna IPv6 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono solo sottoreti. IPv6
- Dualstack: assegna entrambi IPv4 gli indirizzi alle interfacce di rete degli endpoint. IPv6 Questa opzione è supportata solo se tutte le sottoreti selezionate hanno entrambi gli intervalli di indirizzi. IPv4 IPv6

Tipo di indirizzo IP del record DNS per un endpoint dell'interfaccia

Il tipo di indirizzo IP del record DNS supportato da un endpoint dell'interfaccia determina i record DNS creati. Il tipo di indirizzo IP del record DNS di un endpoint dell'interfaccia deve essere compatibile con il tipo di indirizzo IP dell'endpoint dell'interfaccia, come descritto di seguito:

- IPv4— Crea record A per i nomi DNS privati, regionali e zonali. Il tipo di indirizzo IP deve essere IPv4o Dualstack.
- IPv6— Crea record AAAA per i nomi DNS privati, regionali e zonali. Il tipo di indirizzo IP deve essere IPv6o Dualstack.
- Dualstack: consente di creare record A e AAAA per i nomi DNS privati, regionali e zonali. Il tipo di indirizzo IP deve essere Dualstack.

Crea un servizio fornito da AWS PrivateLink

È possibile creare il proprio servizio basato su AWS PrivateLink, noto come servizio endpoint. Tu sei il provider di servizi e i principali AWS che creano connessioni al servizio sono gli utenti del servizio.

I servizi endpoint richiedono un Network Load Balancer o un Gateway Load Balancer. Il load balancer riceve le richieste dagli utenti del servizio e le instrada al servizio. In questo caso, creerai un servizio endpoint utilizzando un Network Load Balancer. Per ulteriori informazioni sulla creazione di un servizio endpoint utilizzando un Gateway Load Balancer, consulta la pagina Accesso alle appliance virtuali.

Indice

Considerazioni

- Un servizio endpoint è disponibile nella regione in cui è stato creato. I consumatori possono accedere al tuo servizio da altre regioni se abiliti l'accesso interregionale o se utilizzano il peering VPC o un gateway di transito.
- Quando gli utenti del servizio recuperano le informazioni relative a un servizio endpoint, possono visualizzare solo le zone di disponibilità in comune con il provider di servizi. Se il provider di servizi e l'utente si trovano in account diversi, un nome della zona di disponibilità, ad esempio `us-east-1a`, potrebbe essere mappato a una zona di disponibilità fisica diversa in ciascun Account AWS. Puoi utilizzare AZ IDs per identificare in modo coerente le zone di disponibilità per il tuo servizio. Per ulteriori informazioni, consulta AZ IDs nella Amazon EC2 User Guide.
- Quando gli utenti del servizio inviano traffico al servizio attraverso un endpoint dell'interfaccia, gli indirizzi IP di origine forniti all'applicazione sono gli indirizzi IP privati dei nodi load balancer e non gli indirizzi IP degli utenti del servizio. Se abiliti il protocollo proxy sul load balancer, puoi ottenere gli indirizzi dei consumatori del servizio e gli endpoint IDs dell'interfaccia dall'intestazione del protocollo proxy. Per ulteriori informazioni, vedere Proxy Protocol nel Manuale dell'utente per Network Load Balancers.
- Un Network Load Balancer può essere associato a un singolo servizio endpoint, ma un servizio endpoint può essere associato a più Network Load Balancer.
- Se un servizio endpoint è associato a molteplici Network Load Balancer, ogni endpoint dell'interfaccia di rete è associato a un sistema di bilanciamento del carico. Quando viene avviata la prima connessione da un'interfaccia di rete endpoint, selezioniamo a caso uno dei Network Load Balancer nella stessa zona di disponibilità dell'interfaccia di rete dell'endpoint. Tutte le richieste di connessione successive da questa interfaccia di rete endpoint utilizzano il sistema di bilanciamento del carico selezionato. Consigliamo di utilizzare la stessa configurazione di ascoltatore e gruppo di destinazione per tutti i sistemi di bilanciamento del carico per un servizio endpoint, in modo che i consumatori possano utilizzare il servizio endpoint con successo indipendentemente dal sistema di bilanciamento del carico scelto.
- Le tue risorse sono soggette a quote. AWS PrivateLink Per ulteriori informazioni, consulta AWS PrivateLink quote.

Prerequisiti

- Creare un VPC per il servizio endpoint con almeno una sottorete in ogni zona di disponibilità in cui il servizio deve essere disponibile.

- Per consentire agli utenti del servizio di creare endpoint VPC di IPv6 interfaccia per il servizio endpoint, il VPC e le sottoreti devono avere blocchi CIDR associati. IPv6
- Creare un Network Load Balancer nel VPC. Seleziona una sottorete per la zona di disponibilità in cui il servizio deve essere reso disponibile agli utenti. Per una bassa latenza e la tolleranza ai guasti, consigliamo di rendere il servizio disponibile in almeno due zone di disponibilità della regione.
- Se il Network Load Balancer dispone di un gruppo di sicurezza, deve consentire il traffico in entrata dagli indirizzi IP dei client. In alternativa, puoi disattivare la valutazione delle regole dei gruppi di sicurezza in entrata per il traffico in transito. AWS PrivateLink Per ulteriori informazioni, consulta Gruppi di sicurezza nella Guida per l'utente di Network Load Balancers.
- Per consentire al servizio endpoint di accettare IPv6 le richieste, i suoi Network Load Balancer devono utilizzare il tipo di indirizzo IP dualstack. Non è necessario che gli obiettivi supportino il traffico. IPv6 Per ulteriori informazioni, consulta la sezione Tipo di indirizzo IP nella Guida per l'utente di Network Load Balancer.

  Se elaborate gli indirizzi IP di origine dall'intestazione del protocollo proxy versione 2, verificate di poter elaborare IPv6 gli indirizzi.
- Avviare le istanze in ogni zona di disponibilità in cui il servizio deve essere disponibile e registrale con un gruppo di destinazione del load balancer. Se non si avviano le istanze in tutte le zone di disponibilità abilitate, è possibile attivare un load balancer su più zone per supportare gli utenti del servizio che utilizzano i nomi host DNS zonali per accedervi. Quando abiliti il load balancer su più zone, si applicano i costi di trasferimento dei dati a livello regionale. Per ulteriori informazioni, consulta Bilanciamento del carico tra zone nella Guida per l'utente di Network Load Balancers.

Creazione di un servizio endpoint

Utilizza la procedura seguente per creare un servizio endpoint utilizzando un Network Load Balancer.

Per creare un servizio endpoint tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Scegli Create Endpoint Service (Crea servizio endpoint).
4. Per Load balancer type (Tipo di load balancer), scegli Network (Rete).
5. In Available load balancers (load balancer disponibili), selezionare i Network Load Balancers da associare al servizio endpoint. Per visualizzare le zone di disponibilità abilitate per il sistema di

bilanciamento del carico selezionato, consulta Dettagli dei sistemi di bilanciamento del carico selezionati, Zone di disponibilità incluse. Il servizio endpoint sarà disponibile in queste zone di disponibilità.

6. (Facoltativo) Per rendere disponibile il servizio endpoint in regioni diverse dalla regione in cui è ospitato, seleziona le regioni tra le Regioni di servizio. Per ulteriori informazioni, consulta the section called “Accesso a più regioni”.
7. In Require acceptance for endpoint (Richiedi accettazione per l'endpoint), seleziona Acceptance required (Accettazione richiesta) per richiedere l'accettazione manuale delle richieste di connessione al servizio endpoint. In caso contrario, queste richieste vengono accettate automaticamente.
8. In Enable private DNS (Abilita nomi DNS privati), seleziona Associate a private DNS name with the service (Associa un nome DNS privato al servizio) per associare un nome DNS privato al servizio e consentire l'accesso agli utenti, quindi immetti il nome DNS privato. Altrimenti, gli utenti del servizio possono utilizzare il nome DNS specifico dell'endpoint fornito da. AWS Il provider di servizi deve dimostrare di essere il proprietario del dominio prima che gli utenti possano utilizzare il nome DNS privato. Per ulteriori informazioni, consulta Gestione dei nomi DNS.
9. Per Supported IP address types (Tipi di indirizzo IP supportati), esegui una delle operazioni seguenti:
   - Seleziona IPv4: abilita il servizio endpoint ad accettare le richieste. IPv4
   - Seleziona IPv6: abilita il servizio endpoint ad accettare IPv6 le richieste.
   - Seleziona IPv4e IPv6: abilita il servizio endpoint ad accettare entrambe IPv4 le IPv6 richieste.
10. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
11. Scegli Create (Crea).

Per creare un servizio endpoint utilizzando la riga di comando

- create-vpc-endpoint-service-configurazione ()AWS CLI
- New-EC2VpcEndpointServiceConfiguration(Strumenti per Windows PowerShell)

Rendi il servizio endpoint disponibile agli utenti del servizio

AWS i responsabili possono connettersi al servizio endpoint in modo privato creando un endpoint VPC di interfaccia. Per mettere a disposizione i propri servizi agli utenti, i provider devono eseguire le operazioni seguenti.

- Aggiungere le autorizzazioni che consentono a ciascun utente del servizio di connettersi al servizio endpoint. Per ulteriori informazioni, consulta the section called “Gestione delle autorizzazioni”.
- Fornire all'utente del servizio il nome del servizio e le zone di disponibilità supportate in modo che possa creare un endpoint dell'interfaccia per connettersi al servizio. Per ulteriori informazioni, consulta the section called “Connessione a un servizio endpoint in qualità di utente del servizio”.
- Accettare la richiesta di connessione all'endpoint inviata dall'utente del servizio. Per ulteriori informazioni, consulta the section called “Accettare o rifiutare le richieste di connessione”.

Connessione a un servizio endpoint in qualità di utente del servizio

Un utente del servizio utilizza la procedura seguente per creare un endpoint dell'interfaccia per connettersi al servizio endpoint.

Per creare un endpoint dell'interfaccia mediante la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Per Tipo, scegli i servizi Endpoint che utilizzano e. NLBs GWLBs
5. Per Nome servizio, inserisci il nome del servizio (ad esempio,`com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`), quindi scegli Verifica servizio.
6. (Facoltativo) Per connetterti a un servizio endpoint disponibile in una regione diversa da quella dell'endpoint, seleziona Area del servizio, Abilita endpoint interregionale, quindi seleziona la regione. Per ulteriori informazioni, consulta the section called “Accesso a più regioni”.
7. Per VPC, seleziona il VPC da cui accederai al servizio endpoint.
8. Per Subnet, seleziona le sottoreti in cui creare interfacce di rete endpoint.
9. Per IP address type (Tipo di indirizzo IP), seleziona una delle opzioni seguenti:

- IPv4— Assegna IPv4 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate hanno intervalli di IPv4 indirizzi e il servizio endpoint accetta le richieste. IPv4
- IPv6— Assegna IPv6 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono IPv6 solo sottoreti e il servizio endpoint accetta le richieste. IPv6
- Dualstack: assegna entrambi gli indirizzi E alle interfacce di rete degli endpoint. IPv4 IPv6 Questa opzione è supportata solo se tutte le sottoreti selezionate hanno entrambi intervalli di IPv6 indirizzi IPv4 e il servizio endpoint accetta entrambe le richieste. IPv4 IPv6

10. Per DNS record IP type (Tipo di IP record DNS), seleziona una delle opzioni seguenti:

    - IPv4— Crea record A per i nomi DNS privati, regionali e zonali. Il tipo di indirizzo IP deve essere IPv4o Dualstack.
    - IPv6— Crea record AAAA per i nomi DNS privati, regionali e zonali. Il tipo di indirizzo IP deve essere IPv6o Dualstack.
    - Dualstack: consente di creare record A e AAAA per i nomi DNS privati, regionali e zonali. Il tipo di indirizzo IP deve essere Dualstack.
    - Servizio definito: consente di creare record A per i nomi DNS privati, regionali e zonali e record AAAA per i nomi DNS regionali e zonali. Il tipo di indirizzo IP deve essere Dualstack.

11. In Security group (Gruppo di sicurezza), selezionare i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint.
12. Seleziona Crea endpoint.

Per creare un endpoint dell'interfaccia mediante la riga di comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Strumenti per Windows) PowerShell

Configurazione di servizio endpoint

Dopo aver creato un servizio endpoint, puoi aggiornarne la configurazione.

Processi

- Gestione delle autorizzazioni

- Accettare o rifiutare le richieste di connessione
- Gestisci i sistemi di bilanciamento del carico
- Associazione di un nome DNS privato
- Modifica le regioni supportate
- Modifica dei tipi di indirizzo IP supportati
- Gestione dei tag

Gestione delle autorizzazioni

La combinazione di autorizzazioni e impostazioni di accettazione consente di controllare quali consumatori (AWS responsabili) del servizio possono accedere al servizio endpoint. Ad esempio, puoi concedere autorizzazioni a principali specifici che ritieni affidabili e accettare automaticamente tutte le richieste di connessione oppure concedere autorizzazioni a un gruppo più ampio di principali e accettare manualmente specifiche richieste di connessione che ritieni affidabili.

Per impostazione predefinita, il servizio endpoint non è disponibile per gli utenti del servizio. È necessario aggiungere autorizzazioni che consentano a AWS responsabili specifici di creare un endpoint VPC di interfaccia per connettersi al servizio endpoint. Per aggiungere le autorizzazioni per un AWS principale, è necessario il relativo Amazon Resource Name (ARN). L'elenco seguente include esempi ARNs di principali supportati AWS .

ARNs per i presidi AWS

Account AWS (include tutti i principali dell'account)

arn:aws:iam: :root *account_id*

Ruolo

arn:aws:iam: :ruolo/ *account_id role_name*

Utente

arn:aws:iam: :user/ *account_id user_name*

Tutti i principi in tutto Account AWS

*

Considerazioni

- Se concedi a tutti gli utenti l'autorizzazione ad accedere al servizio endpoint e lo configuri in modo da accettare tutte le richieste, il load balancer sarà pubblico anche se non dispone di un indirizzo IP pubblico.
- Se rimuovi le autorizzazioni, ciò non influirà sulle connessioni esistenti tra l'endpoint e il servizio che erano state precedentemente accettate.

Gestione delle autorizzazioni per il servizio endpoint tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona il servizio endpoint e scegli la scheda Allow principals (Consenti principali).
4. Per aggiungere le autorizzazioni, scegli Allow principals (Consenti principali). In Principals to add (Entità principali da aggiungere), immetti l'ARN del principale. Per aggiungere un altro principale, scegliere Add principal (Aggiungi principale). Una volta completata l'aggiunta di principali, scegli Allow principals (Consenti principali).
5. Per rimuovere le autorizzazioni, seleziona il principale e scegli Actions (Operazioni), Delete (Elimina). Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Per aggiungere le autorizzazioni per il servizio endpoint mediante la riga di comando

- modify-vpc-endpoint-service-permessi ()AWS CLI
- Edit-EC2EndpointServicePermission(Strumenti per Windows) PowerShell

Accettare o rifiutare le richieste di connessione

La combinazione di autorizzazioni e impostazioni di accettazione consente di controllare quali consumatori (AWS responsabili) del servizio possono accedere al servizio endpoint. Ad esempio, puoi concedere autorizzazioni a principali specifici che ritieni affidabili e accettare automaticamente tutte le richieste di connessione oppure concedere autorizzazioni a un gruppo più ampio di principali e accettare manualmente specifiche richieste di connessione che ritieni affidabili.

Puoi configurare il servizio endpoint per accettare automaticamente le richieste di connessione. In caso contrario, è necessario accettarle o rifiutarle manualmente. Se non accetti una richiesta di connessione, l'utente del servizio non potrà accedere al servizio endpoint.

Se concedi a tutti gli utenti l'autorizzazione ad accedere al servizio endpoint e lo configuri in modo da accettare tutte le richieste, il load balancer sarà pubblico anche se non dispone di un indirizzo IP pubblico.

Puoi scegliere di ricevere una notifica nel momento in cui una richiesta di connessione viene accettata o rifiutata. Per ulteriori informazioni, consulta the section called “Ricezione di avvisi per gli eventi relativi al servizio endpoint”.

Per modificare l'impostazione di accettazione tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Selezionare Actions (Operazioni), Modify endpoint acceptance setting (Modifica impostazione di accettazione Endpoint).
5. Seleziona o deseleziona l'opzione Acceptance required (Accettazione richiesta).
6. Scegli Save changes (Salva modifiche).

Per modificare l'impostazione di accettazione tramite la riga di comando

- modify-vpc-endpoint-service-configurazione ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Strumenti per Windows PowerShell)

Per accettare o rifiutare una richiesta di connessione tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Dalla scheda Endpoint connections (Connessioni endpoint), seleziona la connessione endpoint.
5. Per accettare la richiesta di connessione, scegli Actions (Operazioni), Accept endpoint connection request (Accetta richiesta di connessione endpoint). Quando viene richiesta la conferma, immetti **`accept`** e seleziona Accept (Accetta).
6. Per rifiutare la richiesta di connessione, scegliere Operazioni, Rifiuta la richiesta di connessione endpoint. Quando viene richiesta la conferma, immetti **`reject`** e seleziona Reject (Rifiuta).

Per accettare o rifiutare una richiesta di connessione tramite la riga di comando

- accept-vpc-endpoint-connectionso reject-vpc-endpoint-connections(AWS CLI)
- Approve-EC2EndpointConnectiono Deny-EC2EndpointConnection(Strumenti per Windows PowerShell)

Gestisci i sistemi di bilanciamento del carico

Puoi gestire i sistemi di bilanciamento del carico associati al tuo servizio endpoint. Tuttavia, non puoi dissociare un load balancer se vi sono endpoint collegati al servizio endpoint.

Se abiliti un'altra zona di disponibilità per i tuoi sistemi di bilanciamento del carico, la zona di disponibilità verrà visualizzata nella scheda Load Balancer della pagina dei servizi Endpoint. Tuttavia, non sarà abilitata per il servizio endpoint né elencata nella scheda Dettagli del servizio endpoint su. Console di gestione AWSÈ necessario abilitare il servizio endpoint per la nuova zona di disponibilità.

Potrebbero essere necessari alcuni minuti prima che la zona di disponibilità del sistema di bilanciamento del carico sia pronta per il servizio endpoint. Se utilizzi un'automazione, ti consigliamo di aggiungere un'attesa al processo di automazione prima di abilitare il servizio endpoint per la nuova zona di disponibilità.

Per gestire i sistemi di bilanciamento del carico per il servizio endpoint utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Seleziona Actions (Operazioni), Associate or disassociate load balancers (Associa o dissocia i bilanciatori del carico).
5. Modifica la configurazione del servizio endpoint in base alle esigenze. Ad esempio:
    - Seleziona la casella di controllo relativa a un load balancer per associarlo al servizio endpoint.
    - Deseleziona la casella di controllo relativa a un sistema di bilanciamento del carico per dissociarlo dal servizio endpoint. È necessario mantenere selezionato almeno un sistema di bilanciamento del carico.
6. Scegliere Salva modifiche.

Il servizio endpoint verrà abilitato per tutte le nuove zone di disponibilità aggiunte al sistema di bilanciamento del carico. La nuova zona di disponibilità è elencata nella scheda Load Balancers e nella scheda Dettagli del servizio endpoint.

Dopo aver abilitato una zona di disponibilità per il servizio endpoint, i consumatori del servizio possono aggiungere una sottorete da quella zona di disponibilità agli endpoint VPC di interfaccia.

Per gestire i sistemi di bilanciamento del carico per il servizio endpoint utilizzando la riga di comando

- modify-vpc-endpoint-service-configurazione ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Strumenti per Windows PowerShell)

Per abilitare il servizio endpoint in una zona di disponibilità che è stata recentemente abilitata per il load balancer, è sufficiente chiamare il comando con l'ID del servizio endpoint.

Associazione di un nome DNS privato

Puoi associare un nome DNS privato al servizio endpoint. Dopo aver eseguito questa operazione, devi aggiornare la voce del dominio sul server DNS. Il provider di servizi deve dimostrare di essere il proprietario del dominio prima che gli utenti possano utilizzare il nome DNS privato. Per ulteriori informazioni, consulta Gestione dei nomi DNS.

Per modificare un nome DNS privato del servizio endpoint utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Scegli Actions (Operazioni), Modify Private DNS names (Modifica nomi DNS privati).
5. Seleziona Associate a private DNS name with the service (Associa un nome DNS privato al servizio) e immetti il nome DNS privato.
   - I nomi di dominio devono utilizzare lettere minuscole.
   - Puoi usare caratteri jolly nei nomi di dominio (ad esempio, **`*.myexampleservice.com`**).
6. Scegli Save changes (Salva modifiche).

7. Gli utenti del servizio possono utilizzare il nome DNS privato quando lo stato della verifica è verificato. Se lo stato della verifica cambia, le nuove richieste di connessione vengono rifiutate, senza tuttavia influenzare quelle esistenti.

Per modificare un nome DNS privato del servizio endpoint utilizzando la riga di comando

- modify-vpc-endpoint-service-configurazione ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Strumenti per Windows PowerShell)

Per avviare il processo di verifica del dominio utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Scegli Actions (Operazioni),Verify domain ownership for private DNS name (Verifica la proprietà del dominio per il nome DNS privato).
5. Quando viene richiesta la conferma, immettere **`verify`** e selezionare Verify (Verifica).

Per avviare il processo di verifica del dominio utilizzando la riga di comando

- start-vpc-endpoint-service-private-dns-verification (AWS CLI)
- Start-EC2VpcEndpointServicePrivateDnsVerification(Strumenti per Windows PowerShell)

Modifica le regioni supportate

Puoi modificare il set di regioni supportate per il tuo servizio endpoint. Prima di poter aggiungere una regione opt-in, è necessario effettuare l'attivazione. Non puoi rimuovere la regione che ospita il tuo servizio endpoint.

Dopo aver rimosso una regione, gli utenti del servizio non possono creare nuovi endpoint che la specifichino come regione del servizio. La rimozione di una regione non influisce sugli endpoint esistenti che la specificano come regione di servizio. Quando rimuovi una regione, ti consigliamo di rifiutare tutte le connessioni endpoint esistenti da quella regione.

Per modificare le regioni supportate per il servizio endpoint

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Scegli Azioni, Modifica regioni supportate.
5. Seleziona e deseleziona le regioni in base alle esigenze.
6. Scegli Save changes (Salva modifiche).

Modifica dei tipi di indirizzo IP supportati

Puoi modificare i tipi di indirizzo IP supportati dal servizio endpoint.

Considerazione

Per consentire al servizio endpoint di accettare IPv6 le richieste, i suoi Network Load Balancer devono utilizzare il tipo di indirizzo IP dualstack. Non è necessario che gli obiettivi supportino il traffico. IPv6 Per ulteriori informazioni, consulta la sezione Tipo di indirizzo IP nella Guida per l'utente di Network Load Balancer.

Per modificare i tipi di indirizzi IP supportati mediante la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona il servizio endpoint VPC.
4. Scegli Actions (Operazioni), Modify supported IP address types (Modifica i tipi di indirizzo IP supportati).
5. Per Supported IP address types (Tipi di indirizzo IP supportati), esegui una delle operazioni seguenti:
   - Seleziona IPv4: abilita il servizio endpoint ad accettare IPv4 le richieste.
   - Seleziona IPv6: abilita il servizio endpoint ad accettare IPv6 le richieste.
   - Seleziona IPv4e IPv6: abilita il servizio endpoint ad accettare entrambe IPv4 le IPv6 richieste.
6. Scegli Save changes (Salva modifiche).

Per modificare i tipi di indirizzi IP supportati mediante la riga di comando

- modify-vpc-endpoint-service-configurazione ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Strumenti per Windows PowerShell)

Gestione dei tag

Puoi aggiungere un tag alle risorse per identificarle o classificarle in base alle esigenze dell'organizzazione.

Gestione dei tag per il servizio endpoint tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona il servizio endpoint VPC.
4. Scegliere Actions (Operazioni), Manage tags (Gestisci tag).
5. Per ogni tag da aggiungere, seleziona Add new tag (Aggiungi nuovo tag) e immetti la chiave e il valore per il tag.
6. Per rimuovere un tag, scegli Remove (Rimuovi) a destra della chiave e del valore del tag.
7. Scegli Save (Salva).

Gestione dei tag per le connessioni degli endpoint tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona il servizio dell'endpoint VPC e scegli la scheda Endpoint connections (Connessioni endpoint).
4. Seleziona la connessione all'endpoint, quindi scegli Actions (Operazioni), Manage tags (Gestisci tag).
5. Per ogni tag da aggiungere, seleziona Add new tag (Aggiungi nuovo tag) e immetti la chiave e il valore per il tag.
6. Per rimuovere un tag, scegli Remove (Rimuovi) a destra della chiave e del valore del tag.
7. Scegli Save (Salva).

Aggiunta di tag per le autorizzazioni del servizio endpoint tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona il servizio dell'endpoint VPC e sceglie la scheda Allow principals (Consenti principali).
4. Seleziona il principale, quindi scegli Actions (Operazioni), Manage tags (Gestisci tag).
5. Per ogni tag da aggiungere, seleziona Add new tag (Aggiungi nuovo tag) e immetti la chiave e il valore per il tag.
6. Per rimuovere un tag, scegli Remove (Rimuovi) a destra della chiave e del valore del tag.
7. Scegli Save (Salva).

Per aggiungere e rimuovere i tag utilizzando la riga di comando

- create-tags e delete-tags (AWS CLI)
- New-EC2Tage Remove-EC2Tag(Strumenti per Windows PowerShell)

Gestione dei nomi DNS per i servizi endpoint VPC

I provider di servizi possono configurare i nomi DNS privati per i propri servizi endpoint. Supponiamo che un fornitore di servizi renda disponibile il proprio servizio tramite un endpoint pubblico e come servizio endpoint. Se il fornitore di servizi utilizza il nome DNS dell'endpoint pubblico come nome DNS privato del servizio endpoint, gli utenti del servizio possono accedere all'endpoint pubblico o al servizio endpoint utilizzando la stessa applicazione client, senza modifiche. Se una richiesta proviene dal VPC del consumatore del servizio, i server DNS privati risolvono il nome DNS negli indirizzi IP delle interfacce di rete degli endpoint. Altrimenti, i server DNS pubblici risolvono il nome DNS nell'endpoint pubblico.

Prima di poter configurare un nome DNS privato per il servizio endpoint, devi dimostrare di essere il proprietario del dominio eseguendo una verifica della proprietà del dominio.

Considerazioni

- Un servizio endpoint può avere un solo nome DNS privato.
- Quando il consumatore crea un endpoint di interfaccia per connettersi al tuo servizio, creiamo una zona ospitata privata e la associamo al VPC del consumatore del servizio. Creiamo un record

CNAME nella zona ospitata privata che mappa il nome DNS privato del servizio endpoint al nome DNS regionale dell'endpoint VPC. Quando un consumatore invia una richiesta al nome DNS pubblico del servizio, i server DNS privati risolvono la richiesta agli indirizzi IP delle interfacce di rete degli endpoint.

- Per verificare un dominio, è necessario disporre di un nome host pubblico o di un provider DNS pubblico.
- Puoi verificare il dominio di un sottodominio. Ad esempio, è possibile verificare example.com, anziché a.example.com. Ogni etichetta DNS può contenere fino a 63 caratteri e l'intero nome di dominio non deve superare la lunghezza totale di 255 caratteri.

  Se aggiungi un altro sottodominio, è necessario verificare il sottodominio o il dominio. Ad esempio, supponiamo che hai a.example.com e verifichi example.com. Ora aggiungi b.example.com come nome DNS privato. A questo punto devi verificare example.com o b.example.com prima che gli utenti possano utilizzare il nome.
- I nomi DNS privati non sono supportati per gli endpoint Gateway Load Balancer.

Verifica della proprietà del dominio

Il tuo dominio è associato a un set di record Domain Name System (DNS) gestiti tramite il provider DNS. Un record TXT è un tipo di record DNS che fornisce ulteriori informazioni sul tuo dominio. È formato da un nome e da un valore. Come parte del processo di verifica, devi aggiungere un record TXT al server DNS per il tuo dominio pubblico.

La verifica della proprietà del dominio è completa quando viene rilevata l'esistenza del record TXT nelle impostazioni DNS del dominio.

Dopo aver aggiunto un record, puoi controllare lo stato del processo di verifica del dominio utilizzando la console Amazon VPC. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint). Seleziona il servizio endpoint e controlla il valore di Domain verification status (Stato di verifica del dominio) nella scheda Details (Dettagli). Se la verifica del dominio è in sospeso, attendi qualche minuto e aggiorna la schermata. Se necessario, puoi avviare il processo di verifica manualmente. Scegli Actions (Operazioni),Verify domain ownership for private DNS name (Verifica la proprietà del dominio per il nome DNS privato).

Gli utenti del servizio possono utilizzare il nome DNS privato quando lo stato della verifica è verificato. Se lo stato della verifica cambia, le nuove richieste di connessione vengono rifiutate, senza tuttavia influenzare quelle esistenti.

Se lo stato della verifica è failed (non riuscito), consulta the section called “Risoluzione dei problemi relativi alla verifica del dominio”.

Recupero del nome e del valore

Forniamo il nome e il valore da utilizzare nel record TXT. Queste informazioni sono disponibili, ad esempio, nella Console di gestione AWS. Seleziona il servizio endpoint e visualizza il Domain verification name (Nome di verifica del dominio) e il Domain verification value (Valore di verifica del dominio) nella scheda Details (Dettagli) del servizio endpoint. È inoltre possibile utilizzare il seguente AWS CLI comando describe-vpc-endpoint-service-configurations per recuperare informazioni sulla configurazione del nome DNS privato per il servizio endpoint specificato.

```
aws ec2 describe-vpc-endpoint-service-configurations \
    --service-ids vpce-svc-071afff70666e61e0 \
    --query ServiceConfigurations[*].PrivateDnsNameConfiguration
```

Di seguito è riportato un output di esempio. `Value` e `Name` verranno utilizzati durante la creazione del record TXT.

```
[
    {
        "State": "pendingVerification",
        "Type": "TXT",
        "Value": "vpce:l6p0ERxlTt45jevFwOCp",
        "Name": "_6e86v84tqgqubxbwii1m"
    }
]
```

Si supponga, ad esempio, che il nome di dominio sia example.com e che i parametri di `Value` e `Name` siano quelli mostrati nell'output dell'esempio precedente. Nella tabella seguente è riportato un esempio delle impostazioni del record TXT.

Nome	Tipo	Valore
_6e86v84tqgqubxbwi i1m.example.com	TXT	ERxlvpce:l6p0 TT45jEvfw OCp

Ti consigliamo di usare `Name` come sottodominio record perché il nome del dominio di base potrebbe essere già in uso. Se il provider DNS, tuttavia, non consente caratteri di sottolineatura per

i nomi dei record DNS, è possibile omettere "_6e86v84tqgqubxbwii1m" e utilizzare semplicemente "example.com" nel record TXT.

Dopo aver verificato "_6e86v84tqgqubxbwii1m.example.com", gli utenti del servizio possono utilizzare "example.com" o un sottodominio (ad esempio, "service.example.com" o "my.service.example.com").

Aggiungi un record TXT al server DNS del dominio

La procedura per l'aggiunta di record TXT al server DNS del dominio dipende dal provider del servizio DNS. Il tuo provider DNS potrebbe essere Amazon Route 53 o un altro registrar di nomi di dominio.

Amazon Route 53

Crea un record per la tua zona ospitata pubblica utilizzando una semplice politica di routing. Utilizzare i seguenti valori:

- Per Record name (Nome record) immetti il dominio o il sottodominio.
- Per Record type (Tipo di record), scegli TXT.
- Per Value/Route traffic to (Valore/Instrada il traffico a), immetti il valore verifica del dominio.
- Per TTL (seconds) (TTL [secondi]), immetti **`1800`**.

Per maggiori informazioni, consulta Creazione di registri utilizzando la console nella Guida per gli sviluppatori Amazon Route 53.

Procedura generale

Visita il sito Web del provider DNS e accedi con il tuo account. Trova la pagina per aggiornare i record DNS del dominio. Aggiungi un record TXT con il nome e il valore forniti. Gli aggiornamenti dei record DNS possono richiedere fino a 48 ore, ma spesso diventano effettivi molto più presto.

Per indicazioni più specifiche, consulta la documentazione del provider DNS. La tabella seguente include i collegamenti alla documentazione di vari provider DNS comuni. Questo elenco non è da considerarsi esaustivo e non è da intendersi come una raccomandazione dei prodotti o dei servizi forniti da queste aziende.

Provider DNS/di hosting	Collegamento alla documentazione
GoDaddy	Aggiungi un registro TXT

Provider DNS/di hosting	Collegamento alla documentazione
Dreamhost	Adding custom DNS records
Cloudflare	Manage DNS records
HostGator	Gestisci i record DNS con /eNom HostGator
Namecheap	Come faccio ad aggiungere TXT/SPF/DKIM/DMARC record per il mio dominio?
Names.co.uk	Changing your domain's DNS Settings
Wix	Adding or Updating TXT Records in Your Wix Account

Verifica della pubblicazione del record TXT

Puoi controllare che il record TXT di verifica della proprietà del dominio DNS privato sia stato pubblicato nel server DNS tramite i passaggi seguenti. Eseguirai il nslookup comando, disponibile per Windows e Linux.

Dovrai interrogare i server DNS che servono il tuo dominio perché quei server contengono la maggior parte delle up-to-date informazioni relative al tuo dominio. Le informazioni di dominio possono richiedere tempo per la propagazione ad altri server DNS.

Per verificare che il record TXT sia stato pubblicato nel server DNS

1. Trova i server dei nomi per il tuo dominio con il comando seguente.

   ```
   nslookup -type=NS example.com
   ```

   Nell'output vengono elencati i server dei nomi utilizzati dal dominio. Nella fase successiva, si eseguirà una query su uno di questi server.
2. Verifica che il record TXT sia pubblicato correttamente utilizzando il seguente comando, dove si *name_server* trova uno dei name server che hai trovato nel passaggio precedente.

   ```
   nslookup -type=TXT  _6e86v84tqgqubxbwii1m.example.com name_server
   ```
3. Nell'output della fase precedente, verifica che la stringa dopo `text =` corrisponda al valore TXT.

Nel nostro esempio, se il record è stato pubblicato correttamente, l'output avrà l'aspetto seguente.

```
_6e86v84tqgqubxbwii1m.example.com text = "vpce:l6p0ERxlTt45jevFwOCp"
```

Risoluzione dei problemi relativi alla verifica del dominio

Le informazioni seguenti possono essere utili per risolvere i problemi relativi a un processo di verifica del dominio con esito negativo.

- Verifica se il provider DNS consente l'uso di caratteri di sottolineatura nei nomi di record TXT. Se il tuo provider DNS non consente l'uso di caratteri di sottolineatura, puoi omettere il nome di verifica del dominio (ad esempio "_6e86v84tqgqubxbwii1m") dal record TXT.
- Verifica se il provider DNS ha aggiunto il nome di dominio alla fine del record TXT. Alcuni provider DNS aggiungono automaticamente il nome del dominio al nome dell'attributo del record TXT. Per evitare la duplicazione del nome di dominio, puoi aggiungere un punto alla fine del nome di dominio che hai creato nel record TXT. Questa operazione indica al tuo provider DNS che non è necessario aggiungere il nome di dominio al record TXT.
- Verifica se il provider DNS ha modificato il valore del record DNS in modo da utilizzare solo lettere minuscole. Verifichiamo il tuo dominio solo quando esiste un record di verifica con un valore di attributo che corrisponde esattamente al valore che abbiamo fornito. Se il provider DNS ha modificato i valori dei record TXT in modo da utilizzare solo lettere minuscole, contattalo per assistenza.
- Potrebbe essere necessario verificare più volte il dominio, dal momento che supporta molteplici regioni o Account AWS. Se il provider DNS non consente di avere più record TXT con lo stesso nome di attributo, verifica la possibilità di assegnare più valori di attributo per lo stesso record TXT. Ad esempio, se il tuo DNS è gestito da Amazon Route 53, puoi utilizzare la procedura seguente.
  1. Nella console Route 53, seleziona il record TXT creato al momento della verifica del dominio nella prima regione.
  2. Per Value (Valore), vai alla fine del valore di attributo esistente e quindi premi Invio.
  3. Aggiungi il valore di attributo per la regione aggiuntiva e salva il set di record.

  Se il provider DNS non consente di assegnare più valori per lo stesso record TXT, puoi verificare il dominio una volta con il valore nel nome di attributo del record TXT e un'altra volta con il valore rimosso dal nome di attributo. Tuttavia, puoi verificare lo stesso dominio solo due volte.

Ricezione di avvisi per gli eventi relativi al servizio endpoint

Puoi creare una notifica per ricevere avvisi per eventi specifici relativi al servizio endpoint. Ad esempio, puoi ricevere un'e-mail nel momento in cui una richiesta di connessione viene accettata o rifiutata.

Processi

- Creare una notifica SNS
- Aggiungere una policy di accesso
- Aggiungere una policy della chiave

Creare una notifica SNS

Usa la procedura seguente per creare un argomento Amazon SNS per le notifiche e iscriverti all'argomento.

Per creare una notifica per un servizio endpoint utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Nella scheda Notifications (Notifiche), scegli Create notification (Crea notifica).
5. In Notification ARN (ARN della notifica), scegli l'ARN per l'argomento SNS creato.
6. Per iscriverti a un evento, selezionalo da Events (Eventi).
    - Connect (Connetti): l'utente del servizio ha creato l'endpoint dell'interfaccia. Questa operazione invia una richiesta di connessione al provider di servizi.
    - Accept (Accetta): il provider di servizi ha accettato la richiesta di connessione.
    - Reject (Rifiuta): il provider di servizi ha rifiutato la richiesta di connessione.
    - Delete (Elimina): l'utente del servizio ha eliminato l'endpoint dell'interfaccia.
7. Selezionare Create Notification (Crea notifica).

Per creare una notifica per un servizio endpoint utilizzando la riga di comando

- create-vpc-endpoint-connection-notifica ()AWS CLI

- New-EC2VpcEndpointConnectionNotification(Strumenti per Windows PowerShell)

Aggiungere una policy di accesso

Aggiungi una politica di accesso all'argomento SNS che AWS PrivateLink consenta di pubblicare notifiche per tuo conto, come la seguente. Per ulteriori informazioni, consulta Come modifico la policy di accesso dell'argomento di Amazon SNS? Utilizza le chiavi di condizione globali `aws:SourceArn` e `aws:SourceAccount` per evitare il problema del "confused deputy".

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

Aggiungere una policy della chiave

Se utilizzi argomenti SNS crittografati, la politica delle risorse per la chiave KMS deve essere affidabile per AWS PrivateLink chiamare AWS KMS le operazioni dell'API. Di seguito è riportato un esempio di policy della chiave.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

Eliminazione di un servizio endpoint

Quando un servizio endpoint non è più necessario, è possibile eliminarlo. Non è possibile eliminare un servizio endpoint se a questo sono collegati endpoint con stato `available` o `pending-acceptance`.

L'eliminazione di un servizio endpoint non rimuove il load balancer associato e non influisce sui server dell'applicazione registrati con i gruppi di destinazione del load balancer.

Per eliminare un servizio endpoint utilizzando la console

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

2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Selezionare Actions (Operazioni), Delete endpoint services (Elimina servizi endpoint).
5. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Per eliminare un servizio endpoint utilizzando la riga di comando

- delete-vpc-endpoint-service-configurazioni ()AWS CLI
- Remove-EC2EndpointServiceConfiguration(Strumenti per Windows) PowerShell

Accedi alle risorse VPC tramite AWS PrivateLink

È possibile accedere privatamente a una risorsa VPC in un altro VPC utilizzando un endpoint VPC di risorse (endpoint di risorse). Un endpoint di risorse consente di accedere in modo privato e sicuro a risorse VPC come un database, un' EC2 istanza Amazon, un endpoint dell'applicazione, una destinazione con nome di dominio o un indirizzo IP che può trovarsi in una sottorete privata in un altro VPC o in un ambiente locale. Senza endpoint di risorse, devi aggiungere un gateway Internet al tuo VPC o accedere alla risorsa utilizzando AWS PrivateLink un endpoint di interfaccia e un Network Load Balancer. Gli endpoint delle risorse non richiedono un sistema di bilanciamento del carico, quindi puoi accedere direttamente alla risorsa VPC. Una risorsa VPC è rappresentata da una configurazione di risorse. Una configurazione di risorse è associata a un gateway di risorse.

Prezzi

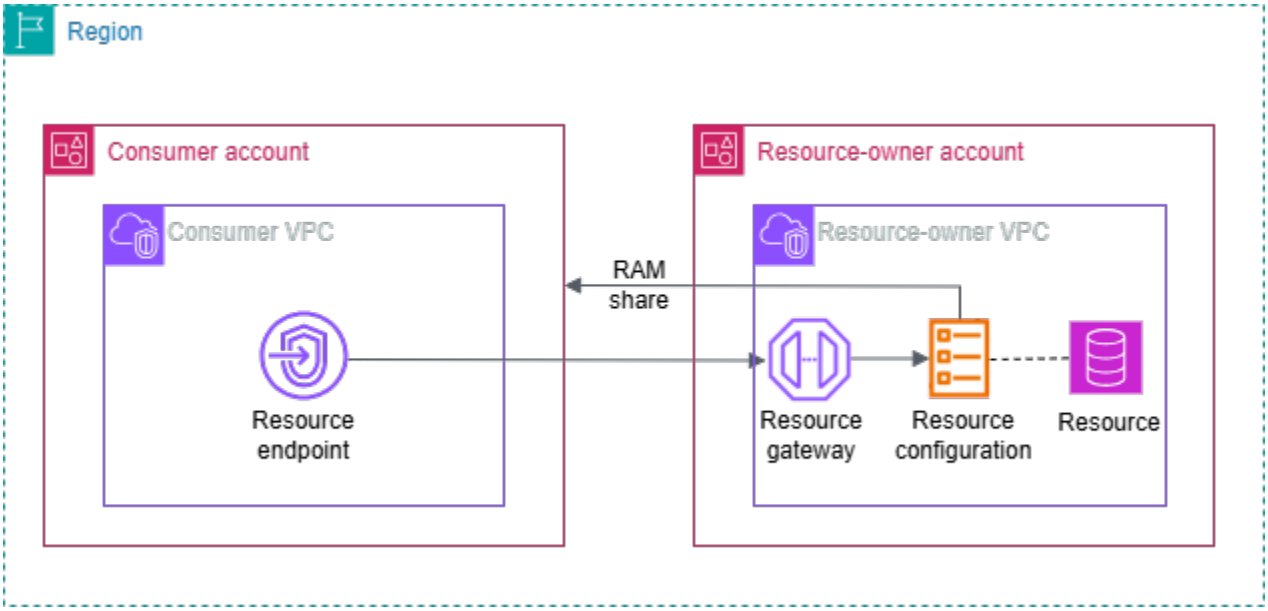
Quando accedi alle risorse utilizzando gli endpoint di risorse, ti viene fatturata ogni ora di provisioning dell'endpoint VPC di risorse. Ti viene inoltre addebitato un importo per GB di dati elaborati quando accedi alle risorse. Per ulteriori informazioni, consultare Prezzi di AWS PrivateLink. Quando abiliti l'accesso alle tue risorse utilizzando configurazioni di risorse e gateway di risorse, ti viene fatturato per GB di dati elaborati dai tuoi gateway di risorse. Per ulteriori informazioni, consultare Prezzi di Amazon VPC Lattice.

Indice

Panoramica

Puoi accedere alle risorse del tuo account o a quelle che sono state condivise con te da un altro account. Per accedere a una risorsa, crei un endpoint VPC di risorse, che stabilisce connessioni tra le sottoreti del tuo VPC e la risorsa utilizzando interfacce di rete. Il traffico destinato alla risorsa viene risolto negli indirizzi IP privati delle interfacce di rete dell'endpoint della risorsa tramite DNS. Quindi, il traffico viene inviato alla risorsa utilizzando la connessione tra l'endpoint VPC e la risorsa tramite il gateway di risorse.

L'immagine seguente mostra un endpoint di risorse in un account consumer che accede a una risorsa di proprietà di un altro account e condivisa tramite: AWS RAM



Considerazioni

- Il traffico TCP è supportato. Il traffico UDP non è supportato.
- Le connessioni di rete devono essere avviate dal VPC che contiene l'endpoint della risorsa e non dal VPC che contiene la risorsa. Il VPC della risorsa non può avviare connessioni di rete nel VPC dell'endpoint.
- Le uniche risorse basate su ARN supportate sono le risorse Amazon RDS.
- Almeno una zona di disponibilità dell'endpoint VPC e del gateway di risorse deve sovrapporsi.

Hostname DNS

Con AWS PrivateLink, invii traffico alle risorse utilizzando endpoint privati. Quando crei un endpoint VPC di risorse, creiamo nomi DNS regionali (chiamati nome DNS predefinito) che puoi utilizzare per comunicare con la risorsa dal tuo VPC e dall'ambiente locale. Ti consigliamo di utilizzare il DNS anziché l'endpoint IPs per connetterti alle tue risorse. Il nome DNS predefinito per l'endpoint VPC di risorse ha la seguente sintassi:

```
endpoint_id.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

Quando crei un endpoint VPC di risorse per determinate configurazioni di risorse che utilizzi ARNs, puoi abilitare il DNS privato. Con il DNS privato, puoi continuare a effettuare richieste alla risorsa utilizzando il nome DNS fornito per la risorsa dal AWS servizio, sfruttando al contempo la connettività privata tramite l'endpoint VPC della risorsa. Per ulteriori informazioni, consulta the section called "Risoluzione DNS".

Il describe-vpc-endpoint-associationscomando seguente visualizza le voci DNS per un endpoint di risorse.

```
aws ec2 describe-vpc-endpoint-associations --vpc-endpoint-id vpce-123456789abcdefgh --
query 'VpcEndpointAssociations[*].*'
```

Di seguito è riportato un esempio di output per un endpoint di risorse per un database Amazon RDS con nomi DNS privati abilitati. Il primo nome DNS è il nome DNS predefinito. Il secondo nome DNS proviene dalla zona ospitata privata nascosta, che risolve le richieste all'endpoint pubblico negli indirizzi IP privati delle interfacce di rete degli endpoint.

```
[
    [
        "vpce-rsc-asc-abcd1234abcd",
        "vpce-123456789abcdefgh",
        "Accessible",
        {
            "DnsName": "vpce-1234567890abcdefg-
snra-1234567890abcdefg.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-
east-1.on.aws",
            "HostedZoneId": "ABCDEFGH123456789000"
        },
        {
```

```
            "DnsName": "database-5-test.cluster-ro-example.us-
east-1.rds.amazonaws.com",
            "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
        },
        "arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890abcdefg",
        "arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890xyz"
    ]
]
```

Risoluzione DNS

I record DNS che creiamo per il tuo endpoint VPC di risorse sono pubblici. Pertanto, questi nomi DNS sono risolvibili pubblicamente. Tuttavia, le richieste DNS dall'esterno del VPC restituiscono comunque gli indirizzi IP privati delle interfacce di rete dell'endpoint di risorse. Puoi utilizzare questi nomi DNS per accedere alla risorsa dall'ambiente locale, purché tu abbia accesso al VPC in cui si trova l'endpoint della risorsa, tramite VPN o Direct Connect.

DNS privato

Se abiliti il DNS privato per il tuo endpoint VPC di risorse per determinate configurazioni di risorse che ARNs utilizzi e il tuo VPC ha sia i nomi host DNS che la risoluzione DNS abilitati, creiamo zone ospitate private nascoste AWS e gestite per configurazioni di risorse con un nome DNS personalizzato. La zona ospitata contiene un set di record per il nome DNS predefinito per la risorsa che lo risolve negli indirizzi IP privati delle interfacce di rete dell'endpoint della risorsa nel tuo VPC.

Amazon fornisce un server DNS per il tuo VPC chiamato il Route 53 Resolver. Il Route 53 Resolver risolve automaticamente i nomi di dominio VPC locali e i record in zone ospitate private. Tuttavia, non puoi utilizzare il Route 53 Resolver dall'esterno del tuo VPC. Se desideri accedere al tuo endpoint VPC dalla tua rete locale, puoi utilizzare il nome DNS personalizzato oppure puoi utilizzare gli endpoint e le regole Resolver di Route 53. Per ulteriori informazioni, consulta Integrazione con and. AWS Transit GatewayAWS PrivateLinkAmazon Route 53 Resolver

Sottoreti e zone di disponibilità

Puoi configurare l'endpoint VPC con una sottorete per zona di disponibilità. Nella sottorete, viene creata un'interfaccia di rete dell'endpoint per l'endpoint VPC. Vengono assegnati indirizzi IP a ogni

interfaccia di rete dell'endpoint dalla relativa sottorete, in base al tipo di indirizzo IP dell'endpoint VPC. In un ambiente di produzione, per un'elevata disponibilità e resilienza, consigliamo di configurare almeno due zone di disponibilità per ogni endpoint VPC.

Tipi di indirizzi IP

Gli endpoint di risorse possono supportare indirizzi o IPv4 dualstack IPv6. Gli endpoint che lo supportano IPv6 possono rispondere alle query DNS con record AAAA. Il tipo di indirizzo IP di un endpoint di risorsa deve essere compatibile con le sottoreti dell'endpoint di risorsa, come descritto di seguito:

- IPv4— Assegna IPv4 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate hanno intervalli di indirizzi. IPv4
- IPv6— Assegna IPv6 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono solo sottoreti. IPv6
- Dualstack: assegna entrambi IPv4 gli indirizzi alle interfacce di rete degli endpoint. IPv6 Questa opzione è supportata solo se tutte le sottoreti selezionate hanno entrambi gli intervalli di indirizzi. IPv4 IPv6

Se un endpoint VPC di risorse supporta IPv4, le interfacce di rete degli endpoint dispongono di indirizzi. IPv4 Se un endpoint VPC di risorse supporta IPv6, le interfacce di rete degli endpoint dispongono di indirizzi. IPv6 L' IPv6 indirizzo per un'interfaccia di rete endpoint non è raggiungibile da Internet. Se descrivi un'interfaccia di rete endpoint con un IPv6 indirizzo, nota che è abilitata. `denyAllIgwTraffic`

Accedere a una risorsa tramite un endpoint VPC di risorse

Puoi accedere a una risorsa VPC come un nome di dominio, un indirizzo IP o un database Amazon RDS utilizzando un endpoint di risorse. Un endpoint di risorse fornisce l'accesso privato a una risorsa. Quando si crea l'endpoint della risorsa, si specifica una configurazione delle risorse di tipo singolo, gruppo o ARN. Un endpoint di risorse può essere associato a una sola configurazione di risorse. La configurazione delle risorse può rappresentare una singola risorsa o un gruppo di risorse.

Prerequisiti

Per creare un endpoint di risorse, è necessario soddisfare i seguenti prerequisiti.

- È necessario disporre di una configurazione delle risorse creata dall'utente o di un altro account creato e condiviso con l'utente tramite. AWS RAM
- Se una configurazione di risorse viene condivisa con te da un altro account, devi esaminare e accettare la condivisione di risorse che contiene la configurazione delle risorse. Per ulteriori informazioni, consulta Accettare e rifiutare gli inviti nella Guida per l'utente di AWS RAM .

Crea un endpoint di risorse VPC

Utilizzare la procedura seguente per creare un endpoint di risorse VPC. Dopo aver creato un endpoint di risorse, puoi solo modificarne i gruppi o i tag di sicurezza.

Per creare un endpoint di risorse VPC

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. È possibile specificare un nome per facilitare la ricerca e la gestione dell'endpoint.
5. Per Tipo, scegli Risorse.
6. Per Configurazioni delle risorse, seleziona la configurazione delle risorse.
7. Per le impostazioni di rete, seleziona il VPC da cui accederai alla risorsa.
8. Se desideri configurare il supporto DNS privato per le configurazioni delle risorse, seleziona Impostazioni aggiuntive, Abilita nome DNS. Per utilizzare questa funzionalità, assicurati che gli attributi Enable DNS hostnames e Enable DNS support siano abilitati per il tuo VPC. Per ulteriori informazioni, consulta the section called “Nomi di dominio personalizzati per i consumatori di risorse”.
9. Per Subnet, seleziona una sottorete in cui creare l'interfaccia di rete degli endpoint.

   In un ambiente di produzione, per un'elevata disponibilità e resilienza, consigliamo di configurare almeno due zone di disponibilità per ogni endpoint VPC.
10. Per i gruppi di sicurezza, seleziona un gruppo di sicurezza.

    Se non specifichi un gruppo di sicurezza, associamo il gruppo di sicurezza predefinito per il VPC.
11. Seleziona Crea endpoint.

Per creare un endpoint di risorse utilizzando la riga di comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Gestisci gli endpoint delle risorse

Dopo aver creato un endpoint di risorse, puoi gestirne i gruppi o i tag di sicurezza.

Processi

- Eliminazione di un endpoint.
- Aggiorna un endpoint

Eliminazione di un endpoint.

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

Per eliminare un endpoint utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint.
4. Seleziona Actions (Operazioni), Delete VPC endpoints (Eliminazione di endpoint VPC).
5. Quando viene richiesta la conferma, immetti **`delete`**.
6. Scegli Elimina.

Per eliminare un endpoint utilizzando la riga di comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Aggiorna un endpoint

Puoi aggiornare un endpoint VPC.

Per aggiornare un endpoint utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint.
4. Scegli Azioni e l'opzione appropriata.
5. Segui i passaggi della console per inviare l'aggiornamento.

Per aggiornare un endpoint utilizzando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Configurazione delle risorse per le risorse VPC

Una configurazione di risorse rappresenta una risorsa o un gruppo di risorse che desideri rendere accessibili ai client di altri VPCs account. Definendo una configurazione delle risorse, puoi consentire la connettività di rete privata, sicura e unidirezionale alle risorse del tuo VPC da client di altri account. VPCs Una configurazione delle risorse è associata a un gateway di risorse attraverso il quale riceve il traffico.

Indice

- Condivisione delle configurazioni delle risorse tramite AWS RAM
- Monitoraggio
- Creare una configurazione delle risorse in VPC Lattice
- Gestire le associazioni per una configurazione di risorse VPC Lattice

Tipi di configurazioni delle risorse

Una configurazione delle risorse può essere di diversi tipi. I diversi tipi aiutano a rappresentare diversi tipi di risorse. I tipi sono:

- Configurazione a risorsa singola: un indirizzo IP o un nome di dominio. Può essere condiviso in modo indipendente.
- Configurazione delle risorse di gruppo: una raccolta di configurazioni di risorse secondarie. Può essere condivisa in modo indipendente.
- Configurazione delle risorse secondarie: un membro di una configurazione di risorse di gruppo. Rappresenta un indirizzo IP o un nome di dominio. Non può essere condiviso indipendentemente e può essere condiviso solo come parte di un gruppo. Può essere aggiunto e rimosso da un gruppo senza problemi. Una volta aggiunto, è automaticamente accessibile a coloro che possono accedere al gruppo.
- Configurazione delle risorse ARN: rappresenta un tipo di risorsa supportato fornito da un servizio. AWS Ad esempio, un database Amazon RDS. Le configurazioni delle risorse secondarie vengono gestite automaticamente da. AWS

Gateway per le risorse

Una configurazione delle risorse è associata a un gateway di risorse. Un gateway di risorse è un insieme di ENIs dispositivi che fungono da punto di ingresso nel VPC in cui si trova la risorsa. È possibile associare più configurazioni di risorse allo stesso gateway di risorse. Quando i client di altri VPCs account accedono a una risorsa nel tuo VPC, la risorsa vede il traffico proveniente localmente dal gateway di risorse in quel VPC.

Nomi di dominio personalizzati per i fornitori di risorse

I provider di risorse possono assegnare un nome di dominio personalizzato a una configurazione di risorse, ad esempio`example.com`, quali risorse possono utilizzare gli utenti per accedere alla

configurazione delle risorse. Il nome di dominio personalizzato può essere di proprietà e verificato dal provider di risorse oppure può essere di terze parti o di un AWS dominio. I provider di risorse possono utilizzare le configurazioni delle risorse per condividere cluster di cache e cluster Kafka, applicazioni basate su TLS o altre risorse. AWS

Le seguenti considerazioni si applicano ai fornitori di configurazioni di risorse:

- Una configurazione di risorse può avere solo un dominio personalizzato.
- Il nome di dominio personalizzato di una configurazione di risorse non può essere modificato.
- Il nome di dominio personalizzato è visibile a tutti gli utenti della configurazione delle risorse.
- Puoi verificare il tuo nome di dominio personalizzato utilizzando il processo di verifica del nome di dominio in VPC Lattice. Per ulteriori informazioni Per ulteriori informazioni, vedere. https://docs.aws.amazon.com/vpc-lattice/latest/ug/create-and-verify.html
- Per le configurazioni delle risorse di tipo group e child, è necessario innanzitutto specificare un dominio di gruppo nella configurazione delle risorse di gruppo. Successivamente, le configurazioni delle risorse secondarie possono avere domini personalizzati che sono sottodomini del dominio del gruppo. Se il gruppo non ha un dominio di gruppo, puoi utilizzare qualsiasi nome di dominio personalizzato per il figlio, ma VPC Lattice non fornirà alcuna zona ospitata per i nomi di dominio figlio nel VPC del consumatore di risorse.

Nomi di dominio personalizzati per i consumatori di risorse

Quando i consumatori di risorse abilitano la connettività a una configurazione di risorse con un nome di dominio personalizzato, possono consentire a VPC Lattice di gestire una zona ospitata privata Route 53 nel proprio VPC. I consumatori di risorse hanno opzioni granulari per i domini per cui desiderano consentire a VPC Lattice di gestire zone ospitate private.

I consumatori di risorse possono impostare il `private-dns-enabled` parametro quando abilitano la connettività alle configurazioni delle risorse tramite un endpoint di risorse, un endpoint di rete di servizi o un'associazione VPC di rete di servizi. Oltre al `private-dns-enabled` parametro, i consumatori possono utilizzare le opzioni DNS per specificare per quali domini desiderano che VPC Lattice gestisca le zone ospitate private. I consumatori possono scegliere tra le seguenti preferenze DNS private:

`ALL_DOMAINS`

VPC Lattice fornisce zone ospitate private per tutti i nomi di dominio personalizzati.

`VERIFIED_DOMAINS_ONLY`

VPC Lattice fornisce una zona ospitata privata solo se il nome di dominio personalizzato è stato verificato dal provider.

`VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`

VPC Lattice fornisce zone ospitate private per tutti i nomi di dominio personalizzati verificati e altri nomi di dominio specificati dal consumatore di risorse. Il consumatore di risorse specifica i nomi di dominio nel parametro. `private DNS specified domains`

`SPECIFIED_DOMAINS_ONLY`

VPC Lattice fornisce una zona ospitata privata per i nomi di dominio specificati dal consumatore di risorse. Il consumatore di risorse specifica i nomi di dominio nel parametro. `private DNS specified domains`

Quando abiliti il DNS privato, VPC Lattice crea una zona ospitata privata nel tuo VPC per il nome di dominio personalizzato associato alla configurazione delle risorse. Per impostazione predefinita, la preferenza DNS privata è impostata su. `VERIFIED_DOMAINS_ONLY` Ciò significa che le zone private ospitate vengono create solo se il nome di dominio personalizzato è stato verificato dal provider di risorse. Se imposti la preferenza DNS privata su `ALL_DOMAINS` o `SPECIFIED_DOMAINS_ONLY` allora VPC Lattice crea zone ospitate private indipendentemente dallo stato di verifica del nome di dominio personalizzato. Quando viene creata una zona ospitata privata per un determinato dominio, tutto il traffico verso quel dominio dal tuo VPC viene instradato tramite VPC Lattice. Ti consigliamo di utilizzare le `SPECIFIED_DOMAINS_ONLY` preferenze `ALL_DOMAINSVERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`, o solo quando desideri che il traffico verso questi nomi di dominio personalizzati passi attraverso VPC Lattice.

Consigliamo ai consumatori di risorse di impostare la propria preferenza DNS privata su. `VERIFIED_DOMAINS_ONLY` Ciò consente ai consumatori di rafforzare il proprio perimetro di sicurezza consentendo a VPC Lattice di fornire zone private ospitate per domini verificati nell'account del consumatore di risorse.

Per selezionare i domini nei domini privati specificati dal DNS, i consumatori di risorse possono inserire un nome di dominio completo, ad esempio o utilizzare un carattere jolly come. `my.example.com` `*.example.com`

Le seguenti considerazioni si applicano agli utenti che utilizzano configurazioni di risorse:

- Il parametro DNS privato abilitato non può essere modificato.

- Il DNS privato deve essere abilitato su un'associazione di risorse di rete di servizio per l'hosting privato da creare in un VPC. Per una configurazione di risorse, lo stato di abilitazione DNS privato dell'associazione di risorse di rete di servizio ha la precedenza sullo stato di abilitazione DNS privato dell'endpoint della rete di servizio o dell'associazione VPC della rete di servizio.

Nomi di dominio personalizzati per i proprietari di reti di servizi

La proprietà DNS privata abilitata dell'associazione di risorse di rete di servizio ha la precedenza sulla proprietà DNS privata abilitata dell'endpoint della rete di servizio e dell'associazione VPC della rete di servizio.

Se il proprietario di una rete di servizi crea un'associazione di risorse di rete di servizio e non abilita il DNS privato, VPC Lattice non fornirà zone ospitate private per quella configurazione di risorse in VPCs nessuna delle aree a cui è connessa la rete di servizio, anche se il DNS privato è abilitato sull'endpoint della rete di servizio o sulle associazioni VPC della rete di servizio.

Per le configurazioni delle risorse di tipo ARN, il flag DNS privato è vero e immutabile.

Definizione delle risorse

Nella configurazione della risorsa, identificate la risorsa in uno dei seguenti modi:

- Con un Amazon Resource Name (ARN): i tipi di risorse supportati, forniti dai AWS servizi, possono essere identificati dal relativo ARN. Sono supportati solo i database Amazon RDS. Non è possibile creare una configurazione delle risorse per un cluster accessibile pubblicamente.
- Per destinazione con nome di dominio: qualsiasi nome di dominio risolvibile pubblicamente. Se il tuo nome di dominio punta a un IP esterno al tuo VPC, devi avere un gateway NAT nel tuo VPC.
- Tramite un indirizzo IP: Per IPv4, specifica un IP privato tra i seguenti intervalli: 10.0.0.0/8, 100.64.0.0/10, 172.16.0.0/12, 192.168.0.0/16. Per IPv6, specifica un IP dal VPC. IPs I pubblici non sono supportati.

Protocollo

Quando crei una configurazione di risorse, puoi definire i protocolli che la risorsa supporterà. Attualmente è supportato solo il protocollo TCP.

Intervalli di porte

Quando si crea una configurazione di risorse, è possibile definire le porte su cui verranno accettate le richieste. L'accesso del client su altre porte non sarà consentito.

Accesso alle risorse

I consumatori possono accedere alle configurazioni delle risorse direttamente dal proprio VPC utilizzando un endpoint VPC o tramite una rete di servizi. In qualità di consumatore, puoi abilitare l'accesso dal tuo VPC a una configurazione di risorse presente nel tuo account o che è stata condivisa con te da un altro account tramite. AWS RAM

- Accesso diretto a una configurazione delle risorse

  Puoi creare un endpoint AWS PrivateLink VPC di tipo risorsa (endpoint di risorse) nel tuo VPC per accedere a una configurazione di risorse in modo privato dal tuo VPC. Per ulteriori informazioni su come creare un endpoint di risorse, consulta Accesso alle risorse VPC nella guida per AWS PrivateLink l'utente.
- Accesso a una configurazione di risorse tramite una rete di servizi

  Puoi associare una configurazione di risorse a una rete di servizi e connettere il tuo VPC alla rete di servizi. Puoi connettere il tuo VPC alla rete di servizio tramite un'associazione o utilizzando un endpoint VPC AWS PrivateLink della rete di servizi.

  Per ulteriori informazioni sulle associazioni delle reti di servizio, consulta Gestire le associazioni per una rete di servizi VPC Lattice.

  Per ulteriori informazioni sugli endpoint VPC della rete di servizio, consulta Accedere alle reti di servizio nella guida per l'AWS PrivateLink utente.

Quando il DNS privato è abilitato per il tuo VPC, non puoi creare un endpoint di risorse e un endpoint di rete di servizi per la stessa configurazione di risorse.

Associazione con il tipo di rete di servizi

Quando condividi una configurazione di risorse con un account consumatore, ad esempio Account-B AWS RAM, tramite Account-B puoi accedere alla configurazione delle risorse direttamente tramite un endpoint VPC di risorse o tramite una rete di servizi.

Per accedere a una configurazione delle risorse tramite una rete di servizi, l'Account-B dovrebbe associare la configurazione delle risorse a una rete di servizi. Le reti di servizio sono condivisibili tra account. Pertanto, l'Account-B può condividere la propria rete di servizi (a cui è associata la configurazione delle risorse) con l'Account-C, rendendo la risorsa accessibile dall'Account-C.

Per impedire tale condivisione transitiva, è possibile specificare che la configurazione delle risorse non può essere aggiunta alle reti di servizi condivisibili tra account. Se lo specifichi, l'Account-B non sarà in grado di aggiungere la configurazione delle risorse alle reti di servizi che sono condivise o che possono essere condivise con un altro account in futuro.

Tipi di reti di servizio

Quando condividi una configurazione di risorse con un altro account, ad esempio Account-B AWS RAM, tramite Account-B puoi accedere alla risorsa in tre modi:

- Utilizzo di un endpoint VPC di tipo risorsa (endpoint VPC di risorsa).
- Utilizzo di un endpoint VPC di tipo rete di servizio (endpoint VPC della rete di assistenza).
- Utilizzo di un'associazione VPC di rete di servizi.

  Quando si utilizza un'associazione di rete di servizi, a ciascuna risorsa viene assegnato un IP per sottorete a partire dal blocco 129.224.0.0/17, che è di proprietà e non è instradabile. AWS Questo si aggiunge all'elenco di prefissi gestiti che VPC Lattice utilizza per indirizzare il traffico verso i servizi sulla rete VPC Lattice. Entrambi IPs vengono aggiornati nella tabella di routing VPC.

Per l'endpoint VPC della rete di servizio e l'associazione VPC della rete di servizio, la configurazione delle risorse dovrebbe essere inserita in una rete di servizi in Account-B. Le reti di servizi sono condivisibili tra account. Pertanto, l'Account-B può condividere la propria rete di servizi (che contiene la configurazione delle risorse) con l'Account-C, rendendo la risorsa accessibile dall'Account-C. Per impedire tale condivisione transitiva, è possibile impedire che la configurazione delle risorse venga aggiunta a reti di servizi condivisibili tra account. Se non consentite questa opzione, l'Account-B non sarà in grado di aggiungere la configurazione delle risorse a una rete di servizi condivisa o condivisa con un altro account.

Condivisione delle configurazioni delle risorse tramite AWS RAM

Le configurazioni delle risorse sono integrate con. AWS Resource Access ManagerÈ possibile condividere la configurazione delle risorse con un altro account tramite AWS RAM. Quando condividi una configurazione di risorse con un AWS account, i client di quell'account possono accedere

privatamente alla risorsa. È possibile condividere una configurazione di risorse utilizzando una condivisione di risorse in AWS RAM.

Usa la AWS RAM console per visualizzare le condivisioni di risorse a cui sei stato aggiunto, le risorse condivise a cui puoi accedere e gli AWS account che hanno condiviso risorse con te. Per ulteriori informazioni, consulta Risorse condivise con te nella Guida AWS RAM per l'utente.

Per accedere a una risorsa da un altro VPC nello stesso account della configurazione della risorsa, non è necessario condividere la configurazione della risorsa tramite. AWS RAM

Monitoraggio

È possibile abilitare i log di monitoraggio sulla configurazione delle risorse. È possibile scegliere una destinazione a cui inviare i log.

Creare una configurazione delle risorse in VPC Lattice

Crea una configurazione delle risorse.

Console di gestione AWS

Per creare una configurazione delle risorse utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, sotto PrivateLink e Lattice, scegli Configurazioni delle risorse.
3. Scegli Crea configurazione delle risorse.
4. Inserisci un nome univoco all'interno del tuo AWS account. Non puoi modificare questo nome dopo aver creato la configurazione delle risorse.
5. Per Tipo di configurazione, scegli Risorsa per una risorsa singola o secondaria o Gruppo di risorse per un gruppo di risorse secondarie.
6. Scegli un gateway di risorse che hai creato in precedenza o creane uno ora.
7. (Facoltativo) Per inserire un nome di dominio personalizzato, effettuate una delle seguenti operazioni:
   - Se disponi di una configurazione delle risorse di tipo single, puoi inserire un nome di dominio personalizzato. I consumatori di risorse possono utilizzare questo nome di dominio per accedere alle configurazioni delle risorse.
   - Se disponi di una configurazione delle risorse di tipo group e child, devi prima specificare un dominio di gruppo nella configurazione delle risorse di gruppo. Successivamente, le

configurazioni delle risorse secondarie possono avere domini personalizzati che sono sottodomini del dominio del gruppo.

8. (Facoltativo) Inserisci l'ID di verifica.

   Fornisci un ID di verifica se desideri che il tuo nome di dominio venga verificato. Ciò consente ai consumatori di risorse di sapere che il nome di dominio è tuo.
9. Scegliete l'identificatore per la risorsa che desiderate che questa configurazione di risorse rappresenti.
10. Scegliete gli intervalli di porte attraverso i quali desiderate condividere la risorsa.
11. Per le impostazioni di associazione, specifica se questa configurazione delle risorse può essere associata a reti di servizi condivisibili.
12. Per la configurazione di condivisione delle risorse, scegli le condivisioni di risorse che identificano i principali che possono accedere a questa risorsa.
13. (Facoltativo) Per il monitoraggio, abilita i registri di accesso alle risorse e la destinazione di consegna se desideri monitorare le richieste e le risposte da e verso la configurazione delle risorse.
14. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
15. Scegli Crea configurazione delle risorse.

AWS CLI

Il create-resource-configurationcomando seguente crea una singola configurazione di risorse e la associa al nome `example.com` di dominio personalizzato.

```
aws vpc-lattice create-resource-configuration \
    --name my-resource-config \
    --type SINGLE \
    --resource-gateway-identifier rgw-0bba03f3d56060135 \
    --resource-configuration-definition 'ipResource={ipAddress=10.0.14.85}' \
    --custom-domain-name example.com \
    --verification-id dv-aaaa0000000111111
```

Il create-resource-configurationcomando seguente crea una configurazione di risorse di gruppo e la associa al nome di dominio personalizzato. `example.com`

```
aws vpc-lattice-custom-dns create-resource-configuration \
```

```
  --name my-custom-dns-resource-config-group \
  --type GROUP \
  --resource-gateway-identifier rgw-0bba03f3d56060135 \
  --domain-verification-identifier dv-aaaa0000000111111
```

Il create-resource-configurationcomando seguente crea una configurazione di risorse secondarie e la associa al nome di dominio personalizzato. `child.example.com`

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-child \
  --type CHILD \
  --resource-configuration-definition 'dnsResource={domainName=my-alb-123456789.us-
west-2.elb.amazonaws.com,ipAddressType=IPV4}' \
  --resource-configuration-group-identifier rcfg-07129f3acded87626 \
  --custom-domain-name child.example.com
```

Gestire le associazioni per una configurazione di risorse VPC Lattice

Gli account consumer con cui condividi una configurazione di risorse e i client del tuo account possono accedere alla configurazione delle risorse direttamente utilizzando un endpoint VPC di risorse o tramite un endpoint di rete di servizi. Di conseguenza, la configurazione delle risorse avrà associazioni di endpoint e associazioni di reti di servizio.

Gestisci le associazioni di risorse della rete di servizio

Creare o eliminare un'associazione di rete di servizio.

> **Note**
>
> Se ricevi un messaggio di accesso negato durante la creazione dell'associazione tra la rete di servizio e la configurazione delle risorse, controlla la versione AWS RAM della tua policy e assicurati che sia la versione 2. Per ulteriori informazioni, consulta la guida per l'AWS RAM utente.

Per gestire un'associazione servizio-rete utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, sotto PrivateLink e Lattice, scegli Configurazioni delle risorse.

3. Seleziona il nome della configurazione della risorsa per aprirne la pagina dei dettagli.
4. Seleziona la scheda Associazioni di rete di servizio.
5. Scegli Crea associazioni.
6. Seleziona una rete di servizi dalle reti di servizi VPC Lattice. Per creare una rete di servizi, scegli Crea una rete VPC Lattice.
7. (Facoltativo) Per aggiungere un tag, espandi Service Association tags, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
8. (Facoltativo) Per abilitare i nomi DNS privati per questa associazione di risorse di rete di servizio, scegli abilita il nome DNS privato. Per ulteriori informazioni, consulta the section called “Nomi di dominio personalizzati per i proprietari di reti di servizi”.
9. Scegli Salva modifiche.
10. Per eliminare un'associazione, seleziona la casella di controllo relativa all'associazione, quindi scegli Azioni, Elimina. Quando viene richiesta la conferma, immettere **`confirm`** e quindi scegliere Elimina.

Per creare un'associazione di rete di servizi utilizzando il AWS CLI

Utilizzare il comando create-service-network-resource-association.

Per eliminare un'associazione di rete di servizi utilizzando AWS CLI

Utilizzare il comando delete-service-network-resource-association.

Gestisci le associazioni degli endpoint VPC delle risorse

Gli account consumer con accesso alla configurazione delle risorse o i client nel tuo account possono accedere alla configurazione delle risorse utilizzando un endpoint VPC di risorse. Se la configurazione delle risorse ha un nome di dominio personalizzato, puoi utilizzare abilita il DNS privato per consentire a VPC Lattice di fornire zone ospitate private per l'endpoint di risorse o l'endpoint della rete di servizi. In questo modo, i client possono modificare direttamente il nome di dominio per accedere alla configurazione delle risorse. Per ulteriori informazioni, consulta the section called “Nomi di dominio personalizzati per i consumatori di risorse”.

Console di gestione AWS

1. Per creare una nuova associazione di endpoint, vai su PrivateLink and Lattice nel riquadro di navigazione a sinistra e scegli Endpoints.

2. Scegli Crea endpoint.
3. Seleziona la configurazione delle risorse che desideri connettere al tuo VPC.
4. Seleziona il VPC, le sottoreti e i gruppi di sicurezza.
5. (Facoltativo) Per attivare il DNS privato e configurare le opzioni DNS, seleziona Abilita nome DNS.
6. (Facoltativo) Per taggare il tuo endpoint VPC, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
7. Seleziona Crea endpoint.

AWS CLI

Il create-vpc-endpointcomando seguente crea un endpoint VPC che utilizza DNS privato. Le preferenze DNS private sono impostate su `VERIFIED_AND_SELECTED` e i domini selezionati sono e. `example.com` `example.org` VPC Lattice fornisce solo zone ospitate private per qualsiasi dominio verificato o o. `example.com` `example.org`

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Resource \
  --vpc-id vpc-111122223333aabbc \
  --subnet-ids subnet-0011aabbcc2233445 \
  --resource-configuration-arn arn:aws:vpc-lattice:us-
west-2:111122223333:resourceconfiguration/rcfg-07129f3acded87625 \
  --private-dns-enabled \
  --private-dns-preferences VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS \
  --private-domains-set example.com, example.org
```

Per creare un'associazione di endpoint VPC utilizzando AWS CLI

Utilizza il comando create-vpc-endpoint.

Per eliminare un'associazione di endpoint VPC utilizzando AWS CLI

Utilizza il comando delete-vpc-endpoint.

Gateway di risorse in VPC Lattice

Un gateway di risorse è un punto di traffico in entrata nel VPC in cui risiede una risorsa. Si estende su più zone di disponibilità.

Un VPC deve disporre di un gateway di risorse se prevedi di rendere accessibili le risorse all'interno del VPC da altri account. VPCs Ogni risorsa condivisa è associata a un gateway di risorse. Quando i client di altri VPCs account accedono a una risorsa nel tuo VPC, la risorsa vede il traffico proveniente localmente dal gateway di risorse in quel VPC. L'IP di origine del traffico è l'indirizzo IP del gateway di risorse. È possibile assegnare più indirizzi IP a un gateway di risorse per consentire più connessioni di rete con la risorsa. È possibile associare più risorse in un VPC allo stesso gateway di risorse.

Un gateway di risorse non fornisce funzionalità di bilanciamento del carico.

Indice

Considerazioni

Le seguenti considerazioni si applicano ai gateway di risorse:

- Affinché la risorsa sia accessibile da tutte le zone di disponibilità, è necessario creare gateway di risorse che coprano il maggior numero possibile di zone di disponibilità.
- Almeno una zona di disponibilità dell'endpoint VPC e del gateway di risorse deve sovrapporsi.
- Un VPC può avere un massimo di 100 gateway di risorse. Per ulteriori informazioni, consulta Quotas for VPC Lattice.
- Non è possibile creare un gateway di risorse in una sottorete condivisa.

Gruppi di sicurezza

È possibile collegare gruppi di sicurezza a un gateway di risorse. Le regole dei gruppi di sicurezza per i gateway di risorse controllano il traffico in uscita dal gateway di risorse alle risorse.

Regole in uscita consigliate per il traffico che scorre da un gateway di risorse a una risorsa di database

Affinché il traffico fluisca da un gateway di risorse a una risorsa, è necessario creare regole in uscita per i protocolli di listener e gli intervalli di porte accettati dalla risorsa.

Destinazione	Protocollo	Intervallo porte	Commento
CIDR range for resource	TCP	3306	Consente il traffico dal gateway di risorse ai database.

Tipi di indirizzi IP

Un gateway di risorse può avere indirizzi IPv6 o IPv4 indirizzi dual-stack. Il tipo di indirizzo IP di un Resource Gateway deve essere compatibile con le sottoreti del Resource Gateway e il tipo di indirizzo IP della risorsa, come descritto di seguito:

- IPv4— Assegna IPv4 indirizzi alle interfacce di rete del gateway. Questa opzione è supportata solo se tutte le sottoreti selezionate hanno intervalli di IPv4 indirizzi e la risorsa dispone anche di un indirizzo. IPv4
- IPv6— Assegna IPv6 indirizzi alle interfacce di rete del gateway. Questa opzione è supportata solo se tutte le sottoreti selezionate sono IPv6 solo sottoreti e la risorsa dispone anche di un indirizzo. IPv6
- Dualstack: assegna entrambi IPv4 gli indirizzi alle interfacce di rete gateway. IPv6 Questa opzione è supportata solo se tutte le sottoreti selezionate hanno entrambi gli intervalli di IPv6 indirizzi IPv4 e la risorsa ha un indirizzo or. IPv4 IPv6

Il tipo di indirizzo IP del Resource Gateway è indipendente dal tipo di indirizzo IP del client o dell'endpoint VPC tramite il quale si accede alla risorsa.

IPv4 indirizzi per ENI

Se il tuo Resource Gateway ha uno IPv4 o un tipo di indirizzo IP dual-stack, puoi configurare il numero di IPv4 indirizzi assegnati a ciascun ENI del tuo Resource Gateway. Quando crei un Resource Gateway, scegli da 1 a 62 indirizzi. IPv4 Una volta impostato il numero di IPv4 indirizzi, il valore non può essere modificato.

Gli IPv4 indirizzi vengono utilizzati per la traduzione degli indirizzi di rete e determinano il numero massimo di IPv4 connessioni simultanee a una risorsa. Per impostazione predefinita, a tutti i gateway

di risorse vengono assegnati 16 IPv4 indirizzi per ENI. Si tratta di un numero adeguato IPs per creare connessioni con le risorse di backend.

Se il Resource Gateway utilizza il tipo di IPv6 indirizzo, il Resource Gateway riceve automaticamente un /80 CIDR per ENI. Questo valore non può essere modificato.

Creare un gateway di risorse in VPC Lattice

Usa la console per creare un gateway di risorse.

Per creare un gateway di risorse utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, sotto PrivateLink e Lattice, scegli Resource gateway.
3. Scegli Crea gateway di risorse.
4. Inserisci un nome univoco all'interno del tuo AWS account.
5. Scegli il tipo di indirizzo IP per il gateway di risorse.
6. Per il tipo di indirizzo IP, scegli il tipo di indirizzo IP per il gateway di risorse.
   - Se hai selezionato IPv4Dualstack per il tipo di indirizzo IP, puoi inserire il numero di IPv4 indirizzi per ENI per il tuo Resource Gateway.

     L'impostazione predefinita è 16 IPv4 indirizzi per ENI. Si tratta di un numero adeguato IPs per creare connessioni con le risorse di backend.
7. Scegli il VPC in cui si trova la risorsa.
8. Scegli fino a cinque gruppi di sicurezza per controllare il traffico in entrata dal VPC alla rete di servizi.
9. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
10. Scegli Crea gateway di risorse.

Per creare un gateway di risorse utilizzando il AWS CLI

Utilizza il comando create-resource-gateway.

Eliminare un gateway di risorse in VPC Lattice

Usa la console per eliminare un gateway di risorse.

Per eliminare un gateway di risorse utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, sotto PrivateLink e Lattice, scegli Resource gateway.
3. Seleziona la casella di controllo relativa al gateway di risorse che desideri eliminare e scegli Azioni, Elimina. Quando viene richiesta la conferma, immettere **`confirm`** e quindi scegliere Elimina.

Per eliminare un gateway di risorse utilizzando il AWS CLI

Utilizza il comando delete-resource-gateway.

Accedi alle reti di servizi tramite AWS PrivateLink

Puoi connetterti privatamente a una rete di servizi dal tuo VPC utilizzando un endpoint VPC della rete di servizio (endpoint di rete di servizio). Un endpoint di rete di servizi consente di accedere in modo privato e sicuro alle risorse e ai servizi associati alla rete di servizi. In questo modo, puoi accedere privatamente a più risorse e servizi tramite un singolo endpoint VPC.

Una rete di servizi è una raccolta logica di configurazioni di risorse e servizi VPC Lattice. Utilizzando un endpoint di rete di servizi, puoi connettere una rete di servizi al tuo VPC e accedere a tali risorse e servizi privatamente dal tuo VPC o dall'ambiente locale. Un endpoint di rete di servizi consente di connettersi a una rete di servizi. Per connetterti a più reti di servizi dal tuo VPC, puoi creare più endpoint di rete di servizio, ognuno dei quali punta a una rete di servizio diversa.

Le reti di servizio sono integrate con (). AWS Resource Access Manager AWS RAMÈ possibile condividere la rete di servizi con un altro account tramite AWS RAM. Quando condividi una rete di servizi con un altro AWS account, quell'account può creare un endpoint di rete di servizio per connettersi alla rete di servizio. È possibile condividere una rete di servizi utilizzando una condivisione di risorse in. AWS RAM

Usa la AWS RAM console per visualizzare le condivisioni di risorse a cui sei stato aggiunto, le reti di servizi condivise a cui puoi accedere e gli AWS account che hanno condiviso le risorse con te. Per ulteriori informazioni, consulta Risorse condivise con te nella Guida AWS RAM per l'utente.

Prezzi

Le configurazioni delle risorse associate alla rete di servizi vengono fatturate su base oraria. Ti viene inoltre addebitato il costo per GB di dati elaborati quando accedi alle risorse tramite l'endpoint VPC della rete di assistenza. Non ti viene addebitata alcuna tariffa oraria per l'endpoint VPC della rete di servizi stesso. Per ulteriori informazioni, consultare Prezzi di Amazon VPC Lattice.

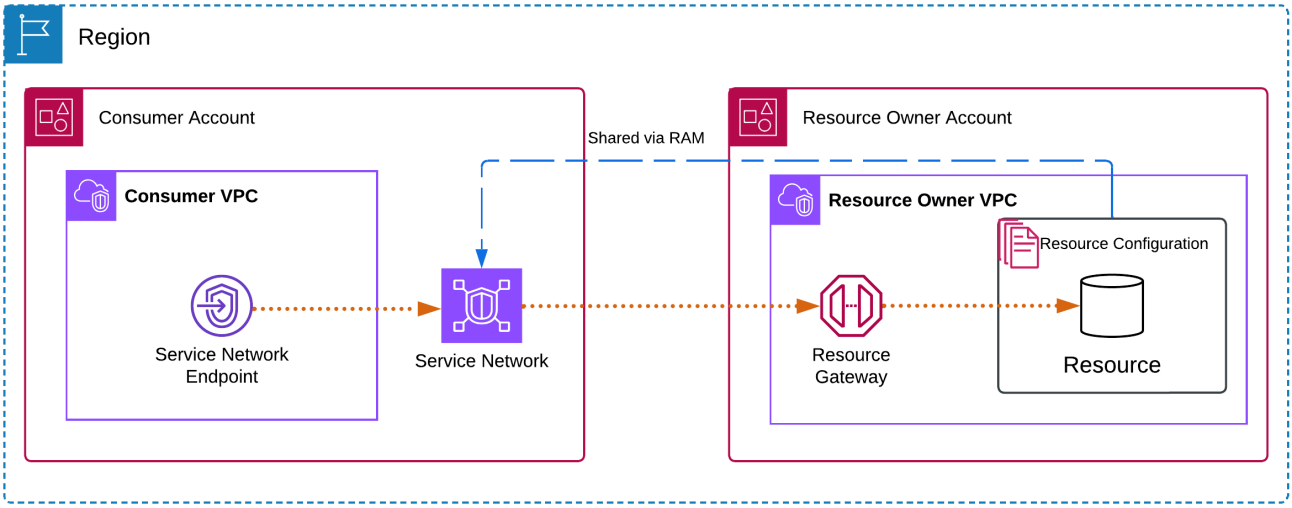
Indice

- Accedi a una rete di servizi tramite un endpoint di rete di servizi
- Gestisci gli endpoint della rete di servizio

Panoramica

Puoi creare la tua rete di servizi oppure condividere con te una rete di servizi da un altro account. In entrambi i casi, puoi creare un endpoint di rete di servizi a cui connetterti dal tuo VPC. Per ulteriori informazioni su come creare una rete di servizi e associarvi configurazioni di risorse, consulta la Amazon VPC Lattice User Guide.

Il diagramma seguente mostra come un endpoint di rete di servizi nel tuo VPC accede a una rete di servizi.



Le connessioni di rete possono essere avviate solo dal VPC che dispone dell'endpoint della rete di servizio alle risorse e ai servizi nella rete di servizio. Il VPC con le risorse e i servizi non può avviare connessioni di rete nel VPC dell'endpoint.

Hostname DNS

Con AWS PrivateLink, invii traffico alle reti di servizio utilizzando endpoint privati. Quando crei un endpoint VPC di rete di servizi, creiamo nomi DNS regionali (denominati nome DNS predefinito) per ogni risorsa e servizio che puoi utilizzare per comunicare con la risorsa e il servizio dal tuo VPC e dall'ambiente locale. Gli indirizzi IP associati all'endpoint possono cambiare. Ti consigliamo di utilizzare il DNS anziché l'endpoint IPs per connetterti alle tue reti di servizio.

Il nome DNS predefinito per una risorsa nella rete di servizi ha la seguente sintassi:

```
endpointId-snraId.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

Il nome DNS predefinito per un servizio Lattice nella rete di servizi ha la seguente sintassi:

```
endpointId-snsaId.randomHash.vpc-lattice-svcs.region.on.aws
```

Se utilizzi il Console di gestione AWS, puoi trovare il nome DNS nella scheda Associazioni. Se stai usando il AWS CLI, usa il describe-vpc-endpoint-associationscomando.

Puoi abilitare il DNS privato solo quando la tua rete di servizi ha una configurazione delle risorse di tipo ARN per un servizio di database Amazon RDS. Con il DNS privato, puoi continuare a effettuare richieste alla risorsa utilizzando il nome DNS fornito per la risorsa dal AWS servizio, sfruttando al contempo la connettività privata tramite l'endpoint VPC della rete di servizio. Per ulteriori informazioni, consulta the section called “Risoluzione DNS”.

Risoluzione DNS

Quando crei un endpoint di rete di servizio, creiamo nomi DNS per ogni configurazione di risorsa e servizio Lattice associato alla rete di servizi. Questi record DNS sono pubblici. Pertanto, questi nomi DNS sono risolvibili pubblicamente. Tuttavia, le richieste DNS dall'esterno del VPC restituiscono comunque gli indirizzi IP privati delle interfacce di rete dell'endpoint della rete di servizio. È possibile utilizzare questi nomi DNS per accedere alla risorsa e ai servizi dall'ambiente locale, purché si abbia accesso al VPC in cui si trova l'endpoint della rete di servizio, tramite VPN o Direct Connect.

DNS privato

Se abiliti il DNS privato per l'endpoint VPC della tua rete di servizi e il tuo VPC ha sia i nomi host DNS che la risoluzione DNS abilitati, creiamo zone ospitate private AWS nascoste e gestite per le configurazioni di risorse con nomi DNS personalizzati. La zona ospitata contiene un set di record per il nome DNS predefinito per la risorsa che lo risolve negli indirizzi IP privati delle interfacce di rete dell'endpoint della rete di servizio nel VPC.

Amazon fornisce un server DNS per il tuo VPC chiamato il Route 53 Resolver. Il Route 53 Resolver risolve automaticamente i nomi di dominio VPC locali e i record in zone ospitate private. Tuttavia, non

puoi utilizzare il Route 53 Resolver dall'esterno del tuo VPC. Se desideri accedere al tuo endpoint VPC dalla tua rete locale, puoi utilizzare i nomi DNS predefiniti oppure puoi utilizzare gli endpoint e le regole Resolver di Route 53. Per ulteriori informazioni, consulta Integrazione con and. AWS Transit GatewayAWS PrivateLinkAmazon Route 53 Resolver

Sottoreti e zone di disponibilità

Puoi configurare l'endpoint VPC con una sottorete per zona di disponibilità. Creiamo un'interfaccia di rete elastica per l'endpoint VPC nella tua sottorete. Assegniamo gli indirizzi IP a ciascuna interfaccia di rete elastica dalla relativa sottorete in multipli di /28, se il tipo di indirizzo IP dell'endpoint VPC è. IPv4 Il numero di indirizzi IP assegnati in ciascuna sottorete dipende dal numero di configurazioni delle risorse e ne aggiungiamo altri in blocchi /28 secondo necessità. IPs In un ambiente di produzione, per un'elevata disponibilità e resilienza, consigliamo di configurare almeno due zone di disponibilità per ogni endpoint VPC e di averne una contigua disponibile. IPs

Tipi di indirizzi IP

Gli endpoint della rete di servizio possono supportare o supportare indirizzi dual-stack. IPv4 IPv6 Gli endpoint che lo supportano IPv6 possono rispondere alle query DNS con record AAAA. Il tipo di indirizzo IP di un endpoint di rete di servizi deve essere compatibile con le sottoreti dell'endpoint di risorse, come descritto di seguito:

- IPv4— Assegna IPv4 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate hanno intervalli di indirizzi. IPv4
- IPv6— Assegna IPv6 indirizzi alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono solo sottoreti. IPv6
- Dualstack: assegna entrambi IPv4 gli indirizzi alle interfacce di rete degli endpoint. IPv6 Questa opzione è supportata solo se tutte le sottoreti selezionate hanno entrambi gli intervalli di indirizzi. IPv4 IPv6

Se un endpoint VPC di rete di servizi supporta IPv4, le interfacce di rete degli endpoint dispongono di indirizzi. IPv4 Se un endpoint VPC di rete di servizi supporta IPv6, le interfacce di rete degli endpoint dispongono di indirizzi. IPv6 L' IPv6 indirizzo per un'interfaccia di rete endpoint non è raggiungibile da Internet. Se descrivi un'interfaccia di rete endpoint con un IPv6 indirizzo, nota che è abilitata. `denyAllIgwTraffic`

Accedi a una rete di servizi tramite un endpoint di rete di servizi

È possibile accedere a una rete di servizi utilizzando un endpoint di rete di servizi. Un endpoint di rete di servizi fornisce l'accesso privato alle configurazioni delle risorse e ai servizi nella rete di servizi.

Prerequisiti

Per creare un endpoint di rete di servizi, è necessario soddisfare i seguenti prerequisiti.

- È necessario disporre di una rete di servizi creata dall'utente o condivisa con l'utente da un altro account tramite. AWS RAM
- Se una rete di servizi viene condivisa con te da un altro account, devi esaminare e accettare la condivisione di risorse che contiene la rete di servizi. Per ulteriori informazioni, consulta Accettare e rifiutare gli inviti nella Guida per l'utente di AWS RAM .
- Un endpoint della rete di servizi richiede inizialmente un blocco /28 di IPv4 indirizzi contiguo disponibile in una zona di disponibilità. Se si aggiunge una configurazione di risorse alla rete di servizi associata all'endpoint, è necessario un blocco /28 aggiuntivo disponibile nella stessa sottorete, poiché ogni risorsa utilizza un IP univoco per zona di disponibilità.

  Se si prevede di aggiungere più di 16 configurazioni di risorse a una rete di servizi, sull'endpoint della rete di servizio vengono utilizzati blocchi /28 aggiuntivi per ospitare nuove risorse. Se è necessario evitare l'uso di VPC CIDR IPs, si consiglia di utilizzare un'associazione VPC di rete di servizi. Per ulteriori informazioni, consulta Manage VPC Endpoint Associations nella Amazon VPC Lattice User Guide.

Crea un endpoint di rete di servizi

Crea un endpoint di rete di servizi per accedere alla rete di servizi condivisa con te. Dopo aver creato un endpoint di rete di servizi, puoi solo modificarne i gruppi o i tag di sicurezza.

Per creare un endpoint di rete di servizi

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, sotto PrivateLink e Lattice, scegli Endpoints.
3. Seleziona Crea endpoint.
4. Puoi specificare un nome per facilitare la ricerca e la gestione dell'endpoint.
5. Per Tipo, scegli Reti di servizio.

6. Per Reti di servizio, seleziona la rete di servizio.
7. Per le impostazioni di rete, seleziona il tuo VPC da cui accederai alla rete di servizio.
8. Se desideri configurare il supporto DNS privato, seleziona Impostazioni aggiuntive, Abilita nome DNS privato. Per utilizzare questa funzionalità, assicurati che gli attributi Enable DNS hostnames e Enable DNS support siano abilitati per il tuo VPC.
9. Per Subnet, seleziona una sottorete in cui creare l'interfaccia di rete degli endpoint.

   In un ambiente di produzione, per un'elevata disponibilità e resilienza, consigliamo di configurare almeno due zone di disponibilità per ogni endpoint VPC.
10. Per i gruppi di sicurezza, seleziona un gruppo di sicurezza.

    Se non specifichi un gruppo di sicurezza, associamo il gruppo di sicurezza predefinito per il VPC.
11. Seleziona Crea endpoint.

Per creare un endpoint di rete di servizi utilizzando la riga di comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Strumenti per Windows) PowerShell

Gestisci gli endpoint della rete di servizio

Dopo aver creato un endpoint di rete di servizi, è possibile aggiornarne i gruppi o i tag di sicurezza.

Processi

- Eliminazione di un endpoint.
- Aggiornare un endpoint di rete di servizi

Eliminazione di un endpoint.

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

Per eliminare un endpoint utilizzando la console

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

3. Seleziona l'endpoint della rete di servizio.
4. Seleziona Actions (Operazioni), Delete VPC endpoints (Eliminazione di endpoint VPC).
5. Quando viene richiesta la conferma, immetti **`delete`**.
6. Scegli Elimina.

Per eliminare un endpoint utilizzando la riga di comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Aggiornare un endpoint di rete di servizi

Puoi aggiornare un endpoint VPC.

Per aggiornare un endpoint utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint.
4. Scegli Azioni e l'opzione appropriata.
5. Segui i passaggi della console per inviare l'aggiornamento.

Per aggiornare un endpoint utilizzando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Strumenti per Windows PowerShell)

Gestione delle identità e degli accessi per AWS PrivateLink

AWS Identity and Access Management (IAM) è un servizio Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS PrivateLink IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Indice

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS PrivateLink svolgi.

Utente del servizio: se utilizzi il AWS PrivateLink servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS PrivateLink funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell’accesso consente di richiedere le autorizzazioni corrette all’amministratore.

Amministratore del servizio: se sei responsabile delle AWS PrivateLink risorse della tua azienda, probabilmente hai pieno accesso a AWS PrivateLink. È tuo compito determinare a quali AWS PrivateLink funzionalità e risorse devono accedere gli utenti del servizio. Devi quindi inviare le richieste all’amministratore IAM per modificare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS PrivateLink.

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per maggiori informazioni sull'accesso, consultare la sezione Come accedere a Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la

federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolonella Guida per l'utente IAM.

I ruoli IAM sono utili per l'accesso federato degli utenti, le autorizzazioni utente IAM temporanee, l'accesso tra account, l'accesso tra servizi e le applicazioni in esecuzione su Amazon. EC2 Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e collegandole a identità o risorse. AWS Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per

l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate sull'identità possono essere policy in linea (incorporate direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consultare 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. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: impostano il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Le policy di sessione sono policy avanzate che si passano come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, 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 Logica di valutazione delle policy nella IAM User Guide.

Come AWS PrivateLink funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS PrivateLink, scopri con quali funzionalità IAM è possibile utilizzare AWS PrivateLink.

Funzionalità IAM	AWS PrivateLink supporto
Policy basate sull'identità	Sì
Policy basate su risorse	Sì
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una panoramica generale di come AWS PrivateLink e altri Servizi AWS utilizzi la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per AWS PrivateLink

Supporta le policy basate sull'identità: sì

Le policy basate sull'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 di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Esempi di politiche basate sull'identità per AWS PrivateLink

Per visualizzare esempi di politiche basate sull' AWS PrivateLink identità, vedere. Esempi di policy basate sull'identità per AWS PrivateLink

Politiche basate sulle risorse all'interno AWS PrivateLink

Supporta le policy basate sulle risorse: sì

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 di IAM e le policy dei bucket di 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. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

AWS PrivateLink il servizio supporta un tipo di policy basata sulle risorse, nota come policy sugli endpoint. Una policy degli endpoint controlla quali principali AWS possono usare l'endpoint per accedere al servizio endpoint. Per ulteriori informazioni, consulta the section called "Policy di endpoint".

Azioni politiche per AWS PrivateLink

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità 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. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Azioni nello spazio dei nomi ec2

Alcune azioni AWS PrivateLink fanno parte dell' EC2 API Amazon. Queste azioni politiche utilizzano il `ec2` prefisso. Per ulteriori informazioni, consulta AWS PrivateLink le azioni nell'Amazon EC2 API Reference.

Azioni nello spazio dei nomi vpce

AWS PrivateLink fornisce anche l'azione solo per le autorizzazioni. `AllowMultiRegion` Questa azione politica utilizza il prefisso. `vpce`

Risorse politiche per AWS PrivateLink

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità 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. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, utilizzare un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Chiavi relative alle condizioni delle politiche per AWS PrivateLink

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

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

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. 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. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Le seguenti chiavi di condizione sono specifiche per AWS PrivateLink:

- `ec2:VpceMultiRegion`
- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`
- `ec2:VpceServiceRegion`
- `ec2:VpceSupportedRegion`

Per ulteriori informazioni, consulta Condition keys for Amazon EC2.

ACLs in AWS PrivateLink

Supporti ACLs: no

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.

ABAC con AWS PrivateLink

Supporta ABAC (tag nelle policy): sì

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AWS PrivateLink

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nelle Guida per l'utente IAM.

Autorizzazioni principali multiservizio per AWS PrivateLink

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per AWS PrivateLink

Supporta i ruoli di servizio: no

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.

Ruoli collegati ai servizi per AWS PrivateLink

Supporta i ruoli collegati ai servizi: no

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 in Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Esempi di policy basate sull'identità per AWS PrivateLink

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS PrivateLink . Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da AWS PrivateLink, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon EC2 nel Service Authorization Reference.

Esempi

- Controlla l'utilizzo degli endpoint VPC
- Controlla la creazione di endpoint VPC in base al proprietario del servizio
- Controllare i nomi DNS privati che possono essere specificati per i servizi endpoint VPC
- Controllare i nomi dei servizi che è possibile specificare per i servizi endpoint VPC

Controlla l'utilizzo degli endpoint VPC

Per impostazione predefinita, gli utenti non dispongono delle autorizzazioni per utilizzare Endpoint. Puoi creare una policy basata sull'identità che concede agli utenti le autorizzazioni per creare, modificare, descrivere ed eliminare gli endpoint. Di seguito è riportato un esempio di :

JSON

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

```
            "Action":"ec2:*VpcEndpoint*",
            "Resource":"*"
        }
    ]
}
```

Per ulteriori informazioni sul controllo dell'accesso ai servizi utilizzando endpoint VPC, consulta the section called “Policy di endpoint”.

Controlla la creazione di endpoint VPC in base al proprietario del servizio

Puoi utilizzare la chiave di condizione `ec2:VpceServiceOwner` per controllare l'endpoint VPC che può essere creato in base al proprietario del servizio (`amazon`, `aws-marketplace` o l'ID account). Nell'esempio seguente viene concessa l'autorizzazione per creare endpoint VPC con il proprietario del servizio specificato. Per utilizzare questo esempio, sostituisci la Regione, l'ID account e il proprietario del servizio.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc/*",
                "arn:aws:ec2:us-east-1:111111111111:security-group/*",
                "arn:aws:ec2:us-east-1:111111111111:subnet/*",
                "arn:aws:ec2:us-east-1:111111111111:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceOwner": [
```

```
                    "amazon"
                ]
            }
        }
    ]
}
```

Controllare i nomi DNS privati che possono essere specificati per i servizi endpoint VPC

Puoi utilizzare la chiave di condizione `ec2:VpceServicePrivateDnsName` per controllare quale servizio endpoint VPC può essere modificato o creato in base al nome DNS privato associato al servizio endpoint VPC. Nell'esempio seguente viene concessa l'autorizzazione per creare un servizio endpoint VPC con il nome DNS privato specificato. Per utilizzare questo esempio, sostituisci la Regione, l'ID account e il nome DNS privato.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint-service/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServicePrivateDnsName": [
                        "example.com"
                    ]
                }
            }
        }
    ]
```

```
}
```

Controllare i nomi dei servizi che è possibile specificare per i servizi endpoint VPC

È possibile utilizzare la chiave di condizione `ec2:VpceServiceName` per controllare quale endpoint VPC può essere creato in base al nome del servizio endpoint VPC. Nell'esempio seguente viene concessa l'autorizzazione per creare un endpoint VPC con il nome del servizio specificato. Per utilizzare questo esempio, sostituisci la Regione, l'ID account e il nome del servizio.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc/*",
                "arn:aws:ec2:us-east-1:111111111111:security-group/*",
                "arn:aws:ec2:us-east-1:111111111111:subnet/*",
                "arn:aws:ec2:us-east-1:111111111111:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.111111111111.s3"
                    ]
                }
            }
        }
    ]
```

```
}
```

Controllo dell'accesso agli endpoint VPC tramite le policy di endpoint

Una policy per gli endpoint è una policy basata sulle risorse che si collega a un endpoint VPC per controllare quali AWS responsabili possono utilizzare l'endpoint per accedere a un. Servizio AWS

Una policy di endpoint non esclude né sostituisce le policy basate sull'identità o sulle risorse. Ad esempio, se utilizzi un endpoint di interfaccia per connetterti ad Amazon S3, puoi anche utilizzare le policy dei bucket di Amazon S3 per controllare l'accesso ai bucket da endpoint specifici o specifici. VPCs

Indice

Considerazioni

- Una policy degli endpoint è un documento di policy JSON che utilizza il linguaggio della policy IAM. Deve contenere un elemento Principal. Le dimensioni di una policy degli endpoint non possono superare i 20.480 caratteri, inclusi gli spazi bianchi.
- Quando crei un'interfaccia o un endpoint gateway per un endpoint Servizio AWS, puoi allegare una singola policy endpoint all'endpoint. Puoi aggiornare la policy degli endpoint in qualsiasi momento. Se non si allega una policy degli endpoint, alleghiamo la policy degli endpoint predefinita.
- Non tutti Servizi AWS supportano le policy relative agli endpoint. Se un dispositivo Servizio AWS non supporta le policy relative agli endpoint, consentiamo l'accesso completo a qualsiasi endpoint per il servizio. Per ulteriori informazioni, consulta the section called “Visualizza il supporto della politica dell'endpoint”.
- Quando crei un endpoint VPC per un servizio endpoint diverso da un Servizio AWS, consentiamo l'accesso completo all'endpoint.

- Non puoi usare caratteri jolly (* o?) o operatori di condizioni numeriche con chiavi di contesto globali che fanno riferimento a identificatori generati dal sistema (ad esempio o). `aws:PrincipalAccount` `aws:SourceVpc`
- Quando si utilizza un operatore di condizione di stringa, è necessario utilizzare almeno sei caratteri consecutivi prima o dopo ogni carattere jolly.
- Quando si specifica un ARN in un elemento risorsa o condizione, la parte relativa all'account dell'ARN può includere un ID account o un carattere jolly, ma non entrambi.
- Dopo avere aggiornato l'endpoint, possono essere necessari alcuni minuti prima che le modifiche diventino effettive.

Policy degli endpoint predefinita

La policy degli endpoint predefinita consente l'accesso completo all'endpoint.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Policy degli endpoint di interfaccia

Ad esempio, le politiche degli endpoint per, vedi. Servizi AWSthe section called “Servizi integrati” La prima colonna della tabella contiene i collegamenti alla AWS PrivateLink documentazione relativa a ciascuna di esse Servizio AWS. Se un dispositivo Servizio AWS supporta le policy relative agli endpoint, la relativa documentazione include esempi di policy per gli endpoint.

Principali per endpoint gateway

Con gli endpoint gateway, l'`Principal`elemento deve essere impostato su. * Per specificare un principale, utilizzate la chiave `aws:PrincipalArn` condition.

```
"Condition": {
```

```
    "StringEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
    }
}
```

Se si specifica il principale nel formato seguente, l'accesso viene concesso Utente root dell'account AWS solo agli utenti e ai ruoli dell'account, non a tutti.

```
"AWS": "account_id"
```

Per esempi di policy degli endpoint gateway, consulta i seguenti argomenti:

- Endpoint per Amazon S3
- Endpoint per DynamoDB

Aggiornamento di una policy di endpoint VPC

Utilizza la procedura seguente per aggiornare una policy degli endpoint per un Servizio AWS. Dopo avere aggiornato l'endpoint, possono essere necessari alcuni minuti prima che le modifiche diventino effettive.

Per aggiornare la policy degli endpoint usando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint VPC.
4. Scegli Actions (Operazioni), Manage policy (Gestisci policy).
5. Scegli Full Access (Accesso completo) per consentire l'accesso completo al servizio oppure scegli Custom (Personalizzato) e specifica una policy personalizzata.
6. Scegli Save (Salva).

Per aggiornare la policy degli endpoint utilizzando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Strumenti per Windows PowerShell)

AWS politiche gestite per AWS PrivateLink

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 Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri 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 maggiori informazioni, consulta Policy gestite da AWS nella Guida per l'utente di IAM.

AWS PrivateLink aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS PrivateLink da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AWS PrivateLink documenti.

Modifica	Descrizione	Data
AWS PrivateLink ha iniziato a tenere traccia delle modifiche	AWS PrivateLink ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	1 marzo 2021

CloudWatch metriche per AWS PrivateLink

AWS PrivateLink pubblica punti dati su Amazon CloudWatch per gli endpoint di interfaccia, gli endpoint Gateway Load Balancer e i servizi endpoint. CloudWatch ti consente di recuperare le statistiche su tali punti dati sotto forma di un insieme ordinato di dati di serie temporali, noti come metriche. Pensa a una metrica come a una variabile da monitorare e ai dati di utilizzo come ai valori di questa variabile nel tempo. A ogni dato sono associati una marcatura temporale e un'unità di misura facoltativa.

Puoi utilizzare le metriche per verificare che le prestazioni del sistema siano quelle previste. Ad esempio, puoi creare un CloudWatch allarme per monitorare una metrica specifica e avviare un'azione (come l'invio di una notifica a un indirizzo e-mail) se la metrica non rientra nell'intervallo che consideri accettabile.

I parametri vengono pubblicati per tutti gli endpoint dell'interfaccia, gli endpoint di Gateway Load Balancer e i servizi dell'endpoint. Non vengono pubblicati per gli endpoint gateway o per i consumatori di servizi endpoint che utilizzano l'accesso interregionale. Per impostazione predefinita, AWS PrivateLink invia le metriche a CloudWatch a intervalli di un minuto, senza costi aggiuntivi.

Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Indice

Parametri e dimensioni dell'endpoint

Lo spazio dei nomi di `AWS/PrivateLinkEndpoints` include i parametri descritti di seguito per endpoint di interfaccia e endpoint di Gateway Load Balancer.

Parametro	Descrizione
`ActiveConnections`	Il numero di connessioni simultanee attive. Questo parametro include connessioni negli stati SYN_SENT ed ESTABLISHED.

Parametro	Descrizione
	Criteri di segnalazione: L'endpoint ha ricevuto traffico durante il periodo di un minuto. Statistiche: le statistiche più utili sono `Average`, `Maximum` e `Minimum`. Dimensioni • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`BytesProcessed`	Il numero di byte scambiati tra endpoint e servizi endpoint, aggregati in entrambe le direzioni. Questo è il numero di byte fatturati al proprietario dell'endpoint. La fattura visualizza questo valore in GB. Criteri di segnalazione: L'endpoint ha ricevuto traffico durante il periodo di un minuto. Statistihe: le statistiche pi\ utili sono `Average`, `Sum`, `Maximum` e `Minimum`. Dimensioni • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Parametro	Descrizione
`NewConnections`	In numero di connessioni stabilite attraverso l'endpoint. Criteri di segnalazione: L'endpoint ha ricevuto traffico durante il periodo di un minuto. Statistihe: le statistiche pi\ utili sono `Average`, `Sum`, `Maximum` e `Minimum`. Dimensioni • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`PacketsDropped`	Il numero di pacchetti ricevuti dall'endpoint. Questo parametro potrebbe non catturare tutti i pacchetti. Valori crescenti potrebbero indicare che il servizio endpoint o endpoint non è sano. Criteri di segnalazione: L'endpoint ha ricevuto traffico durante il periodo di un minuto. Statistiche: le statistiche più utili sono `Average`, `Sum` e `Maximum`. Dimensioni • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Parametro	Descrizione
`RstPacketsReceived`	Il numero di pacchetti RST ricevuti dall'endpoint. Valori crescenti potrebbero indicare che il servizio endpoint o endpoint non è sano. Criteri di segnalazione: L'endpoint ha ricevuto traffico durante il periodo di un minuto. Statistiche: le statistiche più utili sono `Average`, `Sum` e `Maximum`. Dimensioni • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Per filtrare questi parametri, usa le seguenti dimensioni.

Dimensione	Descrizione
`Endpoint Type`	Filtra i dati dei parametri per tipo di endpoint (`Interface` |`GatewayLoadBalancer`).
`Service Name`	Filtra i dati dei parametri per nome del servizio.
`Subnet Id`	Filtra i dati dei parametri per sottorete.
`VPC Endpoint Id`	Filtra i dati dei parametri per endpoint VPC.
`VPC Id`	Filtra i dati dei parametri per VPC.

Parametri e dimensioni del servizio dell'endpoint

Lo spazio dei nomi di `AWS/PrivateLinkServices` include i parametri descritti di seguito per endpoint .

Parametro	Descrizione
`ActiveConnections`	Il numero massimo di connessioni attive dai client alle destinazioni tramite endpoint. Valori crescenti potrebbero indicare la necessità di aggiungere obiettivi al load balancer. Criteri di segnalazione: un endpoint connesso al servizio endpoint ha inviato traffico durante il periodo di un minuto. Statistiche: le statistiche più utili sono `Average` e `Maximum`. Dimensioni • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`BytesProcessed`	Il numero di byte scambiati tra endpoint e servizi endpoint, aggregati in entrambe le direzioni. Criteri di segnalazione: un endpoint connesso al servizio endpoint ha inviato traffico durante il periodo di un minuto. Statistiche: le statistiche più utili sono `Average`, `Sum` e `Maximum`. Dimensioni • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`EndpointsCount`	Il numero di endpoint collegati al servizio endpoint.

Parametro	Descrizione
	Criteri di segnalazione: è presente un valore diverso da zero durante il periodo di cinque minuti. Statistiche: le statistiche più utili sono `Average` e `Maximum`. Dimensioni • `Service Id`
`NewConnections`	Il numero massimo di connessioni attive dai client alle destinazioni tramite endpoint. Valori crescenti potrebbero indicare la necessità di aggiungere obiettivi al load balancer. Criteri di segnalazione: un endpoint connesso al servizio endpoint ha inviato traffico durante il periodo di un minuto. Statistiche: le statistiche più utili sono `Average`, `Sum` e `Maximum`. Dimensioni • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Parametro	Descrizione
`RstPacketsSent`	Il numero di pacchetti RST inviati agli endpoint dal servizio endpoint. Valori crescenti potrebbero indicare che ci sono obiettivi malsani. Criteri di segnalazione: un endpoint connesso al servizio endpoint ha inviato traffico durante il periodo di un minuto. Statistiche: le statistiche più utili sono `Average`, `Sum` e `Maximum`. Dimensioni • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Per filtrare questi parametri, usa le seguenti dimensioni.

Dimensione	Descrizione
`Az`	Consente di filtrare i dati del parametro per zona di disponibilità.
`Load Balancer Arn`	Consente di filtrare i dati del parametro per load balancer.
`Service Id`	Filtra i dati dei parametri per servizio endpoint.
`VPC Endpoint Id`	Filtra i dati dei parametri per endpoint VPC.

Visualizza le CloudWatch metriche

Puoi visualizzare questi CloudWatch parametri utilizzando la console Amazon VPC, CloudWatch la console o come AWS CLI segue.

Per visualizzare i parametri tramite la console di Amazon VPC

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint. Selezionare l'endpoint, quindi scegliere la scheda Monitoring (Monitoraggio).
3. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint). Selezionare l'endpoint, quindi scegliere la scheda Monitoring (Monitoraggio).

Per visualizzare i parametri utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Seleziona lo spazio dei nomi AWS/ PrivateLinkEndpoints.
4. Seleziona lo spazio dei nomi AWS/ PrivateLinkServices.

Per visualizzare le metriche utilizzando il AWS CLI

Utilizza il parametro seguente list-metrics comando per elencare le metriche disponibili per gli endpoint di interfaccia e gli endpoint Gateway Load Balancer:

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkEndpoints
```

Utilizza il seguente comando list-metrics per elencare i parametri disponibili per i servizi di endpoint:

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkServices
```

Utilizza regole integrate di Contributor Insights

AWS PrivateLink fornisce regole integrate di Contributor Insights per i tuoi servizi endpoint per aiutarti a scoprire quali endpoint contribuiscono maggiormente a ciascuna metrica supportata. Per ulteriori informazioni, consulta Contributor Insights nella Amazon CloudWatch User Guide.

AWS PrivateLink fornisce le seguenti regole:

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1`- classifica gli endpoint in base al numero di connessioni attive all'endpoint.

- `VpcEndpointService-BytesByEndpointId-v1`— Classifica gli endpoint in base al numero di byte elaborati.
- `VpcEndpointService-NewConnectionsByEndpointId-v1`- classifica gli endpoint in base al numero di connessioni attive all'endpoint.
- `VpcEndpointService-RstPacketsByEndpointId-v1`- Il numero di pacchetti RST inviati agli endpoint dal servizio endpoint.

Prima di poter utilizzare una regola integrata, è necessario abilitarla. Dopo che una regola è stata abilitato, questa inizia a raccogliere i dati dei collaboratori. Per informazioni sui costi per Contributor Insights, consulta la pagina CloudWatch dei prezzi di Amazon.

Per utilizzare Approfondimenti sulle contribuzioni, devi disporre delle seguenti autorizzazioni:

- `cloudwatch:DeleteInsightRules`: per eliminare le regole di Approfondimenti sulle contribuzioni.
- `cloudwatch:DisableInsightRules`: per disabilitare le regole di Approfondimenti sulle contribuzioni
- `cloudwatch:GetInsightRuleReport`: per ottenere i dati.
- `cloudwatch:ListManagedInsightRules`: per elencare le regole di Approfondimenti sulle contribuzioni disponibili.
- `cloudwatch:PutManagedInsightRules`: per abilitare le regole di Approfondimenti sulle contribuzioni.

Attività

- Abilitazione delle regole di Approfondimenti sulle contribuzioni
- Disabilitazione delle regole di Approfondimenti sulle contribuzioni
- Eliminazione delle regole di Approfondimenti sulle contribuzioni

Abilitazione delle regole di Approfondimenti sulle contribuzioni

Utilizza le seguenti procedure per abilitare le regole integrate per AWS PrivateLink l'utilizzo di Console di gestione AWS o di AWS CLI.

Per abilitare le regole di Contributor Insights per AWS PrivateLink l'utilizzo della console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Nella scheda Contributor Insights (Approfondimenti sulle contribuzioni), scegli Enable (Abilita).
5. (Facoltativo) Per impostazione predefinita, tutte le regole sono abilitate. Per abilitare solo regole specifiche, seleziona le regole desiderate quindi scegli Actions (Operazioni), Disable rule (Disabilita regola). Quando viene richiesta la conferma, seleziona Disable (Disabilita).

Per abilitare le regole di Contributor Insights per l'utilizzo di AWS PrivateLinkAWS CLI

1. Utilizzate il list-managed-insight-rulescomando come segue per enumerare le regole disponibili. Per l'opzione `--resource-arn`, specifica l'ARN del servizio endpoint.

```
aws cloudwatch list-managed-insight-rules --resource-arn
 arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. Nell'output del comando `list-managed-insight-rules`, copia il nome del modello dal campo `TemplateName`. Di seguito è riportato un esempio di questo campo.

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. Utilizzate il put-managed-insight-rulescomando seguente per abilitare la regola. Devi specificare il nome del modello e l'ARN del servizio endpoint.

```
aws cloudwatch put-managed-insight-rules --managed-rules
 TemplateName=VpcEndpointService-NewConnectionsByEndpointId-
v1,ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

Disabilitazione delle regole di Approfondimenti sulle contribuzioni

È possibile disattivare le regole integrate AWS PrivateLink in qualsiasi momento. Una volta disabilitata, una regola interrompe la raccolta dei dati dei collaboratori e i dati esistenti vengono conservati per 15 giorni. Dopo aver disabilitato una regola, potrai abilitarla di nuovo per riprendere la raccolta dei dati dei collaboratori.

Per disabilitare le regole di Contributor Insights per AWS PrivateLink l'utilizzo della console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Nella scheda Contributor Insights (Approfondimenti sulle contribuzioni), scegli Disable all (Disabilita tutto) per disabilitare tutte le regole. In alternativa, espandi il pannello Rules(Regole), seleziona le regole da disabilitare e scegli Actions (Operazioni), Disable rule (Disabilita regola).
5. Quando viene richiesta la conferma, seleziona Disable (Disabilita).

Per disabilitare le regole di Contributor Insights per l'utilizzo di AWS PrivateLinkAWS CLI

Utilizzate il disable-insight-rulescomando per disabilitare una regola.

Eliminazione delle regole di Approfondimenti sulle contribuzioni

Utilizzare le seguenti procedure per eliminare le regole integrate per AWS PrivateLink l'utilizzo di Console di gestione AWS o di AWS CLI. Dopo aver eliminato una regola, questa interrompe la raccolta dei dati dei collaboratori e i dati esistenti vengono eliminati.

Per eliminare le regole di Contributor Insights per AWS PrivateLink l'utilizzo della console

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione scegli Insights (Approfondimenti), quindi Contributor Insights (Approfondimenti sulle contribuzioni).
3. Espandi il pannello Rules (Regole) e seleziona le regole.
4. Scegli Actions (Operazioni), Delete rule (Elimina regola).
5. Quando viene richiesta la conferma, seleziona Delete (Elimina).

Per eliminare le regole di Contributor Insights per l' AWS PrivateLink utilizzo di AWS CLI

Utilizzate il delete-insight-rulescomando per eliminare una regola.

AWS PrivateLink quote

Il tuo AWS account ha delle quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate. Se richiedi di aumentare una quota applicabile per risorsa, viene aumentata la quota per tutte le risorse nella regione.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas.

Limitazione delle richieste

Le azioni API per AWS PrivateLink fanno parte dell' EC2 API Amazon. Amazon EC2 limita le sue richieste API a livello. Account AWS Per ulteriori informazioni, consulta Request throttling nella Amazon EC2 Developer Guide. Inoltre, le richieste API vengono limitate anche a livello di organizzazione per favorire le prestazioni di. AWS PrivateLink Se utilizzi AWS Organizations e ricevi un codice di `RequestLimitExceeded` errore mentre rientri ancora nei limiti dell'API a livello di account, vedi Come identificare AWS gli account che effettuano un numero elevato di chiamate API. Se hai bisogno di aiuto, contatta il team del tuo account o apri una richiesta di supporto tecnico utilizzando il servizio VPC e la categoria VPC Endpoints. Assicurati di allegare un'immagine del codice di errore. `RequestLimitExceeded`

Quote degli endpoint VPC

Il tuo AWS account ha le seguenti quote relative agli endpoint VPC.

Nome	Predefinita	Adattabile	Commenti
Endpoint load balancer di interfaccia e gateway per VPC	50	Sì	Si tratta di una quota combinata di endpoint dell'interfaccia ed endpoint Gateway Load Balancer
Endpoint VPC del gateway per regione	20	Sì	Puoi creare fino a 255 endpoint gateway per VPC
Endpoint VPC di risorse per VPC	200	Sì	

Nome	Predefinita	Adattabile	Commenti
Endpoint VPC della rete di assistenza per VPC	50	Sì	
Caratteri per policy di endpoint VPC	20.480	No	La dimensione massima di una policy dell'endpoint VPC include gli spazi vuoti

Le considerazioni seguenti si applicano al traffico in transito attraverso un endpoint VPC:

- Per impostazione predefinita, ogni endpoint VPC può supportare una larghezza di banda massima di 10 Gpbs per zona di disponibilità e aumenta automaticamente fino a 100 Gbps. La larghezza di banda massima per un endpoint VPC, quando si distribuisce il carico su tutte le zone di disponibilità, è il numero di zone di disponibilità moltiplicato per 100 Gbps. Se l'applicazione richiede una velocità effettiva più elevata, contatta il supporto AWS .
- L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del più grande pacchetto consentito che può essere trasferito attraverso un endpoint VPC. Maggiore è la MTU di una connessione, maggiore è la quantità di dati che possono essere trasferiti in un unico pacchetto. Un endpoint VPC supporta una MTU di 8500 byte. I pacchetti con dimensioni superiori a 8500 byte che arrivano all'endpoint VPC vengono eliminati.
- Il percorso MTU Discovery (PMTUD) non è supportato. Gli endpoint VPC non generano il seguente messaggio ICMP: `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (Tipo 3, Codice 4).
- Gli endpoint VPC applicano il clamping MSS (Maximum Segment Size) a tutti i pacchetti. Per ulteriori informazioni, consulta RFC879.

Cronologia dei documenti per AWS PrivateLink

La tabella seguente descrive le versioni per. AWS PrivateLink

Modifica	Descrizione	Data
Accesso a risorse e reti di servizi	AWS PrivateLink supporta l'accesso a risorse e reti di servizi attraverso i confini di VPC e account.	1 dicembre 2024
Accesso tra regioni	Un fornitore di servizi può ospitare un servizio in una regione e renderlo disponibile in un insieme di AWS regioni. Un consumatore di servizi seleziona le regioni di servizio durante la creazione di un endpoint.	26 novembre 2024
Indirizzi IP designati	È possibile specificare gli indirizzi IP per le interfacce di rete degli endpoint quando crei o modifichi l'endpoint VPC.	17 agosto 2023
IPv6 supporto	È possibile configurare i servizi endpoint Gateway Load Balancer e gli endpoint Gateway Load Balancer in modo che supportino entrambi IPv4 gli indirizzi o solo gli indirizzi. IPv6 IPv6	12 dicembre 2022
Contributor Insights	Puoi utilizzare le regole integrate di Contributor Insights per identificare gli endpoint specifici per i quali	18 agosto 2022

	i principali contributori alle metriche. CloudWatch AWS PrivateLink	
IPv6 supporto	I provider di servizi possono consentire al proprio servizio endpoint di accettare IPv6 le richieste, anche se i servizi di backend supportano solo. IPv4 Se un servizio endpoint accetta IPv6 richieste, gli utenti del servizio possono abilitare il IPv6 supporto per i propri endpoint di interfaccia in modo da poter accedere al servizio endpoint tramite. IPv6	11 maggio 2022
CloudWatch metriche	AWS PrivateLink pubblica CloudWatch metriche per gli endpoint di interfaccia, gli endpoint Gateway Load Balancer e i servizi endpoint.	27 gennaio 2022
Endpoint Gateway Load Balancer	Puoi creare un endpoint Gateway Load Balancer nel VPC per instradare il traffico a un servizio endpoint VPC configurato tramite un Gateway Load Balancer.	10 novembre 2020
Policy di endpoint VPC	È possibile collegare un criterio IAM a un endpoint VPC di interfaccia per un servizio AWS per controllare l'accesso al servizio.	23 marzo 2020

Chiavi di condizione per endpoint VPC e servizi endpoint	Puoi utilizzare le chiavi di condizione EC2 per controllare l'accesso agli endpoint VPC e ai servizi endpoint.	6 marzo 2020
Assegna tag agli endpoint VPC e ai servizi endpoint VPC quando vengono creato	Puoi aggiungere tag quando crei gli endpoint VPC e i servizi endpoint.	5 febbraio 2020
Nomi DNS privati	Puoi accedere ai servizi AWS PrivateLink basati dall'interno del tuo VPC utilizzando nomi DNS privati.	6 gennaio 2020
Servizi endpoint VPC	Puoi creare un tuo servizio endpoint e consentire ad altri utenti e Account AWS di connettersi allo stesso servizio tramite un endpoint VPC di interfaccia. Puoi offrire i tuoi servizi endpoint per l'abbonamento nel Marketplace AWS.	28 novembre 2017
Endpoint VPC di interfaccia per Servizi AWS	È possibile creare un endpoint di interfaccia a cui connettersi con Servizi AWS cui integrars i AWS PrivateLink senza utilizzare un gateway Internet o un dispositivo NAT.	8 Novembre 2017
Endpoint VPC per DynamoDB	Puoi creare un endpoint VPC gateway per accedere ad Amazon DynamoDB dal tuo VPC senza utilizzare un gateway Internet o un dispositivo NAT.	16 agosto 2017

Endpoint VPC per Amazon S3	Puoi creare un endpoint VPC gateway per accedere ad Amazon S3 dal tuo VPC senza utilizzare un gateway Internet o un dispositivo NAT.	11 maggio 2015

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.