AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

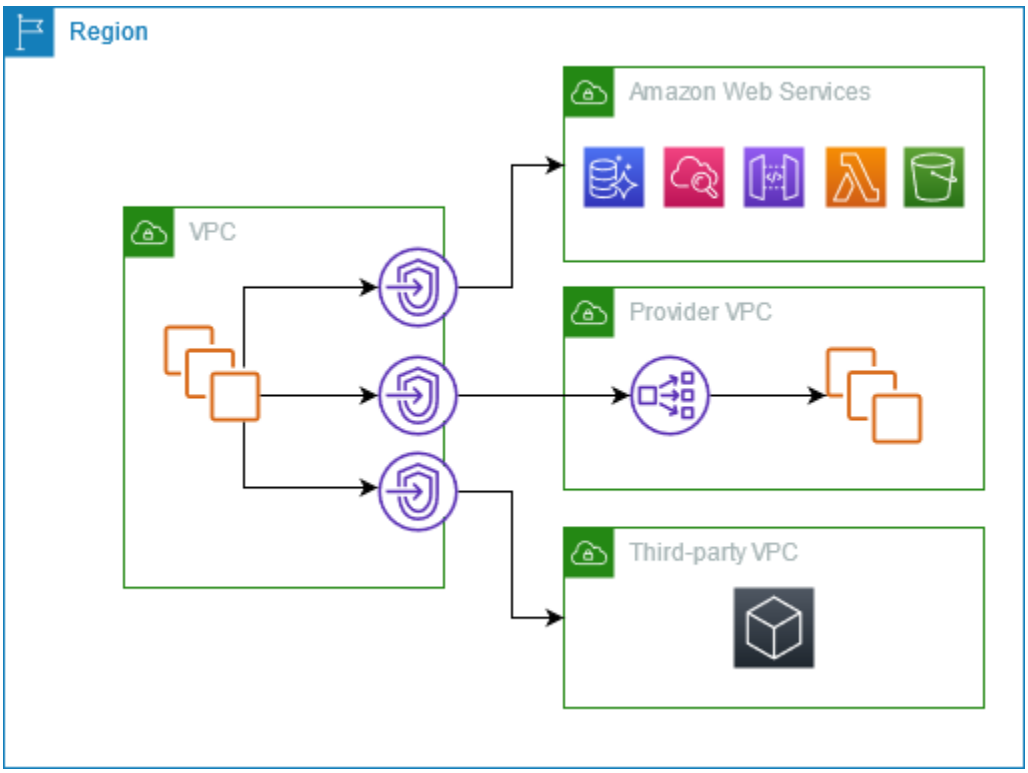
Che cos'è AWS PrivateLink?

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

Casi d'uso

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

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



Ulteriori informazioni

- the section called “Concetti”
- Accesso Servizi AWS
- Accesso ai prodotti SaaS
- Accesso alle appliance virtuali
- Condividi i tuoi servizi

Lavora con VPC gli endpoint

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

- AWS Management Console— Fornisce un'interfaccia web che è possibile utilizzare per accedere alle AWS PrivateLink risorse. Apri la VPC console Amazon e scegli Endpoints o Endpoint services.
- AWS Command Line Interface (AWS CLI) — Fornisce comandi per un'ampia gamma di Servizi AWS, tra cui. AWS PrivateLink Per ulteriori informazioni sui comandi per AWS PrivateLink, consulta ec2 nella Guida ai AWS CLI comandi.

- AWS 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::VPCEndpointConnectionNotification
  - AWS::EC2::VPCEndpointService
  - AWS::EC2::VPCEndpointServicePermissions
  - AWS:: ElasticLoadBalancing V2:: LoadBalancer
- AWS SDKs— Fornire informazioni specifiche per la linguaAPIs. SDKsSi 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.
- Query API: fornisce API azioni di basso livello richiamabili utilizzando le richieste. HTTPS L'utilizzo di Query API è il modo più diretto per accedere ad AmazonVPC. 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 in Amazon EC2 API Reference.

Prezzi

Per informazioni sui prezzi degli VPC endpoint, consulta la pagina AWS PrivateLink Prezzi.

AWS PrivateLink concetti

Puoi usare Amazon VPC per definire un cloud privato virtuale (VPC), che è una rete virtuale logicamente isolata. Puoi consentire ai tuoi client VPC di connettersi a destinazioni esterne. VPC Ad esempio, aggiungi un gateway Internet VPC per consentire l'accesso a Internet o aggiungi una VPN connessione per consentire l'accesso alla rete locale. In alternativa, AWS PrivateLink utilizzatelo per consentire ai vostri client di connettersi VPC ai servizi e alle risorse di altri utenti VPCs utilizzando indirizzi IP privati, come se tali servizi e risorse fossero ospitati direttamente sul vostroVPC.

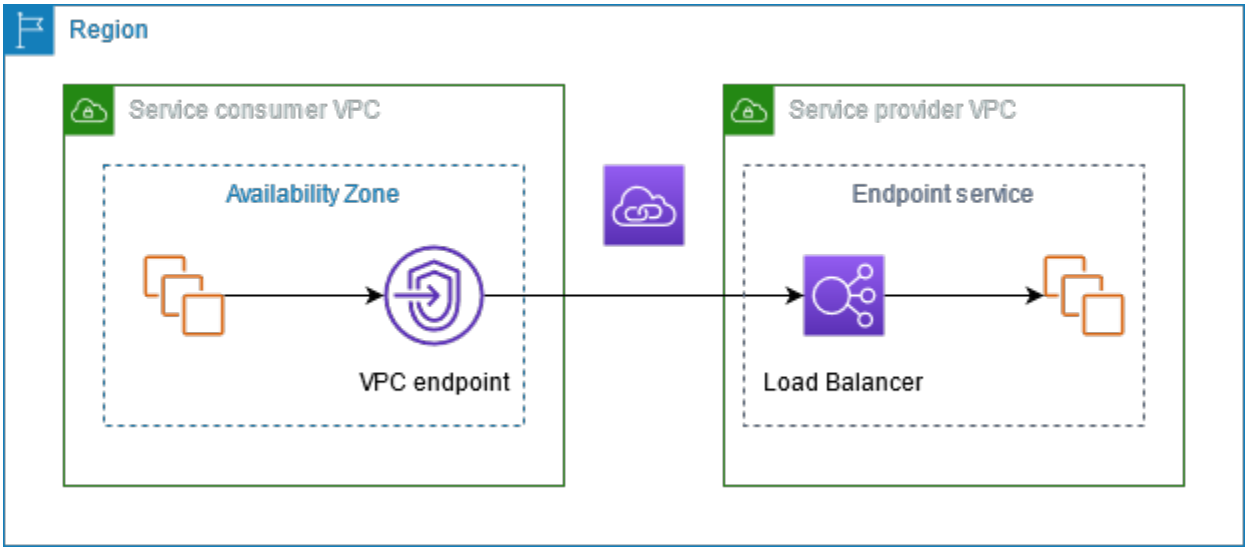
Di seguito sono riportati alcuni concetti fondamentali da conoscere quando si inizia a utilizzare AWS PrivateLink.

Indice

- Provider
- Consumatori di servizi o risorse
- AWS PrivateLink connessioni
- Zone ospitate private

Diagramma architetturale

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



Provider

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, un cluster di nodi o un'istanza, 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 di 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 consumatore del servizio deve specificare il nome del servizio 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:

- `Pending`: il servizio endpoint è in fase di creazione.
- `Available`: il servizio endpoint è disponibile.
- `Failed`: non è possibile creare il servizio endpoint.
- `Deleting`: è in corso l'eliminazione del servizio endpoint stabilita dal provider di servizi.
- `Deleted`: il servizio endpoint è eliminato.

Configurazione delle risorse

Il provider di risorse crea una configurazione di risorse per condividere una risorsa. Una configurazione delle risorse è un oggetto logico che rappresenta una singola risorsa, ad esempio un database, o un gruppo di risorse come un cluster di nodi. Una risorsa può essere un indirizzo IP, una destinazione con nome di dominio o un database Amazon. RDS

In caso di condivisione con altri account, il fornitore di risorse deve condividere la risorsa tramite una condivisione di AWS RAM risorse per consentire a AWS responsabili specifici dell'altro account di connettersi alla risorsa tramite un endpoint di risorse. VPC

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

Gateway di risorse

Un gateway di risorse è un punto di ingresso in un punto VPC da cui una risorsa viene condivisa. Il provider crea un gateway di risorse per condividere le risorse di. 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 VPCendpoint per connettersi a un servizio o una risorsa endpoint. VPC 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 VPC endpoint richiesto.

- `Interface`- Crea un endpoint di interfaccia per inviare TCP o inviare UDP traffico verso un servizio endpoint. Il traffico destinato al servizio endpoint viene risolto utilizzando. DNS

- `GatewayLoadBalancer`: crea un endpoint Gateway Load Balancer per inviare traffico a un parco istanze di appliance virtuali utilizzando indirizzi IP privati. Il traffico viene indirizzato dal proprio VPC endpoint Gateway Load Balancer utilizzando le tabelle di routing. 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 cluster di nodi, un'istanza, un endpoint dell'applicazione, una destinazione con nome di dominio o un indirizzo IP che può trovarsi in una sottorete privata in un altro ambiente o in locale. VPC 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 VPC endpoint`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 ogni sottorete specificata quando create un endpoint, creiamo un'interfaccia di rete VPC endpoint nella sottorete.

Se un VPC endpoint lo supportaIPv4, le relative interfacce di rete degli endpoint dispongono di indirizzi. IPv4 Se un VPC endpoint lo supportaIPv6, le relative interfacce di rete degli endpoint dispongono di indirizzi. IPv6 L'IPv6indirizzo 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 per gli VPC endpoint è una politica IAM delle risorse che si collega a un VPC endpoint. Determina quali principali possono utilizzare l'VPCendpoint per accedere al servizio endpoint. La policy predefinita per gli VPC endpoint consente tutte le azioni da parte di tutti i principali su tutte le risorse dell'endpoint. VPC

Stati dell'endpoint

Quando si crea un endpoint di interfaccia, il servizio VPC 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'VPCendpoint dopo che è entrato nello stato. `Available`

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

- `PendingAcceptance`: la richiesta di connessione è in sospeso. Questo è lo stato iniziale se le richieste vengono accettate manualmente.
- `Pending`: il provider di servizi ha accettato la richiesta di connessione. Questo è lo stato iniziale se le richieste vengono accettate automaticamente. L'VPCendpoint ritorna a questo stato se il consumatore del servizio modifica l'endpoint. VPC
- `Available`- L'VPCendpoint è disponibile per l'uso.
- `Rejected`: 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.
- `Expired`: la richiesta di connessione è scaduta.
- `Failed`- L'VPCendpoint non può essere reso disponibile.
- `Deleting`- L'utente del servizio ha eliminato l'VPCendpoint e l'eliminazione è in corso.
- `Deleted`- L'VPCendpoint viene eliminato.

AWS PrivateLink connessioni

Il traffico proveniente dall'utente VPC viene inviato a un servizio o a una risorsa endpoint utilizzando una connessione tra l'VPCendpoint e il servizio o la risorsa endpoint. Il traffico tra un VPC endpoint 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 VPC endpoint di interfaccia, i consumatori possono utilizzare le policy relative agli endpoint per controllare quali IAM responsabili possono utilizzare un VPC endpoint per accedere a un servizio o a una risorsa endpoint.

Zone ospitate private

Una zona ospitata è un contenitore di DNS record che definisce come indirizzare il traffico verso 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 tuaVPCs.

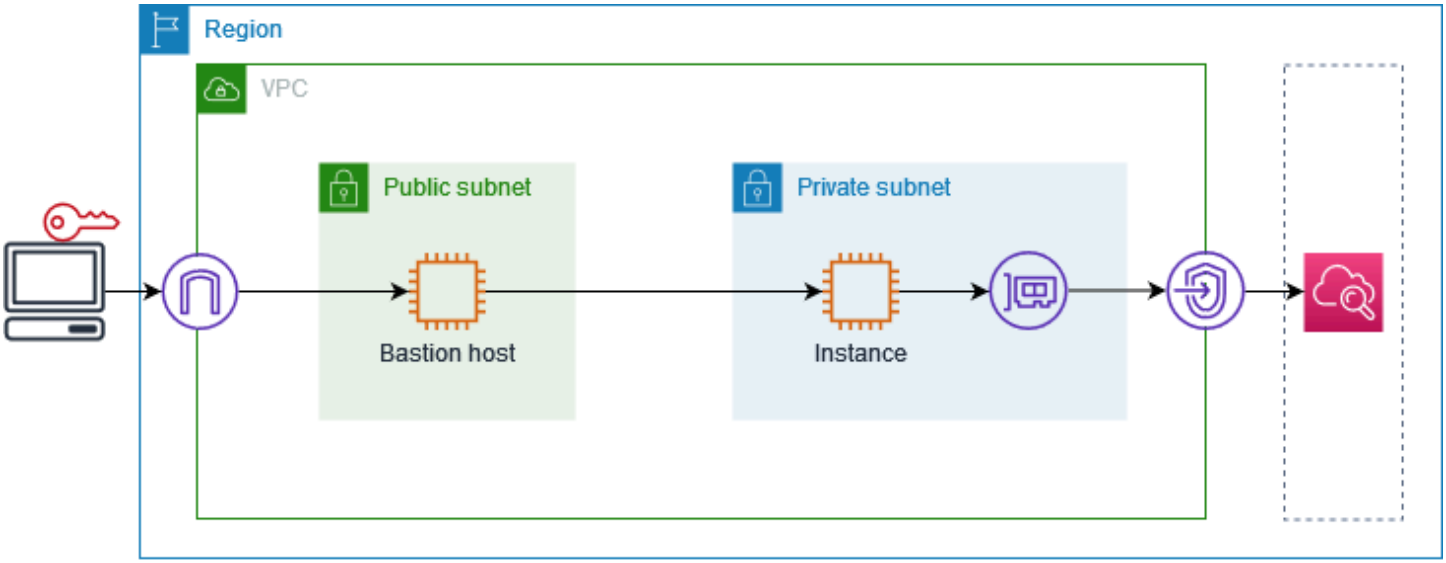
Puoi configurare Amazon Route 53 per indirizzare il traffico di dominio verso un VPC endpoint. Per ulteriori informazioni, consulta Instradamento del traffico verso un VPC endpoint utilizzando il tuo nome di dominio.

Puoi utilizzare Route 53 per configurare split-horizonDNS, in cui utilizzi lo stesso nome di dominio sia per un sito Web pubblico che per un servizio endpoint fornito da. AWS PrivateLink DNSle richieste per il nome host pubblico da parte del consumatore vengono VPC risolte negli indirizzi IP privati delle interfacce di rete degli endpoint, ma le richieste dall'esterno VPC continuano a essere risolte negli endpoint pubblici. Per ulteriori informazioni, consulta DNSMeccanismi per il routing del traffico e l'abilitazione del failover per le distribuzioni. AWS PrivateLink

Inizia con AWS PrivateLink

Questo tutorial dimostra come inviare una richiesta da un'EC2istanza 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 `.pem` file per la chiave privata si trova sul tuo computer, non sull'host bastion, SSH utilizzerai l'inoltro delle chiavi. Quindi, puoi connetterti all'istanza dall'host bastione senza specificare il file `.pem` nel comando ssh. Dopo aver configurato un VPC endpoint per CloudWatch, il traffico proveniente dall'istanza a cui è destinato CloudWatch viene trasferito all'interfaccia di rete dell'endpoint e quindi inviato all'utilizzo dell'endpoint. CloudWatch 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

- Passaggio 1: creare un file con sottoreti VPC
- Fase 2: avvio delle istanze
- Fase 3: Verifica CloudWatch l'accesso
- Passaggio 4: Creare un VPC endpoint a cui accedere CloudWatch
- Fase 5: Testare l'endpoint VPC

Passaggio 1: creare un file con sottoreti VPC

Utilizzare la procedura seguente per creare una sottorete VPC con una sottorete pubblica e una sottorete privata.

Per creare il VPC

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegli Create (Crea) VPC.
3. Per quanto riguarda le risorse da creare, scegli VPCe altro ancora.
4. Per la generazione automatica del tag Nome, inserisci un nome per. 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. Scegli Create (Crea) VPC.

Fase 2: avvio delle istanze

Utilizzando VPC quello che hai creato nel passaggio precedente, avvia l'host bastion 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 bastion che consenta il SSH traffico in entrata dal blocco per il CIDR tuo computer.
- Crea un gruppo di sicurezza per l'istanza che consente il SSH traffico in entrata dal gruppo di sicurezza per l'host bastion.

- Crea un profilo di IAM istanza e allega la CloudWatchReadOnlyAccesspolicy.

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. Perché VPC, scegli il tuoVPC.
    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. Perché VPC, scegli il tuoVPC.
    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). Ad IAMesempio, scegli il tuo profilo di IAM istanza.

8. Scegliere Launch Instance (Avvia istanza).

Fase 3: Verifica CloudWatch l'accesso

Utilizza la procedura seguente per confermare che l'istanza non è in grado di 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'SSHagente 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'`--region`opzione, 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 VPC configurazione corrente.

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

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

Passaggio 4: Creare un VPC endpoint a cui accedere CloudWatch

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

Prerequisito

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

Per creare un VPC endpoint per CloudWatch

1. Apri la VPC console Amazon 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. Per VPC, seleziona il tuo. VPC
8. In Subnets (Sottoreti), seleziona la zona di disponibilità e quindi seleziona la sottorete privata.
9. Per Gruppo di sicurezza, seleziona il gruppo di sicurezza per l'VPCendpoint.
10. Per Policy, seleziona Accesso completo per consentire tutte le operazioni da parte di tutti i principali su tutte le risorse dell'VPCendpoint.
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: Testare l'endpoint VPC

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

Per testare l'endpoint VPC

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

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

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

Se ricevi un `UnauthorizedOperation` errore, assicurati che l'istanza abbia un IAM ruolo 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'`--region`opzione specifica la regione in cui è stato creato l'VPCendpoint.

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 pannello di navigazione, seleziona 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 non ti serve più l'VPCendpoint, puoi eliminarlo.

Per eliminare l'endpoint VPC

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'VPCendpoint.
4. Scegli Azioni, Elimina VPC endpoint.
5. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Accesso Servizi AWS tramite AWS PrivateLink

Si accede e Servizio AWS si utilizza un endpoint. Gli endpoint di servizio predefiniti sono interfacce pubbliche, quindi è necessario aggiungere un gateway Internet VPC in modo che il traffico possa arrivare da a. VPC Servizio AWS Se questa configurazione non soddisfa i tuoi requisiti di sicurezza di rete, puoi utilizzarla AWS PrivateLink per connetterti VPC al tuo computer Servizi AWS come se fosse presente nel tuoVPC, senza l'uso di un gateway Internet.

Puoi accedere privatamente ai dispositivi Servizi AWS che si integrano con l' AWS PrivateLink utilizzo degli VPC endpoint. 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'VPCendpoint 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.

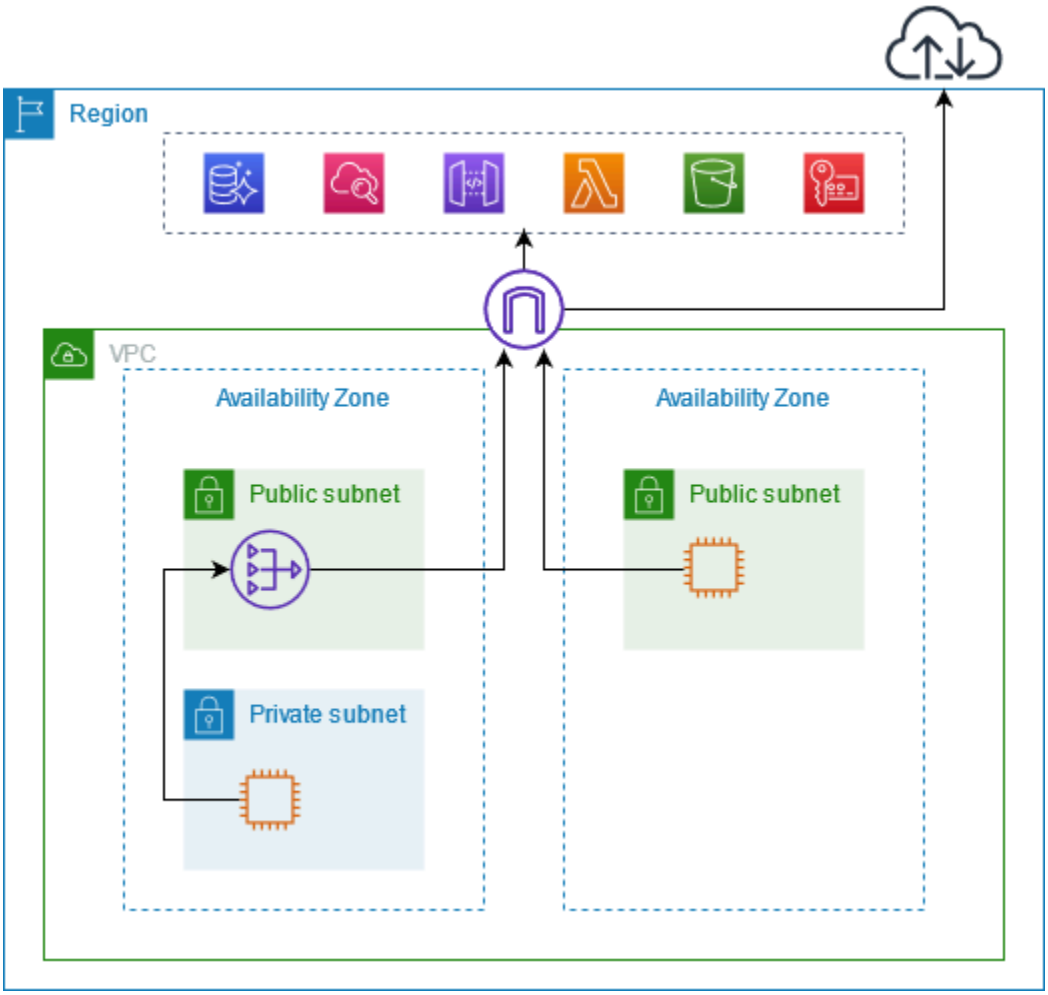
Indice

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.

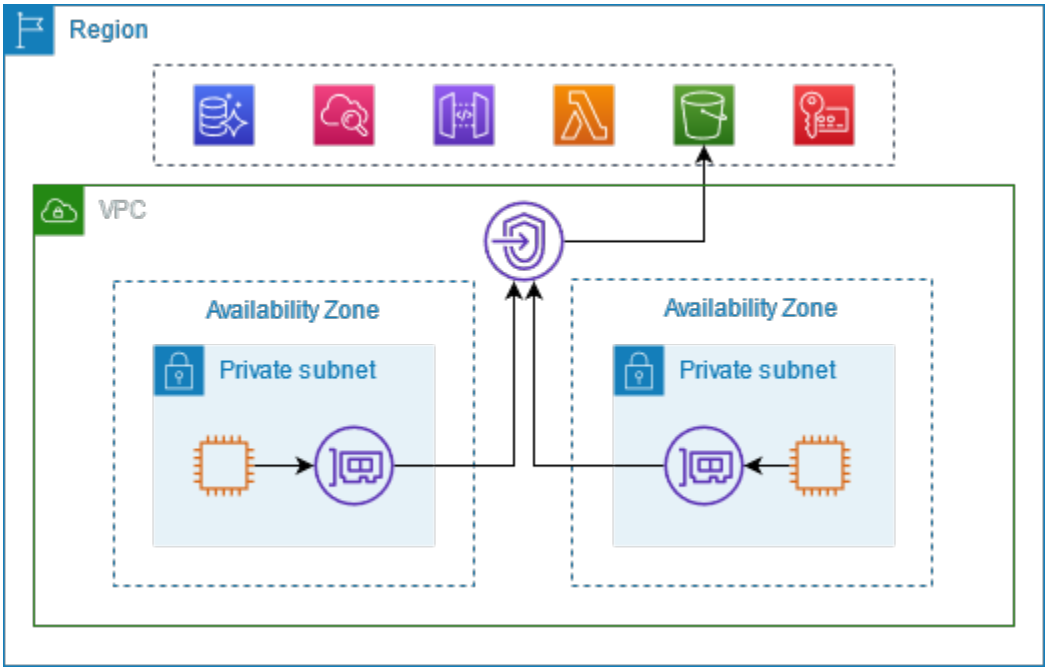
Accesso tramite endpoint del servizio pubblico

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 e quindi versoVPC. Servizio AWS Il traffico Servizio AWS da e verso un'istanza in una sottorete privata viene instradato a un NAT gateway, quindi al gateway Internet per laVPC, e infine a. 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, si crea un VPC endpoint di interfaccia, che stabilisce le connessioni tra le sottoreti presenti nelle interfacce di rete e quelle che le VPC utilizzano. Servizio AWS Il traffico destinato a Servizio AWS viene risolto negli indirizzi IP privati delle interfacce di rete degli endpoint utilizzando e quindi inviato all'utente utilizzando DNS la connessione tra l'endpoint e il Servizio AWS . VPC Servizio AWS



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

DNSnomi host

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 VPC endpoint di interfaccia, creiamo DNS nomi regionali e zonali che puoi usare per comunicare con il Servizio AWS tuo. VPC

Il DNS nome regionale per l'VPCendpoint dell'interfaccia ha la seguente sintassi:

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

I DNS nomi zonali hanno la seguente sintassi:

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

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

Il describe-vpc-endpointscomando seguente visualizza le DNS voci relative a 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 DNS nomi 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"
        }
    ]
]
```

DNSrisoluzione

I DNS record che creiamo per il tuo VPC endpoint di interfaccia sono pubblici. Pertanto, questi DNS nomi sono risolvibili pubblicamente. Tuttavia, DNS le richieste dall'esterno restituiscono VPC comunque gli indirizzi IP privati delle interfacce di rete degli endpoint, quindi questi indirizzi IP non possono essere utilizzati per accedere al servizio endpoint a meno che non si abbia accesso a. VPC

Privato DNS

Se abiliti private DNS per il tuo VPC endpoint di interfaccia e hai VPC abilitato sia i DNSnomi host che la DNS risoluzione, creiamo per te una zona ospitata privata nascosta e AWS gestita. La zona ospitata contiene un set di record per il DNS nome predefinito del servizio che lo risolve negli indirizzi IP privati delle interfacce di rete degli endpoint del tuo dispositivo. 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 i DNS nomi privati per i tuoi VPC endpoint per. Servizi AWS Ciò garantisce che le richieste che utilizzano gli endpoint del servizio pubblico, ad esempio le richieste effettuate tramite un AWS SDK, vengano risolte sul tuo VPC endpoint.

Amazon fornisce un DNS server per teVPC, chiamato Route 53 Resolver. Il Route 53 Resolver risolve automaticamente i nomi di VPC dominio 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 VPC endpoint dalla tua rete locale, puoi utilizzare gli endpoint Route 53 Resolver e le regole Resolver. Per

ulteriori informazioni, consulta Integrazione con and. AWS Transit GatewayAWS PrivateLinkAmazon Route 53 Resolver

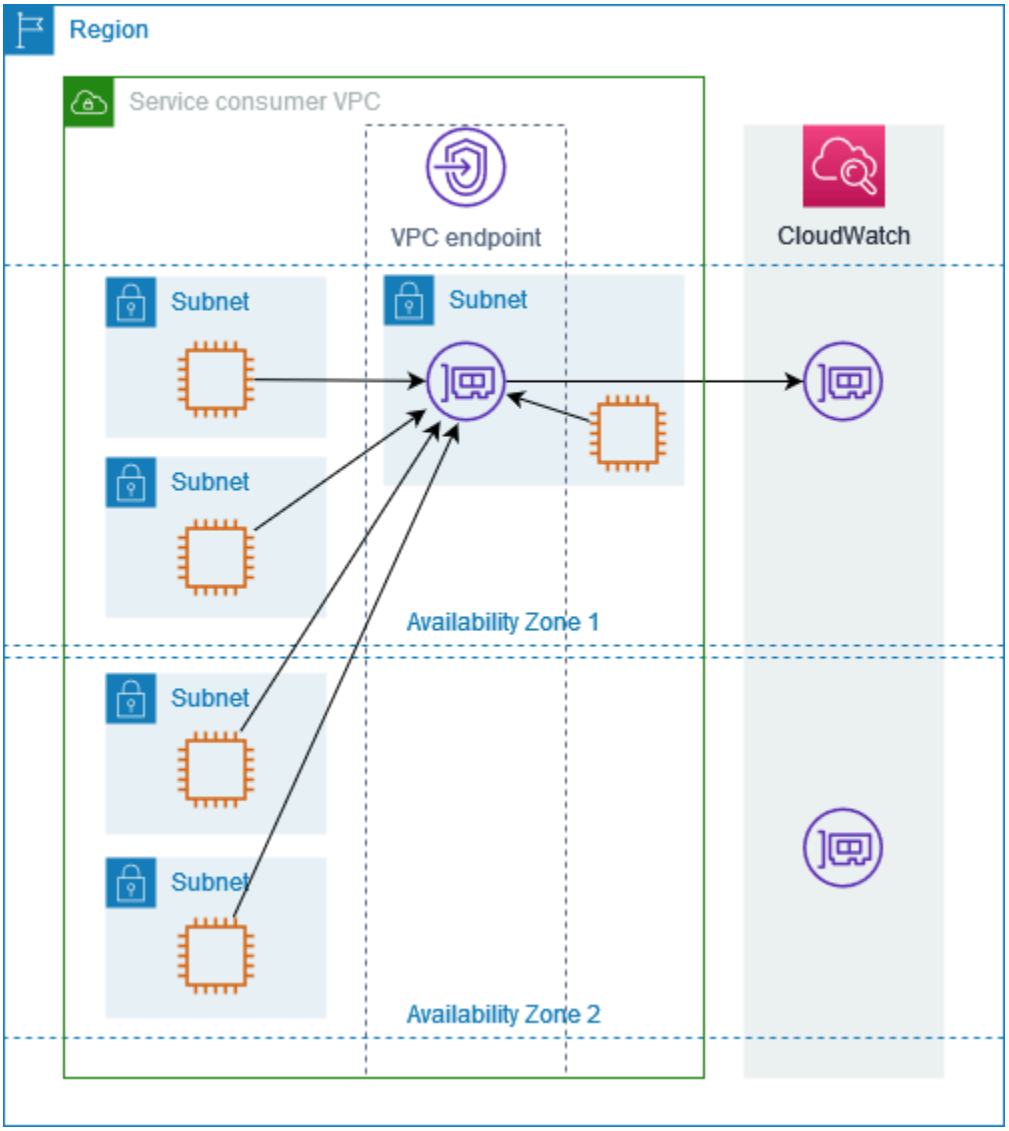
Sottoreti e zone di disponibilità

È possibile configurare l'VPCendpoint con una sottorete per zona di disponibilità. Creiamo un'interfaccia di rete endpoint per l'VPCendpoint nella tua sottorete. Assegniamo gli indirizzi IP a ciascuna 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 endpoint non cambieranno durante la vita dell'endpoint. VPC

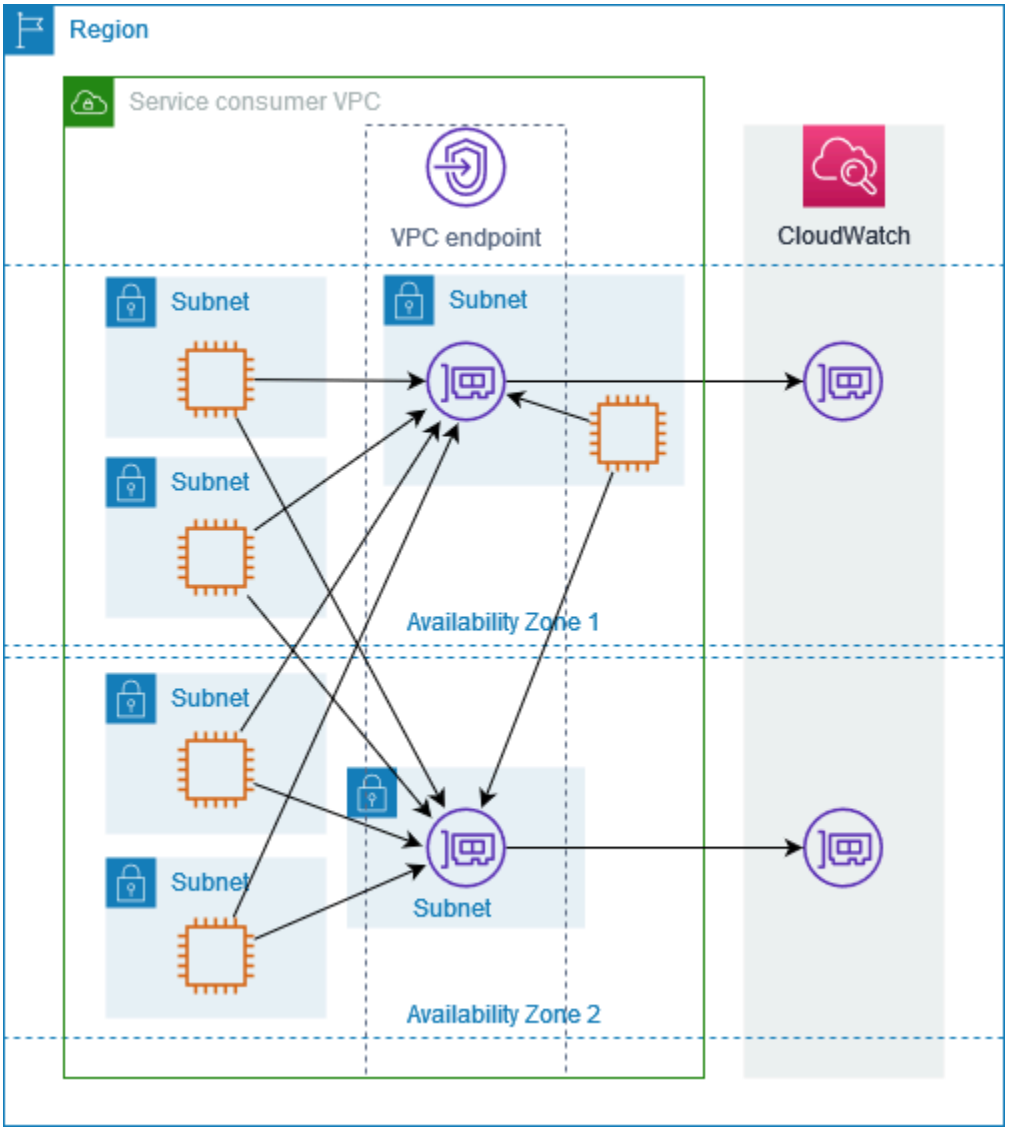
In un ambiente di produzione, per un'elevata disponibilità e resilienza, consigliamo quanto segue:

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

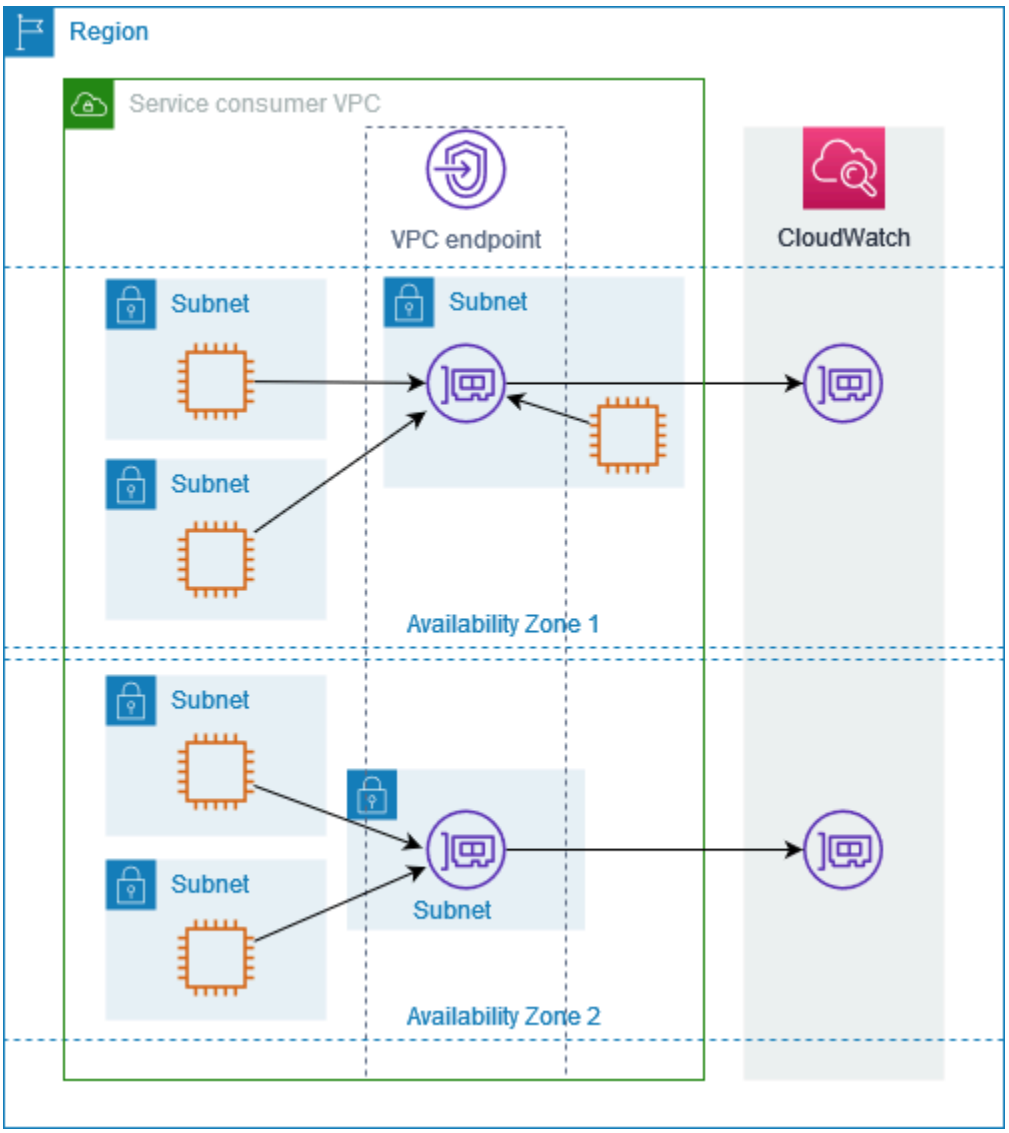
Il diagramma seguente mostra un VPC endpoint per Amazon CloudWatch con un'interfaccia di rete endpoint in un'unica zona di disponibilità. Quando una risorsa in qualsiasi sottorete VPC accede ad Amazon CloudWatch utilizzando il suo endpoint pubblico, risolviamo il traffico verso l'indirizzo IP dell'interfaccia 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 VPC endpoint per Amazon CloudWatch con interfacce di rete endpoint in due zone di disponibilità. Quando una risorsa in qualsiasi sottorete VPC accede ad Amazon CloudWatch 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 IPv6 tramite i propri endpoint pubblici. Gli endpoint che lo supportano IPv6 possono rispondere alle DNS domande con record. AAAA

Requisiti da abilitare IPv6 per un endpoint di interfaccia

- Servizio AWS Deve rendere disponibili i propri endpoint di servizio su. IPv6 Per ulteriori informazioni, consulta the section called “Visualizza il supporto IPv6”.
- 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 un VPC endpoint di interfaccia supportaIPv4, le interfacce di rete degli endpoint dispongono di indirizzi. IPv4 Se un VPC endpoint di interfaccia supportaIPv6, le interfacce di rete degli endpoint dispongono di indirizzi. IPv6 L'IPv6indirizzo 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`

Servizi AWS che si integrano con AWS PrivateLink

Quanto segue si Servizi AWS integra con AWS PrivateLink. Puoi creare un VPC endpoint per connetterti a questi servizi in privato, come se fossero in esecuzione da te. 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 al momento della creazione dell'VPCendpoint di interfaccia o indica che il servizio gestisce l'endpoint.

Servizio AWS	Nome servizio
Access Analyzer	com.amazonaws. *region*.analizzatore di accesso
AWS Account Management	com.amazonaws. *region*.account
Amazon API Gateway	com.amazonaws. *region*.execute-api
AWS AppConfig	com.amazonaws. *region*.app config
	com.amazonaws. *region*.appconfigdata
AWS App Mesh	com.amazonaws. *region*.app mesh
	com.amazonaws. *region*. appmesh-envoy-management

Servizio AWS	Nome servizio
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
Amazon AppStream 2.0	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
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

Servizio AWS	Nome servizio
	com.amazonaws. *region*. bedrock-agent-runtime
	com.amazonaws. *region*.bedrock-runtime
AWS Billing and Cost Management	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 Clean Rooms	com.amazonaws. *region*. camere pulite
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
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
Amazon CloudWatch	com.amazonaws. *region*.segnali applicativi

Servizio AWS	Nome servizio
	com.amazonaws. *region*. approfondimenti sulle applicazioni
	com.amazonaws. *region*. evidentemente
	com.amazonaws. *region*. evidentemente - dataplane
	com.amazonaws. *region*. monitor internet
	com.amazonaws. *region*.internetmonitor-fips
	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
CloudWatch Registri Amazon	com.amazonaws. *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

Servizio AWS	Nome servizio
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
	com.amazonaws. *region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws. *region*.codedeploy
	com.amazonaws. *region*. codedeploy-commands-secure
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
Amazon Connect	com.amazonaws. *region*.app - integrazioni
	com.amazonaws. *region*.casi
	com.amazonaws. *region*campagne.connect
	com.amazonaws. *region*.profilo
	com.amazonaws. *region*.voiceid

Servizio AWS	Nome servizio
	com.amazonaws. *region*.saggezza
AWS Connector Service	com.amazonaws. *region*.connettore.aws
Catalogo di controllo AWS	com.amazonaws. *region*.control catalog
AWS Cost Explorer	com.amazonaws. *region*.ce
Centrale ottimizzazione costi AWS	com.amazonaws. *region*. cost-optimization-hub
AWS Data Exchange	com.amazonaws. *region*. scambio di dati
Esportazioni di dati AWS	com.amazonaws. *region*. bcm-data-exports
Amazon Data Firehose	com.amazonaws. *region*.kinesis-firehose
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
AWS Deadline Cloud	com.amazonaws. *region*.deadline.gestione
	com.amazonaws. *region*.deadline.schedulazione
Amazon DevOps Guru	com.amazonaws. *region*.devops-guru
AWS Directory Service	com.amazonaws. *region*.ds
	com.amazonaws. *region*.ds-dati
Amazon DocumentDB	com.amazonaws. *region*.rds
Amazon DynamoDB	com.amazonaws. *region*.dinamodb
	com.amazonaws. *region*.dynamodb-fips

Servizio AWS	Nome servizio
Amazon EBS diretto APIs	com.amazonaws. *region*.ebs
Amazon EC2	com.amazonaws. *region*.ec2
Amazon EC2 Auto Scaling	com.amazonaws. *region*.scalabilità automatica
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. *region*.agente ecs
	com.amazonaws. *region*.ecs-telemetria
Amazon EKS	com.amazonaws. *region*.eks
	com.amazonaws. *region*.eks-auth
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 elastic
	com.amazonaws. *region*.elasticfilesystem-fips
Elastic Load Balancing	com.amazonaws. *region*. bilanciamento elastico del carico
Amazon ElastiCache	com.amazonaws. *region*. dolore elastico
	com.amazonaws. *region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws. *region*.mediaconnect

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

Servizio AWS	Nome servizio
Amazon FSx	com.amazonaws. *region*.fsx
	com.amazonaws. *region*.fsx-fips
AWS Glue	com.amazonaws. *region*.colla
	com.amazonaws. *region*.colla. dashboard
AWS Glue DataBrew	com.amazonaws. *region*.databrew
Grafana gestito da Amazon	com.amazonaws. *region*.grafana
	com.amazonaws. *region*.grafana - spazio di lavoro
AWS Ground Station	com.amazonaws. *region*. stazione di terra
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*. control-storage-omics
	com.amazonaws. *region*.storage-omics
	com.amazonaws. *region*.tag-omics

Servizio AWS	Nome servizio
	com.amazonaws. *region*.workflows-omics
AWS Identity and Access Management (IAM)	com.amazonaws.iam
IAMCentro di identità	com.amazonaws. *region*. negozio di identità
IAM Roles Anywhere	com.amazonaws. *region*. ruoli ovunque
Amazon Inspector	com.amazonaws. *region*.ispettore 2
	com.amazonaws. *region*.inspector-scan
AWS IoT Core	com.amazonaws. *region*.iot.dati
	com.amazonaws. *region*.iot.credenziali
	com.amazonaws. *region*.iot.fleethub.api
AWS IoT Core Device Advisor	com.amazonaws. *region*.deviceadvisor.iot
AWS IoT Core per LoRaWAN	com.amazonaws. *region*.iotwireless.api
	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

Servizio AWS	Nome servizio
	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. *region*.launchwizard
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

Servizio AWS	Nome servizio
	com.amazonaws. *region*. license-manager-user-subscriptions
Amazon Lookout per le apparecchiature	com.amazonaws. *region*. attrezzatura lookout
Amazon Lookout per le metriche	com.amazonaws. *region*.lookoutmetrics
Amazon Lookout per Vision	com.amazonaws. *region*. lookout vision
Amazon Macie	com.amazonaws. *region*.macie 2
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
Amazon Managed Service per Prometheus	com.amazonaws. *region*.app
	com.amazonaws. *region*.aps-workspaces
Amazon Managed Streaming per Apache Kafka	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

Servizio AWS	Nome servizio
	com.amazonaws. *region*.airflow.ops
AWS Management Console	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
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 PCS	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
Listino prezzi AWS	com.amazonaws. *region*.prezzi. api
AWS 5G privato	com.amazonaws. *region*.reti private
AWS Private Certificate Authority	com.amazonaws. *region*.acm-pca
	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
	com.amazonaws. *region*q.

Servizio AWS	Nome servizio
	com.amazonaws. *region*.app
Abbonamenti utenti Amazon Q	com.amazonaws. *region*.service.user-subscriptions
Amazon QLDB	com.amazonaws. *region*.qldb.session
Amazon QuickSight	com.amazonaws. *region*.quicksight - sito web
Amazon RDS	com.amazonaws. *region*.rds
RDSDati Amazon API	com.amazonaws. *region*.rds-dati
Amazon RDS Performance Insights	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
Dati Amazon Redshift API	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
	com.amazonaws. *region*. streaming-rekognition-fips

Servizio AWS	Nome servizio
AWS Resource Access Manager	com.amazonaws. *region*.ram
AWS Resource Groups	com.amazonaws. *region*.gruppi-risorse
	com.amazonaws. *region*. resource-groups-fips
AWS RoboMaker	com.amazonaws. *region*.robomaker
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
	com.amazonaws. *region*.sagemaker.featurestore-runtime
	com.amazonaws. *region*.sagemaker.metrics
	com.amazonaws. *region*.sagemaker.runtime

Servizio AWS	Nome servizio
	com.amazonaws. *region*.sagemaker.runtime-fips
Savings Plans	com.amazonaws. *region*.piani di risparmio
AWS Secrets Manager	com.amazonaws. *region*. gestore dei segreti
AWS Security Hub	com.amazonaws. *region*.hub di sicurezza
AWS Security Token Service	com.amazonaws. *region*.sts
AWS Serverless Application Repository	com.amazonaws. *region*.repository senza server
Service Catalog	com.amazonaws. *region*.catalogo dei servizi
	com.amazonaws. *region*.servicecatalog-app
Amazon SES	com.amazonaws. *region*.email-smtp
AWS SimSpace Weaver	com.amazonaws. *region*.simspaceweaver
AWS Snow Device Management	com.amazonaws. *region*. snow-device-management
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
Amazon SWF	com.amazonaws. *region*.swf
	com.amazonaws. *region*.swf-fips
AWS Step Functions	com.amazonaws. *region*.stati
	com.amazonaws. *region*.sync-stati
AWS Storage Gateway	com.amazonaws. *region*.gateway di archiviazione
Catena di approvvigionamento di AWS	com.amazonaws. *region*.scn

Servizio AWS	Nome servizio
AWS Systems Manager	com.amazonaws. *region*messaggi.ec2
	com.amazonaws. *region*.ssm
	com.amazonaws. *region*.ssm-contatti
	com.amazonaws. *region*.ssm-incidenti
	com.amazonaws. *region*.ssm - configurazione rapida
	com.amazonaws. *region*messaggi.ssm
AWS Telco Network Builder	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
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
Amazon Translate	com.amazonaws. *region*.tradurre

Servizio AWS	Nome servizio
AWS Trusted Advisor	com.amazonaws. *region*. consulente affidabile
Autorizzazioni verificate da Amazon	com.amazonaws. *region*. autorizzazioni verificate
Amazon VPC Lattice	com.amazonaws. *region*.vpc-reticolo
AWS Well-Architected Tool	com.amazonaws. *region*. ben architettato
Amazon WorkMail	com.amazonaws. *region*.posta di lavoro
Amazon WorkSpaces	com.amazonaws. *region*.spazi di lavoro
Browser sicuro Amazon Workspaces	com.amazonaws. *region*.workspaces-web
	com.amazonaws. *region*. workspaces-web-fips
Amazon WorkSpaces Thin Client	com.amazonaws. *region*.thinclient.api
AWS X-Ray	com.amazonaws. *region*.raggi x

Visualizzazione dei nomi del Servizio AWS disponibili

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

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:

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
```

```
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

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"
                }
            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": [],
            "PrivateDnsNameVerificationState": "verified",
            "SupportedIpAddressTypes": [
                "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.

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

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.

```
[
    "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.cleanrooms-ml",
    "com.amazonaws.us-east-1.cloudtrail",
    "com.amazonaws.us-east-1.codeguru-profiler",
    "com.amazonaws.us-east-1.codeguru-reviewer",
    "com.amazonaws.us-east-1.codepipeline",
    "com.amazonaws.us-east-1.codewhisperer",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.datazone",
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.email-smtp",
    "com.amazonaws.us-east-1.glue.dashboard",
    "com.amazonaws.us-east-1.grafana-workspace",
    "com.amazonaws.us-east-1.iot.credentials",
    "com.amazonaws.us-east-1.iot.data",
    "com.amazonaws.us-east-1.iotwireless.api",
    "com.amazonaws.us-east-1.lorawan.cups",
    "com.amazonaws.us-east-1.lorawan.lns",
    "com.amazonaws.us-east-1.macie2",
    "com.amazonaws.us-east-1.neptune-graph",
    "com.amazonaws.us-east-1.neptune-graph-fips",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.q",
    "com.amazonaws.us-east-1.redshift-data",
    "com.amazonaws.us-east-1.redshift-data-fips",
    "com.amazonaws.us-east-1.refactor-spaces",
    "com.amazonaws.us-east-1.sagemaker.runtime-fips",
    "com.amazonaws.us-east-1.storagegateway",
    "com.amazonaws.us-east-1.transfer",
    "com.amazonaws.us-east-1.transfer.server",
    "com.amazonaws.us-east-1.verifiedpermissions"
]
```

Visualizza il supporto IPv6

È possibile utilizzare il seguente describe-vpc-endpoint-servicescomando 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:

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "com.amazonaws.us-east-1.account",
    "com.amazonaws.us-east-1.applicationinsights",
    "com.amazonaws.us-east-1.apprunner",
    "com.amazonaws.us-east-1.aps",
    "com.amazonaws.us-east-1.aps-workspaces",
    "com.amazonaws.us-east-1.arsenal-discovery",
    "com.amazonaws.us-east-1.athena",
    "com.amazonaws.us-east-1.backup",
    "com.amazonaws.us-east-1.braket",
    "com.amazonaws.us-east-1.cloudcontrolapi",
    "com.amazonaws.us-east-1.cloudcontrolapi-fips",
    "com.amazonaws.us-east-1.cloudhsmv2",
    "com.amazonaws.us-east-1.compute-optimizer",
    "com.amazonaws.us-east-1.codeartifact.api",
    "com.amazonaws.us-east-1.codeartifact.repositories",
    "com.amazonaws.us-east-1.cost-optimization-hub",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.discovery",
    "com.amazonaws.us-east-1.drs",
    "com.amazonaws.us-east-1.ebs",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.elasticbeanstalk",
    "com.amazonaws.us-east-1.elasticbeanstalk-health",
    "com.amazonaws.us-east-1.execute-api",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.grafana",
    "com.amazonaws.us-east-1.groundstation",
    "com.amazonaws.us-east-1.internetmonitor".
    "com.amazonaws.us-east-1.internetmonitor-fips".
    "com.amazonaws.us-east-1.iotfleetwise",
    "com.amazonaws.us-east-1.kinesis-firehose",
    "com.amazonaws.us-east-1.lakeformation",
```

```
    "com.amazonaws.us-east-1.m2".
    "com.amazonaws.us-east-1.macie2".
    "com.amazonaws.us-east-1.networkflowmonitor".
    "com.amazonaws.us-east-1.networkflowmonitorreports".
    "com.amazonaws.us-east-1.pca-connector-scep",
    "com.amazonaws.us-east-1.pcs",
    "com.amazonaws.us-east-1.pcs-fips",
    "com.amazonaws.us-east-1.pi",
    "com.amazonaws.us-east-1.pi-fips",
    "com.amazonaws.us-east-1.polly",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.rbin",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.sagemaker.api",
    "com.amazonaws.us-east-1.securityhub",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.synthetics".
    "com.amazonaws.us-east-1.synthetics-fips".
    "com.amazonaws.us-east-1.textract",
    "com.amazonaws.us-east-1.textract-fips",
    "com.amazonaws.us-east-1.timestream-influxdb",
    "com.amazonaws.us-east-1.timestream-influxdb-fips",
    "com.amazonaws.us-east-1.trustedadvisor",
    "com.amazonaws.us-east-1.workmail",
    "com.amazonaws.us-east-1.xray"
]
```

Accedere e Servizio AWS utilizzare un endpoint di interfaccia VPC

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

Per ogni sottorete specificata dal vostroVPC, creiamo un'interfaccia di rete endpoint nella sottorete e le assegniamo un indirizzo IP privato compreso nell'intervallo di indirizzi di 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 al tuo. Servizio AWS VPC
- Per utilizzare privateDNS, devi abilitare i DNS nomi host e la DNS risoluzione per il tuo. VPC Per ulteriori informazioni, consulta Visualizza e aggiorna DNS gli attributi nella Amazon VPC User Guide.
- IPv6Per abilitare un endpoint di interfaccia, è Servizio AWS necessario supportare l'accesso tramiteIPv6. Per ulteriori informazioni, consulta the section called “Tipi di indirizzi IP”.
- Crea un gruppo di sicurezza per l'interfaccia di rete dell'endpoint che consenta il traffico previsto proveniente dalle risorse del tuo. VPC Ad esempio, per garantire che AWS CLI possano inviare HTTPS richieste a Servizio AWS, il gruppo di sicurezza deve consentire il traffico in entrataHTTPS.
- Se le risorse si trovano in una sottorete con una reteACL, verificate che la rete ACL consenta il traffico tra le risorse delle vostre interfacce di rete VPC e quelle della rete degli endpoint.
- Le tue risorse sono soggette a quote. AWS PrivateLink Per ulteriori informazioni, consulta AWS PrivateLink quote.

Creazione di un endpoint VPC

Utilizzare la procedura seguente per creare un VPC endpoint di interfaccia che si connette a un. Servizio AWS

Per creare un endpoint di interfaccia per un Servizio AWS

1. Apri la VPC console Amazon 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. Per Service name (Nome servizio), seleziona il servizio. Per ulteriori informazioni, consulta the section called “Servizi integrati”.
6. Per VPC, seleziona il VPC da cui accederai a Servizio AWS.
7. Se, nel passaggio 5, hai selezionato il nome del servizio per Amazon S3 e desideri configurare il DNSsupporto privato, seleziona Impostazioni aggiuntive, Abilita DNS nome. Quando effettui questa selezione, seleziona automaticamente anche Enable private DNS only for inbound endpoint. Puoi configurare la modalità privata DNS con un endpoint Resolver in ingresso solo per gli endpoint di interfaccia per Amazon S3. Se non disponi di un endpoint gateway per Amazon S3 e selezioni Enable DNS private only for inbound endpoint, riceverai un errore quando tenti l'ultimo passaggio di questa procedura.

   Se, nel passaggio 5, hai selezionato il nome di servizio per qualsiasi servizio diverso da Amazon S3, Impostazioni aggiuntive, Abilita DNS nome è già selezionato. Ti consigliamo di mantenere l'impostazione predefinita. Ciò garantisce che le richieste che utilizzano gli endpoint del servizio pubblico, ad esempio le richieste effettuate tramite un AWS SDK, vengano risolte sul tuo VPC endpoint.
8. Per Subnet, 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 CIDR blocco di sottorete sono riservati all'uso interno, quindi non puoi specificarli per le interfacce di rete degli 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 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

10. Per Security groups (Gruppi di sicurezza), seleziona i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint. Per impostazione predefinita, associamo il gruppo di sicurezza predefinito per. VPC
11. In 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 politica. Questa opzione è disponibile solo se il servizio supporta le policy VPC degli endpoint. Per ulteriori informazioni, consulta Policy di endpoint.
12. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
13. 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 VPC endpoint nelle sottoreti condivise con te. Tuttavia, puoi utilizzare gli VPC endpoint nelle sottoreti condivise con te.

ICMP

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

Configurazione di un endpoint dell'interfaccia

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

Attività

- Aggiunta o rimozione di sottoreti

- Associazione dei gruppi di sicurezza
- Modifica la politica degli VPC endpoint
- Abilita i DNS nomi 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 VPC console Amazon 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 supportaIPv6, puoi anche inserire un IPv6 indirizzo dall'intervallo di indirizzi di sottorete.

   Se specifichi un indirizzo IP per una sottorete che dispone già di un'interfaccia di rete endpoint per questo VPC endpoint, sostituiamo l'interfaccia di rete dell'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 degli endpoint dalle risorse presenti nel sistemaVPC.

Per modificare i gruppi di sicurezza utilizzando la console

1. Apri la VPC console Amazon 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 la politica degli VPC endpoint

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 VPC console Amazon 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. Seleziona Salva.

Per modificare la policy di endpoint utilizzando la riga di comando

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

Abilita i DNS nomi privati

Ti consigliamo di abilitare DNS i nomi privati per i tuoi VPC endpoint per Servizi AWS. Ciò garantisce che le richieste che utilizzano gli endpoint del servizio pubblico, ad esempio le richieste effettuate tramite un AWS SDK, vengano risolte sul tuo VPC endpoint.

Per utilizzare DNS nomi privati, devi abilitare sia i DNSnomi host che la DNS risoluzione per il tuo. VPC Dopo aver abilitato DNS i nomi privati, potrebbero essere necessari alcuni minuti prima che gli indirizzi IP privati diventino disponibili. I DNS record che creiamo quando abiliti DNS i nomi privati sono privati. Pertanto, il DNS nome privato non è risolvibile pubblicamente.

Per modificare l'opzione dei DNS nomi privati utilizzando la console

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

Per modificare l'opzione dei nomi privati DNS 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 VPC console Amazon 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. Seleziona 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.

Attività

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

Crea una notifica SNS

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

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

1. Apri la VPC console Amazon 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 Notifica ARN, scegli l'ARNSNSargomento 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 politica di accesso all'SNSargomento Amazon che AWS PrivateLink consenta di pubblicare notifiche per tuo conto, come la seguente. Per ulteriori informazioni, consulta Come posso modificare la politica di accesso del mio SNS argomento Amazon? Utilizza le chiavi di condizione globali `aws:SourceArn` e `aws:SourceAccount` per evitare il problema del "confused deputy".

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

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint/endpoint-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

Aggiungere una policy della chiave

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

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

```
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

Eliminazione di un endpoint dell'interfaccia

Quando hai finito con un VPC endpoint, puoi 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 VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint dell'interfaccia.
4. Scegli Azioni, Elimina VPC endpoint.
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

VPCGli endpoint gateway forniscono una connettività affidabile ad Amazon S3 e DynamoDB senza richiedere un gateway Internet o un dispositivo per il tuo. NAT 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 VPC endpoint per Amazon S3

- Tipi di VPC endpoint per Amazon DynamoDB

Prezzi

L'utilizzo di endpoint gateway non comporta costi supplementari.

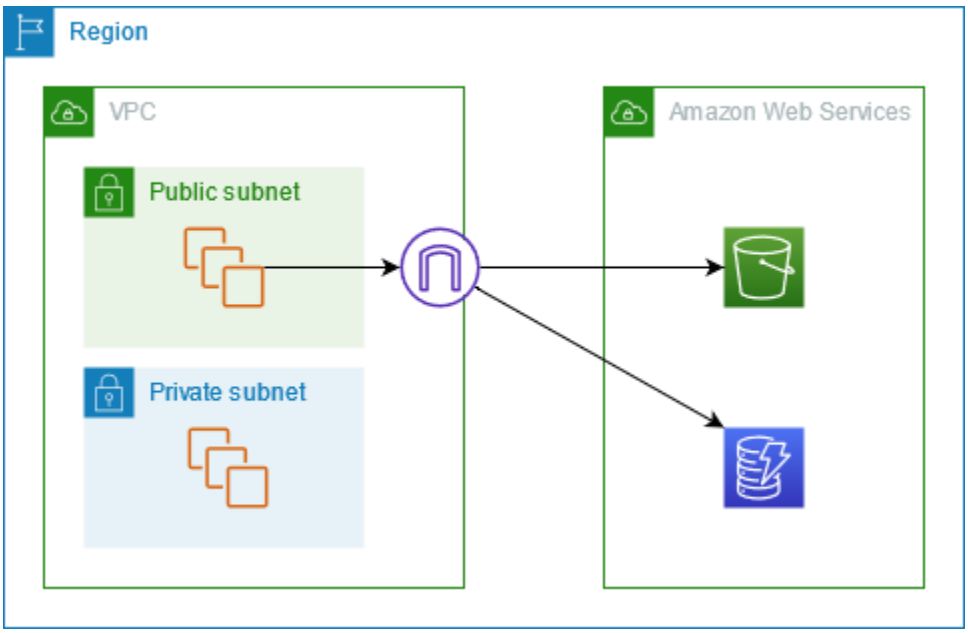
Indice

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.

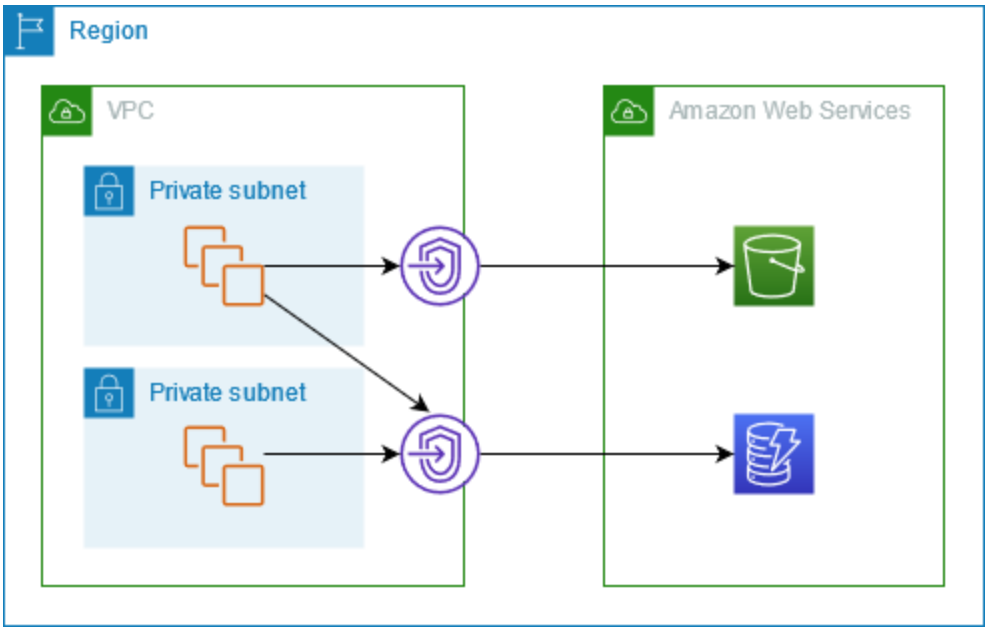
Accesso tramite un gateway Internet

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 proveniente da un'istanza in una sottorete pubblica viene indirizzato al gateway Internet per il servizio e quindi verso il servizio. VPC 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 consentire alle istanze nella sottorete privata di inviare traffico ad Amazon S3 o DynamoDB, è necessario NAT aggiungere un dispositivo alla sottorete pubblica e indirizzare il traffico dalla 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 proveniente VPC da Amazon S3 o DynamoDB viene indirizzato all'endpoint del 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 ulteriori informazioni, consulta AWS-managed prefix lists nella Amazon VPC User Guide.



Routing

Quando si crea un endpoint gateway, si selezionano le tabelle di VPC routing per le sottoreti che si abilitano. 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 ACL regole 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

Endpoint gateway per Amazon S3

Puoi accedere ad Amazon S3 dai tuoi endpoint VPC gatewayVPC. Dopo aver creato l'endpoint gateway, puoi aggiungerlo come destinazione nella tabella di routing per il traffico destinato dal tuo 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 VPC tuo dispositivo, senza richiedere un gateway NAT o

un dispositivo Internet e senza costi aggiuntivi. VPC 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 VPC endpoint per Amazon S3 nella Guida per l'utente di Amazon S3.

Indice

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 DNS server Amazon, devi abilitare sia i DNSnomi host che la DNS risoluzione per i tuoiVPC. Se utilizzi il tuo DNS server, assicurati che le richieste ad Amazon S3 vengano risolte correttamente sugli 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.
- La rete ACL per la sottorete per le istanze che accedono ad Amazon S3 tramite un endpoint gateway deve consentire il traffico da e verso Amazon S3. Non puoi fare riferimento agli elenchi di prefissi nelle ACL regole di rete, ma puoi ottenere l'intervallo di indirizzi IP per Amazon S3 dall'elenco dei prefissi per Amazon S3.
- 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 puoi utilizzare la `aws:SourceIp` condizione in una policy di identità o in una bucket policy per le richieste ad Amazon S3 che VPC attraversano un endpoint. 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 VPC l'endpoint.
- Gli endpoint del gateway supportano solo il traffico. IPv4
- IPv4Gli indirizzi di origine delle istanze nelle sottoreti interessate ricevuti da Amazon S3 passano da IPv4 indirizzi pubblici a indirizzi privati nel tuo. IPv4 VPC Un endpoint cambia i percorsi di rete e disconnette le connessioni aperte. TCP Le connessioni precedenti che utilizzavano IPv4 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 da un. VPC Le risorse sull'altro lato di una VPN connessione, di una connessione VPC peering, di un gateway di transito o di una AWS 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. È inoltre previsto un limite di 255 endpoint gateway per. VPC

Privato DNS

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

Route 53 Resolver

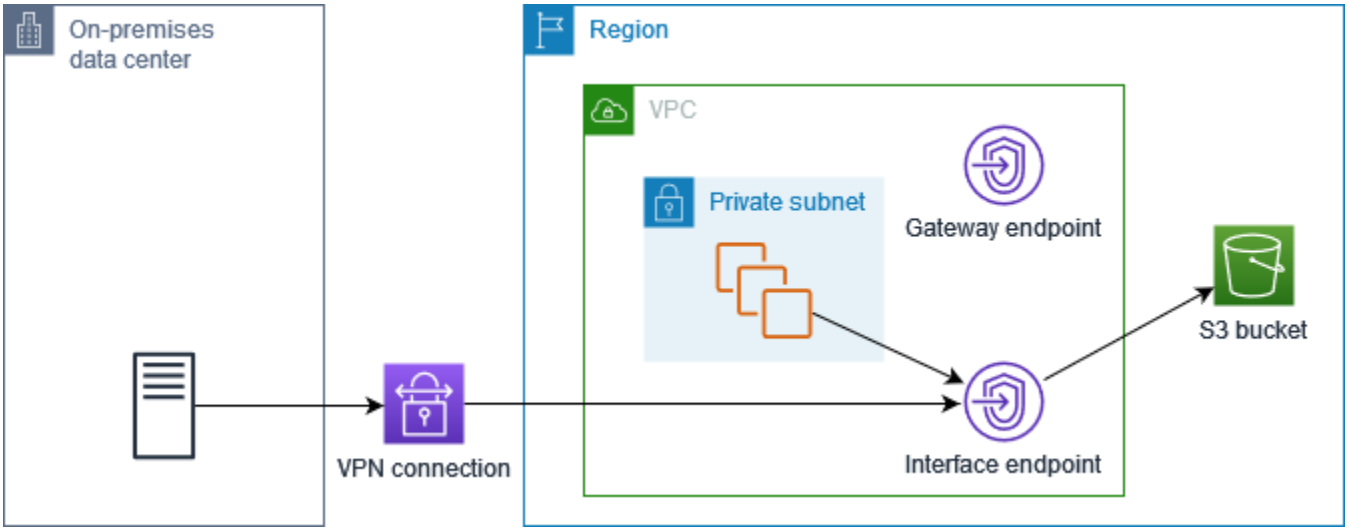
Amazon fornisce un DNS server, chiamato Route 53 Resolver, per te. VPC Il Route 53 Resolver risolve automaticamente i nomi di VPC dominio e i record locali in zone ospitate private. Tuttavia, non puoi utilizzare il Route 53 Resolver dall'esterno del tuo. VPC Route 53 fornisce endpoint Resolver e regole Resolver che consentono di utilizzare il Route 53 Resolver dall'esterno. VPC Un endpoint Resolver in ingresso inoltra le query dalla rete locale al Route 53 Resolver. DNS Un endpoint Resolver in uscita inoltra le query dal Route 53 Resolver alla rete locale. DNS

Quando configuri il tuo endpoint di interfaccia per Amazon S3 per l'uso DNS privato solo per l'endpoint Resolver in ingresso, creiamo un endpoint Resolver in ingresso. L'endpoint Resolver in ingresso risolve le query su Amazon S3 dagli indirizzi IP locali DNS agli indirizzi IP privati dell'endpoint di interfaccia. Aggiungiamo inoltre ALIAS i record per il Route 53 Resolver alla zona

ospitata pubblica per Amazon S3, in modo DNS che le query dal VPC tuo Resolver vengano inviate agli indirizzi IP pubblici di Amazon S3, che indirizzano il traffico verso l'endpoint del gateway.

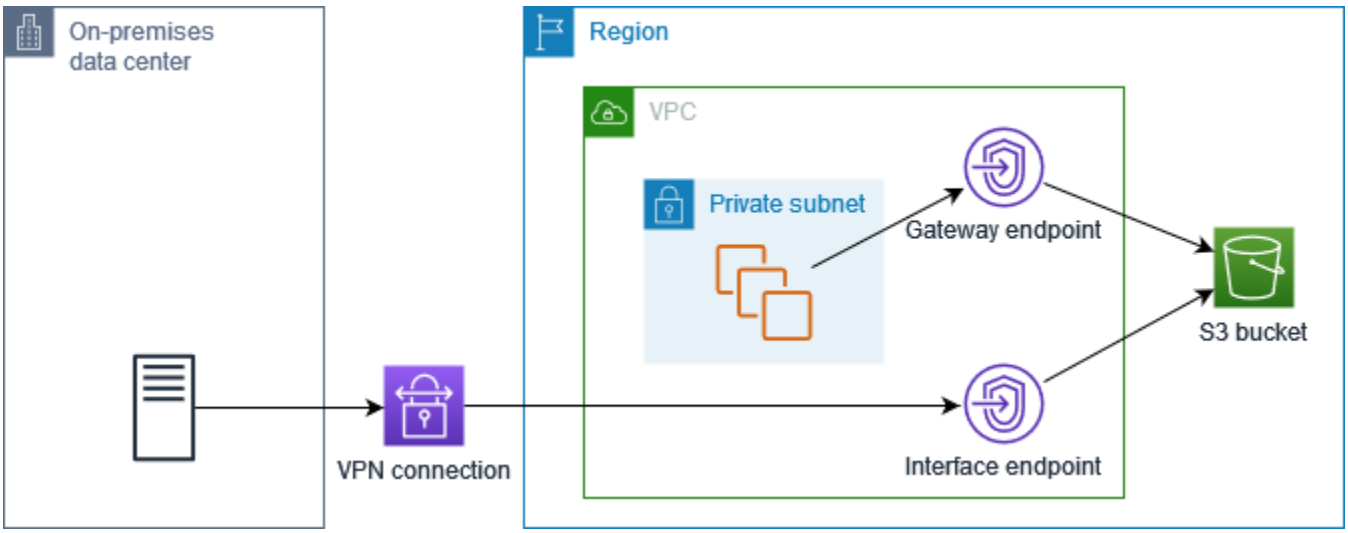
Privato DNS

Se configuri la modalità privata DNS per l'endpoint di interfaccia per Amazon S3 ma non la configurazione DNS privata solo per l'endpoint Resolver in entrata, le richieste provenienti sia dalla tua rete locale che dal tuo endpoint di interfaccia utilizzano l'endpoint di interfaccia per accedere ad Amazon S3. VPC Pertanto, paghi per utilizzare l'endpoint di interfaccia per il traffico proveniente daVPC, anziché utilizzare l'endpoint gateway senza costi aggiuntivi.



Privato DNS solo per l'endpoint Resolver in entrata

Se configuri la modalità privata DNS solo per l'endpoint Resolver in entrata, le richieste provenienti dalla rete locale utilizzano l'endpoint di interfaccia per accedere ad Amazon S3 e le richieste provenienti dal VPC tuo endpoint utilizzano l'endpoint 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.



Configura privato DNS

Puoi configurare private DNS per un endpoint di interfaccia per Amazon S3 al momento della creazione o dopo la creazione. Per ulteriori informazioni, vedere the section called “Creazione di un endpoint VPC” (configurazione durante la creazione) o the section called “Abilita i DNS nomi privati” (configurazione dopo la creazione).

Crea 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 VPC console Amazon 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*.s3.
6. Per VPC, seleziona il punto 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 Accesso completo per consentire tutte le operazioni da parte di tutti i principali su tutte le risorse dell'VPCendpoint. Altrimenti, seleziona Personalizzato per allegare

una policy sull'VPCendpoint che controlli le autorizzazioni di cui dispongono i responsabili per eseguire azioni 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 tramite le policy di bucket

È possibile utilizzare le policy dei bucket per controllare l'accesso ai bucket da endpoint specificiVPCs, 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 bucket policy che limiti l'accesso a un endpoint specifico utilizzando la chiave aws: condition. 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 AWS Management Console.

```
{
  "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: limita l'accesso a un determinato VPC

Puoi creare una bucket policy che limiti l'accesso a determinati utenti VPCs utilizzando la chiave aws: sourceVpc condition. Ciò è utile se hai più endpoint configurati nello stesso. VPC La seguente politica nega l'accesso al bucket specificato utilizzando le azioni specificate a meno che la richiesta non provenga da quello specificato. VPC Tieni presente che questa policy blocca l'accesso al bucket specificato utilizzando le azioni specificate tramite AWS Management Console.

```
{
  "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

È possibile creare una politica che limiti l'accesso a intervalli di indirizzi IP specifici utilizzando la chiave aws: VpcSourceIp condition. 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 AWS Management Console.

```
{
```

```
  "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.

```
{
  "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 VPC console Amazon 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 la politica degli VPC endpoint

Puoi modificare la policy degli endpoint per un endpoint gateway, che controlla l'accesso ad Amazon S3 dall'endpoint VPC all'altro. 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 VPC console Amazon 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. Seleziona 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 ne hai altri Servizi AWS VPC che utilizzano bucket S3.

```
{
  "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: limita l'accesso a un ruolo specifico IAM

È possibile creare una politica che limiti l'accesso a un IAM ruolo specifico. Devi utilizzare `aws:PrincipalArn` per concedere l'accesso a un principale.

```
{
  "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.

```
{
  "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 l'opzione private DNS è abilitata.

Per eliminare un endpoint gateway usando la console

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

2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint gateway.
4. Scegli Azioni, Elimina VPC endpoint.
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 dai VPC tuoi endpoint gateway che utilizzano. VPC Dopo aver creato l'endpoint gateway, puoi aggiungerlo come destinazione nella tabella delle rotte per il traffico destinato dal tuo a VPC 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 VPC tuo computer, senza richiedere un gateway NAT o un dispositivo Internet per te e senza VPC 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 VPC endpoint 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 DNS server Amazon, devi abilitare sia i DNSnomi host che la DNS risoluzione per i tuoiVPC. Se utilizzi il tuo DNS server, assicurati che le richieste 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.
- La rete ACL per la sottorete per le istanze che accedono a DynamoDB tramite un endpoint gateway deve consentire il traffico da e verso DynamoDB. Non è possibile fare riferimento agli elenchi di prefissi nelle ACL regole di rete, ma è possibile ottenere l'intervallo di indirizzi IP per DynamoDB dall'elenco dei prefissi per DynamoDB.
- Se si utilizza AWS CloudTrail per registrare le operazioni DynamoDB, i file di registro contengono gli indirizzi IP privati delle istanze EC2 del service VPC consumer e l'ID dell'endpoint gateway per tutte le richieste eseguite tramite l'endpoint.
- Gli endpoint del gateway supportano solo il traffico. IPv4
- IPv4Gli indirizzi di origine delle istanze nelle sottoreti interessate cambiano da IPv4 indirizzi pubblici a indirizzi privati IPv4 delle tue. VPC Un endpoint cambia i percorsi di rete e disconnette le connessioni aperte. TCP 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 da un. VPC Le risorse sull'altro lato di una VPN connessione, di una connessione VPC peering, di un gateway di transito o di una AWS Direct Connect connessione all'interno dell'utente 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. È inoltre previsto un limite di 255 endpoint gateway per. VPC

Crea 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 VPC console Amazon 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. Per VPC, seleziona il punto 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 Accesso completo per consentire tutte le operazioni da parte di tutti i principali su tutte le risorse dell'VPCendpoint. Altrimenti, seleziona Personalizzato per allegare una policy sull'VPCendpoint che controlli le autorizzazioni di cui dispongono i responsabili per eseguire azioni 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

Controlla l'accesso utilizzando IAM le politiche

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

Example Esempio: limitazione dell'accesso a uno specifico endpoint

È possibile creare una policy che limiti l'accesso a un VPC endpoint specifico utilizzando la chiave aws: condition. sourceVpce La seguente politica nega l'accesso alle tabelle DynamoDB nell'account a meno che non venga utilizzato l'endpoint specificato. VPC Questo esempio presuppone che vi sia anche una dichiarazione di policy che consente l'accesso richiesto per i casi d'uso.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-endpoint",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:region:account-id:table/*",
         "Condition": {
            "StringNotEquals" : {
               "aws:sourceVpce": "vpce-11aa22bb"
            }
         }
      }
   ]
}
```

Example Esempio: consentire l'accesso da un ruolo specifico IAM

È possibile creare una politica che consenta l'accesso utilizzando un IAM ruolo specifico. La seguente politica consente l'accesso al IAM ruolo specificato.

```
{
   "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.

```
{
   "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 VPC console Amazon 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 la politica degli VPC endpoint

È possibile modificare la policy degli endpoint per un endpoint gateway, che controlla l'accesso a DynamoDB dall'endpoint all'altro. VPC 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 VPC console Amazon 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. Seleziona 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 VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint gateway.
4. Scegli Azioni, Elimina VPC endpoint.
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 modo privato, come se fossero eseguiti da te. VPC

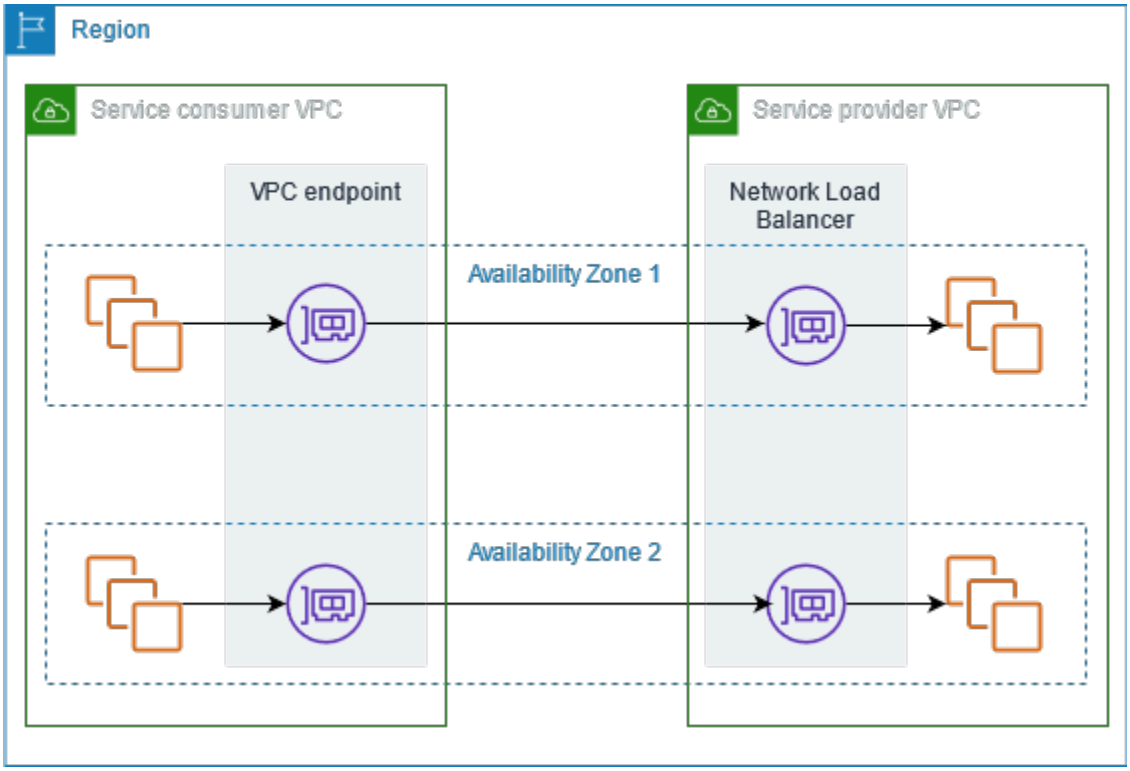
Indice

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 VPC endpoint per connettersi ai prodotti SaaS. Il provider di servizi crea un servizio endpoint e garantisce ai propri clienti l'accesso al servizio endpoint. In qualità di utente del servizio, crei un VPC endpoint di interfaccia che stabilisce connessioni tra una o più sottoreti del servizio e il servizio endpoint. VPC



Creazione di un endpoint di interfaccia

Utilizzare la procedura seguente per creare un VPC endpoint di interfaccia che si connette al prodotto SaaS.

Requisito

Iscriversi al servizio.

Per creare un endpoint di interfaccia a un servizio partener

1. Apri la VPC console Amazon 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 dispositivo da cui accederai al prodotto.
7. Per Sottoreti, 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 nelle interfacce di rete degli endpoint e quelle delle interfacce di reteVPC.
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. Il Gateway Load Balancer viene specificato quando si crea un servizio VPC endpoint. Gli altri principali AWS possono accedere al servizio endpoint creando un Endpoint Gateway Load Balancer.

Prezzi

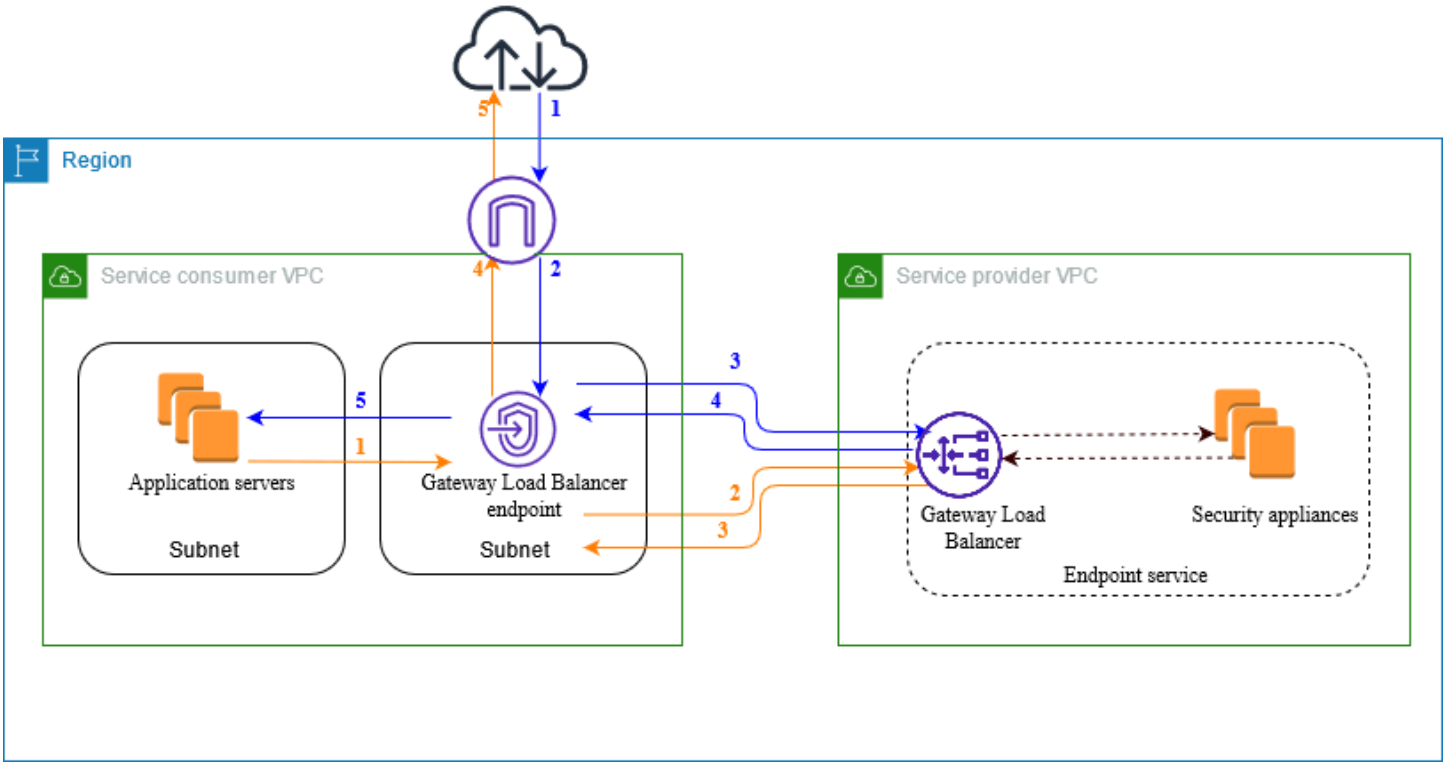
La fatturazione viene calcolata per ogni ora di provisioning dell'endpoint Gateway Load Balancer in ciascuna zona di disponibilità. Ti viene inoltre addebitato un importo per GB di dati elaborati. Per ulteriori informazioni, consultare AWS PrivateLink Prezzi.

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 delle applicazioni vengono eseguiti in una sottorete del consumatore del servizio. VPC Si crea un endpoint Gateway Load Balancer in un'altra sottorete dello stesso. VPC Tutto il traffico che entra nel consumatore del servizio VPC attraverso il gateway Internet viene prima indirizzato all'endpoint Gateway Load Balancer per l'ispezione e quindi indirizzato 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 nell'utente del servizio attraverso il gateway InternetVPC.
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 fornitori di servizi possono rendere disponibili i propri endpoint di servizio ai consumatori di servizi tramite o entrambi IPv4 e IPv4 IPv6IPv6, anche se le loro apparecchiature di sicurezza supportano solo IPv4 il supporto. 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 supportaIPv4, le interfacce di rete degli endpoint dispongono di indirizzi. IPv4 Se un endpoint Gateway Load Balancer supportaIPv6, le interfacce di rete degli endpoint dispongono di indirizzi. IPv6 L'IPv6indirizzo 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

- Le sottoreti VPC e per il servizio endpoint devono avere blocchi associati. IPv6 CIDR
- 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 del servizio consumer VPC devono indirizzare 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. Tieni presente che le IPv6 rotte sono incluse 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

- Crea un fornitore di servizi VPC 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.
- Crea un Gateway Load Balancer nel tuo provider di servizi. VPC 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.
- Avvia le appliance di sicurezza presso il provider di servizi VPC e registrale presso un gruppo target di sistemi di bilanciamento del carico.

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 VPC console Amazon 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 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.
8. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
9. Selezionare 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 vostroVPC, creiamo un'interfaccia di rete endpoint nella sottorete e le assegniamo un indirizzo IP privato compreso nell'intervallo di indirizzi della sottorete. Un'interfaccia di rete endpoint è un'interfaccia di rete gestita dal richiedente; puoi visualizzarla nel tuo 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

- È possibile scegliere una sola zona di disponibilità nel servizio consumer. VPC 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. Il servizio non può avviare richieste alle risorse del tuo dispositivo VPC tramite l'VPCendpoint. L'endpoint restituisce solo le risposte al traffico avviato dalle risorse del tuo. 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 Network Load Balancer non è supportata quando il traffico viene instradato attraverso un endpoint Gateway Load Balancer, anche se la destinazione è la stessa del Network VPC Load Balancer.
- Se i server delle applicazioni e l'endpoint Gateway Load Balancer si trovano nella stessa sottorete, NACL le regole 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

- Crea un consumatore di servizi VPC 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 tue risorse si trovano in una sottorete con una reteACL, verifica che la rete ACL consenta il traffico tra le interfacce della rete degli endpoint e le risorse di. 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 VPC console Amazon 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 NLBs e GWLBs.
5. In Service name (Nome servizio), specifica il nome del servizio, quindi seleziona Verify service (Verifica servizio).
6. Per VPC, seleziona il servizio VPC da cui accederai al servizio endpoint.
7. Per Subnet, 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'IPv6unica sottorete.
   - Dualstack: assegna entrambi IPv6 gli indirizzi all'interfaccia di rete dell'IPv4endpoint. 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

Utilizzare la procedura seguente per configurare le tabelle di routing per il consumatore del servizioVPC. 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 VPC console Amazon 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 offri assistenzaIPv4, scegli Aggiungi percorso. In Destinazione, inserisci il IPv4 CIDR blocco della sottorete per i server delle applicazioni. Per Target, seleziona l'VPCendpoint.
   c. Se lo supportiIPv6, scegli Aggiungi percorso. In Destinazione, inserisci il IPv6 CIDR blocco della sottorete per i server delle applicazioni. Per Target, seleziona l'VPCendpoint.
   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 supportiIPv4, scegli Aggiungi percorso. In Destination (Destinazione), immettere **`0.0.0.0/0`**. Per Target, seleziona l'VPCendpoint.
   c. Se lo supportiIPv6, scegli Aggiungi percorso. In Destination (Destinazione), immettere **`::/0`**. Per Target, seleziona l'VPCendpoint.
   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 lo supportiIPv4, scegli Aggiungi percorso. In Destination (Destinazione), immettere **`0.0.0.0/0`**. Per Target, seleziona il gateway Internet.
   c. Se supportiIPv6, 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)

Gestione dei 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 VPC console Amazon 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. Seleziona 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 VPC console Amazon 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)

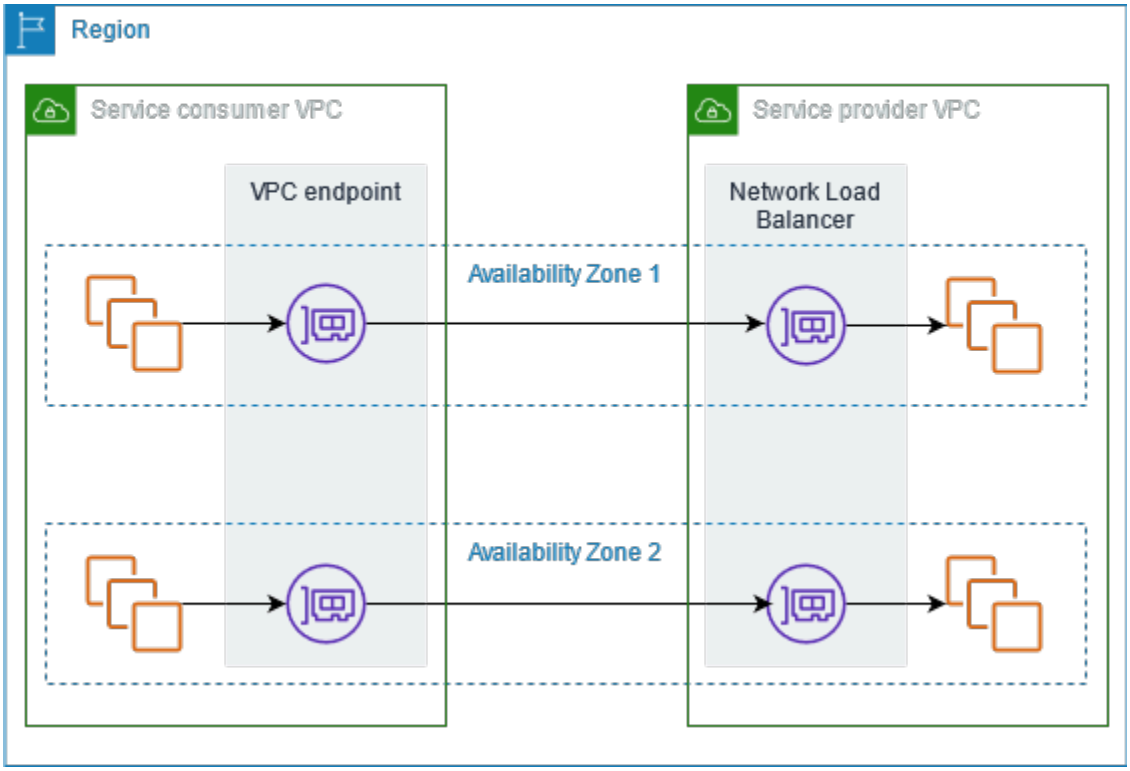
Condividi i tuoi servizi tramite AWS PrivateLink

È possibile ospitare il proprio servizio AWS PrivateLink fornito, 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 fornitore di servizi, crei un Network Load Balancer nel tuo VPC front-end as the service. Quindi selezioni questo load balancer quando crei la configurazione del servizio VPC endpoint. Concedi l'autorizzazione a principali AWS specifici in modo che possano connettersi al servizio. In qualità di consumatore del servizio, il cliente crea un VPC endpoint di interfaccia che stabilisce le connessioni tra le sottoreti selezionate e il servizio endpoint dell'utente. VPC 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.

DNSnomi host

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

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

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

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

Quando un consumatore di servizi crea un VPC endpoint di interfaccia, creiamo DNS nomi regionali e zonali che il consumatore del servizio 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
```

Privato DNS

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

Accesso tra 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.

Autorizzazioni

- Per impostazione predefinita, IAM le entità 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 aree geografiche, un IAM amministratore può creare IAM politiche che consentano l'azione di sola autorizzazione. `vpce:AllowMultiRegion`
- Per controllare le regioni che un'IAMentità può specificare come regione supportata durante la creazione di un servizio endpoint, utilizza la chiave condition. `ec2:VpceSupportedRegion`
- Per controllare le regioni che un'IAMentità può specificare come regione di servizio durante la creazione di un VPC endpoint, usa la chiave `ec2:VpceServiceRegion` condition.

Considerazioni

- Un fornitore 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 ospitante 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, sia i fornitori che i consumatori devono utilizzare almeno due zone di disponibilità. Tieni presente che l'accesso tra regioni non richiede che fornitori e consumatori utilizzino le stesse zone di disponibilità.
- Con l'accesso interregionale, AWS PrivateLink gestisce il failover tra zone di disponibilità. Non gestisce il failover tra le regioni.
- L'accesso tra regioni non è supportato per Marketplace AWS i servizi con un nome intuitivoDNS.
- 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

Tipi di indirizzi IP

I provider di servizi possono rendere disponibili i propri endpoint di servizio agli utenti del servizio tramite o entrambi IPv4 IPv6IPv6, anche se i IPv4 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 un VPC endpoint di interfaccia supportaIPv4, le interfacce di rete degli endpoint dispongono di indirizzi. IPv4 Se un VPC endpoint di interfaccia supportaIPv6, le interfacce di rete degli endpoint dispongono di indirizzi. IPv6 L'IPv6indirizzo 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

- Le sottoreti VPC e per il servizio endpoint devono avere blocchi associati. IPv6 CIDR
- 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

DNSregistra il tipo di indirizzo IP per un endpoint di interfaccia

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

- IPv4— Crea record A per i nomi privati, regionali e DNS zonali. Il tipo di indirizzo IP deve essere IPv4o Dualstack.
- IPv6— Crea AAAA record per i nomi privati, regionali e zonali. DNS Il tipo di indirizzo IP deve essere IPv6o Dualstack.
- Dualstack: crea A e AAAA record per i nomi privati, regionali e zonali. DNS 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 servizio da altre regioni se si abilita l'accesso interregionale o se utilizzano il VPC peering 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

- Crea un servizio VPC per gli 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 di IPv6 interfaccia per il servizio VPC endpoint, le sottoreti VPC e le sottoreti devono avere blocchi associati. IPv6 CIDR
- Crea un Network Load Balancer nel tuo. 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 avvii istanze in tutte le zone di disponibilità abilitate, puoi abilitare il bilanciamento del carico tra zone per supportare gli utenti del servizio che utilizzano nomi DNS host zonali per accedere al servizio. Quando abiliti il load balancer su più zone, si applicano i costi di trasferimento dei dati a livello regionale. Per ulteriori informazioni, consulta il 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 VPC console Amazon 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 tra 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. Per Abilita DNS nome privato, seleziona Associa un DNS nome privato al servizio per associare un DNS nome privato che gli utenti del servizio possono utilizzare per accedere al servizio, quindi inserisci il DNS nome privato. In caso contrario, gli utenti del servizio possono utilizzare il DNS nome specifico dell'endpoint fornito da. AWS Prima che gli utenti del servizio possano utilizzare il DNS nome privato, il fornitore del servizio deve verificare di essere il proprietario del dominio. Per ulteriori informazioni, consulta Gestisci i 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 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.
10. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
11. Selezionare 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 di interfaccia. VPC 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 VPC console Amazon 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 NLBs e 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 tra regioni”.
7. Per VPC, seleziona il servizio 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 il tipo di IP da DNS record, scegli una delle seguenti opzioni:

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

Attività

- Gestione delle autorizzazioni
- Accettare o rifiutare le richieste di connessione
- Gestisci i sistemi di bilanciamento del carico
- Associa un nome privato DNS
- 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 di interfaccia per connettersi al VPC 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 AWS principali supportati.

ARNsper 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 VPC console Amazon 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). Per aggiungere Principal, inserisci ARN il 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 VPC console Amazon 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 VPC console Amazon 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-connectionsoppure 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 un Network Load Balancer, puoi anche abilitare la zona di disponibilità per il tuo servizio endpoint. Dopo aver abilitato una zona di disponibilità per il servizio endpoint, gli utenti del servizio possono aggiungere una sottorete da quella zona di disponibilità agli endpoint di interfaccia. VPC

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

1. Apri la VPC console Amazon 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. Per 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.
   - Se di recente hai abilitato un'altra zona di disponibilità per il tuo sistema di bilanciamento del carico, questa viene visualizzata in Zone di disponibilità incluse. Se si salvano le modifiche nel passaggio successivo, viene abilitato il servizio endpoint per la nuova zona di disponibilità.
6. Scegli Salva modifiche.

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.

Associa un nome privato DNS

Puoi associare un DNS nome privato al tuo servizio endpoint. Dopo aver associato un DNS nome privato, devi aggiornare la voce relativa al dominio sul tuo DNS server. Prima che gli utenti del servizio possano utilizzare il DNS nome privato, il fornitore del servizio deve verificare di essere il proprietario del dominio. Per ulteriori informazioni, consulta Gestisci i nomi DNS.

Per modificare il DNS nome privato di un servizio endpoint utilizzando la console

1. Apri la VPC console Amazon 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 DNS nome privato.
5. Seleziona Associa un DNS nome privato al servizio e inserisci il DNS nome 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. Il DNS nome privato è pronto per l'uso da parte dei consumatori del servizio una volta verificato lo stato di verifica. Se lo stato della verifica cambia, le nuove richieste di connessione vengono rifiutate, senza tuttavia influenzare quelle esistenti.

Per modificare il DNS nome privato di un 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 VPC console Amazon 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, verifica la proprietà del dominio per DNS il nome 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 VPC console Amazon 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 VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona il servizio VPC endpoint.
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 VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona il servizio VPC endpoint.
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. Seleziona Salva.

Gestione dei tag per le connessioni degli endpoint tramite la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona il servizio VPC endpoint, quindi scegli la scheda 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. Seleziona Salva.

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona il servizio VPC endpoint, quindi scegli la scheda 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. Seleziona 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

Gestisci DNS i nomi per i VPC servizi endpoint

I provider di servizi possono configurare DNS nomi 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 DNS nome dell'endpoint pubblico come DNS nome 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 consumatore del servizioVPC, i DNS server privati risolvono il DNS nome negli indirizzi IP delle interfacce di rete degli endpoint. Altrimenti, i DNS server pubblici risolvono il DNS nome nell'endpoint pubblico.

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

Considerazioni

- Un servizio endpoint può avere un solo nome privatoDNS.

- Quando il consumatore crea un endpoint di interfaccia per connettersi al servizio, creiamo una zona ospitata privata e la associamo al consumatore del servizio. VPC Creiamo un CNAME record nella zona ospitata privata che associa il DNS nome privato del servizio endpoint al DNS nome regionale dell'VPCendpoint. Quando un consumatore invia una richiesta al DNS nome pubblico del servizio, i DNS server 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 pubblico. DNS
- Puoi verificare il dominio di un sottodominio. Ad esempio, è possibile verificare example.com, anziché a.example.com. Ogni DNS etichetta 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 privato. DNS A questo punto devi verificare example.com o b.example.com prima che gli utenti possano utilizzare il nome.
- DNSI nomi 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 di domain name service (DNS) che gestisci tramite il tuo DNS provider. Un TXT record è un tipo di DNS record che fornisce informazioni aggiuntive sul tuo dominio. È formato da un nome e da un valore. Come parte del processo di verifica, devi aggiungere un TXT record al DNS server di dominio pubblico.

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

Dopo aver aggiunto un record, puoi controllare lo stato del processo di verifica del dominio utilizzando la VPC console Amazon. 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 Azioni, Verifica la proprietà del dominio per DNS il nome privato.

Il DNS nome privato è pronto per l'uso da parte dei consumatori del servizio una volta verificato lo stato di verifica. 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

Ti forniamo il nome e il valore che usi nel TXT record. Queste informazioni sono disponibili, ad esempio, nella AWS Management Console. 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. Puoi anche utilizzare il seguente AWS CLI comando describe-vpc-endpoint-service-configurations per recuperare informazioni sulla configurazione del DNS nome 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. Utilizzerai `Value` e `Name` quando creerai il 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. La tabella seguente è un esempio delle impostazioni del TXT record.

Nome	Tipo	Valore
_6e86v84tqgqubxbwi i1m.example.com	TXT	vpce: l6p0 ERxlTt45jevFwOCp

Ti consigliamo di usare `Name` come sottodominio record perché il nome del dominio di base potrebbe essere già in uso. Tuttavia, se il tuo DNS provider non consente che i nomi dei DNS record contengano caratteri di sottolineatura, puoi 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 DNS un record al server del tuo dominio TXT

La procedura per aggiungere TXT record al DNS server del dominio dipende da chi fornisce il DNS servizio. Il tuo DNS provider potrebbe essere Amazon Route 53 o un altro registrar di nomi di dominio.

Amazon Route 53

Creare un record per la zona ospitata pubblica. Utilizzare i seguenti valori:

- Per Tipo di record, scegli TXT.
- Per TTL(secondi), immettere**`1800`**.
- In Policy di routing, scegli Routing semplice.
- Per Record name (Nome record) immetti il dominio o il sottodominio.
- Per Value/Route traffic to (Valore/Instrada il traffico a), immetti il valore verifica del dominio.

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

Procedura generale

Vai al sito web del tuo DNS provider e accedi al tuo account. Trova la pagina per aggiornare i DNS record del tuo dominio. Aggiungi un TXT record con il nome e il valore che abbiamo fornito. Possono essere necessarie fino a 48 ore prima che gli aggiornamenti dei DNS record abbiano effetto, ma spesso hanno effetto molto prima.

Per istruzioni più specifiche, consulta la documentazione del tuo DNS provider. La tabella seguente fornisce i collegamenti alla documentazione di diversi DNS provider 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.

DNS/Provider di hosting	Collegamento alla documentazione
GoDaddy	Aggiungi un record TXT
Dreamhost	Aggiungere DNS record personalizzati
Cloudflare	Gestire i DNS record
HostGator	Gestisci DNS i record con HostGator/eNom
Namecheap	Come faccio ad aggiungere TXT/SPF/DKIM/DMARC record per il mio dominio?
Names.co.uk	Modifica delle DNS impostazioni del dominio
Wix	Aggiungere o aggiornare TXT i record nel tuo account Wix

Controlla se il TXT record è stato pubblicato

Puoi verificare che il TXT record di verifica della proprietà DNS del dominio del nome privato sia pubblicato correttamente sul tuo DNS server utilizzando i seguenti passaggi. Eseguirai il nslookup comando, disponibile per Windows e Linux.

Dovrai interrogare i DNS server che servono il tuo dominio perché quei server contengono la maggior parte delle up-to-date informazioni relative al tuo dominio. La propagazione delle informazioni sul tuo dominio ad altri DNS server richiede tempo.

Per verificare che il TXT record sia pubblicato sul 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 TXT record 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 del passaggio precedente, verifica che la stringa che segue `text =` corrisponda al TXT valore.

   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 tuo DNS provider consente i caratteri di sottolineatura nei nomi dei TXT record. Se il tuo DNS provider non consente i caratteri di sottolineatura, puoi omettere il nome di verifica del dominio (ad esempio, «_6e86v84tqgqubxbwii1m») dal record. TXT
- TXTVerifica se il tuo provider DNS ha aggiunto il nome di dominio alla fine del record. Alcuni DNS provider aggiungono automaticamente il nome del tuo dominio al nome dell'attributo del TXT record. Per evitare questa duplicazione del nome di dominio, aggiungi un punto alla fine del nome di dominio quando crei il TXT record. Ciò indica al DNS provider che non è necessario aggiungere il nome di dominio al TXT record.
- Verifica se il tuo DNS provider ha modificato il valore del DNS record per 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 DNS provider ha modificato i valori del TXT record in modo da utilizzare solo lettere minuscole, contattalo per ricevere assistenza.
- Potrebbe essere necessario verificare più volte il dominio, dal momento che supporta molteplici regioni o Account AWS. Se il tuo DNS provider non ti consente di avere più di un TXT record con lo stesso nome di attributo, verifica se il DNS provider ti consente di assegnare più valori di attributo allo stesso record. TXT Ad esempio, se il tuo DNS è gestito da Amazon Route 53, puoi utilizzare la seguente procedura.

  1. Nella console Route 53, scegli il TXT record che hai creato quando hai verificato il 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 tuo DNS provider non ti consente di assegnare più valori allo stesso TXT record, puoi verificare il dominio una volta con il valore nel nome dell'attributo del TXT record e un'altra volta con il valore rimosso dal nome dell'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.

Attività

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

Creare una notifica SNS

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

Per creare una notifica per un servizio endpoint utilizzando la console

1. Apri la VPC console Amazon 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. Per Notifica ARN, scegli l'ARNSNSargomento 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 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'SNSargomento che AWS PrivateLink consenta di pubblicare notifiche per tuo conto, come la seguente. Per ulteriori informazioni, consulta Come posso modificare la politica di accesso del mio SNS argomento Amazon? Utilizza le chiavi di condizione globali `aws:SourceArn` e `aws:SourceAccount` per evitare il problema del "confused deputy".

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

Aggiungere una policy della chiave

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

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

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 VPC console Amazon 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 VPC risorse tramite AWS PrivateLink

È possibile accedere privatamente a una VPC risorsa in un'altra VPC utilizzando un endpoint di risorse (VPCendpoint di risorse). Un endpoint di risorse consente di accedere in modo privato e sicuro a VPC risorse come un database, un cluster di nodi, un'istanza, un endpoint dell'applicazione, una destinazione con nome di dominio o un indirizzo IP che può trovarsi in una sottorete privata in un altro ambiente o in locale. VPC Senza endpoint di risorse, è necessario aggiungere un gateway Internet VPC o accedere alla risorsa utilizzando un endpoint di AWS PrivateLink interfaccia e un Network Load Balancer. Gli endpoint di risorse non richiedono un load balancer, quindi puoi accedere direttamente alla risorsa. VPC Una VPC risorsa è rappresentata da una configurazione di risorse. Una configurazione di risorse è legata a un gateway di risorse.

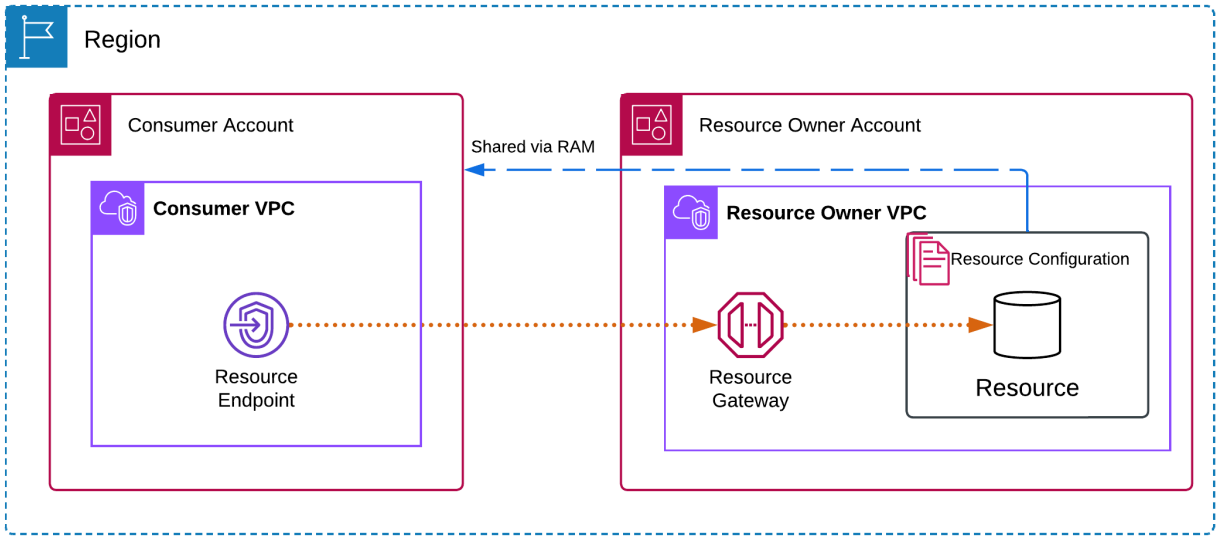
Prezzi

Quando accedi alle risorse utilizzando gli endpoint di risorse, ti viene addebitata una fattura per ogni ora di provisioning dell'VPCendpoint di risorse. Ti viene inoltre addebitato un importo per GB di dati elaborati quando accedi alle risorse. Per ulteriori informazioni, consulta Prezzi di AWS PrivateLink. Quando abiliti l'accesso alle tue risorse utilizzando configurazioni di risorse e gateway di risorse, ti viene addebitato il costo per GB di dati elaborati dai tuoi gateway di risorse. Per ulteriori informazioni, consulta 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 VPC endpoint di risorse, che stabilisce connessioni tra le sottoreti dell'utente 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 utilizzando e quindi inviato alla risorsa utilizzando DNS la connessione tra l'VPCendpoint e la risorsa tramite il gateway di risorse.



Considerazioni

- TCPil traffico è supportato. UDPil traffico non è supportato.
- Le connessioni di rete devono essere avviate dall'endpoint VPC che contiene la risorsa e non dall'endpoint VPC che contiene la risorsa. La risorsa non VPC può avviare connessioni di rete nell'endpoint. VPC
- Le uniche risorse ARN basate su supporto sono RDS le risorse Amazon.

DNSnomi host

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

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

Quando crei un VPC endpoint di risorse per determinate configurazioni di risorse che utilizziARNs, puoi abilitare l'opzione private. DNS Con privateDNS, puoi continuare a fare richieste alla risorsa utilizzando il DNS nome assegnato alla risorsa dal AWS servizio, sfruttando al contempo la connettività privata tramite l'endpoint della risorsa. VPC Per ulteriori informazioni, consulta the section called “DNSrisoluzione”.

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

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

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

```
"DnsEntry": {
                "DnsName": "vpce-1234567890abcdefg-
snra-1234567890abcdefg.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-
east-1.on.aws",
                "HostedZoneId": "ABCDEFGH123456789000"
            },
"PrivateDnsEntry": {
                "DnsName": "database-5-test.cluster-ro-example.us-
east-1.rds.amazonaws.com",
                "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
            }
```

DNSrisoluzione

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

Privato DNS

Se abiliti private DNS per il tuo VPC endpoint di risorse e hai VPC abilitato sia i DNSnomi host che la DNS risoluzione, creiamo zone ospitate private nascoste e AWS gestite per le configurazioni delle risorse con un nome personalizzato. DNS La zona ospitata contiene un set di record per il DNS nome predefinito della risorsa che lo risolve negli indirizzi IP privati delle interfacce di rete dell'endpoint di risorse del tuo. VPC

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

È possibile configurare l'VPCendpoint con una sottorete per zona di disponibilità. Creiamo un'interfaccia di rete endpoint per l'VPCendpoint nella tua sottorete. Assegniamo gli indirizzi IP a ciascuna interfaccia di rete dell'endpoint dalla relativa sottorete, in base al tipo di indirizzo IP dell'endpoint. VPC Il numero di indirizzi IP assegnati in ciascuna sottorete dipende dal numero di configurazioni delle risorse. 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 IPv6 dualstack. Gli endpoint che lo supportano IPv6 possono rispondere alle domande con record. DNS AAAA Il tipo di indirizzo IP di un endpoint di risorse 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 VPC endpoint di risorse lo supportaIPv4, le interfacce di rete degli endpoint dispongono di indirizzi. IPv4 Se un VPC endpoint di risorse lo supportaIPv6, le interfacce di rete degli endpoint dispongono di indirizzi. IPv6 L'IPv6indirizzo 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 risorsa tramite un endpoint di risorse VPC

Puoi accedere a una VPC risorsa come un nome di dominio, un indirizzo IP o un RDS database Amazon utilizzando un endpoint di risorse. Un endpoint di risorse fornisce l'accesso privato a una risorsa. Quando si crea l'endpoint di risorse, si specifica una configurazione delle risorse di tipo singola, di 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 condivisa con l'utente da un altro account 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 VPC risorse

Utilizzare la procedura seguente per creare un endpoint di VPC risorse.

Per creare un endpoint di VPC risorse

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

4. Puoi specificare un nome per facilitare la ricerca e la gestione dell'endpoint.
5. Per Tipo, scegli Risorse.
6. Per le configurazioni delle risorse, seleziona la configurazione delle risorse che è stata condivisa con te.
7. Per le impostazioni di rete, seleziona la VPC modalità da cui accederai alla risorsa.
8. Se desideri configurare il DNS supporto privato, seleziona Impostazioni aggiuntive, Abilita DNS nome. Per utilizzare questa funzionalità, assicurati che gli attributi Abilita DNS nomi host e Abilita DNS supporto siano abilitati per il tuoVPC.
9. 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 aggiornarne la configurazione.

Attività

- Eliminazione di un endpoint.
- Aggiorna un endpoint

Eliminazione di un endpoint.

Quando hai finito con un VPC endpoint, puoi eliminarlo.

Per eliminare un endpoint utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint.
4. Scegli Azioni, Elimina VPC endpoint.
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

È possibile aggiornare un VPC endpoint.

Per aggiornare un endpoint utilizzando la console

1. Apri la VPC console Amazon 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 VPC risorse per le risorse

Una configurazione di risorse rappresenta una risorsa o un gruppo di risorse che si desidera rendere accessibili ai client in altri accountVPCs. Definendo una configurazione delle risorse, puoi consentire la connettività di rete privata, sicura VPCs e unidirezionale alle risorse in tuo possesso VPC da parte dei client di altri account. Una configurazione delle risorse è collegata a un gateway di risorse attraverso il quale riceve il traffico.

Indice

- Definizione della risorsa
- Protocollo
- Intervalli di porte
- Accesso alle risorse
- Associazione con il tipo di rete di servizio
- Tipi di reti di servizio
- Condivisione delle configurazioni delle risorse tramite AWS RAM
- Monitoraggio
- Crea 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 che rappresentano un cluster di nodi. Può essere condivisa indipendentemente.
- 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.
- ARNconfigurazione delle risorse: rappresenta un tipo di risorsa supportato fornito da un servizio. AWS Le configurazioni delle risorse secondarie vengono gestite automaticamente da. AWS

Gateway di risorse

Una configurazione delle risorse è legata a un gateway di risorse. Un gateway di risorse è un insieme di risorse ENIs che funge da punto di ingresso VPC nel quale si trova la risorsa. È possibile collegare più configurazioni di risorse allo stesso gateway di risorse. Quando i client di un altro VPCs account

accedono a una risorsa dell'utenteVPC, la risorsa vede il traffico proveniente localmente dal gateway di risorse in questioneVPC.

Definizione della risorsa

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

- Con un nome di risorsa Amazon (ARN): i tipi di risorse supportati, forniti dai AWS servizi, possono essere identificati in base ai loro. ARN Ad esempio, un RDS database Amazon.
- Per destinazione con nome di dominio: qualsiasi nome di dominio risolvibile pubblicamente.
- Tramite un indirizzo IP: per IPv4 eIPv6, sono supportati solo i. IPs VPC

Protocollo

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

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 VPC utilizzando un VPC endpoint o tramite una rete di servizi. In qualità di consumatore, puoi abilitare l'accesso dal tuo account 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 AWS PrivateLink VPC endpoint di tipo risorsa (endpoint di risorse) in 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 Accedere alle VPC risorse nella guida per l'utente.AWS PrivateLink
- Accesso a una configurazione di risorse tramite una rete di servizi

È possibile associare una configurazione di risorse a una rete di servizi e connettersi VPC alla rete di servizio. È possibile connettersi VPC alla rete di servizio tramite un'associazione o utilizzando un endpoint di AWS PrivateLink rete di serviziVPC.

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

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

Associazione con il tipo di rete di servizio

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 VPC endpoint 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 VPC endpoint di tipo risorsa (endpoint di risorse). VPC
- Utilizzo di un VPC endpoint di tipo service network (service network VPC endpoint).
- Utilizzo di un'associazione di rete VPC di servizi.

Per l'VPCendpoint della rete di servizio e VPC l'associazione della rete di servizio, la configurazione delle risorse dovrebbe essere inserita in una rete di servizi in Account-B. Le reti di servizio 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'altra VPC nello stesso account della configurazione della risorsa, non è necessario condividere la configurazione della risorsa tramite AWS RAM.

Monitoraggio

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

Crea una configurazione delle risorse in VPC Lattice

Usa la console per creare una configurazione delle risorse.

Per creare una configurazione delle risorse utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello 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. Scegli l'identificatore per la risorsa che desideri che questa configurazione di risorse rappresenti.
8. Scegliete gli intervalli di porte attraverso i quali desiderate condividere la risorsa.
9. Per le impostazioni di associazione, specifica se questa configurazione delle risorse può essere associata a reti di servizi condivisibili.
10. Per la configurazione di condivisione delle risorse, scegli le condivisioni di risorse che identificano i principali che possono accedere a questa risorsa.
11. (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.
12. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
13. Scegli Crea configurazione delle risorse.

Per creare una configurazione delle risorse utilizzando il AWS CLI

Utilizza il comando create-resource-configuration.

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 di risorse o tramite un VPC endpoint di rete di servizi. Di conseguenza, la configurazione delle risorse avrà associazioni di endpoint e associazioni di reti di servizio.

Gestisci le associazioni delle reti di servizio

Creare o eliminare un'associazione di rete di servizi.

Per gestire un'associazione servizio-rete utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello 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. Scegli Save changes (Salva modifiche).
9. 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 il AWS CLI

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

Gestisci le associazioni VPC degli endpoint

Gestisci un'associazione di VPC endpoint.

Per gestire un'associazione di VPC endpoint utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello 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. Scegli la scheda Associazioni degli endpoint.
5. Seleziona l'ID dell'associazione per aprirne la pagina dei dettagli. Da qui, puoi modificare o eliminare l'associazione.
6. Per creare una nuova associazione di endpoint, vai su PrivateLink and Lattice nel riquadro di navigazione a sinistra e scegli Endpoints.
7. Scegli Crea endpoint.
8. Seleziona la configurazione delle risorse per connetterti al tuoVPC.
9. Seleziona le VPC sottoreti e i gruppi di sicurezza.

10. (Facoltativo) Per taggare il tuo VPC endpoint, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
11. Seleziona Crea endpoint.

Per creare un'associazione di VPC endpoint utilizzando il AWS CLI

Utilizza il comando create-vpc-endpoint.

Per eliminare un'associazione di VPC endpoint utilizzando il AWS CLI

Utilizza il comando delete-vpc-endpoint.

Gateway di risorse in VPC Lattice

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

VPCÈ necessario disporre di un gateway di risorse se si prevede di rendere VPC accessibili le risorse interne da altri accountVPCs. Ogni risorsa che condividi è legata a un gateway di risorse. Quando i client di un altro VPCs account accedono a una risorsa del tuo accountVPC, la risorsa vede il traffico proveniente localmente dal gateway di risorse in questioneVPC. L'IP di origine del traffico è l'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 VPC possibile collegare più risorse contemporaneamente allo stesso gateway di risorse.

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

Indice

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 disporre IPv4 di indirizzi IPv6 dual-stack o 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 E alle interfacce di rete del 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'VPCendpoint tramite il quale si accede alla risorsa.

Crea 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 VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, sotto PrivateLink e Lattice, scegli Resource gateways.
3. Scegli Crea gateway di risorse.
4. Inserisci un nome univoco all'interno del tuo AWS account.
5. Scegli il tipo di IP per il gateway di risorse.
6. Scegli VPC quello in cui si trova la risorsa.
7. Scegli fino a cinque gruppi di sicurezza per controllare il traffico in entrata dalla rete VPC di servizio.
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 Resource Gateway.

Per creare un gateway di risorse utilizzando AWS CLI

Utilizza il comando create-resource-gateway.

Elimina un gateway di risorse in VPC Lattice

Usa la console per eliminare un Resource Gateway.

Per eliminare un gateway di risorse utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, sotto PrivateLink e Lattice, scegli Resource gateways.
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 Resource Gateway utilizzando il AWS CLI

Utilizza il comando delete-resource-gateway.

Accedi alle reti di servizi tramite AWS PrivateLink

È possibile connettersi privatamente a una rete di servizi VPC utilizzando un endpoint della rete di servizio (VPCendpoint 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, è possibile 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 VPC servizi Lattice. Utilizzando un endpoint di rete di servizi, è possibile connettere una rete di servizi al proprio VPC e accedere a tali risorse e servizi in modo privato dall'utente o dall'ambiente locale. VPC Un endpoint di rete di servizi consente di connettersi a una rete di servizio. Per connetterti a più reti di servizio dalla tuaVPC, puoi creare più endpoint della 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 fatturato per GB di dati elaborati quando accedi alle risorse tramite l'endpoint della rete di assistenza. VPC Non ti viene addebitata alcuna tariffa oraria per l'endpoint della rete di assistenza stesso. VPC Per ulteriori informazioni, consulta Prezzi di Amazon VPC Lattice.

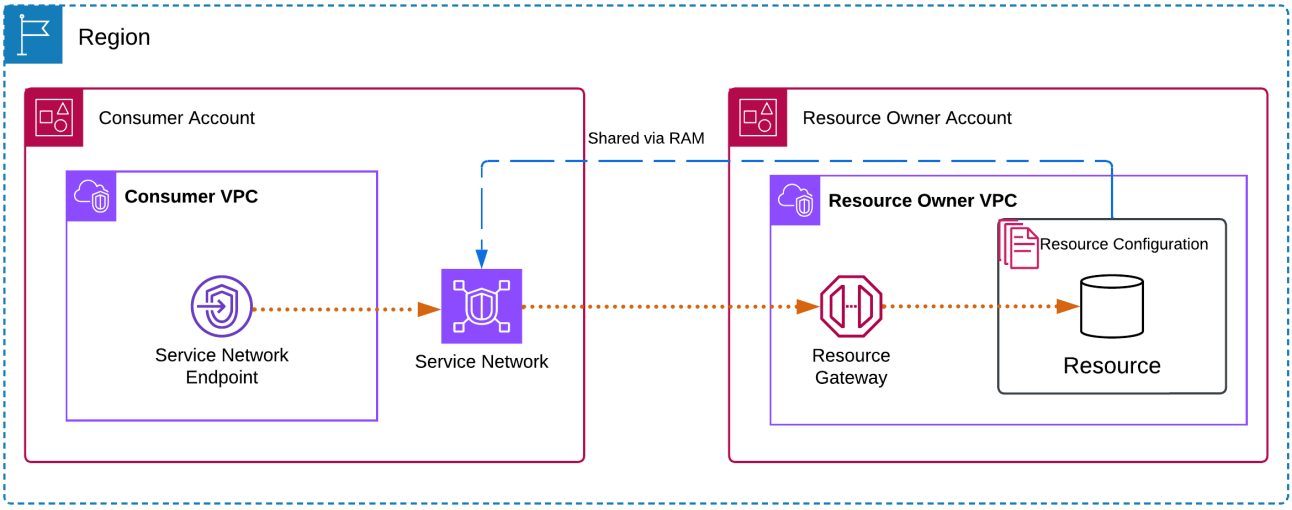
Indice

- Tipi di indirizzi IP
- 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 del tuo computer accede a una rete di servizi. VPC



Le connessioni di rete possono essere avviate solo dall'endpoint della VPC rete di servizio alle risorse e ai servizi della rete di servizio. VPCCon le risorse e i servizi non è possibile avviare connessioni di rete nell'endpoint. VPC

DNSnomi host

Con AWS PrivateLink, invii traffico alle reti di servizi utilizzando endpoint privati. Quando crei un VPC endpoint di rete di servizi, creiamo DNS nomi regionali (denominati DNS nome predefinito) per ogni risorsa e servizio che puoi utilizzare per comunicare con la risorsa e il servizio dall'utente VPC e dall'ambiente locale.

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

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

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

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

Quando la rete di servizi dispone di configurazioni di risorse che utilizzanoARNs, è possibile abilitare la modalità privata. DNS Con privateDNS, puoi continuare a fare richieste alla risorsa utilizzando il DNS nome assegnato alla risorsa dal AWS servizio, sfruttando al contempo la connettività privata tramite l'endpoint della rete di servizio. VPC Per ulteriori informazioni, consulta the section called “DNSrisoluzione”.

DNSrisoluzione

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

Privato DNS

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

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

È possibile configurare l'VPCendpoint con una sottorete per zona di disponibilità. Creiamo un'interfaccia di rete endpoint per l'VPCendpoint nella tua sottorete. Assegniamo gli indirizzi IP a ciascuna 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 della rete di servizio possono supportare o supportare IPv4 indirizzi dual-stack. IPv6 Gli endpoint che lo supportano IPv6 possono rispondere alle domande con record. DNS 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 della rete di servizi lo supportaIPv4, le interfacce di rete degli VPC endpoint dispongono di indirizzi. IPv4 Se un endpoint di rete di servizi lo supporta, le interfacce di rete VPC degli endpoint dispongono di indirizziIPv6. IPv6 L'IPv6indirizzo 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 l'utente da un altro account, è necessario 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 .

Creare un endpoint della rete di assistenza

Crea un endpoint di rete di servizi per accedere alla rete di servizi condivisa con te.

Per creare un endpoint di rete di servizi

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
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 che è stata condivisa con te.
7. Per le impostazioni di rete, seleziona la rete VPC da cui accederai alla rete di servizio.
8. Se desideri configurare il DNS supporto privato, seleziona Impostazioni aggiuntive, Abilita DNS nome. Per utilizzare questa funzionalità, assicurati che gli attributi Abilita DNS nomi host e Abilita DNS supporto siano abilitati per il tuoVPC.
9. 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 la configurazione.

Attività

- Eliminazione di un endpoint.

- Aggiornare un endpoint di rete di servizi

Eliminazione di un endpoint.

Quando hai finito con un VPC endpoint, puoi eliminarlo.

Per eliminare un endpoint utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint della rete di servizio.
4. Scegli Azioni, Elimina 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

È possibile aggiornare un endpoint. VPC

Per aggiornare un endpoint utilizzando la console

1. Apri la VPC console Amazon 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 programma Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS IAMgli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS PrivateLink IAMè un dispositivo Servizio AWS 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 svolgi. AWS PrivateLink

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 ti 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 inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere le nozioni di base di IAM.

IAMamministratore: se sei un IAM amministratore, potresti voler saperne di più su come scrivere politiche per gestire l'accesso AWS PrivateLink.

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta AWS Signature Version 4 per API le richieste nella Guida per l'IAMutente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'AWS IAM Identity Center utente e Autenticazione a AWS più fattori IAM nella Guida per l'IAMutente.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nella Guida AWS IAM Identity Center per l'utente.

IAM users and groups

Un IAMutente è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un gruppo IAM è un'identità che specifica una raccolta di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile assegnare un nome a un gruppo IAMAdminse concedere a tale gruppo le autorizzazioni per amministrare le risorse. IAM

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Casi d'uso per IAM gli utenti nella Guida per l'IAMutente.

Ruoli IAM

Un IAMruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM ma non è associato a una persona specifica. Per assumere temporaneamente un IAM ruolo in AWS Management Console, puoi passare da un utente a un IAM ruolo (console). È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Metodi per assumere un ruolo nella Guida per l'IAMutente.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, consulta Creare un ruolo per un provider di identità di terze parti (federazione) nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (principale attendibile) di un account diverso di accedere alle risorse nel tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse su più account IAM nella Guida per l'utente. IAM
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che quindi avvia un'altra azione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. FASle richieste vengono effettuate solo quando un

servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio da IAM. Per ulteriori informazioni, consulta Creare un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare, ma non modificare le autorizzazioni dei ruoli collegati ai servizi.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o effettuano AWS API richieste. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore

può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, indipendentemente dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da AWS API. AWS CLI

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Definire le IAM autorizzazioni personalizzate con le politiche gestite dal cliente nella Guida per l'utente. IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scegliere tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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 azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

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

Elenchi di controllo degli accessi () ACLs

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioniACLs, consulta la panoramica di Access control list (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM
- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCPLimita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Criteri di controllo delle risorse (RCPs): RCPs sono JSON criteri che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le IAM politiche allegate a ciascuna risorsa di tua proprietà. RCPLimita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations eRCPs, incluso un elenco di Servizi AWS tale

supportoRCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.

- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle politiche nella Guida per l'IAMutente.

Come AWS PrivateLink funziona con IAM

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

Caratteristica IAM	AWS PrivateLink supporto
Policy basate su identità	Sì
Policy basate su risorse	Sì
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC(tag nelle politiche)	Sì

Caratteristica IAM	AWS PrivateLink supporto
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una panoramica generale del funzionamento della maggior parte delle funzionalità, consulta i AWS servizi che Servizi AWS funzionano con IAM la maggior parte delle IAM funzionalità, consulta la Guida per l'IAMutente. AWS PrivateLink

Politiche basate sull'identità per AWS PrivateLink

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Definire le IAM autorizzazioni personalizzate con le politiche gestite dal cliente nella Guida per l'utente. IAM

Con le policy IAM IAM basate su identità, puoi specificare operazioni e risorse consentite o rifiutate, nonché le condizioni in base alle quali le operazioni sono consentite o rifiutate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per maggiori informazioni su tutti gli elementi che puoi utilizzare in una JSON policy, consulta il riferimento agli elementi della IAM JSON policy nella Guida per l'utente. IAM

Esempi di policy 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 politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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 azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso a più account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata su risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta la sezione Cross Account Resource Access IAM nella Guida IAM per l'utente.

AWS PrivateLink il servizio supporta un tipo di policy basata sulle risorse, nota come policy per gli 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 AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

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

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

Azioni nello spazio dei nomi ec2

Alcune azioni AWS PrivateLink fanno parte di Amazon EC2API. Queste azioni politiche utilizzano il `ec2` prefisso. Per ulteriori informazioni, consulta AWS PrivateLink le azioni in 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 di policy: sì

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

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (ARN). È possibile eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Chiavi relative alle condizioni della policy per AWS PrivateLink

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

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano

più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica0R. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi concedere a un utente IAM l'autorizzazione per accedere a una risorsa solo se è stata taggata con il nome utente IAM. Per ulteriori informazioni, consulta Elementi IAM della politica: variabili e tag nella Guida per l'IAMutente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'IAMutente.

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.

ACLsin AWS PrivateLink

SupportiACLs: 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. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

ABACcon AWS PrivateLink

Supporti ABAC (tag nelle politiche): Sì

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare

tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

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

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

Per ulteriori informazioni in meritoABAC, vedere Definizione delle autorizzazioni con ABAC autorizzazione nella Guida per l'IAMutente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Use Attribute-based access control (ABAC) nella Guida per l'utente. IAM

Utilizzo di credenziali temporanee con AWS PrivateLink

Supporta le credenziali temporanee: sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione Servizi AWS relativa alla funzionalità IAM nella Guida per l'IAMutente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta Passare da un utente a un IAM ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere Credenziali di sicurezza temporanee in. IAM

Autorizzazioni principali per più servizi per AWS PrivateLink

Supporta sessioni di accesso diretto (FAS): Sì

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che quindi avvia un'altra azione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

Ruoli di servizio per AWS PrivateLink

Supporta i ruoli di servizio: no

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio da IAM. Per ulteriori informazioni, consulta Creare un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente.

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 nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare, ma non modificare le autorizzazioni dei ruoli collegati ai servizi.

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 . Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

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

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'uso degli VPC endpoint
- Controlla la creazione VPC degli endpoint in base al proprietario del servizio
- Controlla i DNS nomi privati che possono essere specificati per VPC i servizi endpoint
- Controlla i nomi dei servizi che possono essere specificati per i servizi VPC endpoint

Controlla l'uso degli VPC endpoint

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.

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

Per informazioni sul controllo dell'accesso ai servizi tramite gli VPC endpoint, consulta. the section called “Policy di endpoint”

Controlla la creazione VPC degli endpoint in base al proprietario del servizio

Puoi utilizzare la chiave di `ec2:VpceServiceOwner` condizione per controllare quale VPC endpoint può essere creato in base al proprietario del servizio (`amazonaws-marketplace`, o all'ID dell'account). L'esempio seguente concede l'autorizzazione a creare VPC endpoint con il

proprietario del servizio specificato. Per utilizzare questo esempio, sostituisci la Regione, l'ID account e il proprietario del servizio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceOwner": [
                        "amazon"
                    ]
                }
            }
        }
    ]
}
```

Controlla i DNS nomi privati che possono essere specificati per VPC i servizi endpoint

È possibile utilizzare la chiave di `ec2:VpceServicePrivateDnsName` condizione per controllare quale servizio VPC endpoint può essere modificato o creato in base al DNS nome privato associato al servizio VPC endpoint. L'esempio seguente concede l'autorizzazione a creare un servizio VPC endpoint con il nome privato specificato. DNS Per utilizzare questo esempio, sostituisci la regione, l'ID dell'account e il nome privato. DNS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc-endpoint-service/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServicePrivateDnsName": [
                        "example.com"
                    ]
                }
            }
        }
    ]
}
```

Controlla i nomi dei servizi che possono essere specificati per i servizi VPC endpoint

È possibile utilizzare la chiave di `ec2:VpceServiceName` condizione per controllare quale VPC endpoint può essere creato in base al nome del servizio dell'VPCendpoint. L'esempio seguente concede l'autorizzazione a creare un VPC endpoint con il nome di servizio specificato. Per utilizzare questo esempio, sostituisci la Regione, l'ID account e il nome del servizio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
```

```
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.region.s3"
                    ]
                }
            }
        }
    ]
}
```

Controlla l'accesso agli VPC endpoint utilizzando le policy degli endpoint

Una policy sugli endpoint è una policy basata sulle risorse che si allega a un VPC endpoint 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 sugli endpoint è un documento di policy che utilizza il linguaggio JSON delle 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 si crea un'interfaccia o un endpoint gateway per un endpoint Servizio AWS, è possibile allegare una singola policy di 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 VPC endpoint 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 specificate un elemento ARN in una risorsa o in una condizione, la parte relativa all'account ARN può includere un ID account o un carattere jolly, ma non entrambi.

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 Servizi AWS, vedi. the 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

Aggiornare una policy per VPC gli endpoint

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

2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'VPCendpoint.
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. Seleziona 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 Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove API operazioni per i servizi esistenti.

Per ulteriori informazioni, consulta Policy gestite da AWSnellaGuida per l'utente 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 RSS feed 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 sono pubblicati per gli endpoint gateway. 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. Sono incluse le connessio ni negli ESTABLISHED stati SYN _ SENT e.

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 RST pacchetti 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 metrici per endpoint. VPC
`VPC Id`	Filtra i dati delle metriche 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 RST pacchetti 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 metrici per endpoint. VPC

Visualizza le metriche CloudWatch

Puoi visualizzare queste CloudWatch metriche utilizzando la VPC console Amazon, la CloudWatch console o AWS CLI come segue.

Per visualizzare le metriche utilizzando la console Amazon VPC

1. Apri la VPC console Amazon 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 le metriche 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 PrivateLinkEndpoints nomi AWS/.
4. Seleziona lo spazio dei nomi AWSPrivateLinkServices/.

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`— classifica gli endpoint in base al numero di RST pacchetti inviati agli 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 AWS Management Console o di AWS CLI.

Per abilitare le regole di Contributor Insights per AWS PrivateLink l'utilizzo della console

1. Apri la VPC console Amazon 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' AWS PrivateLink utilizzo di AWS CLI

1. Utilizzate il list-managed-insight-rulescomando come segue per enumerare le regole disponibili. Per l'`--resource-arn`opzione, specifica il tuo servizio ARN 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. È necessario specificare il nome del modello e il ARN 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

Puoi disabilitare 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 VPC console Amazon 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' AWS PrivateLink utilizzo di AWS 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 AWS Management Console 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 API azioni per AWS PrivateLink fanno parte di Amazon EC2API. Amazon EC2 limita le sue API richieste a livello di livello. Account AWS Per ulteriori informazioni, consulta la sezione Request throttling nella Amazon EC2 Developer Guide. Inoltre, API le richieste 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 API limiti a livello di account, vedi Come identificare AWS gli account che effettuano un numero elevato di chiamate. API Se hai bisogno di assistenza, contatta il team del tuo account o apri una richiesta di supporto tecnico utilizzando il VPCservizio e la categoria VPCEndpoints. Assicurati di allegare un'immagine del codice di `RequestLimitExceeded` errore.

VPCquote degli endpoint

Il tuo AWS account ha le seguenti quote relative agli endpoint. VPC

Nome	Predefinita	Adattabile	Commenti
Endpoint di Interface e Gateway Load Balancer per VPC	50	Sì	Si tratta di una quota combinata di endpoint dell'interfaccia ed endpoint Gateway Load Balancer
VPCEndpoint gateway per regione	20	Sì	È possibile creare fino a 255 endpoint gateway per VPC
Politica relativa ai caratteri per VPC endpoint	20.480	No	La dimensione massima di una policy per gli VPC endpoint, inclusi gli spazi bianchi

Le seguenti considerazioni si applicano al traffico che attraversa un VPC endpoint:

- Per impostazione predefinita, ogni VPC endpoint può supportare una larghezza di banda fino a 10 Gbps per zona di disponibilità e scalare automaticamente fino a 100 Gbps. La larghezza di banda massima per un VPC endpoint, quando si distribuisce il carico tra 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 di trasmissione massima (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto più grande consentito che può essere passato attraverso un endpoint. VPC Più grande èMTU, maggiore è il numero di dati che possono essere trasmessi in un singolo pacchetto. Un VPC endpoint supporta 8500 MTU byte. I pacchetti di dimensioni superiori a 8500 byte che arrivano all'endpoint vengono eliminati. VPC
- Path MTU Discovery (PMTUD) non è supportato. VPCgli endpoint non generano il seguente ICMP messaggio: `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (Tipo 3, Codice 4).
- VPCgli endpoint impongono il bloccaggio della dimensione massima del segmento (MSS) per tutti i pacchetti. Per ulteriori informazioni, vedere. 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 oltre VPC i confini degli 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 si crea o si modifica l'endpoint. VPC	17 agosto 2023
Supporto IPv6	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	18 agosto 2022

	endpoint specifici per i quali i principali contributori alle metriche. CloudWatch AWS PrivateLink	
Supporto IPv6	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 tuo computer VPC per indirizzare il traffico verso un servizio VPC endpoint che hai configurato utilizzando un Gateway Load Balancer.	10 novembre 2020
VPCpolitiche degli endpoint	È possibile allegare una IAM policy a un VPC endpoint di interfaccia per un AWS servi zio per controllare l'accesso al servizio.	23 marzo 2020

Chiavi di condizione per VPC endpoint e servizi endpoint	È possibile utilizzare i tasti EC2 condizionali per controlla re l'accesso agli endpoint e ai servizi VPC endpoint.	6 marzo 2020
Etichetta gli VPC endpoint e i servizi endpoint al momento della creazione	Puoi aggiungere tag quando crei endpoint e VPC servizi endpoint.	5 febbraio 2020
Nomi privati DNS	Puoi accedere ai servizi AWS PrivateLink basati dall'interno VPC usando DNS nomi privati.	6 gennaio 2020
VPCservizi endpoint	Puoi creare i tuoi servizi di endpoint e consentire ad altri Account AWS utenti di connettersi al tuo servizio tramite un endpoint di interfacc iaVPC. Puoi offrire i tuoi servizi endpoint per l'abbonamento nel Marketplace AWS.	28 novembre 2017
Endpoint di interfaccia VPC 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 o NAT un dispositivo Internet.	8 Novembre 2017
VPCendpoint per DynamoDB	Puoi creare un VPC endpoint gateway per accedere ad Amazon DynamoDB VPC dal tuo dispositivo senza utilizzar e un gateway o un dispositivo Internet. NAT	16 agosto 2017

VPCendpoint per Amazon S3	Puoi creare un VPC endpoint gateway per accedere ad Amazon S3 dal VPC tuo dispositivo senza utilizzare un gateway NAT o un dispositivo Internet.	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.