AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

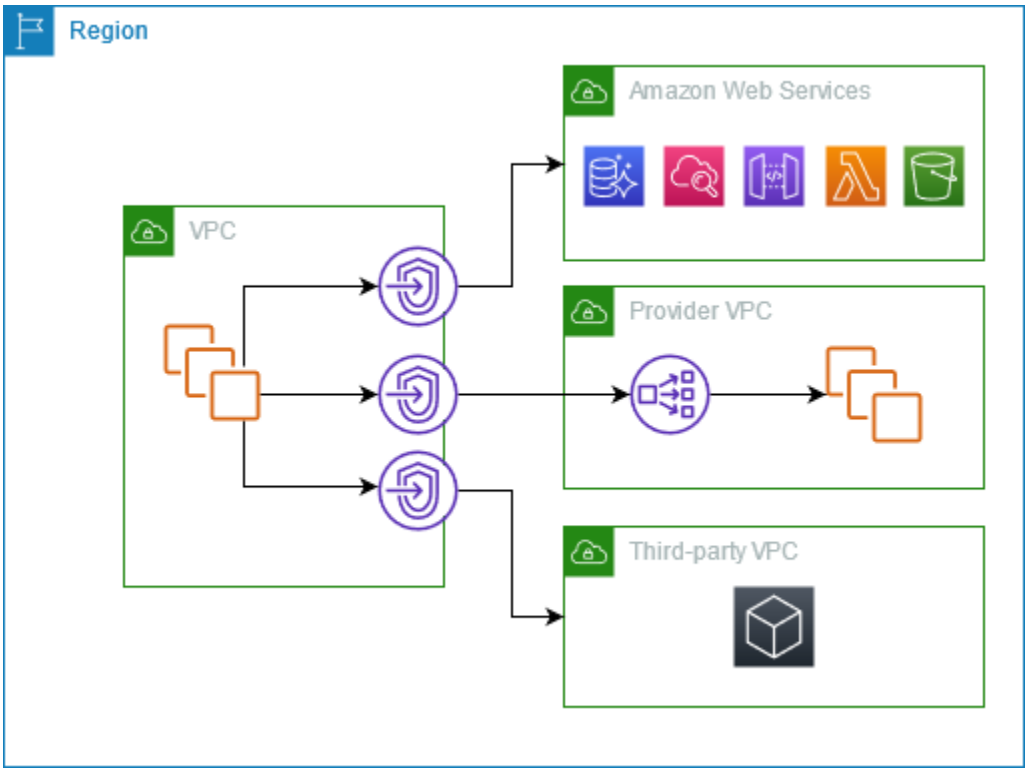
Che cos'è AWS PrivateLink?

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

Casi d'uso

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

Nel diagramma seguente, il VPC a sinistra ha diverse istanze EC2 in una sottorete privata e tre endpoint VPC dell'interfaccia. L'endpoint VPC più in alto si connette a un. Servizio AWS L'endpoint VPC centrale si connette a un servizio ospitato da un altro (Account AWS un servizio endpoint VPC). L'endpoint VPC inferiore si connette a un Marketplace AWS servizio partner.



Ulteriori informazioni

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

Utilizza gli endpoint VPC

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

- AWS Management Console— Fornisce un'interfaccia web che è possibile utilizzare per accedere alle risorse. AWS PrivateLink
- 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 AWS PrivateLink risorse:
  - AWS::EC2::VPCEndpoint
  - AWS::EC2::VPCEndpointConnectionNotification
  - AWS::EC2::VPCEndpointService
  - AWS::EC2::VPCEndpointServicePermissions
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS SDK: forniscono API specifiche per la lingua. Gli SDK di gestiscono molti dei dettagli della connessione, ad esempio il calcolo delle firme, la gestione dei nuovi tentativi di richiesta e la gestione degli errori. Per ulteriori informazioni, consulta SDK di AWS.
- API di query: forniscono operazioni API di basso livello accessibili tramite richieste HTTPS. L'utilizzo dell'API di query è il modo più diretto di accedere ad Amazon VPC. Tuttavia, richiede che l'applicazione gestisca dettagli di basso livello, come la generazione dell'hash per firmare la richiesta e la gestione degli errori. Per ulteriori informazioni, consulta Operazioni di AWS PrivateLink, nella Documentazione di riferimento delle API di Amazon EC2.

Prezzi

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

AWS PrivateLink concetti

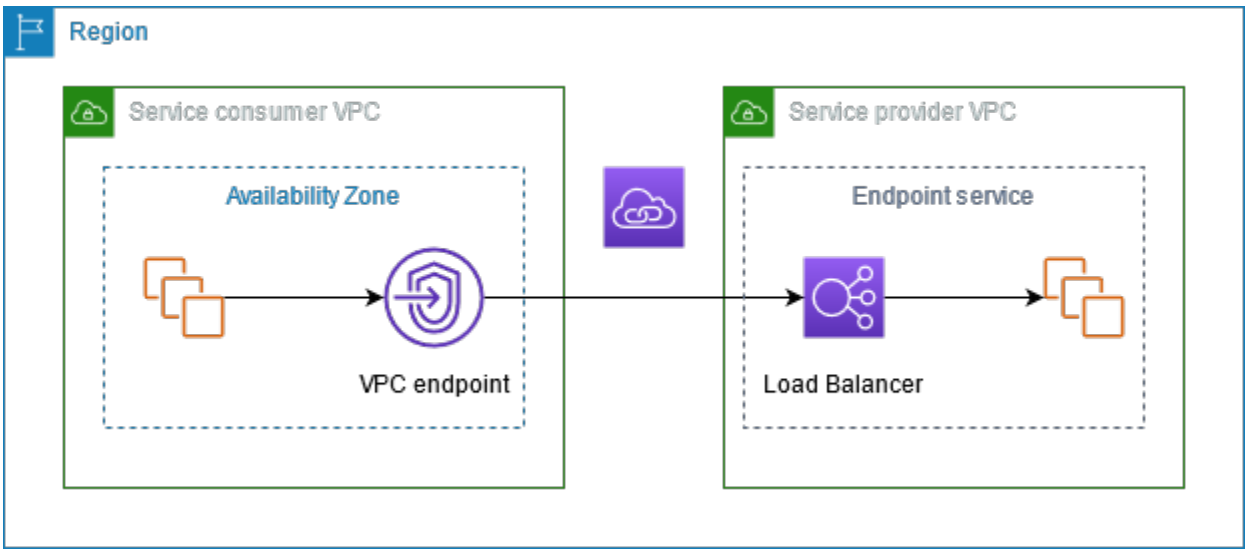
È possibile utilizzare Amazon VPC per definire un cloud privato virtuale (VPC), ossia una rete virtuale isolata logicamente. Puoi avviare AWS risorse nel tuo VPC. e consentirne la connessione a risorse esterne. Ad esempio, puoi aggiungere un gateway Internet al VPC per consentire l'accesso a Internet o aggiungere una connessione VPN per consentire l'accesso alla tua rete on-premise. In alternativa, AWS PrivateLink utilizzalo per consentire alle risorse del tuo VPC di connettersi ai servizi di altri VPC utilizzando indirizzi IP privati, come se tali servizi fossero ospitati direttamente nel tuo VPC.

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

Indice

Diagramma architetturale

Il diagramma seguente fornisce una panoramica di alto livello del funzionamento. AWS PrivateLink Gli utenti del servizio creano endpoint VPC dell'interfaccia per connettersi ai servizi endpoint ospitati dai provider di servizi.



Provider 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 fornitori di servizi possono ospitare i propri servizi utilizzando AWS risorse, come le istanze EC2, o utilizzando server locali.

Concetti

- Servizi endpoint
- Nomi dei servizi
- Stati del servizio

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 soggetti specifici di connettersi al AWS servizio endpoint.

Nomi dei servizi

Ogni servizio endpoint è identificato da un nome del servizio. Un utente del servizio deve specificare tale nome durante la creazione di un endpoint VPC. I consumatori del servizio possono richiedere i

nomi dei servizi per. Servizi AWS I provider di servizi devono condividere i nomi dei loro servizi con gli utenti.

Stati del servizio

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

- `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.

Utenti del servizio

Il consumatore di un servizio è un utente del servizio. Gli utenti dei servizi possono accedere ai servizi endpoint da AWS risorse, come le istanze EC2, o dai server locali.

Concetti

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

Endpoint VPC

Un utente del servizio crea un endpoint VPC per connettere il proprio VPC a un servizio endpoint. Un utente del servizio deve specificare il nome del servizio endpoint durante la creazione di un endpoint VPC. Esistono diversi tipi di endpoint VPC. È necessario creare il tipo di endpoint VPC richiesto dal servizio endpoint.

- `Interface` - Crea un endpoint di interfaccia per inviare traffico TCP a un servizio endpoint. Il traffico destinato al servizio endpoint viene risolto utilizzando il DNS.
- `GatewayLoadBalancer`: crea un endpoint Gateway Load Balancer per inviare traffico a un parco istanze di appliance virtuali utilizzando indirizzi IP privati. Puoi instradare il traffico dal tuo VPC

all'endpoint Gateway Load Balancer tramite le tabelle di instradamento. Gateway Load Balancer distribuisce il traffico alle appliance virtuali e può scalare in base alla domanda.

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

Interfacce di rete dell'endpoint

Con interfaccia di rete dell'endpoint si intende un'interfaccia di rete gestita dal richiedente che funge da punto di ingresso per il traffico destinato a un servizio endpoint. Per ciascuna sottorete specificata durante la creazione di un endpoint VPC, viene creata un'interfaccia di rete dell'endpoint nella sottorete.

Se un endpoint VPC supporta IPv4, le relative interfacce di rete dell'endpoint dispongono di indirizzi IPv4. Se un endpoint VPC supporta IPv6, le relative interfacce di rete dell'endpoint dispongono di indirizzi IPv6. L'indirizzo IPv6 per un'interfaccia di rete dell'endpoint non è raggiungibile da Internet. Quando descrivi un'interfaccia di rete dell'endpoint con un indirizzo IPv6, l'opzione `denyAllIgwTraffic` sarà abilitata.

Gli indirizzi IP di un'interfaccia di rete dell'endpoint non cambieranno durante la durata del relativo endpoint VPC.

Policy di endpoint

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

Stati dell'endpoint

Quando crei un endpoint VPC, il servizio endpoint riceve una richiesta di connessione. Il provider di servizi può accettare o rifiutare tale richiesta. Se il provider di servizi accetta la richiesta, l'utente del servizio può utilizzare l'endpoint VPC nel momento in cui questo passa allo stato `Available`.

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

- `PendingAcceptance`: la richiesta di connessione è in sospeso. Questo è lo stato iniziale se le richieste vengono accettate manualmente.
- `Pending`: il provider di servizi ha accettato la richiesta di connessione. Questo è lo stato iniziale se le richieste vengono accettate automaticamente. L'endpoint VPC torna in questo stato se l'utente del servizio modifica l'endpoint VPC.
- `Available`: l'endpoint VPC 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`: non è possibile rendere disponibile l'endpoint VPC.
- `Deleting`: è in corso l'eliminazione dell'endpoint VPC stabilità dall'utente del servizio.
- `Deleted`: l'endpoint VPC è eliminato.

AWS PrivateLink connessioni

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

Con un endpoint VPC di interfaccia, gli utenti del servizio possono utilizzare le policy di endpoint per controllare quali principali IAM possono usare l'endpoint VPC per accedere al servizio endpoint.

Zone ospitate private

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

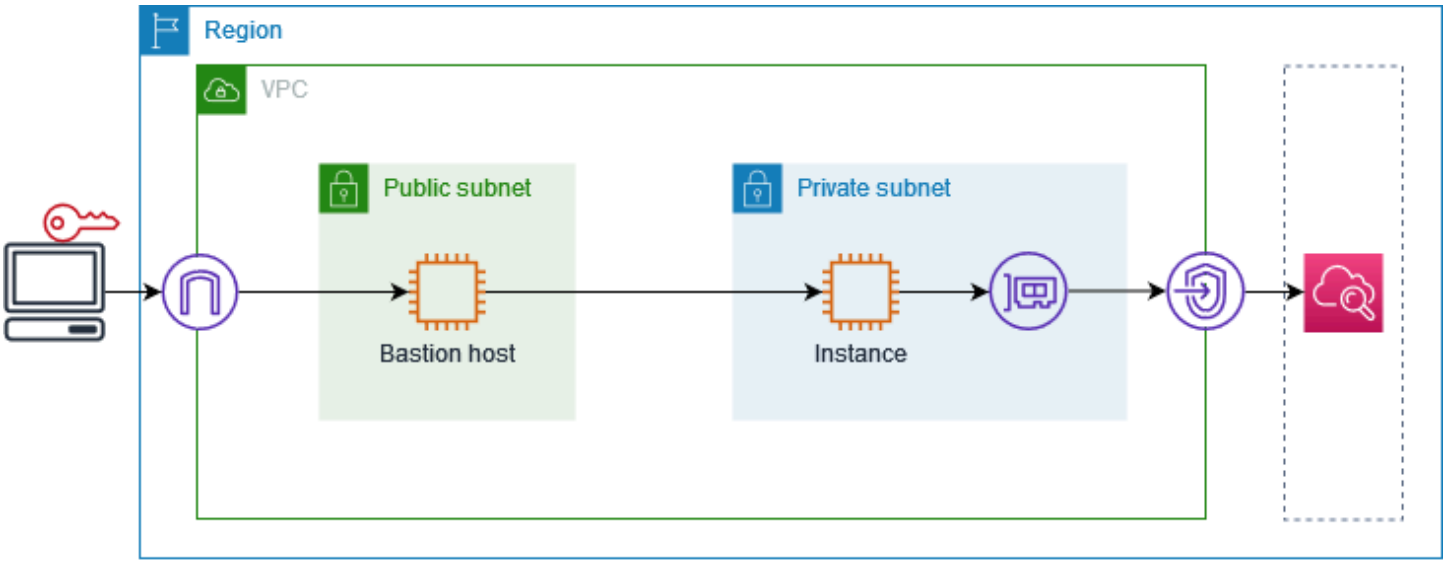
Puoi configurare Amazon Route 53 per instradare il traffico di dominio verso un endpoint VPC. Per ulteriori informazioni, consulta la pagina Routing del traffico a un endpoint VPC utilizzando il proprio nome dominio.

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

Inizia con AWS PrivateLink

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

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



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

Attività

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

Fase 1: creazione di un VPC con sottoreti

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

Per creare il VPC

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Seleziona Crea VPC.
3. Per Resources to create (Risorse da creare), scegli VPC and more (VPC e altro).
4. Per Name tag auto-generation (Generazione automatica di tag nome), immetti un nome per il VPC.
5. Per configurare le sottoreti, procedi come segue:
    a. Per Number of Availability Zones (Numero di zone di disponibilità), scegli 1 o 2, a seconda delle tue esigenze.
    b. Per Number of public subnets (Numero di sottoreti pubbliche), assicurati di avere una sottorete pubblica per zona di disponibilità.
    c. Per Number of private subnets (Numero di sottoreti private), assicurati di avere una sottorete privata per ogni zona di disponibilità.
6. Seleziona Crea VPC.

Fase 2: avvio delle istanze

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

Prerequisiti

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

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

Per avviare l'host bastione

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

Per avviare l'istanza

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

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

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

Fase 3: Verifica CloudWatch l'accesso

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

Per testare l'accesso CloudWatch

1. Dal computer, aggiungi la coppia di chiavi all'agente SSH tramite 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. Eseguite il comando CloudWatch list-metrics sull'istanza come segue. Per l'opzione `--region`, specifica la regione in cui hai creato il VPC.

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

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

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

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

Fase 4: Creare un endpoint VPC a cui accedere CloudWatch

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

Prerequisito

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

Per creare un endpoint VPC per CloudWatch

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

Fase 5: test dell'endpoint VPC

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

Per testare l'endpoint VPC

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

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

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

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

Se la richiesta scade, verifica quanto segue:

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

Fase 6: pulizia

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

Per terminare le istanze

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

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

Per eliminare l'endpoint VPC

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

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

Accesso Servizi AWS tramite AWS PrivateLink

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

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

Prezzi

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

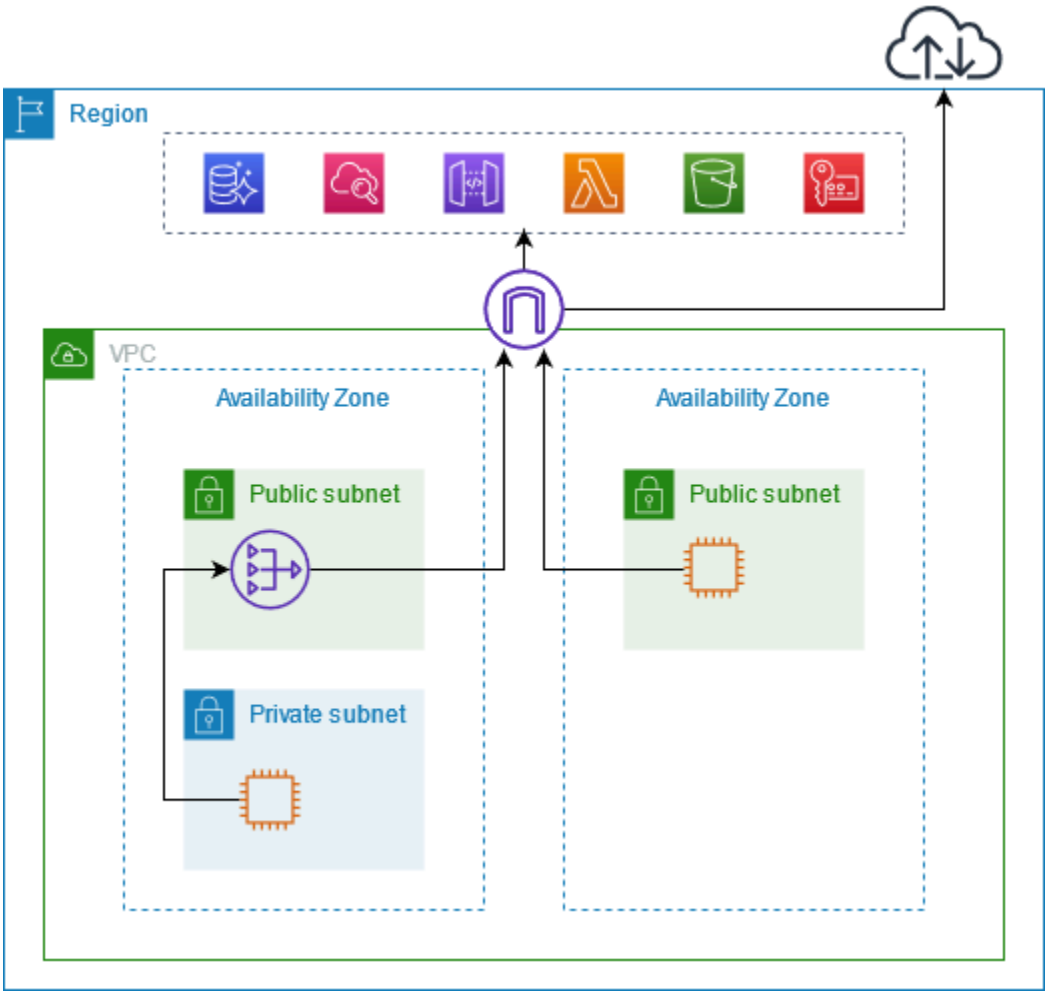
Indice

Panoramica

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

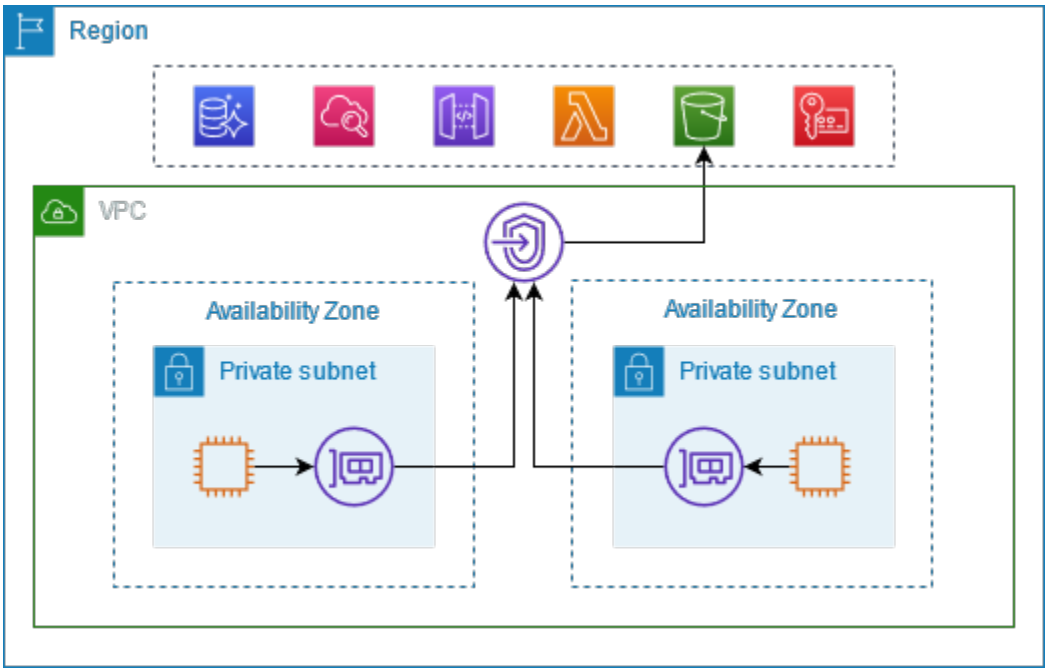
Accesso tramite endpoint del servizio pubblico

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



Connect tramite AWS PrivateLink

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



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

Hostname DNS

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

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

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

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

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

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

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

I nomi DNS zonali sono caratterizzati dalla sintassi seguente:

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

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

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

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

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

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

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

Risoluzione DNS

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

DNS privato

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

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

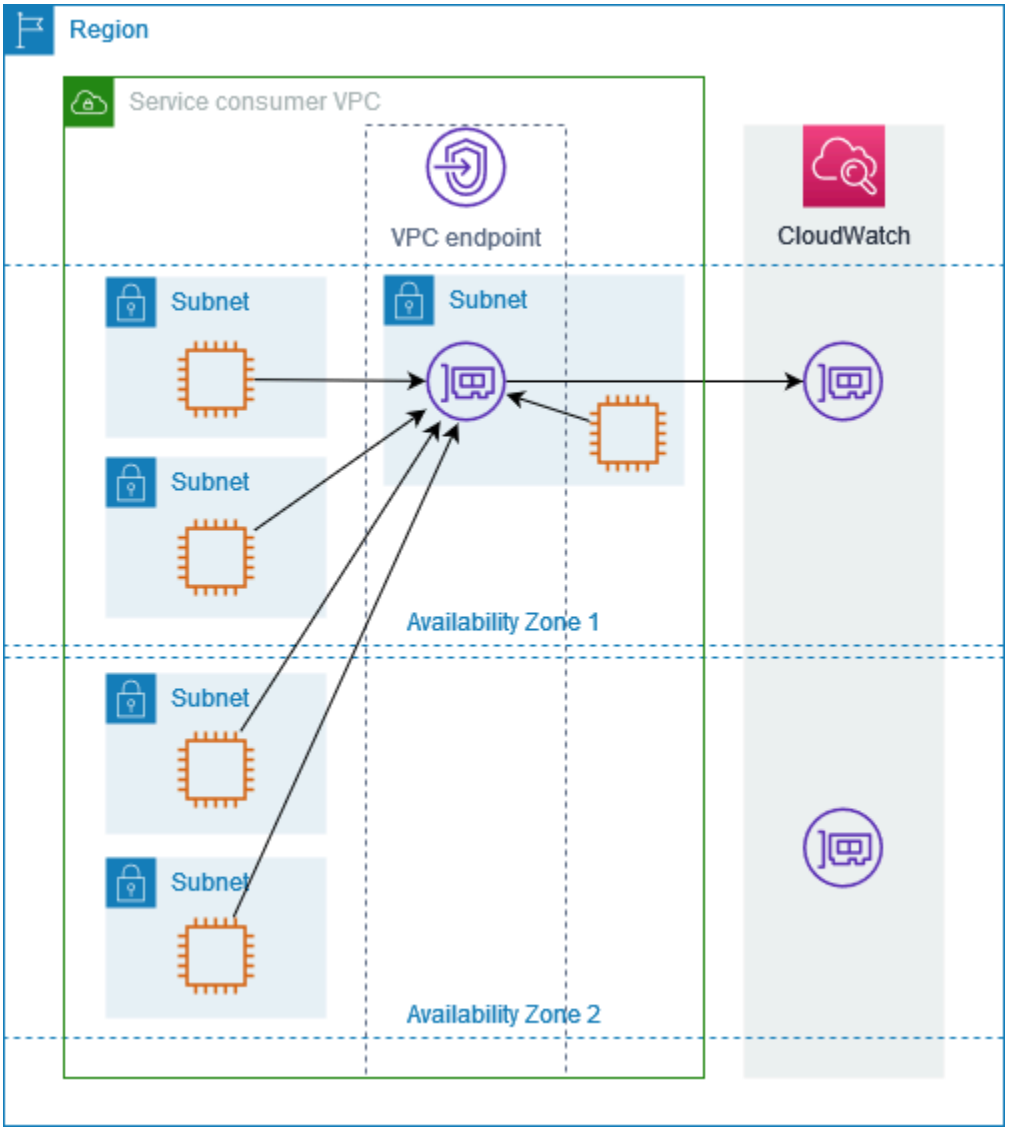
Sottoreti e zone di disponibilità

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

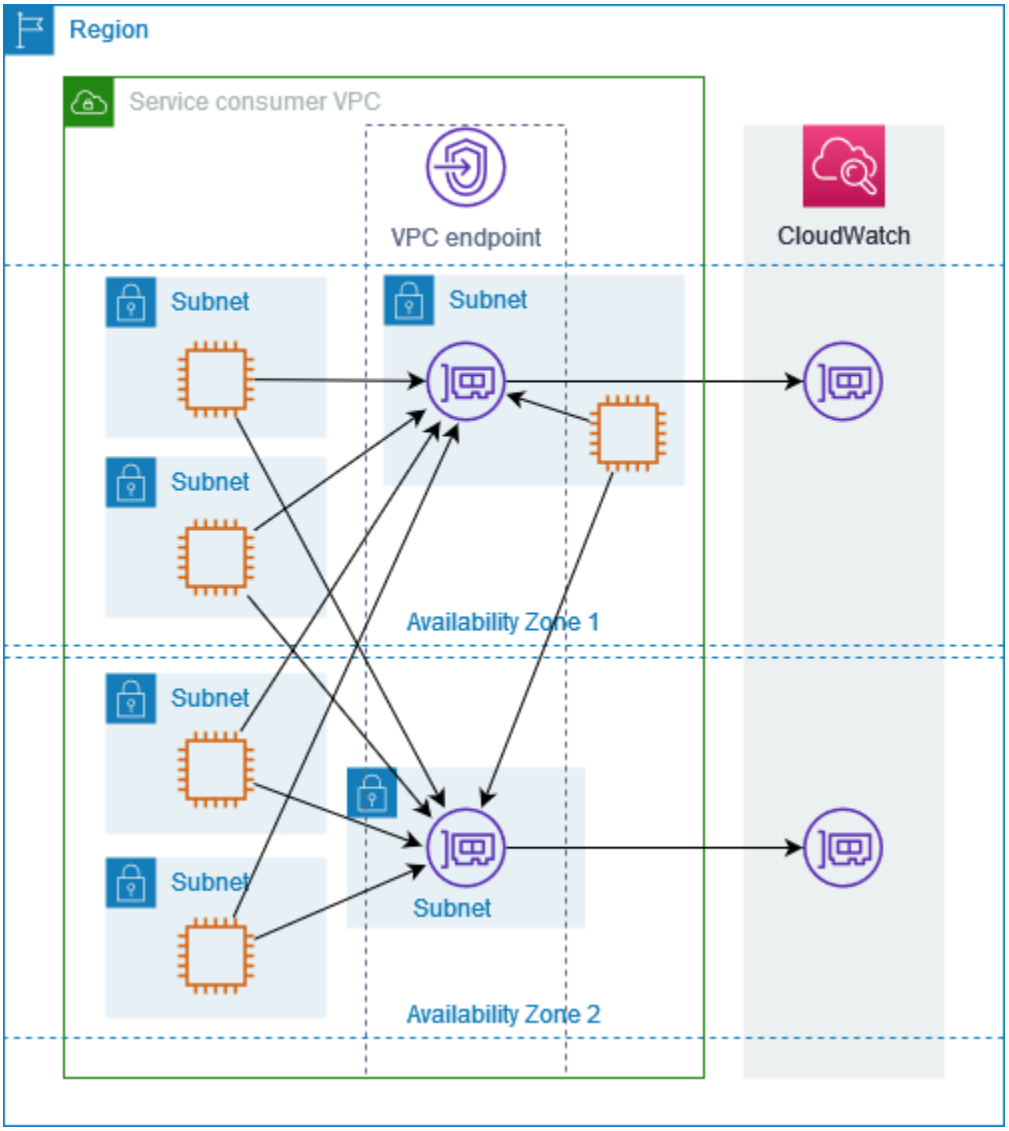
In un ambiente di produzione, per un'elevata disponibilità e resilienza, consigliamo quanto segue:

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

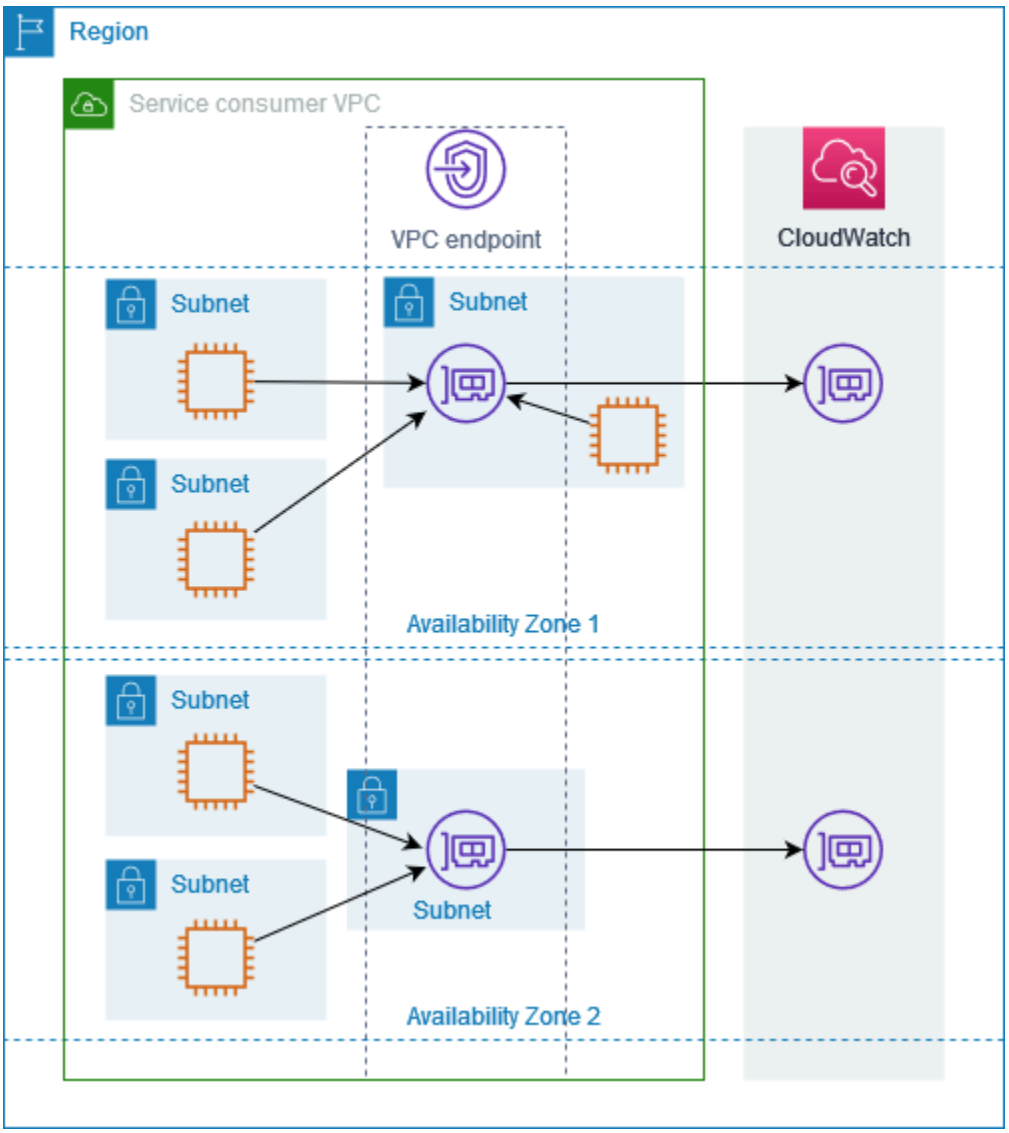
Il diagramma seguente mostra un endpoint VPC per CloudWatch Amazon con un'interfaccia di rete endpoint in un'unica zona di disponibilità. Quando una risorsa in qualsiasi sottorete del VPC accede ad CloudWatch Amazon utilizzando il suo endpoint pubblico, risolviamo il traffico all'indirizzo IP dell'interfaccia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



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



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



Tipi di indirizzi IP

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

Requisiti per abilitare IPv6 per un endpoint dell'interfaccia

- Servizio AWS Deve rendere disponibili i propri endpoint di servizio tramite 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: consente di assegnare indirizzi IPv4 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4.
- IPv6: consente di assegnare indirizzi IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono sottoreti solo IPv6.
- Dualstack: consente di assegnare sia indirizzi IPv4 che IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e IPv6.

Se un endpoint VPC dell'interfaccia supporta IPv4, le interfacce di rete dell'endpoint presentano indirizzi IPv4. Se un endpoint VPC dell'interfaccia supporta IPv6, le interfacce di rete dell'endpoint presentano indirizzi IPv6. L'indirizzo IPv6 per un'interfaccia di rete dell'endpoint non è raggiungibile da Internet. Se si descrive un'interfaccia di rete dell'endpoint con un indirizzo IPv6, l'opzione `denyAllIgwTraffic` sarà abilitata.

Servizi AWS che si integrano con AWS PrivateLink

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

Scegli il link nella Servizio AWScolonna per visualizzare la documentazione relativa ai servizi che si integrano con AWS PrivateLink. La colonna Nome servizio contiene il nome del servizio specificato alla creazione dell'endpoint VPC dell'interfaccia o indica il servizio che gestisce l'endpoint.

Servizio AWS	Nome servizio
Access Analyzer	com.amazonaws.*region*.access-analyzer
AWS Account Management	com.amazonaws.*region*.account
Gateway Amazon API	com.amazonaws.*region*.execute-api
AWS AppConfig	com.amazonaws.*region*.appconfig
	com.amazonaws.*region*.appconfigdata
AWS App Mesh	com.amazonaws.*region*.appmesh

Servizio AWS	Nome servizio
	com.amazonaws. *regione.* appmesh-envoy-management
AWS App Runner	com.amazonaws.*region*.apprunner
Servizi AWS App Runner	com.amazonaws.*region*.apprunner.requests
Application Auto Scaling	com.amazonaws.*region*.application-autoscaling
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*.athena
AWS Audit Manager	com.amazonaws.*region*.auditmanager
Amazon Aurora	com.amazonaws.*region*.rds
AWS Auto Scaling	com.amazonaws.*region*.autoscaling-plans
AWS Scambio di dati B2B	com.amazonaws.*region*.b2bi
AWS Backup	com.amazonaws.*region*.backup
	com.amazonaws.*region*.backup-gateway
AWS Batch	com.amazonaws.*region*.batch
Amazon Bedrock	com.amazonaws.*region*.bedrock
	com.amazonaws. *regione .bedrock-agent*
	com.amazonaws. *regione.* bedrock-agent-runtime

Servizio AWS	Nome servizio
	com.amazonaws.*region*.bedrock-runtime
AWS Billing Conductor	com.amazonaws.*region*.billingconductor
Amazon Braket	com.amazonaws.*region*.braket
AWS Clean Rooms	com.amazonaws.*region*.cleanrooms
AWS Camere pulite ML	com.amazonaws. *regione .cleanrooms-ml*
AWS Cloud Control API	com.amazonaws.*region*.cloudcontrolapi
	com.amazonaws.*region*.cloudcontrolapi-fips
Directory del cloud Amazon	com.amazonaws.*region*.clouddirectory
AWS CloudFormation	com.amazonaws.*region*.cloudformation
AWS CloudHSM	com.amazonaws.*region*.cloudhsmv2
AWS Cloud Map	com.amazonaws.*region*.servicediscovery
	com.amazonaws.*region*.servicediscovery-fips
	com.amazonaws.*region*.data-servicediscovery
	com.amazonaws. *regione.* data-servicediscovery-fips
AWS CloudTrail	com.amazonaws.*region*.cloudtrail
Amazon CloudWatch	com.amazonaws.*region*.evidently
	com.amazonaws.*region*.evidently-dataplane
	com.amazonaws.*region*.monitoring
	com.amazonaws.*region*.rum
	com.amazonaws.*region*.rum-dataplane

Servizio AWS	Nome servizio
	com.amazonaws.*region*.synthetics
CloudWatch Eventi Amazon	com.amazonaws.*region*.events
CloudWatch Registri Amazon	com.amazonaws.*region*.logs
Monitoraggio CloudWatch di rete Amazon	com.amazonaws. *regione. networkmonitor*
AWS CodeArtifact	com.amazonaws.*region*.codeartifact.api
	com.amazonaws.*region*.codeartifact.repositories
AWS CodeBuild	com.amazonaws.*region*.codebuild
	com.amazonaws.*region*.codebuild-fips
AWS CodeCommit	com.amazonaws.*region*.codecommit
	com.amazonaws.*region*.codecommit-fips
	com.amazonaws.*region*.git-codecommit
	com.amazonaws. *regione.* git-codecommit-fips
AWS CodeConnections	com.amazonaws. *regione .codeconnections.api*
	com.amazonaws.*region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws.*region*.codedeploy
	com.amazonaws. *regione.* codedeploy-commands-secure
Amazon CodeGuru Profiler	com.amazonaws.*region*.codeguru-profiler
CodeGuru Revisore Amazon	com.amazonaws.*region*.codeguru-reviewer

Servizio AWS	Nome servizio
AWS CodePipeline	com.amazonaws.*region*.codepipeline
Amazon CodeWhisperer	com.amazonaws.*regione*.codewhisperer
Amazon Comprehend	com.amazonaws.*region*.comprehend
Amazon Comprehend Medical	com.amazonaws.*region*.comprehendmedical
AWS Config	com.amazonaws.*region*.config
Amazon Connect	com.amazonaws.*region*.app-integrations
	com.amazonaws.*region*.cases
	com.amazonaws.*region*.connect-campaigns
	com.amazonaws.*region*.profile
	com.amazonaws.*region*.voiceid
	com.amazonaws.*region*.wisdom
AWS Connector Service	com.amazonaws.*region*.awsconnector
AWS Catalogo di controllo	com.amazonaws. *regione.controlcatalog*
AWS Data Exchange	com.amazonaws.*region*.dataexchange
AWS Database Migration Service	com.amazonaws.*region*.dms
	com.amazonaws.*region*.dms-fips
AWS DataSync	com.amazonaws.*region*.datasync
Amazon DataZone	com.amazonaws.*region*.datazone
AWS Deadline Cloud	com.amazonaws. *regione .deadline.manageme nt*

Servizio AWS	Nome servizio
	com.amazonaws. *regione .deadline.scheduling*
Amazon DevOps Guru	com.amazonaws.*region*.devops-guru
AWS Directory Service	com.amazonaws.*region*.ds
Amazon DynamoDB	com.amazonaws. *regione .dynamodb*
API dirette di Amazon EBS	com.amazonaws.*region*.ebs
Amazon EC2	com.amazonaws.*region*.ec2
Dimensionamento automatico Amazon EC2	com.amazonaws.*region*.autoscaling
EC2 Image Builder	com.amazonaws.*region*.imagebuilder
Amazon ECR	com.amazonaws.*region*.ecr.api
	com.amazonaws.*region*.ecr.dkr
Amazon ECS	com.amazonaws.*region*.ecs
	com.amazonaws.*region*.ecs-agent
	com.amazonaws.*region*.ecs-telemetry
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*.elasticfilesystem

Servizio AWS	Nome servizio
	com.amazonaws.*region*.elasticfilesystem-fips
Amazon Elastic Inference	com.amazonaws.*region*.elastic-inference.runtime
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing
Amazon ElastiCache	com.amazonaws.*region*.elasticache
	com.amazonaws.*region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws.*region*.mediaconnect
Amazon EMR	com.amazonaws.*region*.elasticmapreduce
Amazon EMR su EKS	com.amazonaws.*region*.emr-containers
Amazon EMR Serverless	com.amazonaws.*region*.emr-serverless
Amazon EMR WAL	com.amazonaws. *regione .emrwal.prod*
AWS Entity Resolution	com.amazonaws.*region*.entityresolution
Amazon EventBridge	com.amazonaws.*region*.events
AWS Fault Injection Service	com.amazonaws.*region*.fis
Amazon FinSpace	com.amazonaws.*region*.finspace
	com.amazonaws.*region*.finspace-api
Amazon Forecast	com.amazonaws.*region*.forecast
	com.amazonaws.*region*.forecastquery
	com.amazonaws.*region*.forecast-fips
	com.amazonaws.*region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws.*region*.frauddetector

Servizio AWS	Nome servizio
Amazon FSx	com.amazonaws.*region*.fsx
	com.amazonaws.*region*.fsx-fips
AWS Glue	com.amazonaws.*region*.glue
AWS Glue DataBrew	com.amazonaws.*region*.databrew
Grafana gestito da Amazon	com.amazonaws.*region*.grafana
	com.amazonaws.*region*.grafana-workspace
AWS Ground Station	com.amazonaws.*region*.groundstation
Amazon GuardDuty	com.amazonaws.*region*.guardduty-data
	com.amazonaws. *regione.* guardduty-data-fips
AWS HealthImaging	com.amazonaws.*regione*.medical-imaging
	com.amazonaws. *regione.* runtime-medical-imaging
AWS HealthLake	com.amazonaws.*region*.healthlake
IAM Identity Center	com.amazonaws.*region*.identitystore
IAM Roles Anywhere	com.amazonaws.*region*.rolesanywhere
Amazon Inspector	com.amazonaws.*region*.inspector2
AWS IoT Core	com.amazonaws.*region*.iot.data
	com.amazonaws.*region*.iot.credentials
	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

Servizio AWS	Nome servizio
	com.amazonaws.*region*.lorawan.cups
	com.amazonaws.*region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws.*region*.iotfleetwise
AWS IoT Greengrass	com.amazonaws.*region*.greengrass
AWS IoT RoboRunner	com.amazonaws.*region*.iotroborunner
AWS IoT SiteWise	com.amazonaws.*region*.iotsitewise.api
	com.amazonaws.*region*.iotsitewise.data
AWS IoT TwinMaker	com.amazonaws.*region*.iottwinmaker.api
	com.amazonaws.*region*.iottwinmaker.data
Amazon Kendra	com.amazonaws.*region*.kendra
	aws.api.*region*.kendra-ranking
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
Amazon Data Firehose	com.amazonaws.*region*.kinesis-firehose
Flusso di dati Amazon Kinesis	com.amazonaws.*region*.kinesis-streams
AWS Lake Formation	com.amazonaws.*region*.lakeformation
AWS Lambda	com.amazonaws.*region*.lambda
Amazon Lex	com.amazonaws.*region*.models-v2-lex

Servizio AWS	Nome servizio
	com.amazonaws.*region*.runtime-v2-lex
AWS License Manager	com.amazonaws.*region*.license-manager
	com.amazonaws. *regione.* license-manager-fips
	com.amazonaws. *regione.* license-manager-user-subscriptions
Amazon Lookout per le apparecchiature	com.amazonaws.*region*.lookoutequipment
Amazon Lookout per le metriche	com.amazonaws.*region*.lookoutmetrics
Amazon Lookout per Vision	com.amazonaws.*region*.lookoutvision
Amazon Macie	com.amazonaws.*region*.macie2
AWS Mainframe Modernization	com.amazonaws.*region*.m2
Blockchain gestita da Amazon	com.amazonaws.*regione*.managedblockchain-query
	com.amazonaws.*regione*.managedblockchain.bitcoin.mainnet
	com.amazonaws.*regione*.managedblockchain.bitcoin.testnet
Amazon Managed Service per Prometheus	com.amazonaws.*region*.aps
	com.amazonaws.*region*.aps-workspaces
Flussi di lavoro gestiti da Amazon per Apache Airflow	com.amazonaws.*region*.airflow.api
	com.amazonaws.*region*.airflow.env
	com.amazonaws.*region*.airflow.ops
AWS Management Console	com.amazonaws.*region*.console

Servizio AWS	Nome servizio
	com.amazonaws.*region*.signin
Amazon MemoryDB per Redis	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-strategy
Analisi di Amazon Neptune	com.amazonaws.*region*.neptune-graph
Amazon Nimble Studio	com.amazonaws.*region*.nimble
AWS HealthOmics	com.amazonaws.*region*.analytics-omics
	com.amazonaws. *regione.* control-storage-omics
	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.workflows-omics
OpenSearch Servizio Amazon	Questi endpoint sono gestiti dai servizi
AWS Organizations	com.amazonaws. *regione. organizzazioni*
	com.amazonaws. *regione .organizations-fips*
AWS Panorama	com.amazonaws.*region*.panorama
AWS Crittografia dei pagamenti	com.amazonaws.*region*.payment-cryptography.controlplane

Servizio AWS	Nome servizio
	com.amazonaws.*region*.payment-cryptography.datap lane
Amazon Personalize	com.amazonaws.*region*.personalize
	com.amazonaws.*region*.personalize-events
	com.amazonaws.*region*.personalize-runtime
Catena di approvvigionamento di AWS	com.amazonaws. *regione .scn*
Amazon Pinpoint	com.amazonaws.*region*.pinpoint
	com.amazonaws. *regione.* pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws.*region*.polly
AWS 5G privato	com.amazonaws.*region*.private-networks
AWS Private Certificate Authority	com.amazonaws.*region*.acm-pca
	com.amazonaws. *regione.* pca-connector-ad
AWS Proton	com.amazonaws.*region*.proton
Amazon QLDB	com.amazonaws.*region*.qldb.session
Amazon QuickSight	com.amazonaws. *regione.quicksight-website*
Amazon RDS	com.amazonaws.*region*.rds
API dati di Amazon RDS	com.amazonaws.*region*.rds-data
AWS re:Post privato	com.amazonaws. *regione .repostspace*
Amazon Redshift	com.amazonaws.*region*.redshift
	com.amazonaws.*region*.redshift-fips

Servizio AWS	Nome servizio
API dati di Amazon Redshift	com.amazonaws.*region*.redshift-data
Amazon Rekognition	com.amazonaws.*region*.rekognition
	com.amazonaws.*region*.rekognition-fips
	com.amazonaws.*region*.streaming-rekognition
	com.amazonaws. *regione.* streaming-rekognition-fips
AWS RoboMaker	com.amazonaws.*region*.robomaker
Amazon S3	com.amazonaws.*region*.s3
Punti di accesso multi-Regione di Amazon S3	com.amazonaws.s3-global.accesspoint
Amazon S3 su Outposts	com.amazonaws.*region*.s3-outposts
Amazon SageMaker	aws.sagemaker.*region*.notebook
	aws.sagemaker.*region*.studio
	com.amazonaws.*region*.sagemaker.api
	com.amazonaws.*region*.sagemaker.featurestore-runtime
	com.amazonaws.*region*.sagemaker.metrics
	com.amazonaws.*region*.sagemaker.runtime
	com.amazonaws.*region*.sagemaker.runtime-fips
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
AWS Security Hub	com.amazonaws.*region*.securityhub
AWS Security Token Service	com.amazonaws.*region*.sts

Servizio AWS	Nome servizio
Catalogo dei servizi	com.amazonaws.*region*.servicecatalog
	com.amazonaws.*region*.servicecatalog-appregistry
Amazon SES	com.amazonaws.*region*.email-smtp
AWS SimSpace Weaver	com.amazonaws.*region*.simspaceweaver
AWS Snow Device Management	com.amazonaws. *regione.* 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*.states
	com.amazonaws.*region*.sync-states
AWS Storage Gateway	com.amazonaws.*region*.storagegateway
AWS Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssm-contacts
	com.amazonaws.*region*.ssm-incidents
	com.amazonaws.*region*.ssmmessages
AWS Costruttore di reti di telecomunicazioni	com.amazonaws.*region*.tnb
Amazon Textract	com.amazonaws.*region*.textract
	com.amazonaws.*region*.textract-fips

Servizio AWS	Nome servizio
Amazon Timestream	com.amazonaws.*region*.timestream.ingest-*cell*
	com.amazonaws.*region*.timestream.query-*cell*
Amazon Timestream per InfluxDB	com.amazonaws. *regione* .*timestream-influxdb*
Amazon Transcribe	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
Amazon Transcribe Medical	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
AWS Transfer for SFTP	com.amazonaws.*region*.transfer
	com.amazonaws.*region*.transfer.server
Amazon Translate	com.amazonaws.*region*.translate
AWS Trusted Advisor	com.amazonaws.*region*.trustedadvisor
Autorizzazioni verificate da Amazon	com.amazonaws.*region*.verifiedpermissions
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice
Amazon WorkSpaces	com.amazonaws.*region*.workspaces
Amazon WorkSpaces Thin Client	com.amazonaws. *regione* .*thinclient.api*
AWS X-Ray	com.amazonaws.*region*.xray

Visualizzazione dei nomi del Servizio AWS disponibili

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

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

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

Di seguito è riportato un output di esempio:

```
[
    "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",
    "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.deadline.management",
    "com.amazonaws.us-east-1.deadline.scheduling",
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.ebs",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.elastic-inference.runtime",
    "com.amazonaws.us-east-1.email-smtp",
    "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.nimble",
    "com.amazonaws.us-east-1.organizations",
    "com.amazonaws.us-east-1.redshift-data",
    "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 describe-vpc-endpoint-servicescomando seguente per visualizzare l'accesso a Servizi AWS cui è possibile accedere tramite 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",
    "com.amazonaws.us-east-1.athena",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.timestream-influxdb"
]
```

Accedere e Servizio AWS utilizzare un endpoint VPC di interfaccia

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

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

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

Indice

Prerequisiti

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

Creare un endpoint VPC

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

Per creare un endpoint di interfaccia per un Servizio AWS

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Per Service category (Categoria servizio), scegli Servizi AWS.
5. Per 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 al Servizio AWS.
7. Se nel passaggio 5 hai selezionato il nome del servizio per Amazon S3 e desideri configurare il supporto DNS privato, seleziona Impostazioni aggiuntive, Abilita nome DNS. Quando si effettua questa selezione, viene automaticamente selezionata anche l'opzione Abilita il DNS privato solo per l'endpoint in entrata. Puoi configurare il DNS privato con un endpoint del resolver in entrata solo per gli endpoint di interfaccia per Amazon S3. Se non disponi di un endpoint gateway per Amazon S3 e selezioni Abilita il DNS privato solo per l'endpoint in entrata, riceverai un errore quando tenterai il passaggio finale di questa procedura.

   Se nel passaggio 5 hai selezionato il nome del servizio per qualsiasi servizio diverso da Amazon S3, Impostazioni aggiuntive, Abilita nome DNS sarà già selezionato. Ti consigliamo di mantenere l'impostazione predefinita.
8. Per Subnets (Sottoreti), seleziona una sottorete per ogni zona di disponibilità dalla quale accederai al Servizio AWS. Non è possibile selezionare più sottoreti dalla stessa zona di disponibilità. Viene creata un'interfaccia di rete dell'endpoint in ciascuna sottorete selezionata. 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 Imposta indirizzi IP e inserisci un indirizzo IPv4 dall'intervallo di indirizzi di sottorete. Se il servizio endpoint supporta IPv6, puoi anche inserire un indirizzo IPv6 dall'intervallo di indirizzi di sottorete.
9. Per IP address type (Tipo di indirizzo IP), seleziona una delle opzioni seguenti:

   - IPv4: consente di assegnare indirizzi IPv4 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e il servizio accetta richieste IPv4.
   - IPv6: consente di assegnare indirizzi IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono sottoreti solo IPv6 e il servizio accetta richieste IPv6.

- Dualstack: consente di assegnare sia indirizzi IPv4 che IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e IPv6 e il servizio accetta sia richieste IPv4 e IPv6.

10. Per Gruppi di sicurezza, seleziona i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint per l'endpoint VPC. Per impostazione predefinita, per il VPC viene associato il gruppo di sicurezza predefinito.
11. Per Policy, seleziona Full access (Accesso completo) per consentire tutte le operazioni da parte di tutti i principali su tutte le risorse dell'endpoint VPC. In caso contrario, seleziona Custom (Personalizza) per allegare una policy dell'endpoint VPC in grado di verificare le autorizzazioni di cui dispongono i principali per eseguire operazioni sulle risorse dell'endpoint VPC. Questa opzione è disponibile solo se il servizio supporta le policy dell'endpoint VPC. 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-EC2 VpcEndpoint (strumenti per Windows) PowerShell

Sottoreti condivise

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

Configurazione di un endpoint dell'interfaccia

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

Attività

- Aggiunta o rimozione di sottoreti
- Associazione dei gruppi di sicurezza
- Modifica della policy di endpoint VPC

- Abilitazione dei nomi DNS privati
- Gestione dei tag

Aggiunta o rimozione di sottoreti

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

Per modificare le sottoreti utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (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 Imposta indirizzi IP e inserisci un indirizzo IPv4 dall'intervallo di indirizzi di sottorete. Se il servizio endpoint supporta IPv6, puoi anche inserire un indirizzo IPv6 dall'intervallo di indirizzi di sottorete.

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

Per modificare le sottoreti utilizzando la riga di comando

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

Associazione dei gruppi di sicurezza

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

Per modificare i gruppi di sicurezza utilizzando la console

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

Per modificare i gruppi di sicurezza utilizzando la riga di comando

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

Modifica della policy di endpoint VPC

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

Per modificare la policy di endpoint usando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (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. Selezionare Salva.

Per modificare la policy di endpoint utilizzando la riga di comando

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

Abilitazione dei nomi DNS privati

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

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

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

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

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

Gestione dei tag

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

Per gestire i tag utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (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. Selezionare 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

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

Creare una notifica SNS

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

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

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

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

- create-vpc-endpoint-connection-notifica ()AWS CLI
- New-EC2 VpcEndpointConnectionNotification (strumenti per Windows) PowerShell

Aggiungere una policy di accesso

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

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

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

Per eliminare un endpoint dell'interfaccia tramite la console

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

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

- delete-vpc-endpoints (AWS CLI)
- Remove-ec2 VpcEndpoint (strumenti per Windows) PowerShell

Endpoint gateway

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

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

- Tipi di endpoint VPC per Amazon S3

- Tipi di endpoint VPC per Amazon DynamoDB

Prezzi

L'utilizzo di endpoint gateway non comporta costi supplementari.

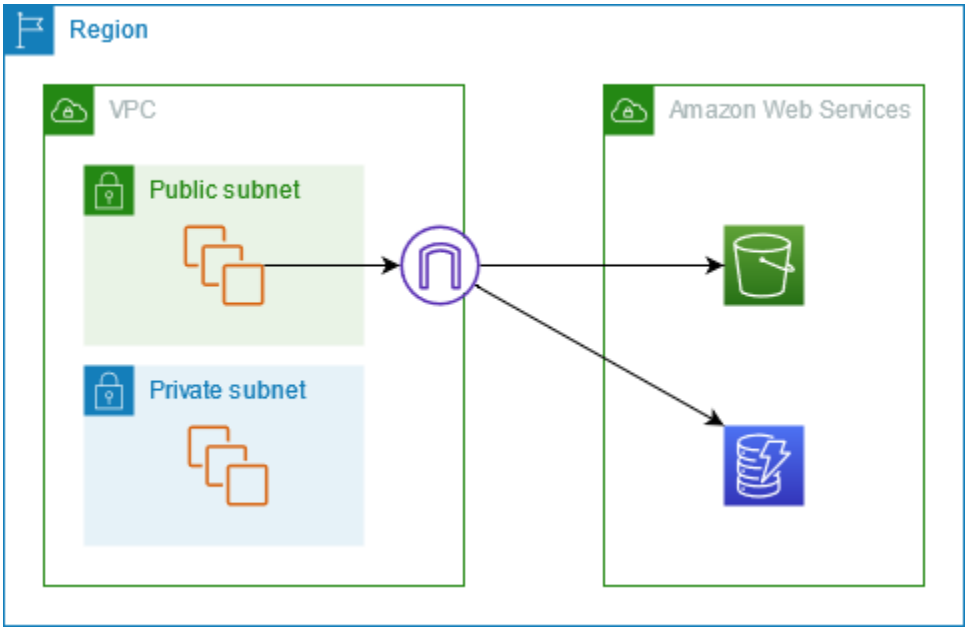
Indice

Panoramica

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

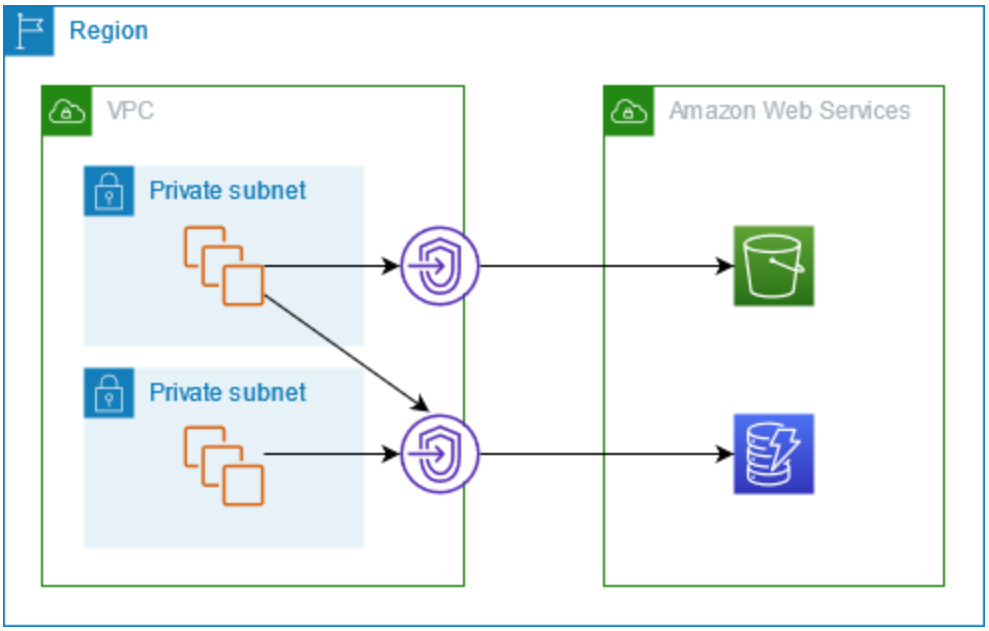
Accesso tramite un gateway Internet

Il diagramma seguente mostra il modo in cui le istanze accedono ad Amazon S3 e DynamoDB tramite i loro endpoint di servizio pubblico. Il traffico verso Amazon S3 o DynamoDB da un'istanza presente in una sottorete pubblica viene instradato al gateway Internet del VPC e successivamente al servizio. Le istanze presenti in una sottorete privata non possono inviare traffico ad Amazon S3 o DynamoDB, perché per definizione le sottoreti private non hanno route verso un gateway Internet. Per abilitare le istanze nella sottorete privata per inviare il traffico ad Amazon S3 o DynamoDB, è necessario aggiungere un dispositivo NAT alla sottorete pubblica e instradare il traffico nella sottorete privata al dispositivo NAT. Sebbene il traffico verso Amazon S3 o DynamoDB attraversi il gateway Internet, non esce dalla rete. AWS



Accesso tramite un endpoint gateway

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



Routing

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

Destinazione	Target
prefix_list_id	*gateway_endpoint_id*

Considerazioni

- Puoi esaminare le route dell'endpoint che aggiungiamo alla tabella di instradamento, ma non puoi modificarle o eliminarle. Per aggiungere una route dell'endpoint a una tabella di instradamento, associala all'endpoint gateway. La route dell'endpoint viene eliminata quando si dissocia la tabella di instradamento dall'endpoint gateway o quando si rimuove l'endpoint gateway.
- Tutte le istanze nelle sottoreti associate a una tabella di instradamento, a sua volta associata a un endpoint gateway, utilizzano automaticamente l'endpoint gateway per accedere al servizio. Le istanze presenti nelle sottoreti non associate a queste tabelle di instradamento utilizzano l'endpoint del servizio pubblico, non l'endpoint gateway.
- Una tabella di instradamento può presentare sia una route dell'endpoint verso Amazon S3 sia una route dell'endpoint verso DynamoDB. È possibile avere route dell'endpoint che fanno riferimento allo stesso servizio (Amazon S3 o DynamoDB) in più tabelle di instradamento. Tuttavia, non è possibile avere più route dell'endpoint per lo stesso servizio (Amazon S3 o DynamoDB) in una singola tabella di instradamento.
- La route più specifica che corrisponde al traffico viene utilizzata per determinare come istradare il traffico (corrispondenza prefisso più lungo). Per le tabelle di instradamento con una route dell'endpoint, questo significa che:
  - Se disponi di una route che invia tutto il traffico Internet (0.0.0.0/0) a un gateway Internet, la route dell'endpoint ha la precedenza per il traffico destinato al servizio (Amazon S3 o DynamoDB) nella regione corrente. Il traffico destinato a un altro utente Servizio AWS utilizza il gateway Internet.
  - Il traffico destinato al servizio (Amazon S3 o DynamoDB) in una regione diversa viene indirizzato verso il gateway Internet perché gli elenchi di prefissi sono specifici per una regione.

- Se disponi di una route che specifica l'intervallo esatto di indirizzi IP per il servizio (Amazon S3 o DynamoDB) nella stessa regione, tale route ha la precedenza sulla route dell'endpoint.

Sicurezza

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

Destinazione	Protocollo	Intervallo porte
prefix_list_id	TCP	443

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

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

Endpoint gateway per Amazon S3

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

L'utilizzo di endpoint gateway non comporta costi supplementari.

Amazon S3 supporta sia gli endpoint gateway che gli endpoint di interfaccia. Con un endpoint gateway, puoi accedere ad Amazon S3 dal tuo VPC senza richiedere un gateway Internet o

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

Indice

Considerazioni

- Un endpoint gateway è disponibile solo nella regione in cui è stato creato. Assicurati di creare l'endpoint gateway nella stessa regione dei bucket S3.
- Se utilizzi i server Amazon DNS, devi abilitare i nomi host DNS e la risoluzione DNS per il VPC. In alternativa, se utilizzi un server DNS, assicurati che le richieste destinate ad Amazon S3 vengano risolte correttamente negli indirizzi IP gestiti da AWS.
- Le regole per i gruppi di sicurezza per le istanze che accedono ad Amazon S3 tramite l'endpoint gateway devono consentire il traffico da e verso Amazon S3. Puoi fare riferimento all'ID dell'elenco dei prefissi per Amazon S3 nelle regole del gruppo di sicurezza.
- L'ACL di rete per la sottorete per le istanze che accedono ad Amazon S3 tramite l'endpoint gateway devono consentire il traffico da e verso Amazon S3. Non è possibile fare riferimento agli elenchi di prefissi nelle regole ACL di rete, ma è possibile ottenere gli intervalli di indirizzi IP per Amazon S3 dal relativo elenco di prefissi.
- Verifica se stai utilizzando un bucket S3 Servizio AWS che richiede l'accesso a un bucket S3. Ad esempio, un servizio potrebbe richiedere l'accesso a bucket che contengono file di log o potrebbe richiedere il download di driver o agenti sulle istanze EC2. In tal caso, assicurati che la policy dell'endpoint consenta alla risorsa Servizio AWS o di accedere a questi bucket utilizzando l'azione. `s3:GetObject`

- Non è possibile utilizzare la condizione `aws:SourceIp` in una policy di identità o in una policy di bucket per le richieste ad Amazon S3 che attraversano un endpoint VPC. Utilizza invece la condizione `aws:VpcSourceIp`. In alternativa, puoi utilizzare le tabelle di routing per controllare quali istanze EC2 possono accedere ad Amazon S3 tramite l'endpoint VPC.
- Gli endpoint gateway supportano solo il traffico IPv4.
- Gli indirizzi IPv4 di origine delle istanze nelle sottoreti interessate, come ricevuti da Amazon S3, passano da indirizzi IPv4 pubblici a indirizzi IPv4 privati nel VPC. Un endpoint cambia i percorsi di rete E disconnette le connessioni TCP aperte. Le connessioni precedenti che utilizzavano indirizzi IPv4 pubblici non vengono ripristinate. Ti consigliamo di non eseguire attività critiche quando crei o modifichi un endpoint; oppure di verificare che il software utilizzato sia in grado di riconnettersi automaticamente ad Amazon S3 dopo l'interruzione della connessione.
- Le connessioni endpoint non possono essere Estese all'esterno di un VPC. Le risorse sull'altro lato di una connessione VPN, di una connessione peering VPC, di un gateway di transito o di una 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. Esiste inoltre un limite di 255 endpoint gateway per VPC.

DNS privato

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

Route 53 Resolver

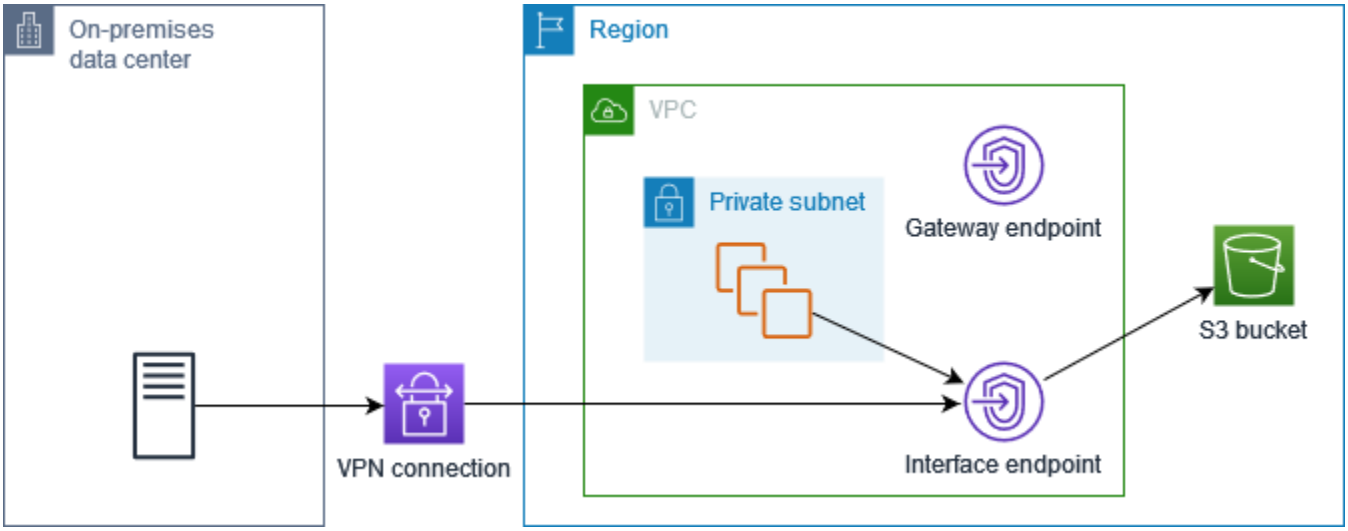
Amazon fornisce un server DNS chiamato il Route 53 Resolver per il tuo VPC. Il Route 53 Resolver risolve automaticamente i nomi di dominio VPC locali e i record in zone ospitate private. Tuttavia, non puoi utilizzare il Route 53 Resolver dall'esterno del tuo VPC. Route 53 fornisce gli endpoint e le regole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

Quando configuri l'endpoint di interfaccia per Amazon S3 per utilizzare il DNS privato solo per l'endpoint del resolver in entrata, creiamo un endpoint del resolver in entrata. L'endpoint del resolver in entrata risolve le query DNS verso Amazon S3 dagli indirizzi IP on-premise a quelli privati dell'endpoint di interfaccia. Aggiungiamo anche i record ALIAS per il Resolver Route 53 alla zona

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

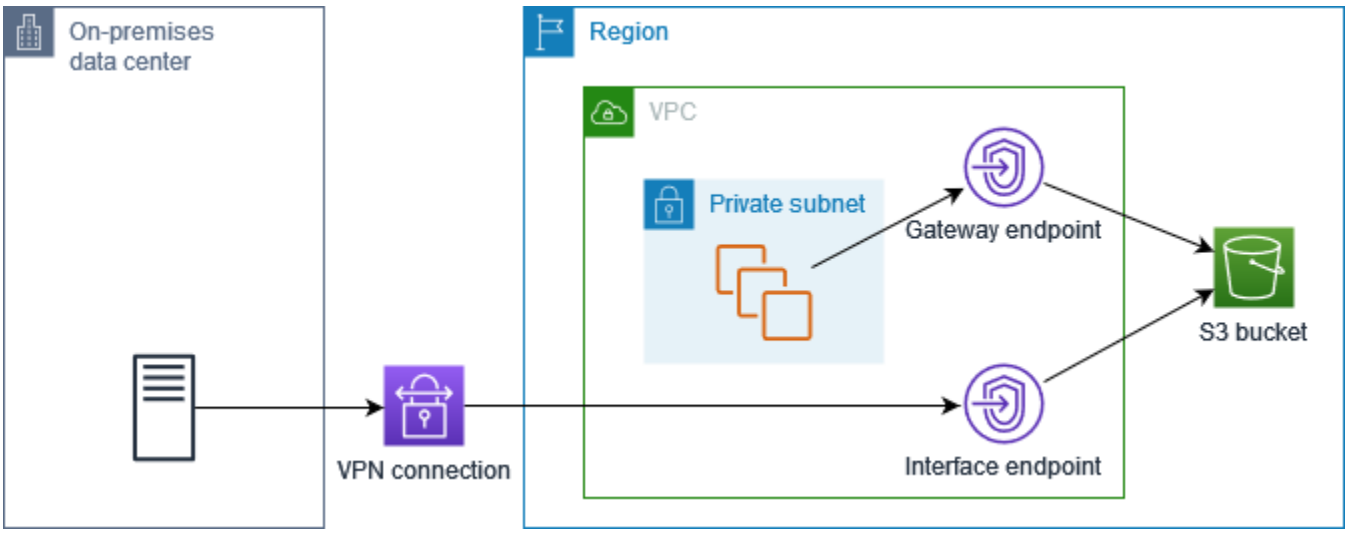
DNS privato

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



DNS privato solo per l'endpoint del resolver in entrata

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



Configura il DNS privato

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

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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Per Service category (Categoria servizio), scegli Servizi AWS.
5. Per Services (Servizi), aggiungi il filtro Type: Gateway (Tipo: Gateway) e seleziona com.amazonaws.*region*.s3.
6. In VPC, seleziona un VPC in cui creare l'endpoint.
7. In Route tables (Tabelle di instradamento), seleziona le tabelle di instradamento che devono essere utilizzate dall'endpoint. Viene aggiunta automaticamente una route che indirizza il traffico destinato per il servizio all'interfaccia di rete dell'endpoint.
8. Per Policy, seleziona Full access (Accesso completo) per consentire tutte le operazioni da parte di tutti i principali su tutte le risorse dell'endpoint VPC. In caso contrario, seleziona Custom

(Personalizza) per allegare una policy dell'endpoint VPC in grado di verificare le autorizzazioni di cui dispongono i principali per eseguire operazioni sulle risorse dell'endpoint VPC.

9. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
10. Seleziona Crea endpoint.

Per creare un endpoint gateway utilizzando la riga di comando

- create-vpc-endpoint (AWS CLI)
- VpcEndpointNew-EC2 (strumenti per Windows) PowerShell

Controllo dell'accesso tramite le policy di bucket

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

Example Esempio: limitazione dell'accesso a uno specifico endpoint

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

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

Puoi creare una policy che limiti l'accesso a intervalli di indirizzi IP specifici utilizzando la chiave aws: condition. VpcSourceIp La policy seguente nega l'accesso al bucket specificato utilizzando le azioni specificate a meno che non si utilizzi l'indirizzo IP specificato. Tieni presente che questa policy blocca l'accesso al bucket specificato utilizzando le azioni specificate tramite 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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint gateway.
4. Selezionare Actions (Operazioni), Manage route tables (Gestisci tabelle di routing).
5. Seleziona o deseleziona le tabelle di instradamento in base alle esigenze.
6. Scegli Modify route tables (Modifica le tabelle di routing).

Per associare le tabelle di instradamento utilizzando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2 VpcEndpoint (strumenti per Windows) PowerShell

Modifica della policy di endpoint VPC

Puoi modificare la policy di endpoint per un endpoint gateway, che controlla l'accesso ad Amazon S3 dal VPC, tramite l'endpoint. La policy predefinita consente l'accesso completo. Per ulteriori informazioni, consulta Policy di endpoint.

Per modificare la policy di endpoint usando la console

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

6. Selezionare Salva.

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

Example Esempio: limitazione dell'accesso a uno specifico bucket

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

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

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

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

```
{
  "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 è abilitato il DNS privato.

Per eliminare un endpoint gateway usando la console

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

2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint gateway.
4. Seleziona Actions (Operazioni), Delete VPC endpoints (Eliminazione di endpoint VPC).
5. Quando viene richiesta la conferma, immetti **`delete`**.
6. Scegli Elimina.

Per eliminare un endpoint gateway usando la riga di comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2 (strumenti per Windows) VpcEndpoint PowerShell

Endpoint gateway per Amazon DynamoDB

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

L'utilizzo di endpoint gateway non comporta costi supplementari.

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

Indice

Considerazioni

- Un endpoint gateway è disponibile solo nella regione in cui è stato creato. Assicurati di creare l'endpoint gateway nella stessa regione delle tabelle DynamoDB.
- Se utilizzi i server Amazon DNS, devi abilitare i nomi host DNS e la risoluzione DNS per il VPC. In alternativa, se utilizzi un server DNS, assicurati che le richieste destinate a DynamoDB vengano risolte correttamente negli indirizzi IP gestiti da AWS.
- Le regole per i gruppi di sicurezza per le istanze che accedono a DynamoDB tramite l'endpoint gateway devono consentire il traffico da e verso DynamoDB. Puoi fare riferimento all'ID dell'elenco dei prefissi per DynamoDB nelle regole del gruppo di sicurezza.
- L'ACL di rete per la sottorete per le istanze che accedono a DynamoDB tramite l'endpoint gateway devono consentire il traffico da e verso DynamoDB. Non è possibile fare riferimento agli elenchi di prefissi nelle regole ACL di rete, ma è possibile ottenere gli intervalli di indirizzi IP per DynamoDB dal relativo elenco di prefissi.
- Se si utilizza AWS CloudTrail per registrare le operazioni DynamoDB, i file di registro contengono gli indirizzi IP privati delle istanze EC2 nel VPC del service consumer e l'ID dell'endpoint gateway per tutte le richieste eseguite tramite l'endpoint.
- Gli endpoint gateway supportano solo il traffico IPv4.
- Gli indirizzi IPv4 di origine delle istanze nelle sottoreti interessate cambiano da indirizzi IPv4 pubblici in indirizzi IPv4 privati dal VPC. Un endpoint cambia le route di rete e disconnette le connessioni TCP aperte. Le connessioni precedenti che utilizzavano indirizzi IPv4 pubblici non vengono ripristinate. Ti consigliamo di non eseguire attività critiche quando crei o modifichi un endpoint gateway. In alternativa, verifica che il software utilizzato sia in grado di riconnettersi automaticamente a DynamoDB in caso di interruzione della connessione.
- Le connessioni endpoint non possono essere Estese all'esterno di un VPC. Le risorse sull'altro lato di una connessione VPN, di una connessione peering VPC, di un gateway di transito o di una AWS Direct Connect connessione nel VPC non possono utilizzare un endpoint gateway per comunicare con DynamoDB.
- Il tuo account ha una quota predefinita, ma modificabile, di 20 endpoint gateway per regione. Esiste inoltre un limite di 255 endpoint gateway per VPC.

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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Per Service category (Categoria servizio), scegli Servizi AWS.
5. Per Services (Servizi), aggiungi il filtro Type: Gateway (Tipo: Gateway) e seleziona com.amazonaws.*region*.dynamodb.
6. In VPC, seleziona un VPC in cui creare l'endpoint.
7. In Route tables (Tabelle di instradamento), seleziona le tabelle di instradamento che devono essere utilizzate dall'endpoint. Viene aggiunta automaticamente una route che indirizza il traffico destinato per il servizio all'interfaccia di rete dell'endpoint.
8. Per Policy, seleziona Full access (Accesso completo) per consentire tutte le operazioni da parte di tutti i principali su tutte le risorse dell'endpoint VPC. In caso contrario, seleziona Custom (Personalizza) per allegare una policy dell'endpoint VPC in grado di verificare le autorizzazioni di cui dispongono i principali per eseguire operazioni sulle risorse dell'endpoint VPC.
9. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
10. Seleziona Crea endpoint.

Per creare un endpoint gateway utilizzando la riga di comando

- create-vpc-endpoint (AWS CLI)
- New-EC2 (strumenti per Windows) VpcEndpoint PowerShell

Controllo dell'accesso utilizzando le policy IAM

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

Example Esempio: limitazione dell'accesso a uno specifico endpoint

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

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

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

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

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

Per associare le tabelle di instradamento utilizzando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- VpcEndpointEdit-EC2 (strumenti per Windows) PowerShell

Modifica della policy di endpoint VPC

Puoi modificare la policy di endpoint per un endpoint gateway, che controlla l'accesso a DynamoDB dal VPC, tramite l'endpoint. La policy predefinita consente l'accesso completo. Per ulteriori informazioni, consulta Policy di endpoint.

Per modificare la policy di endpoint usando la console

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

Per modificare un endpoint gateway usando la riga di comando

- modify-vpc-endpoint (AWS CLI)
- VpcEndpointEdit-EC2 (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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint gateway.
4. Seleziona Actions (Operazioni), Delete VPC endpoints (Eliminazione di endpoint VPC).
5. Quando viene richiesta la conferma, immetti **`delete`**.
6. Scegli Elimina.

Per eliminare un endpoint gateway usando la riga di comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2 (strumenti per Windows) VpcEndpoint PowerShell

Accedi ai prodotti SaaS tramite AWS PrivateLink

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

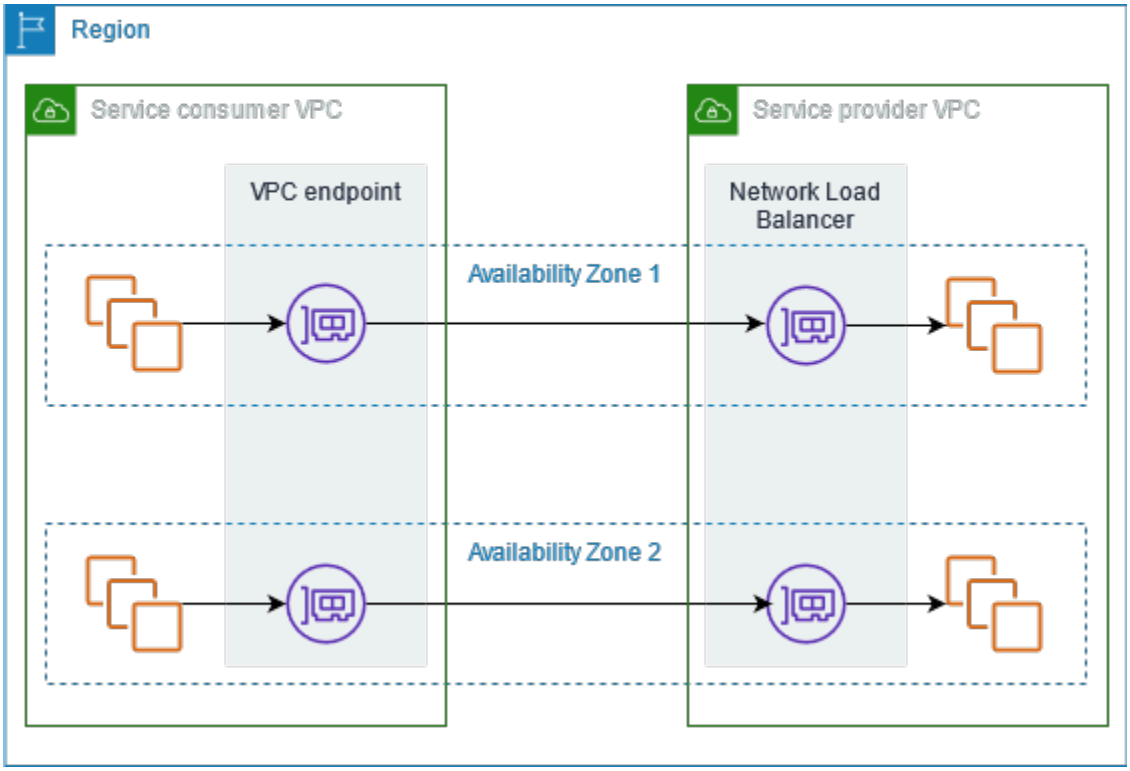
Indice

Panoramica

Puoi scoprire, acquistare ed effettuare il provisioning di prodotti SaaS con tecnologia Through. AWS PrivateLink Marketplace AWS Per ulteriori informazioni, vedere Marketplace AWS: - PrivateLink.

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

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



Creazione di un endpoint di interfaccia

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

Requisito

Iscriversi al servizio.

Per creare un endpoint di interfaccia a un servizio partener

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

   a. Per la categoria Service, scegli PrivateLink Ready Partner Services.
   b. Immetti il nome del servizio e seleziona Verify service (Verifica del servizio).
6. Per VPC, seleziona il VPC da cui accederai al prodotto.
7. Per Subnets (Sottoreti), seleziona una sottorete per la zona di disponibilità da cui accedere al prodotto.
8. In Security group (Gruppo di sicurezza), selezionare i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint. Le regole del gruppo di sicurezza devono consentire il traffico tra le risorse nel VPC e le interfacce di rete dell'endpoint.
9. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
10. Seleziona Crea endpoint.

Per configurare un endpoint di interfaccia

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

Accedi alle appliance virtuali tramite AWS PrivateLink

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

Prezzi

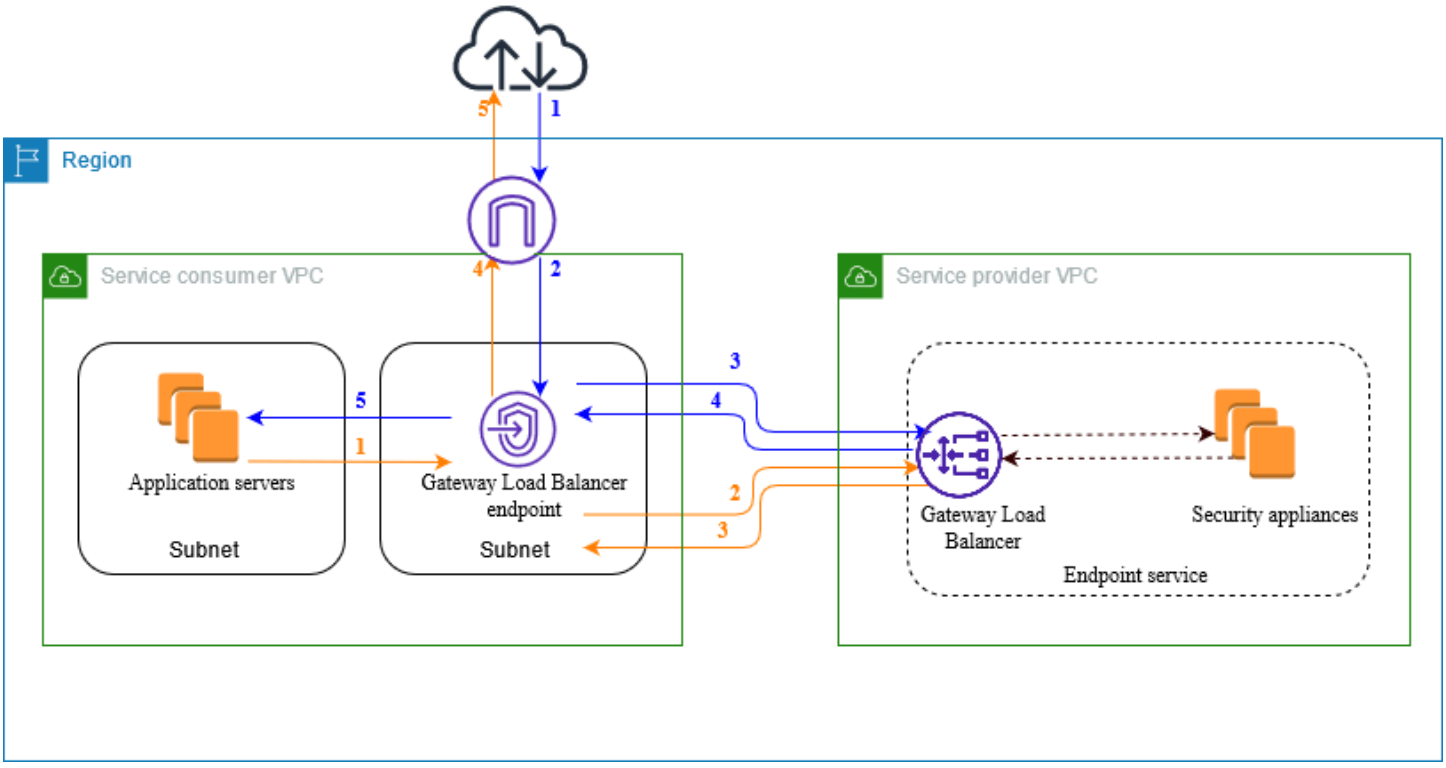
La fatturazione viene calcolata per ogni ora di provisioning dell'endpoint Gateway Load Balancer in ciascuna zona di disponibilità. Ti viene inoltre addebitato un importo per GB di dati elaborati. Per ulteriori informazioni, consulta la sezione Prezzi di AWS PrivateLink.

Indice

Per ulteriori informazioni, consultare Bilanciatori del carico del gateway.

Panoramica

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



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

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

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

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

5. Il traffico viene reindirizzato a Internet.

Tipi di indirizzi IP

I provider di servizi possono rendere i propri endpoint di servizio disponibili agli utenti tramite IPv4, IPv6 o entrambi, anche se le appliance di sicurezza supportano solo IPv4. Se si abilita il supporto dualstack, gli utenti esistenti possono continuare a utilizzare IPv4 per accedere al servizio, mentre i nuovi utenti possono scegliere di utilizzare IPv6.

Se un endpoint Gateway Load Balancer supporta IPv4, le interfacce di rete dell'endpoint dispongono di indirizzi IPv4. Se un endpoint Gateway Load Balancer supporta IPv6, le interfacce di rete dell'endpoint dispongono di indirizzi IPv6. L'indirizzo IPv6 per un'interfaccia di rete dell'endpoint non è raggiungibile da Internet. Se si descrive un'interfaccia di rete dell'endpoint con un indirizzo IPv6, l'opzione `denyAllIgwTraffic` sarà abilitata.

Requisiti per abilitare IPv6 per un servizio endpoint

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

Requisiti per abilitare IPv6 per 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: consente di assegnare indirizzi IPv4 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4.
  - IPv6: consente di assegnare indirizzi IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono sottoreti solo IPv6.
  - Dualstack: consente di assegnare sia indirizzi IPv4 che IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e IPv6.
- Le tabelle di instradamento per le sottoreti nel VPC del consumer del servizio devono instradare il traffico IPv6 e le ACL di rete per queste sottoreti devono 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. Ricorda che le route IPv6 sono incluse in 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
CIDR IPv4 del VPC	Locale
CIDR IPv6 del VPC	Locale
CIDR IPv4 sottorete applicazione	*vpc-endpoint-id*
CIDR IPv6 sottorete applicazione	*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
CIDR IPv4 del VPC	Locale
CIDR IPv6 del VPC	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
CIDR IPv4 del VPC	Locale
CIDR IPv6 del VPC	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 gli ID AZ per identificare in modo coerente le zone di disponibilità del servizio. Per ulteriori informazioni, consulta ID AZ nella Guida per l'utente di Amazon EC2 per le istanze Linux.
- Le tue AWS PrivateLink risorse sono soggette a quote. Per ulteriori informazioni, consulta AWS PrivateLink quote.

Prerequisiti

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

Creazione del servizio endpoint

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

Per creare un servizio endpoint tramite la console

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

6. In Require acceptance for endpoint (Richiedi accettazione per l'endpoint), seleziona Acceptance required (Accettazione richiesta) per richiedere l'accettazione manuale delle richieste di connessione al servizio endpoint. In caso contrario, queste vengono accettate automaticamente.
7. Per Supported IP address types (Tipi di indirizzo IP supportati), esegui una delle operazioni seguenti:
   - Seleziona IPv4 per consentire al servizio endpoint di accettare richieste IPv4.
   - Seleziona IPv6 per consentire al servizio endpoint di accettare richieste IPv6.
   - Seleziona IPv4 e IPv6 per consentire al servizio endpoint di accettare richieste IPv4 e IPv6.
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-EC2 VpcEndpointServiceConfiguration (strumenti per Windows) PowerShell

Rendere disponibile il servizio endpoint

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

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

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

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

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

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

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

Indice

Considerazioni

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

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

Prerequisiti

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

Creare l'endpoint

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

Per creare un endpoint Gateway Load Balancer utilizzando la console

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

4. In Service category (Categoria del servizio), scegli Other endpoint services (Altri servizi endpoint).
5. In Service name (Nome servizio), specifica il nome del servizio, quindi seleziona Verify service (Verifica servizio).
6. In VPC, seleziona un VPC in cui creare l'endpoint.
7. In Subnets (Sottoreti), selezionare la sottorete in cui creare l'endpoint.
8. Per IP address type (Tipo di indirizzo IP), seleziona una delle opzioni seguenti:
   - IPv4: consente di assegnare indirizzi IPv4 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4.
   - IPv6: consente di assegnare indirizzi IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono sottoreti solo IPv6.
   - Dualstack: consente di assegnare sia indirizzi IPv4 che IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e 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-EC2 VpcEndpoint (strumenti per Windows) PowerShell

Configurazione del routing

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

Per configurare l'instradamento utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Route Tables (Tabelle di routing).
3. Seleziona la tabella di instradamento per il gateway Internet ed esegui le operazioni seguenti:

a. Selezionare Actions (Operazioni), Edit routes (Modifica route).

b. Se supporti IPv4, scegli Add route (Aggiungi route). Per Destination (Destinazione), immetti il blocco CIDR IPv4 della sottorete per i server dell'applicazione. Per Target, seleziona l'endpoint VPC.

c. Se supporti IPv6, scegli Add route (Aggiungi route). Per Destination (Destinazione), immetti il blocco CIDR IPv6 della sottorete per i server dell'applicazione. Per Target, seleziona l'endpoint VPC.

d. Seleziona Salvataggio delle 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 supporti IPv4, scegli Add route (Aggiungi route). In Destination (Destinazione), immettere **`0.0.0.0/0`**. Per Target, seleziona l'endpoint VPC.

c. Se supporti IPv6, scegli Add route (Aggiungi route). In Destination (Destinazione), immettere **`::/0`**. Per Target, seleziona l'endpoint VPC.

d. Seleziona Salvataggio delle modifiche.

5. Seleziona la tabella di instradamento per la sottorete con l'endpoint Gateway Load Balancer ed esegui le operazioni seguenti:

a. Selezionare Actions (Operazioni), Edit routes (Modifica route).

b. Se supporti IPv4, scegli Add route (Aggiungi route). In Destination (Destinazione), immettere **`0.0.0.0/0`**. Per Target, seleziona il gateway Internet.

c. Se supporti IPv6, scegli Add route (Aggiungi route). In Destination (Destinazione), immettere **`::/0`**. Per Target, seleziona il gateway Internet.

d. Seleziona Salvataggio delle 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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (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. Selezionare Salva.

Per gestire i tag utilizzando la riga di comando

- create-tags e delete-tags (AWS CLI)
- New-EC2Tag e 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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Endpoints (Endpoint) e selezionare l'endpoint.
3. Selezionare Actions (Operazioni), Delete Endpoint (Elimina endpoint).
4. Nella schermata di conferma, selezionare Yes, Delete (Sì, elimina).

Per eliminare un endpoint Gateway Load Balancer

- delete-vpc-endpoints (AWS CLI)
- AWS Tools for Windows PowerShell Rimuovi-ec2 VpcEndpoint ()

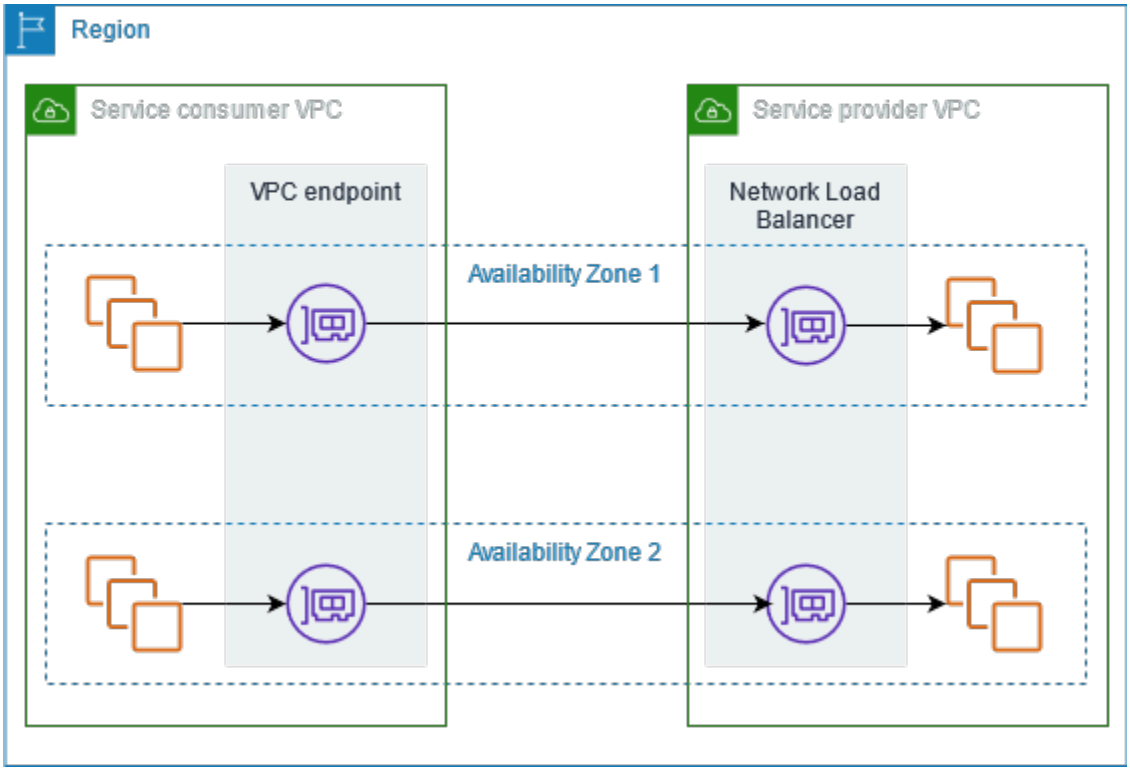
Condividi i tuoi servizi tramite AWS PrivateLink

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

Indice

Panoramica

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



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

Hostname DNS

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

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

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

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

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

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

I nomi zonali sono caratterizzati dalla sintassi seguente:

```
endpoint_id-zone.endpoint_service_id.region.vpce.amazonaws.com
```

DNS privato

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

Tipi di indirizzi IP

I provider di servizi possono rendere i propri endpoint di servizio disponibili agli utenti tramite IPv4, IPv6 o entrambi, anche se i server back-end supportano solo IPv4. Se si abilita il supporto dualstack, gli utenti esistenti possono continuare a utilizzare IPv4 per accedere al servizio, mentre i nuovi utenti possono scegliere di utilizzare IPv6.

Se un endpoint VPC dell'interfaccia supporta IPv4, le interfacce di rete dell'endpoint presentano indirizzi IPv4. Se un endpoint VPC dell'interfaccia supporta IPv6, le interfacce di rete dell'endpoint presentano indirizzi IPv6. L'indirizzo IPv6 per un'interfaccia di rete dell'endpoint non è raggiungibile da Internet. Se si descrive un'interfaccia di rete dell'endpoint con un indirizzo IPv6, l'opzione `denyAllIgwTraffic` sarà abilitata.

Requisiti per abilitare IPv6 per un servizio endpoint

- Il VPC e le sottoreti per il servizio endpoint devono disporre di blocchi CIDR IPv6 associati.
- Tutti i Network Load Balancer per il servizio endpoint devono utilizzare il tipo di indirizzo IP dualstack. Le destinazioni non devono supportare il traffico IPv6. Se il servizio elabora gli indirizzi IP di origine dall'intestazione della versione 2 del protocollo proxy, deve elaborare gli indirizzi IPv6.

Requisiti per abilitare IPv6 per un endpoint dell'interfaccia

- Il servizio endpoint deve supportare le richieste 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: consente di assegnare indirizzi IPv4 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4.
  - IPv6: consente di assegnare indirizzi IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono sottoreti solo IPv6.
  - Dualstack: consente di assegnare sia indirizzi IPv4 che IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e IPv6.

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

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

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

Crea un servizio fornito da AWS PrivateLink

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

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

Indice

- Prerequisiti
- Creazione di un servizio endpoint
- Rendi il servizio endpoint disponibile agli utenti del servizio

Considerazioni

- Un servizio endpoint è disponibile nella regione in cui è stato creato. Puoi accedere al servizio endpoint da altre regioni utilizzando il peering VPC.
- Un servizio endpoint supporta solo il traffico via TCP.
- 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 gli ID AZ per identificare in modo coerente le zone di disponibilità del servizio. Per ulteriori informazioni, consulta ID AZ nella Guida per l'utente di Amazon EC2 per le istanze Linux.
- 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 si abilita il protocollo proxy sul load balancer, è possibile ottenere gli indirizzi degli utenti del servizio e gli ID degli endpoint dell'interfaccia dall'intestazione del protocollo proxy. Per ulteriori informazioni, vedere Proxy Protocol nel Manuale dell'utente per Network Load Balancers.
- 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 AWS PrivateLink risorse sono soggette a quote. Per ulteriori informazioni, consulta AWS PrivateLink quote.

Prerequisiti

- Creare un VPC per il servizio endpoint con almeno una sottorete in ogni zona di disponibilità in cui il servizio deve essere disponibile.
- Per consentire agli utenti del servizio di creare endpoint VPC con interfaccia IPv6 per il servizio endpoint, il VPC e le sottoreti devono avere blocchi CIDR IPv6 associati.
- Creare un Network Load Balancer nel VPC. Seleziona una sottorete per la zona di disponibilità in cui il servizio deve essere reso disponibile agli utenti. Per una bassa latenza e la tolleranza ai guasti, consigliamo di rendere il servizio disponibile in almeno due zone di disponibilità della regione.
- Per consentire al servizio endpoint di accettare richieste IPv6, i relativi Network Load Balancer devono utilizzare il tipo di indirizzo IP dualstack. Le destinazioni non devono supportare il traffico IPv6. Per ulteriori informazioni, consulta la sezione Tipo di indirizzo IP nella Guida per l'utente di Network Load Balancer.

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

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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Scegli Create Endpoint Service (Crea servizio endpoint).
4. Per Load balancer type (Tipo di load balancer), scegli Network (Rete).

5. In Available load balancers (load balancer disponibili), selezionare i Network Load Balancers da associare al servizio endpoint.
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 richieste vengono accettate automaticamente.
7. In Enable private DNS (Abilita nomi DNS privati), seleziona Associate a private DNS name with the service (Associa un nome DNS privato al servizio) per associare un nome DNS privato al servizio e consentire l'accesso agli utenti, quindi immetti il nome DNS privato. In caso contrario, gli utenti del servizio possono utilizzare il nome DNS specifico dell'endpoint fornito da. AWS Il provider di servizi deve dimostrare di essere il proprietario del dominio prima che gli utenti possano utilizzare il nome DNS privato. Per ulteriori informazioni, consulta Gestione dei nomi DNS.
8. Per Supported IP address types (Tipi di indirizzo IP supportati), esegui una delle operazioni seguenti:
   - Seleziona IPv4 per consentire al servizio endpoint di accettare richieste IPv4.
   - Seleziona IPv6 per consentire al servizio endpoint di accettare richieste IPv6.
   - Seleziona IPv4 e IPv6 per consentire al servizio endpoint di accettare richieste IPv4 e IPv6.
9. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
10. Selezionare Crea.

Per creare un servizio endpoint utilizzando la riga di comando

- create-vpc-endpoint-service-configurazione ()AWS CLI
- New-EC2 VpcEndpointServiceConfiguration (strumenti per Windows) PowerShell

Rendi il servizio endpoint disponibile agli utenti del servizio

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

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

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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. In Service category (Categoria del servizio), scegli Other endpoint services (Altri servizi endpoint).
5. In Service name (Nome servizio), immetti il nome del servizio (ad esempio `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`) e seleziona Verify service (Verifica del servizio).
6. In VPC, selezionare un VPC in cui creare l'endpoint.
7. In Subnets (Sottoreti), seleziona le sottoreti (zone di disponibilità) da cui accederai al servizio endpoint.
8. Per IP address type (Tipo di indirizzo IP), seleziona una delle opzioni seguenti:
   - IPv4: consente di assegnare indirizzi IPv4 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e il servizio endpoint accetta richieste IPv4.
   - IPv6: consente di assegnare indirizzi IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono sottoreti solo IPv6 e il servizio endpoint accetta richieste IPv6.

- Dualstack: consente di assegnare sia indirizzi IPv4 che IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e IPv6 e il servizio endpoint accetta sia richieste IPv4 e IPv6.

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

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

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

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

- create-vpc-endpoint (AWS CLI)
- VpcEndpointNew-EC2 (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
- Modifica dell'associazione del load balancer
- Associazione di un nome DNS privato
- Modifica dei tipi di indirizzo IP supportati
- Gestione dei tag

Gestione delle autorizzazioni

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

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

ARN per presidi AWS

Account AWS (include tutti i principali dell'account)

arn:aws:iam::*account_id*:root

Ruolo

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

Utente

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

Tutti i principali in tutto Account AWS

*

Considerazione

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.

Gestione delle autorizzazioni per il servizio endpoint tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).

3. Seleziona il servizio endpoint e scegli la scheda Allow principals (Consenti principali).
4. Per aggiungere le autorizzazioni, scegli Allow principals (Consenti principali). In Principals to add (Entità principali da aggiungere), immetti l'ARN del principale. Per aggiungere un altro principale, scegliere Add principal (Aggiungi principale). Una volta completata l'aggiunta di principali, scegli Allow principals (Consenti principali).
5. Per rimuovere le autorizzazioni, seleziona il principale e scegli Actions (Operazioni), Delete (Elimina). Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

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

- modify-vpc-endpoint-service-permessi ()AWS CLI
- Edit-EC2 EndpointServicePermission (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.

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”.

Considerazione

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.

Per modificare l'impostazione di accettazione tramite la console

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

2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Selezionare Actions (Operazioni), Modify endpoint acceptance setting (Modifica impostazione di accettazione Endpoint).
5. Seleziona o deseleziona l'opzione Acceptance required (Accettazione richiesta).
6. Scegli Save changes (Salva modifiche).

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

- modify-vpc-endpoint-service-configurazione ()AWS CLI
- Edit-EC2 VpcEndpointServiceConfiguration (strumenti per Windows) PowerShell

Per accettare o rifiutare una richiesta di connessione tramite la console

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

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

- accept-vpc-endpoint-connectionso () reject-vpc-endpoint-connectionsAWS CLI
- Approve-EC2 EndpointConnection o EndpointConnectionDeny-EC2 (strumenti per Windows) PowerShell

Modifica dell'associazione del load balancer

Puoi modificare il load balancer associato al servizio endpoint. Tuttavia, non puoi dissociare un load balancer se vi sono endpoint collegati al servizio endpoint.

Per modificare i load balancer per il servizio endpoint tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Seleziona Actions (Operazioni), Associate or disassociate load balancers (Associa o dissocia i bilanciatori del carico).
5. Aggiungi o rimuovi i load balancer in base alle esigenze.
6. Scegli Save changes (Salva modifiche).

Per modificare i load balancer per il servizio endpoint tramite la riga di comando

- modify-vpc-endpoint-service AWS CLI-configurazione ()
- Edit-EC2 VpcEndpointServiceConfiguration (strumenti per Windows) PowerShell

Associazione di un nome DNS privato

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

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

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

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

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

- modify-vpc-endpoint-service-configurazione ()AWS CLI
- Edit-EC2 VpcEndpointServiceConfiguration (strumenti per Windows) PowerShell

Per avviare il processo di verifica del dominio utilizzando la console

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

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

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

Modifica 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 richieste IPv6, i relativi Network Load Balancer devono utilizzare il tipo di indirizzo IP dualstack. Le destinazioni non devono supportare 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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona il servizio endpoint VPC.
4. Scegli Actions (Operazioni), Modify supported IP address types (Modifica i tipi di indirizzo IP supportati).
5. Per Supported IP address types (Tipi di indirizzo IP supportati), esegui una delle operazioni seguenti:
   - Seleziona IPv4 per consentire al servizio endpoint di accettare richieste IPv4.
   - Seleziona IPv6 per consentire al servizio endpoint di accettare richieste IPv6.
   - Seleziona IPv4 e IPv6 per consentire al servizio endpoint di accettare richieste IPv4 e IPv6.
6. Seleziona Salvataggio delle modifiche.

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

- modify-vpc-endpoint-service-configurazione ()AWS CLI
- Edit-EC2 VpcEndpointServiceConfiguration (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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona il servizio endpoint VPC.
4. Scegliere Actions (Operazioni), Manage tags (Gestisci tag).
5. Per ogni tag da aggiungere, seleziona Add new tag (Aggiungi nuovo tag) e immetti la chiave e il valore per il tag.
6. Per rimuovere un tag, scegli Remove (Rimuovi) a destra della chiave e del valore del tag.
7. Selezionare Salva.

Gestione dei tag per le connessioni degli endpoint tramite la console

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

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

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

Per aggiungere e rimuovere i tag utilizzando la riga di comando

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

Gestione dei nomi DNS per i servizi endpoint VPC

I provider di servizi possono configurare i nomi DNS privati per i propri servizi endpoint. Quando un provider di servizi utilizza un nome DNS pubblico esistente come nome DNS privato per il proprio

servizio endpoint, gli utenti del servizio non devono modificare le applicazioni che utilizzano il nome DNS pubblico esistente. Prima di poter configurare un nome DNS privato per il servizio endpoint, devi dimostrare di essere il proprietario del dominio eseguendo una verifica della proprietà del dominio.

Considerazioni

- Un servizio endpoint può avere un solo nome DNS privato.
- Non è necessario creare un record A per il nome DNS privato, in modo che solo i server nel VPC dell'utente del servizio possano risolvere il nome DNS privato.
- I nomi DNS privati non sono supportati per gli endpoint Gateway Load Balancer.
- Per verificare un dominio, è necessario disporre di un nome host pubblico o di un provider DNS pubblico.
- Puoi verificare il dominio di un sottodominio. Ad esempio, è possibile verificare example.com, anziché a.example.com. Come specificato nello standard RFC 1034, ogni etichetta DNS può contenere fino a 63 caratteri e l'intero nome di dominio non può superare una lunghezza totale di 255 caratteri.

  Se aggiungi un altro sottodominio, è necessario verificare il sottodominio o il dominio. Ad esempio, supponiamo che hai a.example.com e verifichi example.com. Ora aggiungi b.example.com come nome DNS privato. A questo punto devi verificare example.com o b.example.com prima che gli utenti possano utilizzare il nome.

Verifica della proprietà del dominio

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

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

Dopo aver aggiunto un record, puoi controllare lo stato del processo di verifica del dominio utilizzando la console Amazon VPC. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint). Seleziona il servizio endpoint e controlla il valore di Domain verification status (Stato di verifica del dominio) nella scheda Details (Dettagli). Se la verifica del dominio è in sospeso, attendi qualche minuto e aggiorna la schermata. Se necessario, puoi avviare il processo di verifica manualmente.

Scegli Actions (Operazioni),Verify domain ownership for private DNS name (Verifica la proprietà del dominio per il nome DNS privato).

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

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

Recupero del nome e del valore

Forniamo il nome e il valore da utilizzare nel record TXT. Queste informazioni sono disponibili, ad esempio, nella 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. È inoltre possibile utilizzare il seguente AWS CLI comando describe-vpc-endpoint-service-configurations per recuperare informazioni sulla configurazione del nome DNS privato per il servizio endpoint specificato.

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

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

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

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

Nome	Type	Valore
_6e86v84tqgqubxbwi i1m.example.com	TXT	RxlTtVPCE: L6P0E 45jEvFwOCP

Ti consigliamo di usare `Name` come sottodominio record perché il nome del dominio di base potrebbe essere già in uso. Se il provider DNS, tuttavia, non consente caratteri di sottolineatura per i nomi dei record DNS, è possibile omettere "_6e86v84tqgqubxbwii1m" e utilizzare semplicemente "example.com" nel record TXT.

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

Aggiungi un record TXT al server DNS del dominio

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

Amazon Route 53

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

- Per Record type (Tipo di record), scegli TXT.
- Per TTL (seconds) (TTL [secondi]), immetti **`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

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

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

Provider DNS/di hosting	Collegamento alla documentazione
GoDaddy	Aggiungi un registro TXT
Dreamhost	Adding custom DNS records
Cloudflare	Manage DNS records
HostGator	Gestisci i record DNS con /eNOM HostGator
Namecheap	How do I add TXT/SPF/DKIM/DMARC records for my domain?
Names.co.uk	Changing your domain's DNS Settings
Wix	Adding or Updating TXT Records in Your Wix Account

Verifica della pubblicazione del record TXT

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

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

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

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

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

   Nell'output vengono elencati i server dei nomi utilizzati dal dominio. Nella fase successiva, si eseguirà una query su uno di questi server.

2. Verifica che il record TXT sia stato pubblicato correttamente utilizzando il comando seguente, dove *name_server* rappresenta uno dei server di nomi trovati nella fase precedente.

```
nslookup -type=TXT  _6e86v84tqgqubxbwii1m.example.com name_server
```

3. Nell'output della fase precedente, verifica che la stringa dopo `text =` corrisponda al valore TXT.

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

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

Risoluzione dei problemi relativi alla verifica del dominio

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

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

  1. Nella console Route 53, seleziona il record TXT creato al momento della verifica del dominio nella prima regione.

2. Per Value (Valore), vai alla fine del valore di attributo esistente e quindi premi Invio.
3. Aggiungi il valore di attributo per la regione aggiuntiva e salva il set di record.

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

Ricezione di avvisi per gli eventi relativi al servizio endpoint

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

Attività

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

Creare una notifica SNS

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

Per creare una notifica per un servizio endpoint utilizzando la console

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

- Reject (Rifiuta): il provider di servizi ha rifiutato la richiesta di connessione.
- Delete (Elimina): l'utente del servizio ha eliminato l'endpoint dell'interfaccia.

7. Selezionare Create Notification (Crea notifica).

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

- create-vpc-endpoint-connection-notifica ()AWS CLI
- New-EC2 VpcEndpointConnectionNotification (strumenti per Windows) PowerShell

Aggiungere una policy di accesso

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

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

```
{
  "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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Selezionare Actions (Operazioni), Delete endpoint services (Elimina servizi endpoint).
5. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Per eliminare un servizio endpoint utilizzando la riga di comando

- delete-vpc-endpoint-service-configurazioni ()AWS CLI
- Remove-ec2 EndpointServiceConfiguration (Strumenti per Windows) PowerShell

Gestione delle identità e degli accessi per AWS PrivateLink

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

Indice

Destinatari

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

Utente del servizio: se utilizzi il AWS PrivateLink servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS PrivateLink funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso 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 i concetti di base relativi a IAM.

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

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

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

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

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

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

Account AWS utente root

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

Identità federata

Come 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 ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

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

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

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

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

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per

effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

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

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

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

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

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

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

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

Liste di controllo degli accessi (ACL)

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

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

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente 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 scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come AWS PrivateLink funziona con IAM

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

Funzionalità IAM che puoi utilizzare con AWS PrivateLink

Funzionalità 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
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
☻Ruoli di servizio	No
Ruoli collegati al servizio	No

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

Politiche basate sull'identità per AWS PrivateLink

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

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

Esempi di politiche basate sull'identità per AWS PrivateLink

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

Politiche basate sulle risorse all'interno AWS PrivateLink

Supporta le policy basate su risorse	Sì

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il

principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile 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 Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

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 azioni di policy	Sì

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

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

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

AWS PrivateLink condivide il suo spazio dei nomi API con Amazon EC2. Le azioni politiche AWS PrivateLink utilizzano il seguente prefisso prima dell'azione:

```
ec2
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

```
]
```

È possibile specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `Describe`, includi la seguente operazione:

```
"Action": "ec2:Describe*"
```

Per visualizzare un elenco di AWS PrivateLink azioni, consulta AWS PrivateLink le azioni nel riferimento alle API di Amazon EC2. Per ulteriori informazioni, consulta Operazioni definite da Amazon EC2 nella Documentazione di riferimento per l'autorizzazione ai servizi.

Risorse politiche per AWS PrivateLink

Supporta le risorse di policy	Sì

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

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

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

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

Chiavi relative alle condizioni delle politiche per AWS PrivateLink

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

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

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

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

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

Le seguenti chiavi di condizione sono specifiche per AWS PrivateLink:

- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`

Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta Operazioni definite da Amazon Ec2.

ACL in AWS PrivateLink

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AWS PrivateLink

Supporta ABAC (tag nelle policy)	Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

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

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

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con 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 relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua 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 sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS 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, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali multiservizio per AWS PrivateLink

Supporta sessioni di accesso diretto (FAS)	Sì

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

Ruoli di servizio per AWS PrivateLink

Supporta i ruoli di servizio	No

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

Ruoli collegati ai servizi per AWS PrivateLink

Supporta i ruoli collegati ai servizi	No

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

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 l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

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

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

Esempi

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

Controlla l'utilizzo degli endpoint VPC

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

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

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

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

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

Puoi utilizzare la chiave di condizione `ec2:VpceServiceOwner` per controllare l'endpoint VPC che può essere creato in base al proprietario del servizio (`amazon`, `aws-marketplace` o l'ID account). Nell'esempio seguente viene concessa l'autorizzazione per creare endpoint VPC con il proprietario del servizio specificato. Per utilizzare questo esempio, sostituisci la Regione, l'ID account e il proprietario del servizio.

```
{
    "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"
                    ]
                }
```

```
            }
        }
    ]
}
```

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

Puoi utilizzare la chiave di condizione `ec2:VpceServicePrivateDnsName` per controllare quale servizio endpoint VPC può essere modificato o creato in base al nome DNS privato associato al servizio endpoint VPC. Nell'esempio seguente viene concessa l'autorizzazione per creare un servizio endpoint VPC con il nome DNS privato specificato. Per utilizzare questo esempio, sostituisci la Regione, l'ID account e il nome DNS privato.

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Controllare i nomi dei servizi che è possibile specificare per i servizi endpoint VPC

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

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Controllo dell'accesso agli endpoint VPC tramite le policy di endpoint

Una policy per gli endpoint è una policy basata sulle risorse che si collega a un endpoint VPC per controllare quali AWS responsabili possono utilizzare l'endpoint per accedere a un. Servizio AWS

Una policy di endpoint non esclude né sostituisce le policy basate sull'identità o sulle risorse. Ad esempio, se stai utilizzando un endpoint dell'interfaccia per connetterti ad Amazon S3, puoi anche utilizzare le policy dei bucket Amazon S3 per controllare l'accesso ai bucket da endpoint o VPC specifici.

Indice

Considerazioni

- Una policy degli endpoint è un documento di policy JSON che utilizza il linguaggio della policy IAM. Deve contenere un elemento Principal. Le dimensioni di una policy degli endpoint non possono superare i 20.480 caratteri, inclusi gli spazi bianchi.
- Quando si crea un'interfaccia o un endpoint gateway per un endpoint Servizio AWS, è possibile allegare una singola policy endpoint all'endpoint. Puoi aggiornare la policy degli endpoint in qualsiasi momento. Se non si allega una policy degli endpoint, alleghiamo la policy degli endpoint predefinita.
- Non tutti Servizi AWS supportano le policy relative agli endpoint. Se un dispositivo Servizio AWS non supporta le policy relative agli endpoint, consentiamo l'accesso completo a qualsiasi endpoint per il servizio. Per ulteriori informazioni, consulta the section called “Visualizza il supporto della politica dell'endpoint”.
- Quando crei un endpoint VPC per un servizio endpoint diverso da un Servizio AWS, consentiamo l'accesso completo all'endpoint.

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

Aggiornamento di una policy di endpoint VPC

Utilizza la procedura seguente per aggiornare una policy degli endpoint per un Servizio AWS. Dopo avere aggiornato l'endpoint, possono essere necessari alcuni minuti prima che le modifiche diventino effettive.

Per aggiornare la policy degli endpoint usando la console

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

Per aggiornare la policy degli endpoint utilizzando la riga di comando

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

Parametri CloudWatch per AWS PrivateLink

AWS PrivateLink pubblica i punti dati ad Amazon CloudWatch per gli endpoint dell'interfaccia, gli endpoint di Gateway Load Balancer e i servizi dell'endpoint. CloudWatch ti consente di recuperare le statistiche su quei punti di dati come set ordinato di dati di serie temporali, i cosiddetti parametri. 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 allarme CloudWatch per monitorare un parametro specificato e avviare un'operazione (come l'invio di una notifica a un indirizzo e-mail) se il parametro non rientra in un 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 parametri a CloudWatch in intervalli di un minuto, senza costi aggiuntivi.

Per ulteriori informazioni, consulta la Guida per l'utente di Amazon CloudWatch.

Indice

Parametri e dimensioni dell'endpoint

Lo spazio dei nomi di `AWS/PrivateLinkEndpoints` include i parametri descritti di seguito per endpoint di interfaccia e endpoint di Gateway Load Balancer.

Parametro	Descrizione
`ActiveConnections`	Il numero di connessioni simultanee attive. Questo parametro include connessioni negli stati SYN_SENT ed ESTABLISHED.

Parametro	Descrizione
	Criteri di segnalazione: L'endpoint ha ricevuto traffico durante il periodo di un minuto. Statistics (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. Statistics (Statistiche): le statistiche più utili sono `Average`, `Sum` e `Maximum`. Dimensioni • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Parametro	Descrizione
`RstPacketsReceived`	Il numero di pacchetti RST ricevuti dall'endpoint. Valori crescenti potrebbero indicare che il servizio endpoint o endpoint non è sano. Criteri di segnalazione: L'endpoint ha ricevuto traffico durante il periodo di un minuto. Statistics (Statistiche): le statistiche più utili sono `Average`, `Sum` e `Maximum`. Dimensioni • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Per filtrare questi parametri, usa le seguenti dimensioni.

Dimensione	Descrizione
`Endpoint Type`	Filtra i dati dei parametri per tipo di endpoint (`Interface` |`GatewayLoadBalancer`).
`Service Name`	Filtra i dati dei parametri per nome del servizio.
`Subnet Id`	Filtra i dati dei parametri per sottorete.
`VPC Endpoint Id`	Filtra i dati dei parametri per endpoint VPC.
`VPC Id`	Filtra i dati dei parametri per VPC.

Parametri e dimensioni del servizio dell'endpoint

Lo spazio dei nomi di `AWS/PrivateLinkServices` include i parametri descritti di seguito per endpoint .

Parametro	Descrizione
`ActiveConnections`	Il numero massimo di connessioni attive dai client alle destinazioni tramite endpoint. Valori crescenti potrebbero indicare la necessità di aggiungere obiettivi al load balancer. Criteri di segnalazione: un endpoint connesso al servizio endpoint ha inviato traffico durante il periodo di un minuto. Statistiche: le statistiche più utili sono `Average` e `Maximum`. Dimensioni • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`BytesProcessed`	Il numero di byte scambiati tra endpoint e servizi endpoint, aggregati in entrambe le direzioni. Criteri di segnalazione: un endpoint connesso al servizio endpoint ha inviato traffico durante il periodo di un minuto. Statistics (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. Statistics (Statistiche): le statistiche più utili sono `Average`, `Sum` e `Maximum`. Dimensioni • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Parametro	Descrizione
`RstPacketsSent`	Il numero di pacchetti RST inviati agli endpoint dal servizio endpoint. Valori crescenti potrebbero indicare che ci sono obiettivi malsani. Criteri di segnalazione: un endpoint connesso al servizio endpoint ha inviato traffico durante il periodo di un minuto. Statistics (Statistiche): le statistiche più utili sono `Average`, `Sum` e `Maximum`. Dimensioni • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Per filtrare questi parametri, usa le seguenti dimensioni.

Dimensione	Descrizione
`Az`	Consente di filtrare i dati del parametro per zona di disponibilità.
`Load Balancer Arn`	Consente di filtrare i dati del parametro per load balancer.
`Service Id`	Filtra i dati dei parametri per servizio endpoint.
`VPC Endpoint Id`	Filtra i dati dei parametri per endpoint VPC.

Visualizzazione dei parametri di CloudWatch

Puoi esaminare questi parametri CloudWatch tramite la console Amazon VPC, la console CloudWatch, la AWS CLI o l'API di CloudWatch.

Per visualizzare i parametri tramite la console di Amazon VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint). Selezionare l'endpoint, quindi scegliere la scheda Monitoring (Monitoraggio).
3. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint). Selezionare l'endpoint, quindi scegliere la scheda Monitoring (Monitoraggio).

Per visualizzare i parametri utilizzando la console CloudWatch

1. Aprire la console CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, selezionare Parametri.
3. Seleziona il Endpoint AWS per link privati spazio dei nomi.
4. Seleziona il Servizi di AWS (Private Link) spazio dei nomi.

Visualizzazione dei parametri usando 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 crea regole integrate di Approfondimenti sulle contribuzioni per i servizi endpoint per aiutarti a individuare quali endpoint sono i maggiori contributori di ciascun parametro supportato. Per ulteriori informazioni, consulta Utilizzo di Contributor Insights nella Guida per l'utente Amazon CloudWatch.

AWS PrivateLink fornisce le seguenti regole:

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1`- classifica gli endpoint in base al numero di connessioni attive all'endpoint.

- `VpcEndpointService-BytesByEndpointId-v1`— Classifica gli endpoint in base al numero di byte elaborati.
- `VpcEndpointService-NewConnectionsByEndpointId-v1`- classifica gli endpoint in base al numero di connessioni attive all'endpoint.
- `VpcEndpointService-RstPacketsByEndpointId-v1`- Il numero di pacchetti RST inviati agli endpoint dal servizio endpoint.

Prima di poter utilizzare una regola integrata, è necessario abilitarla. Dopo che una regola è stata abilitato, questa inizia a raccogliere i dati dei collaboratori. Per ulteriori informazioni sulle tariffe per Approfondimenti sulle contribuzioni, consulta la pagina Prezzi di Amazon CloudWatch.

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.

Processi

- 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 utilizzando la AWS Management Console o la AWS CLI.

Abilitazione delle regole di Approfondimenti sulle contribuzioni per AWS PrivateLink tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Nella scheda Contributor Insights (Approfondimenti sulle contribuzioni), scegli Enable (Abilita).
5. (Facoltativo) Per impostazione predefinita, tutte le regole sono abilitate. Per abilitare solo regole specifiche, seleziona le regole desiderate quindi scegli Actions (Operazioni), Disable rule (Disabilita regola). Quando viene richiesta la conferma, seleziona Disable (Disabilita).

Abilitazione delle regole di Approfondimenti sulle contribuzioni per AWS PrivateLink tramite la AWS CLI

1. Utilizza il comando list-managed-insight-rules come riportato di seguito per enumerare le regole disponibili. Per l'opzione `--resource-arn`, specifica l'ARN del servizio endpoint.

```
aws cloudwatch list-managed-insight-rules --resource-arn
 arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. Nell'output del comando `list-managed-insight-rules`, copia il nome del modello dal campo `TemplateName`. Di seguito è riportato un esempio di questo campo.

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. Utilizza il comando put-managed-insight-rules come riportato di seguito per abilitare la regola. Devi specificare il nome del modello e l'ARN del servizio endpoint.

```
aws cloudwatch put-managed-insight-rules --managed-rules
 TemplateName=VpcEndpointService-NewConnectionsByEndpointId-v1,
 ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

Disabilitazione delle regole di Approfondimenti sulle contribuzioni

Puoi disabilitare le regole integrate per 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.

Disabilitazione delle regole di Approfondimenti sulle contribuzioni per AWS PrivateLink tramite la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Selezionare il servizio endpoint.
4. Nella scheda Contributor Insights (Approfondimenti sulle contribuzioni), scegli Disable all (Disabilita tutto) per disabilitare tutte le regole. In alternativa, espandi il pannello Rules(Regole), seleziona le regole da disabilitare e scegli Actions (Operazioni), Disable rule (Disabilita regola).
5. Quando viene richiesta la conferma, seleziona Disable (Disabilita).

Disabilitazione delle regole di Approfondimenti sulle contribuzioni per AWS PrivateLink tramite la AWS CLI

Utilizza il comando disable-insight-rules per disabilitare una regola.

Eliminazione delle regole di Approfondimenti sulle contribuzioni

Utilizza le seguenti procedure per eliminare le regole integrate per AWS PrivateLink utilizzando la AWS Management Console o la AWS CLI. Dopo aver eliminato una regola, questa interrompe la raccolta dei dati dei collaboratori e i dati esistenti vengono eliminati.

Eliminazione delle regole di Approfondimenti sulle contribuzioni per AWS PrivateLink tramite la console

1. Aprire la console CloudWatch 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).

Eliminazione delle regole di Approfondimenti sulle contribuzioni per AWS PrivateLink tramite la AWS CLI

Usa il comando delete-insight-rules per eliminare una regola.

AWS PrivateLink quote

Nelle tabelle che seguono sono elencate le quote, precedentemente dette limiti, relativi alle risorse AWS PrivateLink per regione per il tuo account. Se non è diversamente indicato, è possibile chiedere un aumento di queste quote. Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'utente per Service Quotas.

Se richiedi di aumentare una quota applicabile per risorsa, viene aumentata la quota per tutte le risorse nella regione.

Nome	Predefinita	Adattabile	Commenti
Endpoint load balancer di interfaccia e gateway per VPC	50	Sì	Si tratta di una quota combinata di endpoint dell'interfaccia ed endpoint Gateway Load Balancer
Endpoint VPC del gateway per regione	20	Sì	Puoi creare fino a 255 endpoint gateway per VPC
Caratteri per policy di endpoint VPC	20.480	No	La dimensione massima di una policy dell’endpoint VPC include gli spazi vuoti

Le considerazioni seguenti si applicano al traffico in transito attraverso un endpoint VPC:

- Per impostazione predefinita, ogni endpoint VPC può supportare una larghezza di banda massima di 10 Gpbs per zona di disponibilità e aumenta automaticamente fino a 100 Gbps. La larghezza di banda massima per un endpoint VPC, quando si distribuisce il carico su tutte le zone di disponibilità, è il numero di zone di disponibilità moltiplicato per 100 Gbps. Se l'applicazione richiede una velocità effettiva più elevata, contatta il supporto AWS .
- L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del più grande pacchetto consentito che può essere trasferito attraverso un endpoint VPC. Maggiore è la MTU di una connessione, maggiore è la quantità di dati che possono essere trasferiti in un unico pacchetto. Un endpoint VPC supporta una MTU di 8500 byte. I pacchetti con dimensioni superiori a 8500 byte che arrivano all'endpoint VPC vengono eliminati.

- Il percorso MTU Discovery (PMTUD) non è supportato. Gli endpoint VPC non generano il seguente messaggio ICMP: `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (Tipo 3, Codice 4).
- Gli endpoint VPC applicano il clamping MSS (Maximum Segment Size) a tutti i pacchetti. Per maggiori informazioni, consulta RFC879.

Cronologia dei documenti per AWS PrivateLink

La tabella seguente descrive le versioni per. AWS PrivateLink

Modifica	Descrizione	Data
Indirizzi IP designati	È possibile specificare gli indirizzi IP per le interfacce di rete degli endpoint quando crei o modifichi l'endpoint VPC.	17 agosto 2023
Supporto IPv6	Puoi configurare i servizi endpoint Gateway Load Balancer e gli endpoint Gateway Load Balancer in modo che supportino indirizzi IPv4 e IPv6 o solo indirizzi IPv6.	12 dicembre 2022
Contributor Insights	Puoi utilizzare le regole integrate di Contributor Insights per identificare gli endpoint specifici per i quali i principali contributori alle CloudWatch metriche. AWS PrivateLink	18 agosto 2022
Supporto IPv6	I provider di servizi possono consentire al servizio endpoint di accettare richieste IPv6, anche se i servizi back-end supportano solo IPv4. Se un servizio endpoint accetta richieste IPv6, gli utenti del servizio possono abilitare il supporto IPv6 per i propri endpoint di interfaccia in modo	11 maggio 2022

	da poter accedere al servizio endpoint tramite IPv6.	
CloudWatch metriche	AWS PrivateLink pubblica le CloudWatch metriche per gli endpoint di interfaccia, gli endpoint Gateway Load Balancer e i servizi endpoint.	27 gennaio 2022
Endpoint Gateway Load Balancer	Puoi creare un endpoint Gateway Load Balancer nel VPC per instradare il traffico a un servizio endpoint VPC configurato tramite un Gateway Load Balancer.	10 novembre 2020
Policy di endpoint VPC	È possibile collegare un criterio IAM a un endpoint VPC di interfaccia per un servizio AWS per controllare l'accesso al servizio.	23 marzo 2020
Chiavi di condizione per endpoint VPC e servizi endpoint	È possibile utilizzare le chiavi di condizione EC2 per controllare l'accesso ai servizi endpoint ed endpoint VPC.	6 marzo 2020
Assegna tag agli endpoint VPC e ai servizi endpoint VPC quando vengono creato	Puoi aggiungere tag quando crei gli endpoint VPC e i servizi endpoint.	5 febbraio 2020
Nomi DNS privati	Puoi accedere ai servizi AWS PrivateLink basati dall'interno del tuo VPC utilizzando nomi DNS privati.	6 gennaio 2020

Servizi endpoint VPC	Puoi creare un tuo servizio endpoint e consentire ad altri utenti e Account AWS di connettersi allo stesso servizio tramite un endpoint VPC di interfaccia. Puoi offrire i tuoi servizi endpoint per l'abbonamento nel Marketplace AWS.	28 novembre 2017
Endpoint VPC di interfaccia per Servizi AWS	È possibile creare un endpoint di interfaccia a cui connettersi con Servizi AWS cui integrarsi AWS PrivateLink senza utilizzare un gateway Internet o un dispositivo NAT.	8 Novembre 2017
Endpoint VPC per DynamoDB	Puoi creare un endpoint VPC gateway per accedere ad Amazon DynamoDB dal tuo VPC senza utilizzare un gateway Internet o un dispositivo NAT.	16 agosto 2017
Endpoint VPC per Amazon S3	Puoi creare un endpoint VPC gateway per accedere ad Amazon S3 dal tuo VPC senza utilizzare un gateway Internet o un dispositivo NAT.	11 maggio 2015

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.