AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

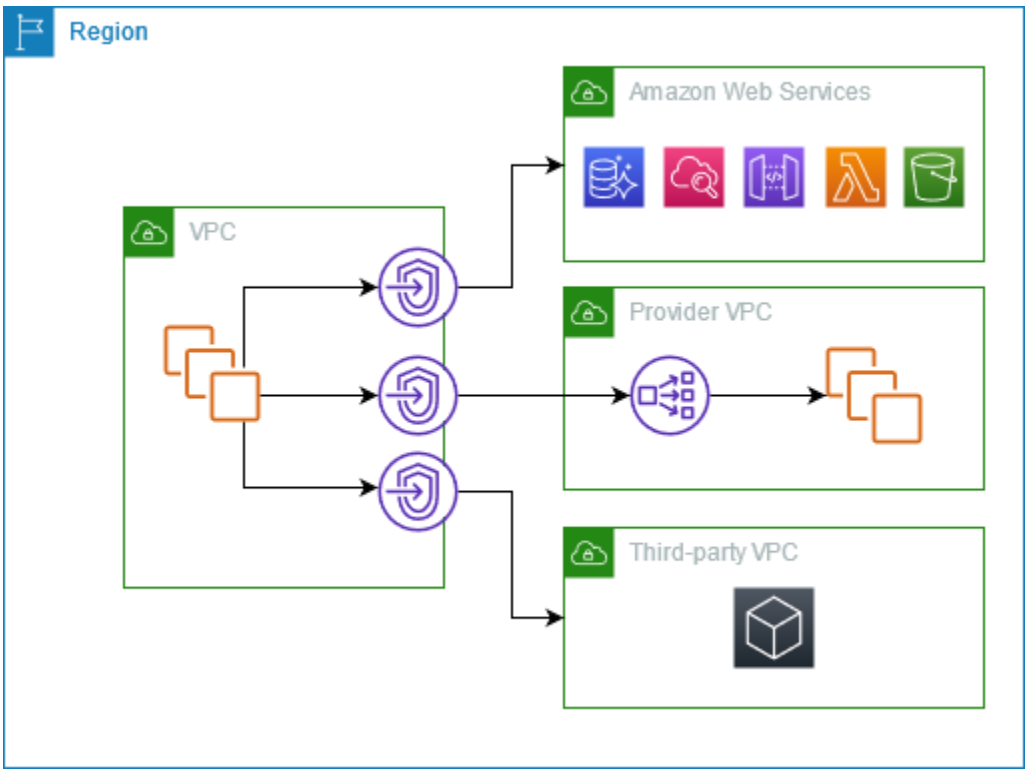
Was ist AWS PrivateLink?

AWS PrivateLink ist eine hochverfügbare, skalierbare Technologie, mit der Sie Ihre VPC privat mit Diensten verbinden können, als ob sie sich in Ihrer VPC befinden würden. Sie müssen kein Internet-Gateway, kein NAT-Gerät, keine öffentliche IP-Adresse, Verbindung oder AWS Direct Connect AWS Site-to-Site VPN Verbindung verwenden, um die Kommunikation mit dem Dienst von Ihren privaten Subnetzen aus zu ermöglichen. Daher steuern Sie die spezifischen API-Endpunkte, Websites und Services, die von Ihrer VPC aus erreichbar sind.

Anwendungsfälle

Sie können VPC-Endpoints erstellen, um Ressourcen in Ihrer VPC mit Diensten zu verbinden, die sich in integrieren lassen. AWS PrivateLink Sie können Ihren eigenen VPC-Endpunktdienst erstellen und ihn anderen AWS Kunden zur Verfügung stellen. Weitere Informationen finden Sie unter the section called “Konzepte”.

Im folgenden Diagramm verfügt die VPC auf der linken Seite über mehrere EC2-Instances in einem privaten Subnetz und drei Schnittstellen-VPC-Endpunkte. Der oberste VPC-Endpunkt stellt eine Verbindung zu einem her. AWS-Service Der mittlere VPC-Endpunkt stellt eine Verbindung zu einem Dienst her, der von einem anderen gehostet wird AWS-Konto (einem VPC-Endpunktdienst). Der untere VPC-Endpunkt stellt eine Verbindung zu einem AWS Marketplace Partnerdienst her.



Weitere Informationen

- the section called “Konzepte”
- Zugriff AWS-Services
- Zugriff auf SaaS-Produkte
- Zugriff auf virtuelle Appliances
- Teilen Sie Ihre Services

Arbeiten mit VPC-Endpunkten

Sie können VPC-Endpunkte mit einer der folgenden Funktionen erstellen, darauf zugreifen und verwalten:

- AWS Management Console— Stellt eine Weboberfläche bereit, über die Sie auf Ihre AWS PrivateLink Ressourcen zugreifen können. Öffnen Sie die Amazon VPC-Konsole und wählen Sie Endpoints oder Endpoint Services.
- AWS Command Line Interface (AWS CLI) — Stellt Befehle für eine Vielzahl von Befehlen bereit AWS-Services, darunter. AWS PrivateLink Weitere Informationen zu Befehlen für AWS PrivateLink finden Sie unter ec2 in der AWS CLI Befehlsreferenz.

- AWS CloudFormation – Erstellen Vorlagen, die Ihre AWS -Ressourcen beschreiben. Mit den Vorlagen können Sie diese Ressourcen als Einheit bereitstellen und verwalten. Weitere Informationen finden Sie in den folgenden AWS PrivateLink Ressourcen:
  - AWS::EC2::VPCEndpoint
  - AWS: :EC2: :VPC-Benachrichtigung EndpointConnection
  - AWS::EC2::VPCEndpointService
  - AWS: :EC2: :VPC-Berechtigungen EndpointService
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS SDKs — Stellen sprachspezifische APIs bereit. Die -SDKs kümmern sich um viele der Verbindungsdetails, wie z. B. das Berechnen von Signaturen, die Verarbeitung von Anforderungswiederholungen und die Behandlung von Fehlern. Weitere Informationen finden Sie unter Tools, auf denen Sie aufbauen können. AWS
- Abfrage-API – Bietet API-Aktionen auf niedriger Ebene, die Sie mithilfe von HTTPS-Anforderungen aufrufen. Die Verwendung der Abfrage-API ist die direkteste Möglichkeit für den Zugriff auf Amazon VPC. Allerdings müssen dann viele technische Abläufe, wie beispielsweise das Erzeugen des Hashwerts zum Signieren der Anforderung und zur Fehlerbehandlung, in der Anwendung durchgeführt werden. Weitere Informationen finden Sie unter AWS PrivateLink -Aktionen in der Amazon-EC2-API-Referenz.

Preisgestaltung

Weitere Informationen zu den Preisen für VPC-Endpunkte finden Sie unter AWS PrivateLink -Preise.

AWS PrivateLink Konzepte

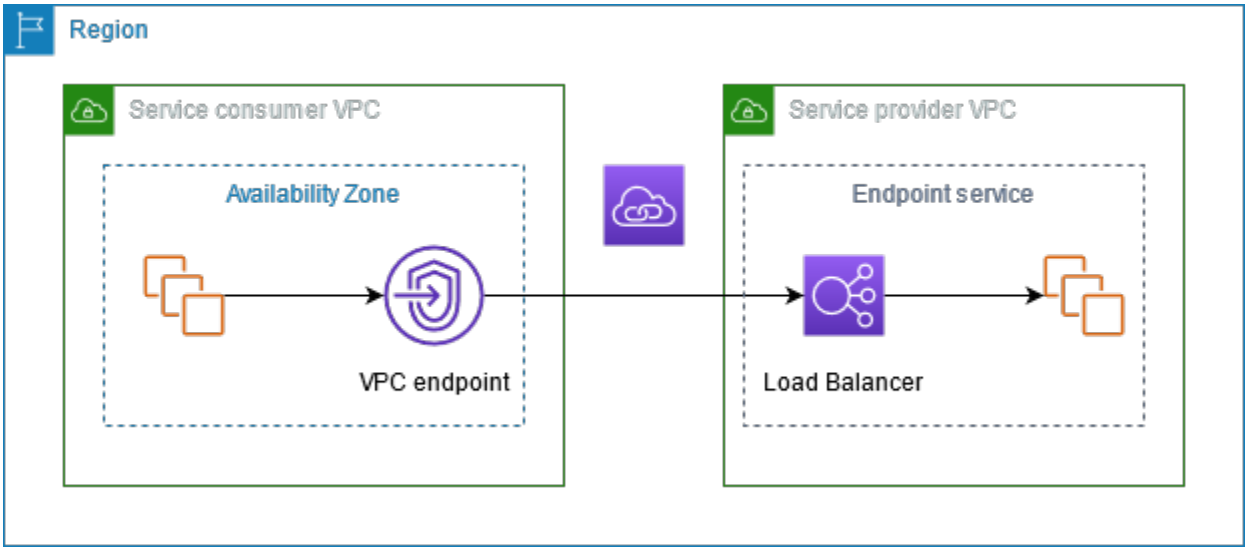
Sie können mithilfe von Amazon VPC eine Virtual Private Cloud (VPC) definieren. Dabei handelt es sich um ein logisch isoliertes virtuelles Netzwerk. Sie können AWS Ressourcen in Ihrer VPC starten. Sie können zulassen, dass die Ressourcen in Ihrer VPC eine Verbindung zu Ressourcen außerhalb dieser VPC herstellen. Fügen Sie beispielsweise ein Internet-Gateway zur VPC hinzu, um den Zugriff auf das Internet zu ermöglichen, oder fügen Sie eine VPN-Verbindung hinzu, um den Zugriff auf Ihr On-Premises-Netzwerk zu ermöglichen. Alternativ können Sie es AWS PrivateLink den Ressourcen in Ihrer VPC ermöglichen, über private IP-Adressen eine Verbindung zu Diensten in anderen VPCs herzustellen, als ob diese Dienste direkt in Ihrer VPC gehostet würden.

Die folgenden Konzepte sollten Sie verstehen, wenn Sie mit der Verwendung von AWS PrivateLink beginnen.

Inhalt

Architekturdiagramm

Das folgende Diagramm bietet einen allgemeinen Überblick über die Funktionsweise. AWS PrivateLink Service-Verbraucher erstellen Schnittstellen-VPC-Endpunkte, um eine Verbindung zu Endpunkt-Services herzustellen, die von Service-Anbietern gehostet werden.



Service-Anbieter

Der Besitzer eines Services ist der Service-Anbieter. Zu den Dienstanbietern gehören AWS AWS Partner und andere AWS-Konten. Dienstanbieter können ihre Dienste mithilfe von AWS Ressourcen wie EC2-Instances oder mithilfe von lokalen Servern hosten.

Konzepte

- Endpunkt-Services

Endpunkt-Services

Ein Service-Anbieter erstellt einen Endpunkt-Service, um ihren Service in einer Region verfügbar zu machen. Ein Service-Anbieter muss beim Erstellen eines Endpunkt-Services einen Load Balancer angeben. Der Load Balancer erhält Anfragen von Service-Verbrauchern und leitet sie an Ihren Service weiter.

Standardmäßig ist Ihr Endpunkt-Service für Service-Verbraucher nicht verfügbar. Sie müssen Berechtigungen hinzufügen, die es bestimmten AWS Prinzipalen ermöglichen, eine Verbindung zu Ihrem Endpunktdienst herzustellen.

Service-Namen

Jeder Endpunkt-Service wird durch einen Service-Namen identifiziert. Ein Service-Verbraucher muss beim Erstellen eines VPC-Endpunkts den Namen des Services angeben. Dienstnutzer können die Dienstnamen für AWS-Services abfragen. Service-Anbieter müssen die Namen ihrer Services mit den Service-Verbrauchern teilen.

Service-Zustände

Die folgenden Zustände sind für einen Endpunkt-Service möglich:

- `Pending` – Der Endpunkt-Service wird gerade erstellt.
- `Available` – Der Endpunkt-Service ist verfügbar.
- `Failed` – Der Endpunktservice konnte nicht erstellt werden.
- `Deleting` – Der Service-Anbieter hat den Endpunkt-Service gelöscht und der Löschvorgang ist im Gange.
- `Deleted` – Der Endpunkt-Service wurde gelöscht.

Service-Verbraucher

Der Benutzer eines Services ist ein Service-Verbraucher. Dienstnutzer können über AWS Ressourcen wie EC2-Instances oder über lokale Server auf Endpunktdienste zugreifen.

Konzepte

- VPC-Endpunkte
- Endpunkt-Netzwerkschnittstellen
- Endpunktrichtlinien
- Endpunktzustände

VPC-Endpunkte

Service-Verbraucher können einen VPC-Endpunkt erstellen, um seine VPC mit einem Endpunkt-Service zu verbinden. Ein Service-Verbraucher muss beim Erstellen eines VPC-Endpunkts den Servicenamen des Endpunktservices angeben. Es gibt mehrere Arten von VPC-Endpunkten. Sie müssen die Art von VPC-Endpunkt erstellen, die von dem Endpunktservice benötigt wird.

- `Interface` – Erstellen Sie einen Schnittstellenendpunkt, um Netzwerkdatenverkehr zu einem Endpunktservice zu senden. Der für den Endpunkt-Service bestimmte Datenverkehr wird mithilfe von DNS aufgelöst.
- `GatewayLoadBalancer` – Erstellen Sie einen Gateway-Load-Balancer-Endpunkt, um Datenverkehr an eine Flotte virtueller Appliances unter Verwendung privater IP-Adressen zu senden. Sie können den Datenverkehr von Ihrer VPC mithilfe von Routing-Tabellen an den Gateway-Load-Balancer-Endpunkt leiten. Der Gateway Load Balancer verteilt den Datenverkehr an die virtuellen Appliances und kann je nach Bedarf skalieren.

Es gibt einen anderen VPC-Endpunkt, `Gateway`, der einen Gateway-Endpunkt erstellt, um Datenverkehr an Amazon S3 oder DynamoDB zu senden. Gateway-Endpunkte verwenden im AWS PrivateLink Gegensatz zu den anderen Arten von VPC-Endpunkten nicht. Weitere Informationen finden Sie unter the section called “Gateway-Endpunkte”.

Endpunkt-Netzwerkschnittstellen

Eine Endpunkt-Netzwerkschnittstelle ist eine vom Anforderer verwaltete Netzwerkschnittstelle, die als Einstiegspunkt für Datenverkehr dient, der für einen Endpunkt-Service bestimmt ist. Für jedes Subnetz, das Sie beim Erstellen eines VPC-Endpunkts angeben, erstellen wir eine Endpunkt-Netzwerkschnittstelle im Subnetz.

Wenn ein VPC-Endpunkt IPv4 unterstützt, verfügen Endpunkt-Netzwerkschnittstellen über IPv4-Adressen. Wenn ein VPC-Endpunkt IPv6 unterstützt, verfügen Endpunkt-Netzwerkschnittstellen

über IPv6-Adressen. Die IPv6-Adresse für eine Endpunkt-Netzwerkschnittstelle ist aus dem Internet nicht erreichbar. Wenn Sie eine Endpunktnetzwerkschnittstelle mit einer IPv6-Adresse beschreiben, beachten Sie, dass `denyAllIgwTraffic` aktiviert ist.

Die IP-Adressen einer Endpunkt-Netzwerkschnittstelle ändern sich während der Lebensdauer ihres VPC-Endpunkts nicht.

Endpunktrichtlinien

Eine VPC-Endpunktrichtlinie ist eine IAM-Ressourcenrichtlinie, die Sie Ihrem VPC-Endpunkt anfügen können. Sie bestimmt, welche Prinzipale den VPC-Endpunkt verwenden können, um auf den Endpunkt-Service zuzugreifen. Die standardmäßige VPC-Endpunktrichtlinie erlaubt alle Aktionen aller Prinzipale auf allen Ressourcen über den VPC-Endpunkt.

Endpunktzustände

Wenn Sie einen VPC-Endpunkt erstellen, empfängt der Endpunkt-Service eine Verbindungsanfrage. Der Service-Anbieter kann die Anfrage annehmen oder ablehnen. Wenn der Service-Anbieter die Anforderung akzeptiert, kann der Service-Verbraucher den VPC-Endpunkt verwenden, nachdem er in den `Available`-Status eingetreten ist.

Die folgenden Zustände sind für einen VPC-Endpunkt möglich:

- `PendingAcceptance` – Die Verbindungsanfrage steht noch aus. Dies ist der Ausgangszustand, wenn Anfragen manuell akzeptiert werden.
- `Pending` – Der Service-Anbieter hat die Verbindungsanfrage akzeptiert. Dies ist der Ausgangszustand, wenn Anfragen automatisch akzeptiert werden. Der VPC-Endpunkt kehrt in diesen Zustand zurück, wenn der Service-Verbraucher den VPC-Endpunkt ändert.
- `Available` – Der VPC-Endpunkt steht zur Verwendung zur Verfügung.
- `Rejected` – Der Service-Anbieter hat die Verbindungsanfrage abgelehnt. Der Service-Anbieter kann eine Verbindung auch ablehnen, nachdem sie zur Verwendung verfügbar ist.
- `Expired` – Die Verbindungsanfrage ist abgelaufen.
- `Failed` – Der VPC-Endpunkt konnte nicht verfügbar gemacht werden.
- `Deleting` – Der Service-Verbraucher hat den VPC-Endpunkt gelöscht und der Löschvorgang ist im Gange.
- `Deleted` – Der VPC-Endpunkt wurde gelöscht.

AWS PrivateLink Verbindungen

Datenverkehr von Ihrer VPC wird über eine Verbindung zwischen dem VPC-Endpunkt und dem Endpunktservice an einen Endpunktservice gesendet. Der Verkehr zwischen einem VPC-Endpunkt und einem Endpunktdienst verbleibt im AWS Netzwerk, ohne das öffentliche Internet zu durchqueren.

Ein Serviceanbieter fügt Berechtigungen hinzu, damit Servicenutzer auf den Endpunktservice zugreifen können. Der Servicenutzer initiiert die Verbindung und der Serviceanbieter akzeptiert die Verbindungsanfrage oder lehnt sie ab.

Mit Schnittstellen-VPC-Endpunkten können Servicenutzer Endpunktrichtlinien verwenden, um zu steuern, welche IAM-Prinzipale einen VPC-Endpunkt für den Zugriff auf einen Endpunktservice verwenden können.

Private gehostete Zonen

Eine gehostete Zone ist ein Container für DNS-Einträge, die definieren, wie der Datenverkehr für eine Domain oder Subdomain weitergeleitet werden soll. Bei einer öffentlich gehosteten Zone geben die Datensätze an, wie der Datenverkehr im Internet weitergeleitet werden soll. Bei einer privat gehosteten Zone geben die Datensätze an, wie der Datenverkehr in Ihren VPCs weitergeleitet werden soll.

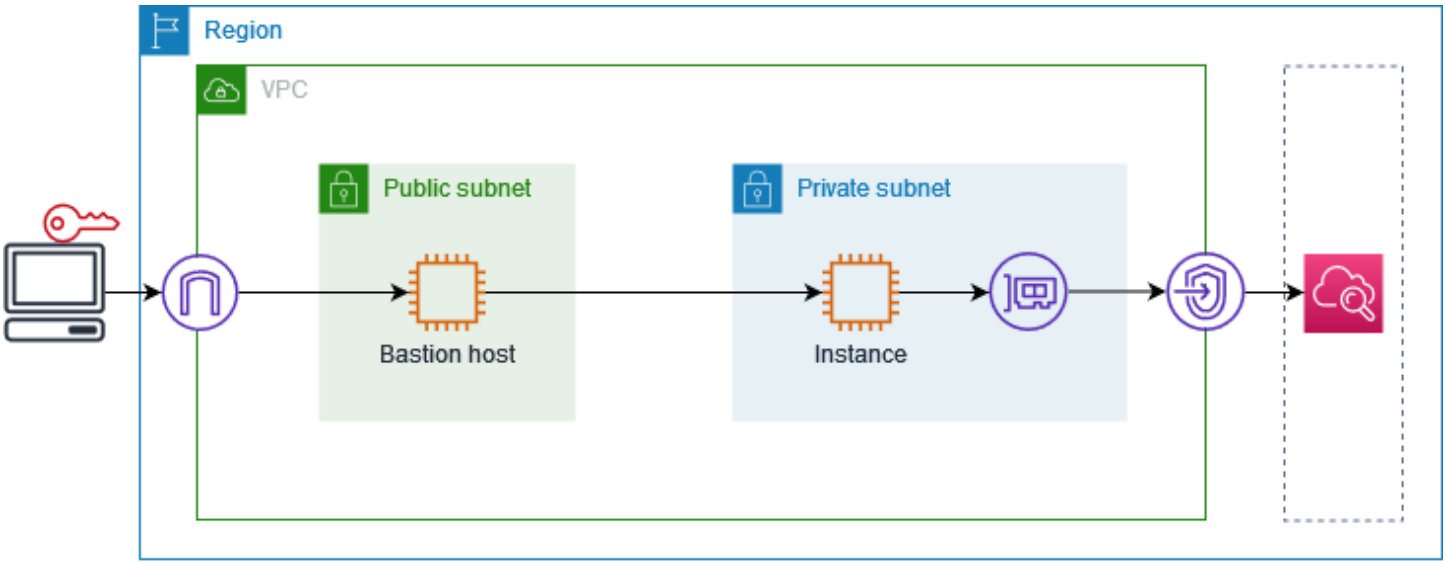
Sie können Amazon Route 53 so konfigurieren, dass der Domain-Datenverkehr an einen VPC-Endpunkt weitergeleitet wird. Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs an einen VPC-Endpunkt mit Ihrem Domain-Namen.

Sie können Route 53 verwenden, um Split-Horizon-DNS zu konfigurieren, wobei Sie denselben Domainnamen sowohl für eine öffentliche Website als auch für einen Endpunktdienst verwenden, der von betrieben wird. AWS PrivateLink DNS-Anfragen für den öffentlichen Hostnamen von der Verbraucher-VPC werden in die privaten IP-Adressen der Endpunkt-Netzwerkschnittstellen aufgelöst, aber Anfragen von außerhalb der VPC werden weiterhin an die öffentlichen Endpunkte aufgelöst. Weitere Informationen finden Sie unter DNS-Mechanismen zum Routing des Datenverkehrs und Aktivieren von Failover für AWS PrivateLink -Bereitstellungen.

Fangen Sie an mit AWS PrivateLink

Dieses Tutorial zeigt, wie Sie mithilfe von eine EC2-Instance in einem privaten Subnetz eine Anfrage an Amazon CloudWatch senden. AWS PrivateLink

Das folgende Diagramm gibt einen Überblick über dieses Szenario. Um eine Verbindung von Ihrem Computer zur Instance im privaten Subnetz herzustellen, müssen Sie zunächst eine Verbindung zu einem Bastion-Host in einem öffentlichen Subnetz herstellen. Sowohl der Bastion-Host als auch die Instance müssen das gleiche Schlüsselpaar verwenden. Da sich die `.pem`-Datei für den privaten Schlüssel auf Ihrem Computer und nicht auf dem Bastion-Host befindet, verwenden Sie die SSH-Schlüsselweiterleitung. Dann können Sie über den Bastion-Host eine Verbindung mit der Instance herstellen, ohne die `.pem`-Datei im ssh-Befehl anzugeben. Nachdem Sie einen VPC-Endpunkt für eingerichtet haben CloudWatch, wird der Datenverkehr von der Instance, für die bestimmt CloudWatch ist, zur Endpunkt-Netzwerkschnittstelle aufgelöst und dann an die CloudWatch Verwendung des VPC-Endpunkts gesendet.



Zu Testzwecken können Sie eine einzelne Availability Zone verwenden. In der Produktion empfehlen wir Ihnen, mindestens zwei Availability Zones für niedrige Latenz und hohe Verfügbarkeit zu verwenden.

Aufgaben

- Schritt 1: Erstellen einer VPC mit Subnetzen
- Schritt 2: Starten der Instances
- Schritt 3: Testen CloudWatch Sie den Zugriff

Schritt 1: Erstellen einer VPC mit Subnetzen

Gehen Sie wie folgt vor, um eine VPC mit einem öffentlichen Subnetz und einem privaten Subnetz zu erstellen.

So erstellen Sie die VPC

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie VPC erstellen aus.
3. Wählen Sie unter Resources to create (Zu erstellende Ressourcen) die Option VPC and more (VPC und mehr) aus.
4. Geben Sie unter Name tag auto-generation (Automatische Generierung des Namens-Tags) einen Namen für die VPC ein.
5. Führen Sie zur Konfiguration der Subnetze folgende Schritte aus:
    a. Wählen Sie unter Number of Availability Zones (Anzahl der Availability Zones) je nach Bedarf 1 oder 2 aus.
    b. Stellen Sie unter Number of public subnets (Anzahl der öffentlichen Subnetze) sicher, dass ein öffentliches Subnetz pro Availability Zone vorhanden ist.
    c. Stellen Sie unter Number of private subnets (Anzahl der privaten Subnetze) sicher, dass ein privates Subnetz pro Availability Zone vorhanden ist.
6. Wählen Sie VPC erstellen aus.

Schritt 2: Starten der Instances

Starten Sie unter Verwendung der im vorherigen Schritt erstellten VPC den Bastion-Host im öffentlichen Subnetz und die Instance im privaten Subnetz.

Voraussetzungen

- Erstellen Sie ein Schlüsselpaar im PEM-Format. Sie müssen dieses Schlüsselpaar auswählen, wenn Sie sowohl den Bastion-Host als auch die Instance starten.

- Erstellen Sie eine Sicherheitsgruppe für den Bastion-Host, die eingehenden SSH-Verkehr vom CIDR-Block für Ihren Computer zulässt.
- Erstellen Sie eine Sicherheitsgruppe für die Instance, die eingehenden SSH-Verkehr von der Sicherheitsgruppe für den Bastion-Host zulässt.
- Erstellen Sie ein IAM-Instanzprofil und fügen Sie die Zugriffsrichtlinie an. CloudWatch ReadOnly

Starten des Bastion-Hosts

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Launch Instance (Instance starten) aus.
3. Geben Sie unter Name einen Namen für Ihren Bastion-Host ein.
4. Behalten Sie das Standard-Image und den Instance-Typ bei.
5. Wählen Sie unter Key pair (Schlüsselpaar) Ihr Schlüsselpaar aus.
6. Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:
    a. Wählen Sie unter VPC Ihre VPC aus.
    b. Wählen Sie unter Subnet (Subnetz) das öffentliche Subnetz aus.
    c. Wählen Sie unter Auto-assign public IP (Öffentlche IP automatisch zuweisen) die Option Enable (Aktivieren) aus.
    d. Wählen Sie unter Firewall die Option Select existing security group (Vorhandene Sicherheitsgruppe auswählen) aus und wählen Sie dann die Sicherheitsgruppe für den Bastion-Host aus.
7. Wählen Sie Launch Instance (Instance starten) aus.

So starten Sie die Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Launch Instance (Instance starten) aus.
3. Geben Sie unter Name einen Namen für Ihre Instance ein.
4. Behalten Sie das Standard-Image und den Instance-Typ bei.
5. Wählen Sie unter Key pair (Schlüsselpaar) Ihr Schlüsselpaar aus.
6. Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:
    a. Wählen Sie unter VPC Ihre VPC aus.

b. Wählen Sie unter Subnet (Subnetz) das private Subnetz aus.

c. Wählen Sie unter Auto-assign public IP (Öffentliche IP automatisch zuweisen) die Option Disable (Deaktivieren) aus.

d. Wählen Sie unter Firewall die Option Select existing security group (Vorhandene Sicherheitsgruppe auswählen) aus und wählen Sie dann die Sicherheitsgruppe für die Instance aus.

7. Erweitern Sie Advanced Details (Erweiterte Details). Wählen Sie unter IAM instance profile (IAM-Instance-Profil) Ihre IAM-Instance-Profil aus.
8. Wählen Sie Launch Instance (Instance starten) aus.

Schritt 3: Testen CloudWatch Sie den Zugriff

Gehen Sie wie folgt vor, um zu bestätigen, dass die Instanz nicht darauf zugreifen kann CloudWatch. Dazu verwenden Sie einen schreibgeschützten AWS CLI Befehl für. CloudWatch

Um den Zugriff zu testen CloudWatch

1. Fügen Sie auf Ihrem Computer das Schlüsselpaar mit dem folgenden Befehl zum SSH-Agent hinzu, wobei *key.pem* der Name Ihrer PEM-Datei ist.

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

   Wenn Sie die Fehlermeldung erhalten, dass die Berechtigungen für Ihr Schlüsselpaar zu offen sind, führen Sie den folgenden Befehl aus und wiederholen Sie dann den vorherigen Befehl.

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

2. Stellen Sie auf Ihrem Computer eine Verbindung mit dem Bastion-Host her. Sie müssen die Option `-A`, den Benutzernamen der Instance (z. B. `ec2-user`) und die öffentliche IP-Adresse des Bastion-Hosts angeben.

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

3. Stellen Sie über den Bastion-Host eine Verbindung zur Instance her. Sie müssen den Benutzernamen der Instance (z. B. `ec2-user`) und die private IP-Adresse der Instance angeben.

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

4. Führen Sie den Befehl CloudWatch list-metrics auf der Instance wie folgt aus. Geben Sie für die Option `--region` die Region an, in der Sie die VPC erstellt haben.

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

5. Nach einigen Minuten tritt ein Timeout für den Befehl auf. Dies zeigt, dass Sie CloudWatch von der Instance aus mit der aktuellen VPC-Konfiguration nicht darauf zugreifen können.

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

6. Bleiben Sie mit Ihrer Instance verbunden. Nachdem Sie den VPC-Endpunkt erstellt haben, führen Sie diesen list-metrics.Befehl erneut aus.

Schritt 4: Erstellen Sie einen VPC-Endpunkt für den Zugriff CloudWatch

Gehen Sie wie folgt vor, um einen VPC-Endpunkt zu erstellen, mit dem eine Verbindung hergestellt wird. CloudWatch

Voraussetzung

Erstellen Sie eine Sicherheitsgruppe für den VPC-Endpunkt, zu CloudWatch der Datenverkehr zugelassen wird. Fügen Sie zum Beispiel eine Regel hinzu, die HTTPS-Datenverkehr vom VPC-CIDR-Block zulässt.

So erstellen Sie einen VPC-Endpunkt für CloudWatch

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Geben Sie unter Name tag (Name-Tag) einen Namen für den Endpunkt ein.
5. Wählen Sie für Servicekategorie die Option AWS-Services aus.
6. Wählen Sie unter Service die Option com.amazonaws.***region***.monitoring aus.
7. Wählen Sie im Feld VPC Ihre VPC aus.

8. Wählen Sie unter Subnets (Subnetze) die Availability Zone und dann das private Subnetz aus.
9. Wählen Sie unter Security group (Sicherheitsgruppe) die Sicherheitsgruppe für den VPC-Endpunkt aus.
10. Wählen Sie für Policy (Richtlinie) Full access (Vollzugriff), um alle Operationen aller Prinzipale auf allen Ressourcen über den VPC-Endpunkt zuzulassen.
11. (Optional) Sie fügen ein Tag hinzu, indem Sie neuen Tag hinzufügen auswählen und den Schlüssel und den Wert für den Tag eingeben.
12. Wählen Sie Endpunkt erstellen. Der Anfangsstatus lautet Pending (Ausstehend). Bevor Sie mit dem nächsten Schritt fortfahren, warten Sie, bis der Status Available (Verfügbar) ist. Dies kann einige Minuten dauern.

Schritt 5: Testen des VPC-Endpunkts

Stellen Sie sicher, dass der VPC-Endpunkt Anfragen von Ihrer Instance an CloudWatch sendet.

So testen Sie den VPC-Endpunkt

Führen Sie den folgenden Befehl auf Ihrer Instance aus. Geben Sie für die Option `--region` die Region an, in der Sie den VPC-Endpunkt erstellt haben.

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

Wenn Sie eine Antwort erhalten, auch wenn es sich um eine Antwort mit leeren Ergebnissen handelt, sind Sie mit der CloudWatch Verwendung AWS PrivateLink verbunden.

Wenn Sie eine `UnauthorizedOperation` Fehlermeldung erhalten, stellen Sie sicher, dass die Instance über eine IAM-Rolle verfügt, die den Zugriff CloudWatch auf ermöglicht.

Wenn bei der Anforderung eine Zeitüberschreitung auftritt, überprüfen Sie Folgendes:

- Die Sicherheitsgruppe für den Endpunkt ermöglicht den Datenverkehr zu CloudWatch.
- Die Option `--region` gibt die Region an, in der Sie den VPC-Endpunkt erstellt haben.

Schritt 6: Bereinigen

Wenn Sie den Bastion-Host und die Instance, die Sie für dieses Tutorial erstellt haben, nicht mehr benötigen, können Sie sie beenden.

So beenden Sie die Instances

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie beide Test-Instances aus und wählen Sie dann Instance state (Instance-Status), Terminate instance (Instance beenden).
4. Wählen Sie Terminate (Kündigen) aus, wenn Sie zur Bestätigung aufgefordert werden.

Wenn Sie den VPC-Endpunkt nicht mehr benötigen, können Sie ihn löschen.

Löschen des VPC-Endpunkts

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den VPC-Endpunkt.
4. Wählen Sie Actions (Aktionen), Delete VPC Endpoint (VPC-Endpunkte löschen).
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.

Zugriff AWS-Services über AWS PrivateLink

Sie greifen auf einen Endpunkt zu und AWS-Service verwenden ihn. Die standardmäßigen Service-Endpunkte sind öffentliche Schnittstellen, daher müssen Sie Ihrer VPC ein Internet-Gateway hinzufügen, damit der Datenverkehr von der VPC zur AWS-Service gelangen kann. Wenn diese Konfiguration Ihren Netzwerksicherheitsanforderungen nicht entspricht, können Sie Ihre VPC so AWS PrivateLink verbinden, AWS-Services als ob sie sich in Ihrer VPC befinden würden, ohne ein Internet-Gateway verwenden zu müssen.

Sie können privat auf diejenigen zugreifen AWS-Services , die AWS PrivateLink mithilfe von VPC-Endpunkten integriert sind. Sie können alle Ebenen Ihres Anwendungs-Stacks erstellen und verwalten, ohne ein Internet-Gateway zu verwenden.

Preisgestaltung

Ihnen wird jede Stunde in Rechnung gestellt, in der Ihr Schnittstellen-VPC-Endpunkt in jeder Availability Zone bereitgestellt wird. Ihnen wird auch pro GB verarbeiteter Daten in Rechnung gestellt. Weitere Informationen finden Sie unter AWS PrivateLink -Preisgestaltung.

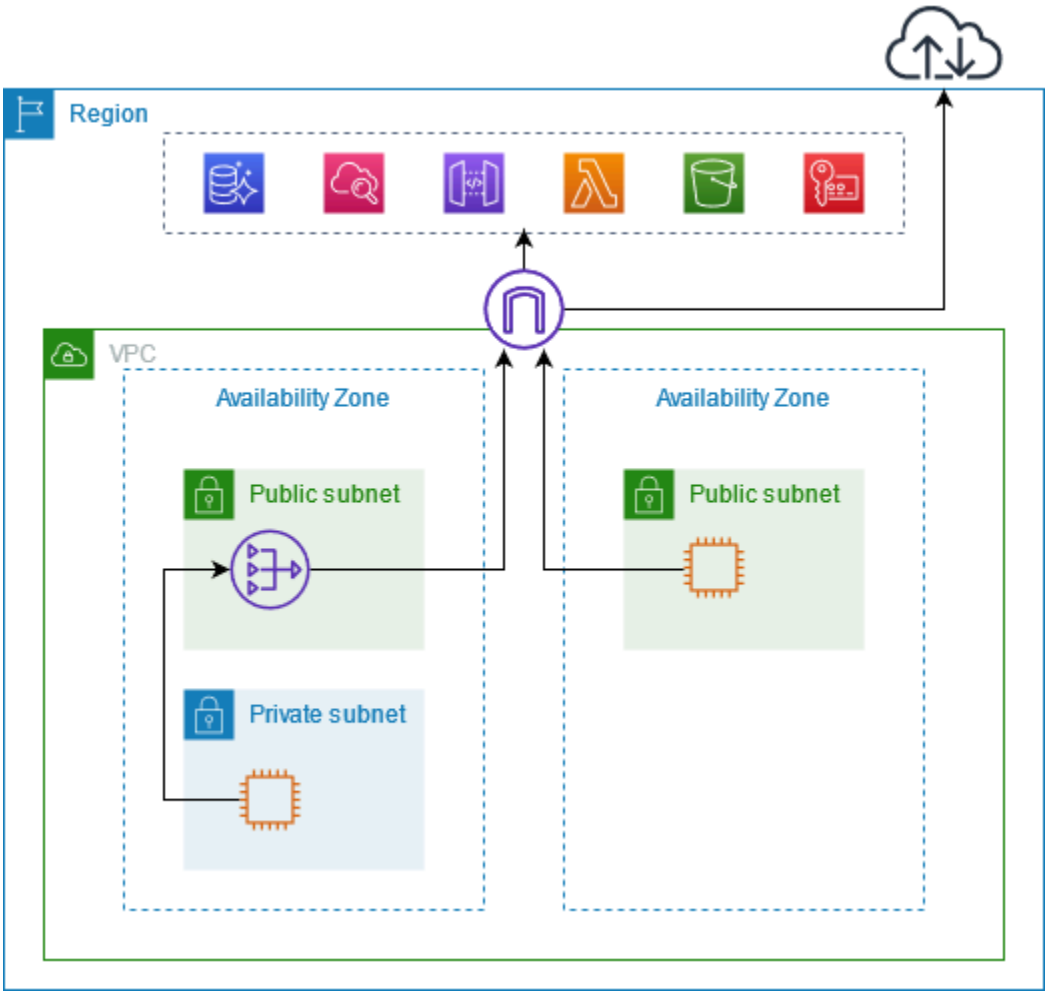
Inhalt

Übersicht

Sie können AWS-Services über ihre öffentlichen Dienstendpunkte darauf zugreifen oder eine Verbindung zu unterstützten AWS-Services Benutzern herstellen. AWS PrivateLink In dieser Übersicht werden diese Methoden verglichen.

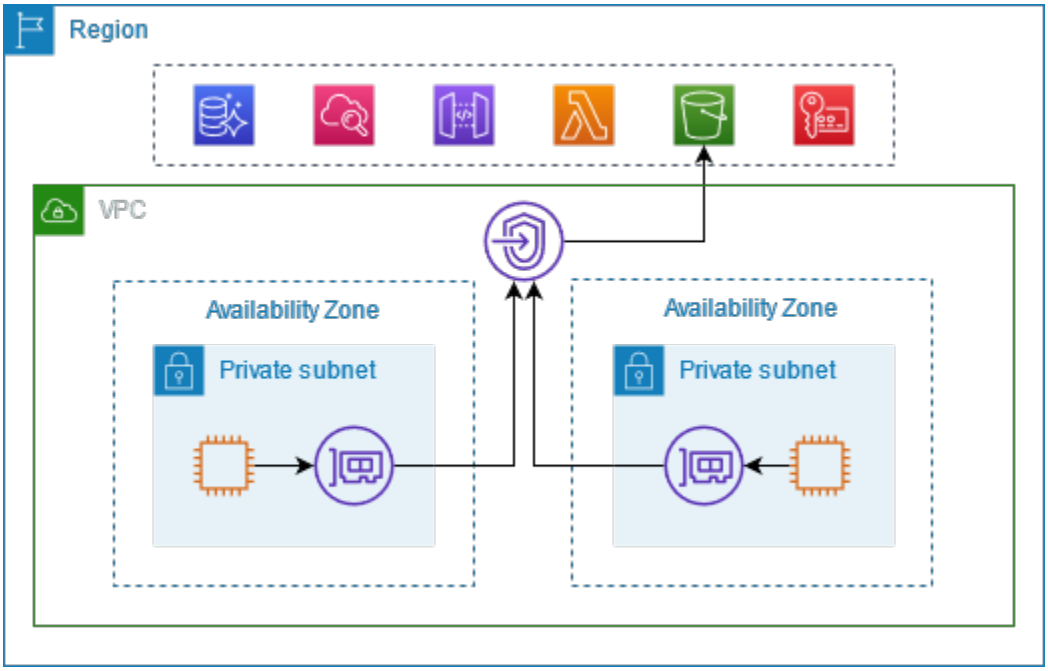
Zugang über Endpunkte für öffentliche Services

Das folgende Diagramm zeigt, wie Instanzen AWS-Services über die Endpunkte des öffentlichen Dienstes zugreifen. Der Datenverkehr zu und AWS-Service von einer Instance in einem öffentlichen Subnetz wird an das Internet-Gateway für die VPC und dann an die weitergeleitet. AWS-Service Datenverkehr zu einem AWS-Service von einer Instance in einem privaten Subnetz wird zu einem NAT-Gateway, dann zum Internet-Gateway für die VPC und dann an die AWS-Service geroutet. Dieser Datenverkehr durchquert zwar das Internet-Gateway, verlässt das Netzwerk jedoch nicht. AWS



Connect über AWS PrivateLink

Das folgende Diagramm zeigt, wie Instanzen AWS-Services über zugreifen AWS PrivateLink. Zunächst erstellen Sie einen VPC-Schnittstellen-Endpunkt, der Verbindungen zwischen den Subnetzen in Ihrer VPC und einer AWS-Service verwendenden Netzwerkschnittstelle herstellt. Der für den bestimmte Datenverkehr AWS-Service wird mithilfe von DNS an die privaten IP-Adressen der Endpunkt-Netzwerkschnittstellen aufgelöst und dann an die Verbindung gesendet, die die Verbindung zwischen dem VPC-Endpunkt und dem AWS-Service verwendet. AWS-Service



AWS-Services akzeptiert Verbindungsanfragen automatisch. Der Service kann keine Anfragen an Ressourcen über den VPC-Endpunkt veranlassen.

DNS-Hostnamen

Die meisten AWS-Services bieten öffentliche regionale Endpunkte an, die die folgende Syntax haben.

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

Der öffentliche Endpunkt für Amazon CloudWatch in us-east-2 lautet beispielsweise wie folgt.

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

Mit AWS PrivateLink senden Sie Traffic über private Endpunkte an den Service. Wenn Sie einen VPC-Schnittstellen-Endpunkt erstellen, erstellen wir regionale und zonale DNS-Namen, mit denen Sie AWS-Service von Ihrer VPC aus kommunizieren können.

Der regionale DNS-Name für Ihren Schnittstellen-VPC-Endpunkt hat die folgende Syntax:

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

Die zonalen DNS-Namen haben die folgende Syntax:

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

Wenn Sie einen VPC-Schnittstellen-Endpunkt für einen erstellen AWS-Service, können Sie privates DNS aktivieren. Mit Private DNS können Sie weiterhin Anfragen an einen Dienst unter Verwendung des DNS-Namens für seinen öffentlichen Endpunkt stellen, während Sie die private Konnektivität über den VPC-Endpunkt der Schnittstelle nutzen. Weitere Informationen finden Sie unter the section called “DNS-Auflösung”.

Der folgende Befehl describe-vpc-endpoints zeigt die DNS-Einträge für einen Schnittstellenendpunkt an.

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

Im Folgenden finden Sie eine Beispielausgabe für einen Schnittstellenendpunkt für Amazon CloudWatch mit aktivierten privaten DNS-Namen. Der erste Eintrag ist der private regionale Endpunkt. Die nächsten drei Einträge sind die privaten zonalen Endpunkte. Der letzte Eintrag stammt aus der versteckten privaten gehosteten Zone, die Anforderungen an den öffentlichen Endpunkt an die privaten IP-Adressen der Endpunkt-Netzwerkschnittstellen auflöst.

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

DNS-Auflösung

Die DNS-Einträge, die wir für Ihren Schnittstellen-VPC-Endpunkt erstellen, sind öffentlich. Daher sind diese DNS-Namen öffentlich auflösbar. DNS-Anfragen von außerhalb der VPC geben jedoch weiterhin die privaten IP-Adressen der Endpunkt-Netzwerkschnittstellen zurück, sodass diese IP-Adressen nur dann für den Zugriff auf den Endpunkt-Service verwendet werden können, wenn Sie Zugriff auf die VPC haben.

Privates DNS

Wenn Sie privates DNS für Ihren Schnittstellen-VPC-Endpunkt aktivieren und in Ihrer VPC sowohl DNS-Hostnamen als auch DNS-Auflösung aktiviert sind, erstellen wir eine versteckte, AWS verwaltete private gehostete Zone für Sie. Die gehostete Zone enthält einen Datensatz für den DNS-Standardnamen für den Service, der in die privaten IP-Adressen der Endpunktnetzwerkschnittstellen in Ihrer VPC aufgelöst wird. Wenn Sie also bereits über Anwendungen verfügen, die Anfragen an einen öffentlichen regionalen Endpunkt senden, werden diese Anfragen jetzt über die Netzwerkschnittstellen der Endgeräte weitergeleitet, ohne dass Sie Änderungen an diesen Anwendungen vornehmen müssen. AWS-Service

Wir empfehlen Ihnen, private DNS-Namen für Ihre VPC-Endpunkte für zu aktivieren. AWS-Services Dadurch wird sichergestellt, dass Anfragen, die die Endpunkte des öffentlichen Dienstes verwenden, z. B. Anfragen, die über ein AWS SDK gestellt wurden, an Ihren VPC-Endpunkt weitergeleitet werden.

Amazon stellt einen DNS-Server für Ihre VPC zu Verfügung, den Route 53 Resolver. Der Route 53 Resolver löst automatisch lokale VPC-Domainnamen und Datensätze in privaten gehosteten Zonen. Sie können den Route 53 Resolver jedoch nicht von außerhalb Ihrer VPC verwenden. Wenn Sie auf Ihren VPC-Endpunkt von Ihrem On-Premises-Netzwerk aus zugreifen möchten, können Sie Route 53 Resolver-Endpunkte und Resolver-Regeln verwenden. Weitere Informationen finden Sie unter Integration AWS Transit Gateway mit AWS PrivateLink und. Amazon Route 53 Resolver

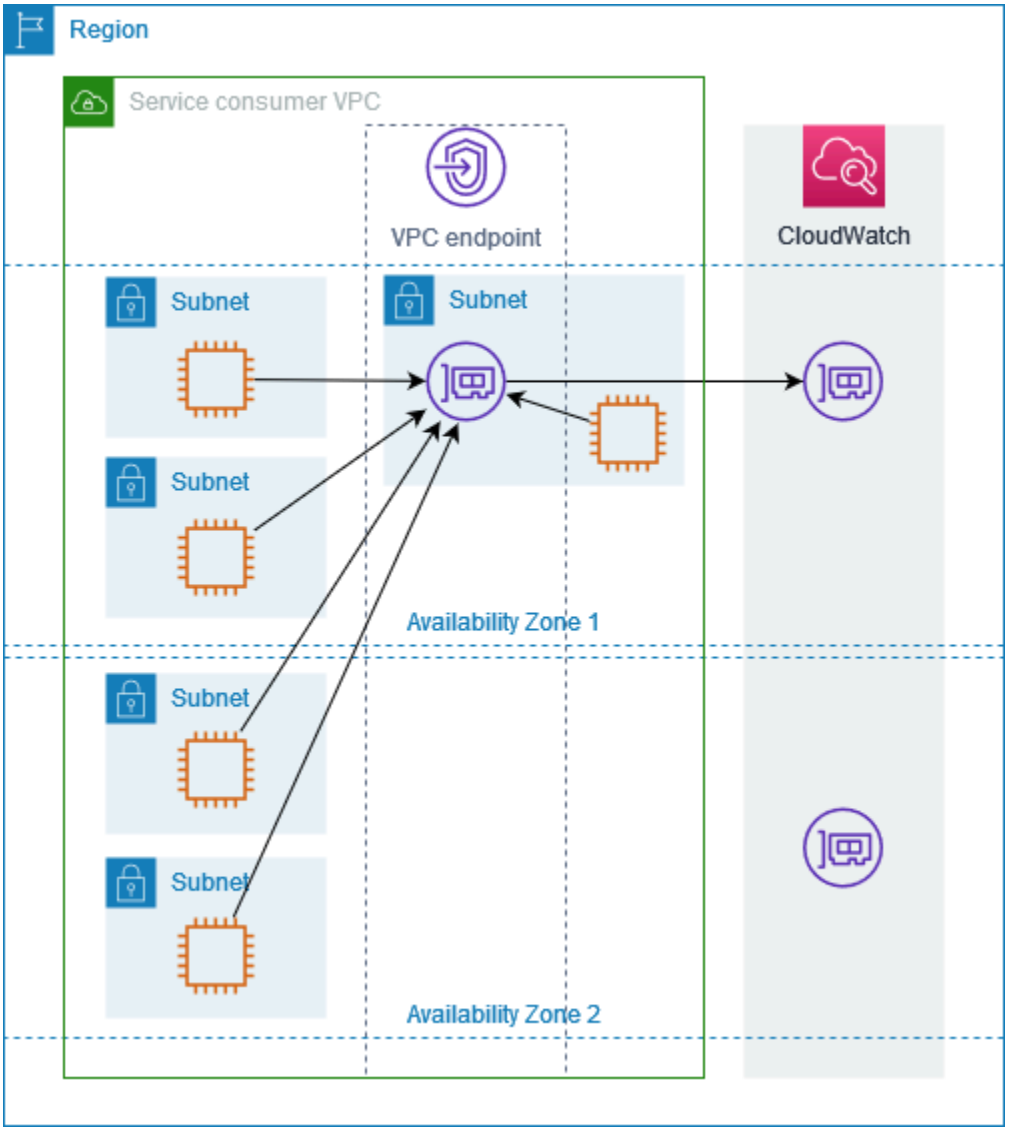
Subnetze und Availability Zones

Sie können Ihre VPC-Endpunkte mit einem Subnetz pro Availability Zone konfigurieren. Wir erstellen eine Endpunkt-Netzwerkschnittstelle für den VPC-Endpunkt in Ihrem Subnetz. Wir weisen jeder Endpunkt-Netzwerkschnittstelle aus ihrem Subnetz IP-Adressen zu, basierend auf dem IP-Adresstyp des VPC-Endpunkts. Die IP-Adressen einer Endpunkt-Netzwerkschnittstelle ändern sich während der Lebensdauer ihres VPC-Endpunkts nicht.

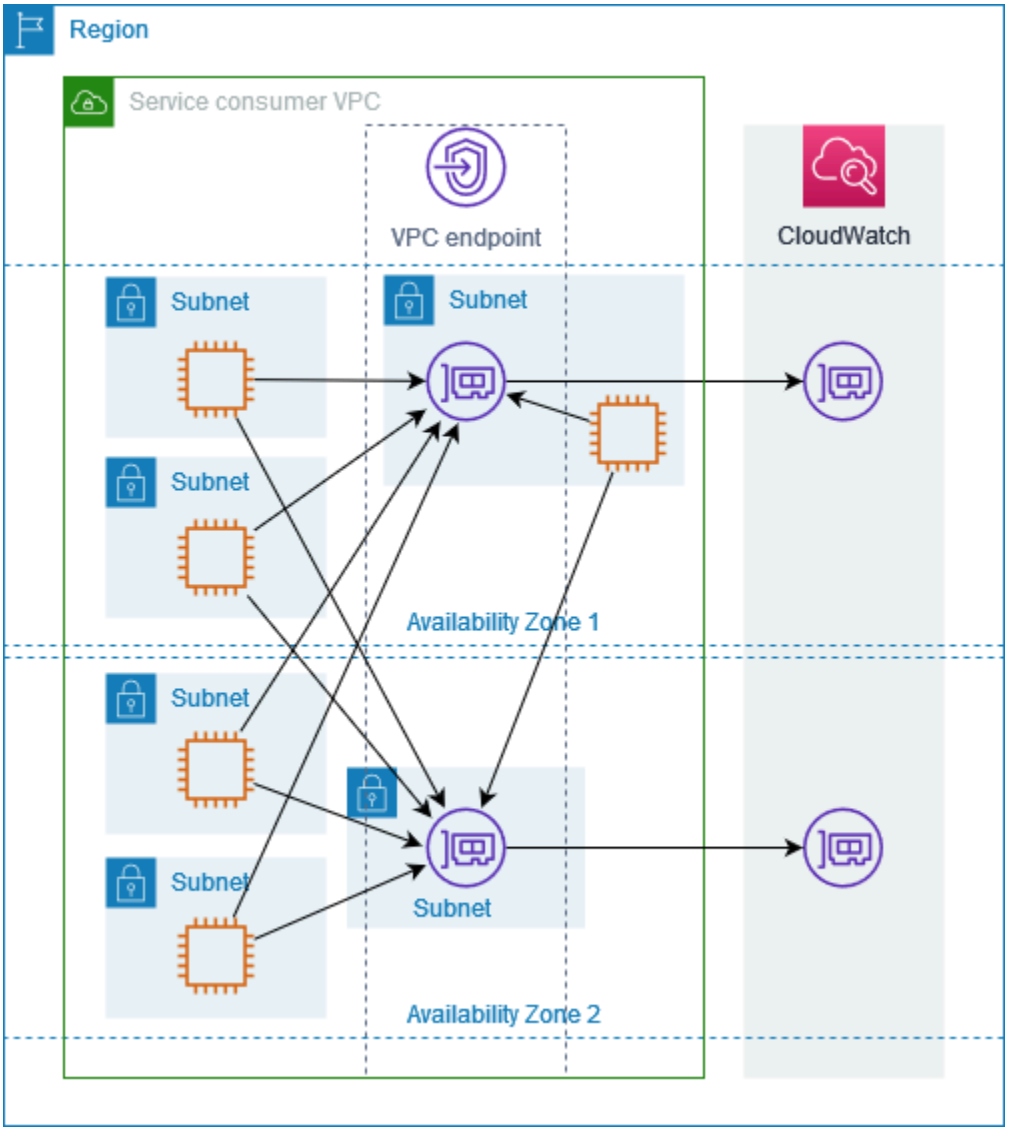
In einer Produktionsumgebung empfehlen wir für hohe Verfügbarkeit und Ausfallsicherheit Folgendes:

- Konfigurieren Sie mindestens zwei Availability Zones pro VPC-Endpunkt und stellen Sie Ihre AWS Ressourcen bereit, die auf diese Availability Zones zugreifen müssen. AWS-Service
- Konfigurieren Sie private DNS-Namen für den VPC-Endpunkt.
- Greifen Sie AWS-Service über den regionalen DNS-Namen zu, der auch als öffentlicher Endpunkt bezeichnet wird.

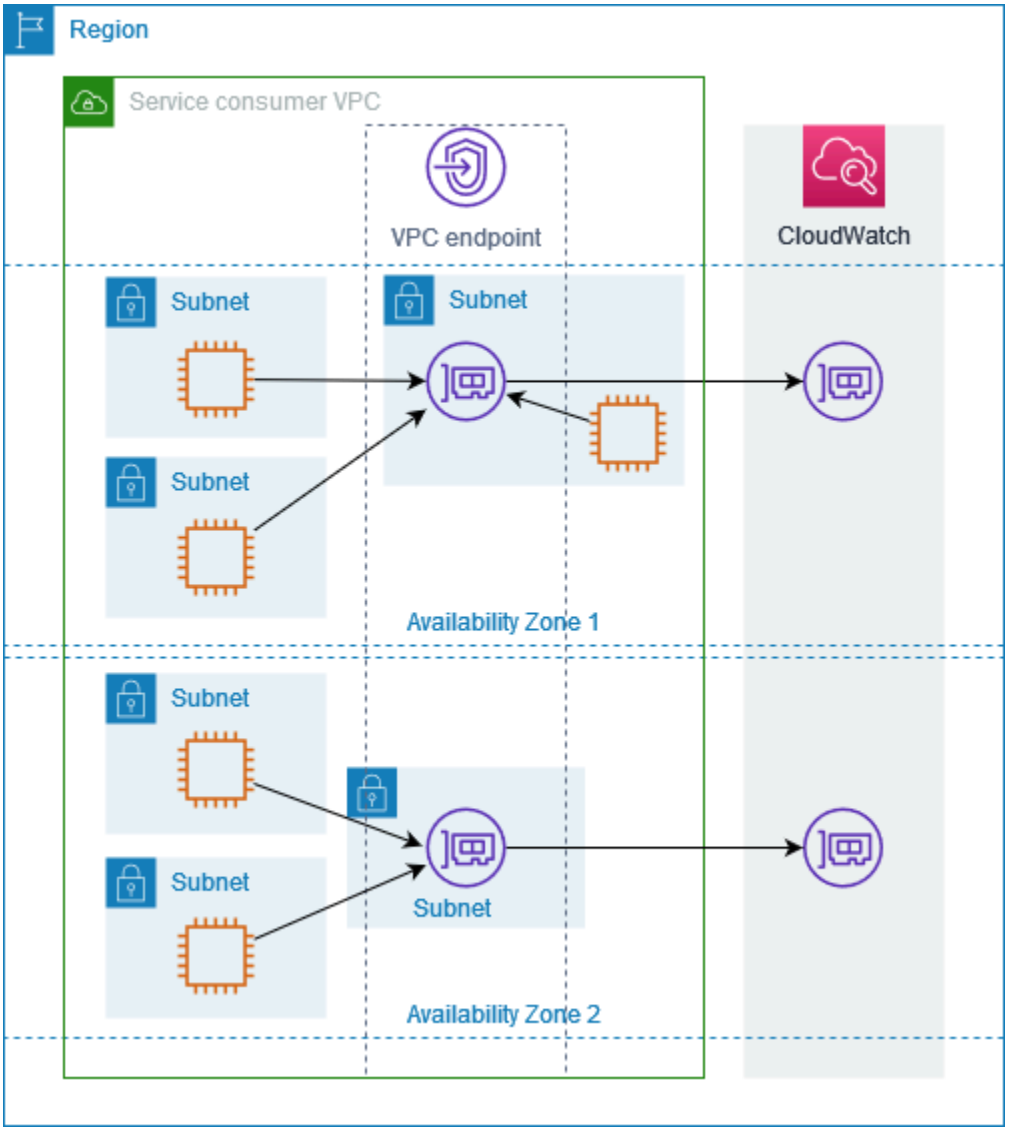
Das folgende Diagramm zeigt einen VPC-Endpunkt für Amazon CloudWatch mit einer Endpunkt-Netzwerkschnittstelle in einer einzigen Availability Zone. Wenn eine Ressource in einem Subnetz in der VPC CloudWatch über ihren öffentlichen Endpunkt auf Amazon zugreift, lösen wir den Datenverkehr an die IP-Adresse der Endpunkt-Netzwerkschnittstelle auf. Dazu gehört auch Datenverkehr von Subnetzen in anderen Availability Zones. Wenn Availability Zone 1 jedoch beeinträchtigt ist, verlieren die Ressourcen in Availability Zone 2 den Zugriff auf Amazon CloudWatch.



Das folgende Diagramm zeigt einen VPC-Endpunkt für Amazon CloudWatch mit Endpunkt-Netzwerkschnittstellen in zwei Availability Zones. Wenn eine Ressource in einem Subnetz in der VPC über ihren öffentlichen Endpunkt auf Amazon CloudWatch zugreift, wählen wir eine funktionierende Endpunkt-Netzwerkschnittstelle aus und verwenden den Round-Robin-Algorithmus, um zwischen ihnen zu wechseln. Anschließend leiten wir den Datenverkehr an die IP-Adresse der ausgewählten Endpunkt-Netzwerkschnittstelle weiter.



Wenn es für Ihren Anwendungsfall besser ist, können Sie den Datenverkehr von Ihren Ressourcen über die Endpunkt-Netzwerkschnittstelle in derselben Availability Zone an den AWS-Service senden. Verwenden Sie dazu den privaten zonalen Endpunkt oder die IP-Adresse der Endpunkt-Netzwerkschnittstelle.



IP-Adresstypen

AWS-Services kann IPv6 über ihre privaten Endpunkte unterstützen, auch wenn sie IPv6 nicht über ihre öffentlichen Endpunkte unterstützen. Endpunkte, die IPv6 unterstützen, können auf DNS-Abfragen mit AAAA-Datensätzen antworten.

Anforderungen zum Aktivieren von IPv6 für einen Schnittstellenendpunkt

- Sie AWS-Service müssen ihre Dienstendpunkte über IPv6 verfügbar machen. Weitere Informationen finden Sie unter the section called “Anzeigen der IPv6-Unterstützung”.
- Der IP-Adresstyp eines Schnittstellenendpunkts muss mit den Subnetzen für den Schnittstellenendpunkt kompatibel sein, wie hier beschrieben:

- IPv4 – Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv4-Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze über IPv4-Adressbereiche verfügen.
- IPv6 – Weisen Sie Ihren Endpunktnetzwerkschnittstellen IPv6-Adressen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze reine IPv6-Subnetze sind.
- Dualstack – Zuweisen von IPv4- und IPv6-Adressen zu Ihren Endpunktnetzwerkschnittstellen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze sowohl IPv4- als auch IPv6-Adressbereiche aufweisen.

Wenn ein Schnittstellen-VPC-Endpunkt IPv4 unterstützt, verfügen die Endpunkt-Netzwerkschnittstellen über IPv4-Adressen. Wenn ein Schnittstellen-VPC-Endpunkt IPv6 unterstützt, verfügen die Endpunkt-Netzwerkschnittstellen über IPv6-Adressen. Die IPv6-Adresse für eine Endpunkt-Netzwerkschnittstelle ist aus dem Internet nicht erreichbar. Wenn Sie eine Endpunktnetzwerkschnittstelle mit einer IPv6-Adresse beschreiben, beachten Sie, dass `denyAllIgwTraffic` aktiviert ist.

AWS-Services die sich integrieren mit AWS PrivateLink

Folgendes AWS-Services lässt sich in integrieren AWS PrivateLink. Sie können einen VPC-Endpunkt erstellen, um eine private Verbindung zu diesen Services herzustellen, als würden sie in Ihrer eigenen VPC ausgeführt werden.

Klicken Sie auf den Link in der AWS-ServiceSpalte, um die Dokumentation für Dienste anzuzeigen, die in integriert AWS PrivateLink werden können. Die Spalte Dienstname enthält den Dienstnamen, den Sie angeben, wenn Sie den Schnittstellen-VPC-Endpunkt erstellen, oder sie gibt an, dass der Dienst den Endpunkt verwaltet.

AWS-Service	Service-Name
Access Analyzer	com.amazonaws.*region*.access-analyzer
AWS Account Management	com.amazonaws.*region*.account
Amazon API Gateway	com.amazonaws.*region*.execute-api
AWS AppConfig	com.amazonaws.*region*.appconfig
	com.amazonaws.*region*.appconfigdata

AWS-Service	Service-Name
AWS App Mesh	com.amazonaws.*region*.appmesh
	com.amazonaws.*region*.appmesh-envoy-management
AWS App Runner	com.amazonaws.*region*.apprunner
Services von AWS App Runner	com.amazonaws.*region*.apprunner.requests
Application Auto Scaling	com.amazonaws.*region*.application-autoscaling
AWS Dienst zur Anwendungsmigration	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 B2B-Datenaustausch	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. *Region. Bedrock-Agent*

AWS-Service	Service-Name
	com.amazonaws.*region*.bedrock-Kundendienstmitarbeiter-Laufzeit.
	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 Saubere Räume ML	com.amazonaws. *region .cleanrooms-ml*
AWS Cloud Control API	com.amazonaws.*region*.cloudcontrolapi
	com.amazonaws.*region*.cloudcontrolapi-fips
Amazon Cloud Directory	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.*region*.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

AWS-Service	Service-Name
	com.amazonaws.*region*.rum-dataplane
	com.amazonaws.*region*.synthetics
CloudWatch Amazon-Protokolle	com.amazonaws.*region*.logs
Amazon CloudWatch Netzwerkmonitor	com.amazonaws. *region* *.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.*region*.git-codecommit-fips
AWS CodeConnections	com.amazonaws. *region* *.codeconnections.api*
	com.amazonaws.*region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws.*region*.codedeploy
	com.amazonaws.*region*.codedeploy-commands-secure
Amazon CodeGuru Profiler	com.amazonaws.*region*.codeguru-profiler
CodeGuru Amazon-Rezensent	com.amazonaws.*region*.codeguru-reviewer
AWS CodePipeline	com.amazonaws.*region*.codepipeline
Amazon CodeWhisperer	com.amazonaws.*region*.codewhisperer

AWS-Service	Service-Name
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 Katalog kontrollieren	com.amazonaws. *region* *.controlcatalog*
AWS Data Exchange	com.amazonaws.*region*.dataexchange
Amazon Data Firehose	com.amazonaws.*region*.kinesis-firehose
AWS Database Migration Service	com.amazonaws.*region*.dms
	com.amazonaws.*region*.dms-fips
AWS DataSync	com.amazonaws.*region*.datasync
Amazon DataZone	com.amazonaws.*region*.datazone
AWS Deadline Cloud	com.amazonaws. *region* *.deadline.management*
	com.amazonaws. *region* *.deadline.scheduling*
DevOpsAmazon-Guru	com.amazonaws.*region*.devops-guru

AWS-Service	Service-Name
AWS Directory Service	com.amazonaws.*region*.ds
Amazon-DynamoDB	com.amazonaws. *region* .*dynamodb*
Amazon EBS Direct-APIs	com.amazonaws.*region*.ebs
Amazon EC2	com.amazonaws.*region*.ec2
Amazon EC2 Auto Scaling	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
	com.amazonaws.*region*.elasticfilesystem-fips
Amazon Elastic Inference	com.amazonaws.*region*.elastic-inference.runtime
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing

AWS-Service	Service-Name
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 in EKS	com.amazonaws.*region*.emr-containers
Amazon EMR Serverless	com.amazonaws.*region*.emr-serverless
Amazon EMR WAL	com.amazonaws. *region .emrwal.prod*
AWS Entity Resolution	com.amazonaws.*region*.entityresolution
Amazon EventBridge	com.amazonaws.*region*.events
	com.amazonaws. *region .pipes-data*
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
Amazon FSx	com.amazonaws.*region*.fsx
	com.amazonaws.*region*.fsx-fips

AWS-Service	Service-Name
AWS Glue	com.amazonaws.*region*.glue
AWS Glue DataBrew	com.amazonaws.*region*.databrew
Amazon Managed Grafana	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.*region*.guardduty-data-fips
AWS HealthImaging	com.amazonaws. *region .dicom-medizinische Bildgebung*
	com.amazonaws.*region*.medical-imaging
	com.amazonaws.*region*.runtime-medical-imaging
AWS HealthLake	com.amazonaws.*region*.healthlake
AWS HealthOmics	com.amazonaws.*region*.analytics-omics
	com.amazonaws.*region*.control-storage-omics
	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.tags-omics
	com.amazonaws.*region*.workflows-omics
IAM Identitätszentrum	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

AWS-Service	Service-Name
	com.amazonaws.*region*.iot.credentials
	com.amazonaws.*region*.iot.fleethub.api
AWS IoT Core Device Advisor	com.amazonaws.*region*.deviceadvisor.iot
AWS IoT Core for LoRaWAN	com.amazonaws.*region*.iotwireless.api
	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 (für Apache Cassandra)	com.amazonaws.*region*.cassandra
	com.amazonaws.*region*.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws.*region*.kinesis-streams

AWS-Service	Service-Name
AWS Lake Formation	com.amazonaws.*region*.lakeformation
AWS Lambda	com.amazonaws.*region*.lambda
Amazon Lex	com.amazonaws.*region*.models-v2-lex
	com.amazonaws.*region*.runtime-v2-lex
AWS License Manager	com.amazonaws.*region*.license-manager
	com.amazonaws.*region*.license-manager-fips
	com.amazonaws.*region*.license-manager-user-subscriptions
Amazon Lookout für Equipment	com.amazonaws.*region*.lookoutequipment
Amazon Lookout for Metrics	com.amazonaws.*region*.lookoutmetrics
Amazon Lookout for Vision	com.amazonaws.*region*.lookoutvision
Amazon Macie	com.amazonaws.*region*.macie2
AWS Mainframe Modernization	com.amazonaws.*region*.m2
Amazon Managed Blockchain	com.amazonaws.*region*.managedblockchain-query
	com.amazonaws.*region*.managedblockchain.bitcoin.mainnet
	com.amazonaws.*region*.managedblockchain.bitcoin.testnet
Amazon Managed Service for Prometheus	com.amazonaws.*region*.aps
	com.amazonaws.*region*.aps-workspaces
Amazon Managed Workflows für Apache Airflow	com.amazonaws.*region*.airflow.api

AWS-Service	Service-Name
	com.amazonaws.*region*.airflow.env
	com.amazonaws.*region*.airflow.ops
AWS Management Console	com.amazonaws.*region*.console
	com.amazonaws.*region*.signin
Amazon MemoryDB für Redis	com.amazonaws.*region*.memory-db
	com.amazonaws.*region*.memorydb-fips
AWS Migration Hub Orchestrator	com.amazonaws.*region*.migrationhub-orchestrator
AWS Migration Hub Refactor Spaces	com.amazonaws.*region*.refactor-spaces
Migration Hub Strategie-Empfehlungen	com.amazonaws.*region*.migrationhub-strategy
Amazon Neptune Analytics	com.amazonaws.*region*.neptune-graph
Amazon Nimble Studio	com.amazonaws.*region*.nimble
OpenSearch Amazon-Dienst	Diese Endpunkte sind serviceverwaltet.
AWS Organizations	com.amazonaws. *Region. Organisationen*
	com.amazonaws. *region .organizations-fips*
AWS Outposts	com.amazonaws. *Region. Außenposten*
AWS Panorama	com.amazonaws.*region*.panorama
AWS Kryptografie im Zahlungsverkehr	com.amazonaws.*region*.payment-cryptography.controlplane
	com.amazonaws.*region*.payment-cryptography.dataplane

AWS-Service	Service-Name
Amazon Personalize	com.amazonaws.*region*.personalize
	com.amazonaws.*region*.personalize-events
	com.amazonaws.*region*.personalize-runtime
AWS Supply Chain	com.amazonaws. *region .scn*
Amazon Pinpoint	com.amazonaws.*region*.pinpoint
	com.amazonaws.*region*.pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws.*region*.polly
AWS Privates 5G	com.amazonaws.*region*.private-networks
AWS Private Certificate Authority	com.amazonaws.*region*.acm-pca
	com.amazonaws.*region*.pca-connector-ad
AWS Proton	com.amazonaws.*region*.proton
Amazon Q Business	aws.api. *region .qbusiness*
Amazon QLDB	com.amazonaws.*region*.qldb.session
Amazon QuickSight	com.amazonaws. *region .quicksight-Webseite*
Amazon RDS	com.amazonaws.*region*.rds
Amazon RDS Daten-API	com.amazonaws.*region*.rds-data
AWS Re:Post Privat	com.amazonaws. *region .repostspace*
Amazon-Redshift	com.amazonaws.*region*.redshift
	com.amazonaws.*region*.redshift-fips
Amazon Redshift-Daten-API	com.amazonaws.*region*.redshift-data

AWS-Service	Service-Name
	com.amazonaws. *region* .redshift-data-fips
Amazon Rekognition	com.amazonaws.*region*.rekognition
	com.amazonaws.*region*.rekognition-fips
	com.amazonaws.*region*.streaming-rekognition
	com.amazonaws.*region*.streaming-rekognition-fips
AWS RoboMaker	com.amazonaws.*region*.robomaker
Amazon S3	com.amazonaws.*region*.s3
Mulitiregionale Amazon-S3-Zugriffspunkte	com.amazonaws.s3-global.accesspoint
Amazon S3 in 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

AWS-Service	Service-Name
Servicekatalog	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.*region*.snow-device-management
Amazon SNS	com.amazonaws.*region*.sns
Amazon SQS	com.amazonaws.*region*.sqs
Amazon SWF	com.amazonaws.*region*.swf
	com.amazonaws.*region*.swf-fips
AWS Step Functions	com.amazonaws.*region*.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 Telco Network Builder	com.amazonaws.*region*.tnb
Amazon Textract	com.amazonaws.*region*.textract
	com.amazonaws.*region*.textract-fips

AWS-Service	Service-Name
Amazon Timestream	com.amazonaws.*region*.timestream.ingest-*cell*
	com.amazonaws.*region*.timestream.query-*cell*
Amazon Timestream für InfluxDB	com.amazonaws. *region* .*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
Amazon Verified Permissions	com.amazonaws.*region*.verifiedpermissions
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice
Amazon WorkSpaces	com.amazonaws.*region*.workspaces
Amazon WorkSpaces Thin Client	com.amazonaws. *region* .*thinclient.api*
AWS X-Ray	com.amazonaws.*region*.xray

Verfügbare AWS-Service -Namen anzeigen

Sie können den Befehl describe-vpc-endpoint-services verwenden, um die Servicenamen anzuzeigen, die VPC-Endpunkte unterstützen.

Das folgende Beispiel zeigt die Endpunkte AWS-Services , die Schnittstellen in der angegebenen Region unterstützen. Die Option `--query` beschränkt die Ausgabe auf die Servicenamen.

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

Das Folgende ist Ausgabebeispiel:

```
[
    "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",
    ...
]
```

Anzeigen von Informationen über einen Service

Wenn Sie den Servicenamen kennen, können Sie den Befehl describe-vpc-endpoint-services verwenden, um detaillierte Informationen über jeden Endpunktservice anzuzeigen.

Im folgenden Beispiel werden Informationen zum CloudWatch Amazon-Schnittstellenendpunkt in der angegebenen Region angezeigt.

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

Es folgt eine Beispielausgabe. `VpcEndpointPolicySupported` gibt an, ob Endpunkt-Richtlinien unterstützt werden. `SupportedIpAddressTypes` gibt an, welche IP-Adresstypen unterstützt werden.

```
{
    "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"
    ]
}
```


Anzeigen der Unterstützung für Endpunkt-Richtlinien

Um zu überprüfen, ob ein Service Endpunkt-Richtlinien unterstützt, rufen Sie den Befehl describe-vpc-endpoint-services auf und überprüfen Sie den Wert von `VpcEndpointPolicySupported`. Die möglichen Werte sind `true` und `false`.

Im folgenden Beispiel wird geprüft, ob der angegebene Service Endpunktrichtlinien in der angegebenen Region unterstützt. Die Option `--query` beschränkt die Ausgabe auf den Wert von `VpcEndpointPolicySupported`.

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

Es folgt eine Beispielausgabe.

```
True
```

Das folgende Beispiel listet die Richtlinien auf AWS-Services , die Endpunktrichtlinien in der angegebenen Region unterstützen. Die Option `--query` beschränkt die Ausgabe auf die Servicenamen. Um diesen Befehl über die Windows-Befehlszeile auszuführen, entfernen Sie die einfachen Anführungszeichen rund um die Abfragezeichenfolge und ändern Sie das Zeilenfortsetzungszeichen von \ auf ^.

```
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'
```

Es folgt eine Beispielausgabe.

```
[
    "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",
    ...
]
```

Das folgende Beispiel listet diejenigen auf AWS-Services , die in der angegebenen Region keine Endpunktrichtlinien unterstützen. Die Option `--query` beschränkt die Ausgabe auf die

Servicenamen. Um diesen Befehl über die Windows-Befehlszeile auszuführen, entfernen Sie die einfachen Anführungszeichen rund um die Abfragezeichenfolge und ändern Sie das Zeilenfortsetzungszeichen von \ auf ^.

```
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'
```

Es folgt eine Beispielausgabe.

```
[
    "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.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.outposts",
```

```
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.redshift-data",
    "com.amazonaws.us-east-1.redshift-data-fips",
    "com.amazonaws.us-east-1.refactor-spaces",
    "com.amazonaws.us-east-1.sagemaker.runtime-fips",
    "com.amazonaws.us-east-1.storagegateway",
    "com.amazonaws.us-east-1.transfer",
    "com.amazonaws.us-east-1.transfer.server",
    "com.amazonaws.us-east-1.verifiedpermissions"
]
```

Anzeigen der IPv6-Unterstützung

Sie können den folgenden Befehl describe-vpc-endpoint-services verwenden, um die anzuzeigen, auf AWS-Services die Sie in der angegebenen Region über IPv6 zugreifen können. Die Option `--query` beschränkt die Ausgabe auf die Servicenamen.

```
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
```

Das Folgende ist Ausgabebeispiel:

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "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"
]
```

Zugriff und AWS-Service Verwendung eines VPC-Endpunkts mit einer Schnittstelle

Sie können einen VPC-Schnittstellen-Endpunkt erstellen, um eine Verbindung zu Diensten herzustellen AWS PrivateLink, von denen viele AWS-Services unterstützt werden. Eine Übersicht finden Sie unter the section called “Konzepte” und Zugriff AWS-Services.

Für jedes Subnetz, das Sie in Ihrer VPC angeben, erstellen wir eine Endpunkt-Netzwerkschnittstelle im Subnetz und weisen ihr eine private IP-Adresse aus dem Subnetz-Adressbereich zu. Eine Endpunkt-Netzwerkschnittstelle ist eine vom Anforderer verwaltete Netzwerkschnittstelle. Sie können sie in Ihrem AWS-Konto anzeigen, aber Sie können sie nicht selbst verwalten.

Die stündliche Nutzung und Datenverarbeitungsgebühren werden Ihnen in Rechnung gestellt. Weitere Informationen finden Sie auf Preise zu Schnittstellenendpunkte.

Inhalt

Voraussetzungen

- Stellen Sie die Ressourcen bereit, die auf die zugreifen, AWS-Service in Ihrer VPC.
- Um privates DNS zu verwenden, müssen Sie DNS-Hostnamen und die DNS-Auflösung für Ihre VPC aktivieren. Mehr Informationen finden Sie unter Anzeigen und Aktualisieren von DNS-Attributen im Amazon-VPC-Benutzerhandbuch.
- Um IPv6 für einen Schnittstellenendpunkt zu aktivieren, AWS-Service müssen diese den Zugriff über IPv6 unterstützen. Weitere Informationen finden Sie unter the section called “IP-Adresstypen”.
- Erstellen Sie eine Sicherheitsgruppe für die Endpunkt-Netzwerkschnittstelle, die den erwarteten Datenverkehr von den Ressourcen in Ihrer VPC zulässt. Um beispielsweise sicherzustellen, dass sie HTTPS-Anfragen an die senden AWS CLI kann AWS-Service, muss die Sicherheitsgruppe eingehenden HTTPS-Verkehr zulassen.
- Wenn sich Ihre Ressourcen in einem Subnetz mit einer Netzwerk-ACL befinden, stellen Sie sicher, dass die Netzwerk-ACL den Verkehr zwischen den Ressourcen in Ihrer VPC und den Netzwerkschnittstellen der Endpunkte zulässt.

- Es gibt Kontingente für Ihre AWS PrivateLink Ressourcen. Weitere Informationen finden Sie unter AWS PrivateLink -Kontingente.

Erstellen eines VPC-Endpunkts

Gehen Sie wie folgt vor, um einen Schnittstellen-VPC-Endpunkt zu erstellen, der eine Verbindung zu einem AWS-Service herstellt.

Um einen Schnittstellenendpunkt für ein zu erstellen AWS-Service

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Wählen Sie für Servicekategorie die Option AWS-Services aus.
5. Wählen Sie für Service name (Servicename) den Service aus. Weitere Informationen finden Sie unter the section called “Services, die integrieren”.
6. Wählen Sie für VPC die VPC aus, von der aus Sie auf AWS-Service zugreifen.
7. Wenn Sie in Schritt 5 den Servicenamen für Amazon S3 ausgewählt haben und die Unterstützung für privates DNS konfigurieren möchten, wählen Sie Zusätzliche Einstellungen, DNS-Namen aktivieren aus. Wenn Sie diese Auswahl treffen, wird automatisch auch die Option Private DNS nur für eingehenden Endpunkt aktivieren ausgewählt. Sie können privates DNS mit einem eingehenden Resolver-Endpunkt nur für Schnittstellenendpunkte für Amazon S3 konfigurieren. Wenn Sie keinen Gateway-Endpunkt für Amazon S3 haben und die Option Private DNS nur für eingehende Endpunkte aktivieren wählen, erhalten Sie eine Fehlermeldung, wenn Sie den letzten Schritt in diesem Verfahren ausführen.

   Wenn Sie in Schritt 5 den Servicenamen für einen anderen Dienst als Amazon S3 ausgewählt haben, ist Zusätzliche Einstellungen, DNS-Namen aktivieren bereits ausgewählt. Wir empfehlen Ihnen, die Standardeinstellungen beizubehalten. Dadurch wird sichergestellt, dass Anfragen, die die Endpunkte des öffentlichen Dienstes verwenden, z. B. Anfragen, die über ein AWS SDK gestellt wurden, an Ihren VPC-Endpunkt weitergeleitet werden.
8. Wählen Sie für Subnetze ein Subnetz pro Availability Zone aus, von dem aus Sie auf AWS-Service zugreifen. Sie können nicht mehrere Subnetze aus derselben Availability Zone auswählen. Weitere Informationen finden Sie unter the section called “Subnetze und Availability Zones”.

Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie auswählen. Standardmäßig wählen wir IP-Adressen aus den Subnetz-IP-Adressbereichen aus und weisen sie den Endpunkt-Netzwerkschnittstellen zu. Um die IP-Adressen für eine Endpunkt-Netzwerkschnittstelle auszuwählen, wählen Sie Geben Sie IP-Adressen an und geben Sie eine IPv4-Adresse aus dem Subnetz-Adressbereich ein. Wenn der Endpunktdienst IPv6 unterstützt, können Sie auch eine IPv6-Adresse aus dem Subnetz-Adressbereich eingeben. Beachten Sie, dass die ersten vier IP-Adressen und die letzte IP-Adresse in einem CIDR-Block für den internen Gebrauch reserviert sind, sodass Sie sie nicht für Ihre Endpunkt-Netzwerkschnittstellen angeben können.

9. Wählen Sie für IP address type (IP-Adressentyp) eine der folgenden Optionen aus:

   - IPv4 – Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv4-Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4-Adressbereiche haben und der Dienst IPv4-Anfragen akzeptiert.
   - IPv6 – Weisen Sie Ihren Endpunktnetzwerkschnittstellen IPv6-Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze reine IPv6-Subnetze sind und der Dienst IPv6-Anfragen akzeptiert.
   - Dualstack – Zuweisen von IPv4- und IPv6-Adressen zu Ihren Endpunktnetzwerkschnittstellen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze sowohl IPv4- als auch IPv6-Adressbereiche haben und der Dienst sowohl IPv4- als auch IPv6-Anfragen akzeptiert.

10. Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppen aus, die den Endpunkt-Netzwerkschnittstellen für den VPC-Endpunkt zugeordnet werden sollen. Standardmäßig ordnen wir die Standard-Sicherheitsgruppe für die VPC zu.
11. Wählen Sie für Policy (Richtlinie) Full access (Vollzugriff), um alle Operationen aller Prinzipale auf allen Ressourcen über den VPC-Endpunkt zuzulassen. Wählen Sie andernfalls Custom (Benutzerdefiniert), um eine VPC-Endpunktrichtlinie anzufügen, die die Berechtigungen steuert, die Prinzipale zum Ausführen von Aktionen für Ressourcen über den VPC-Endpunkt haben. Diese Option ist nur verfügbar, wenn der Service VPC-Endpunktrichtlinien unterstützt. Weitere Informationen finden Sie unter Endpunktrichtlinien.
12. (Optional) Sie fügen ein Tag hinzu, indem Sie Neuen Tag hinzufügen auswählen und den Schlüssel und den Wert für den Tag eingeben.
13. Wählen Sie Endpunkt erstellen.

So erstellen Sie einen Schnittstellenendpunkt mithilfe der Befehlszeile

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Tools für Windows) PowerShell

Gemeinsam genutzte Subnetze

Sie können VPC-Endpunkte in Subnetzen, die mit Ihnen geteilt werden, nicht erstellen, beschreiben, ändern oder löschen. Sie können die VPC-Endpunkte jedoch in Subnetzen verwenden, die mit Ihnen geteilt werden.

Konfigurieren eines Schnittstellenendpunkts

Nachdem Sie einen Schnittstellen-VPC-Endpunkt erstellt haben, können Sie dessen Konfiguration aktualisieren.

Aufgaben

- Hinzufügen oder Entfernen von Subnetzen
- Weisen Sie Sicherheitsgruppen zu
- Bearbeiten der VPC-Endpunktrichtlinie
- Aktivieren von privaten DNS-Namen
- Verwalten von Tags

Hinzufügen oder Entfernen von Subnetzen

Sie können ein Subnetz pro Availability Zone für Ihren Schnittstellenendpunkt auswählen. Wenn Sie ein Subnetz hinzufügen, erstellen wir eine Endpunktnetzwerkschnittstelle im Subnetz und weisen ihr eine private IP-Adresse aus dem IP-Adressbereich des Subnetzes zu. Wenn Sie ein Subnetz entfernen, löschen wir dessen Endpunkt-Netzwerkschnittstelle. Weitere Informationen finden Sie unter the section called “Subnetze und Availability Zones”.

So ändern Sie die Subnetze mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.

3. Wählen Sie den Schnittstellenendpunkt.
4. Wählen Sie Actions (Aktionen), Manage Subnets (Subnetze verwalten).
5. Aktivieren oder deaktivieren Sie Availability Zones nach Bedarf. Wählen Sie für jede Availability Zone ein Subnetz aus. Standardmäßig wählen wir IP-Adressen aus den Subnetz-IP-Adressbereichen aus und weisen sie den Endpunkt-Netzwerkschnittstellen zu. Um die IP-Adressen für eine Endpunkt-Netzwerkschnittstelle auszuwählen, wählen Sie Geben Sie IP-Adressen an und geben Sie eine IPv4-Adresse aus dem Subnetz-Adressbereich ein. Wenn der Endpunktdienst IPv6 unterstützt, können Sie auch eine IPv6-Adresse aus dem Subnetz-Adressbereich eingeben.

   Wenn Sie eine IP-Adresse für ein Subnetz angeben, das bereits über eine Endpunkt-Netzwerkschnittstelle für diesen VPC-Endpunkt verfügt, ersetzen wir die Endpunkt-Netzwerkschnittstelle durch eine neue. Dieser Prozess trennt vorübergehend die Verbindung zwischen dem Subnetz und dem VPC-Endpunkt.
6. Wählen Sie Modify subnets (Subnetze modifizieren).

So ändern Sie die Subnetze über die Befehlszeile

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Tools für Windows PowerShell)

Weisen Sie Sicherheitsgruppen zu

Sie können die Sicherheitsgruppen ändern, die den Netzwerkschnittstellen für Ihren Schnittstellenendpunkt zugeordnet sind. Die Sicherheitsgruppenregeln steuern den Datenverkehr, der von den Ressourcen in Ihrer VPC zur Endpunkt-Netzwerkschnittstelle zulässig ist.

Ändern der Sicherheitsgruppen mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Schnittstellenendpunkt.
4. Wählen Sie Actions (Aktionen), Manage security groups (Verwalten von Sicherheitsgruppen).
5. Aktivieren oder deaktivieren Sie die Auswahl von Sicherheitsgruppen nach Bedarf.
6. Wählen Sie Modify security groups (Ändern von Sicherheitsgruppen).

Ändern der Sicherheitsgruppen mithilfe der Befehlszeile

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Tools für Windows PowerShell)

Bearbeiten der VPC-Endpunktrichtlinie

Wenn der AWS-Service Endpunktrichtlinien unterstützt, können Sie die Endpunktrichtlinie für den Endpunkt bearbeiten. Nachdem Sie eine Endpunktrichtlinie aktualisiert haben, kann es einige Minuten dauern, bis die Änderungen wirksam werden. Weitere Informationen finden Sie unter Endpunktrichtlinien.

So ändern Sie die Endpunktrichtlinie mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Schnittstellenendpunkt.
4. Wählen Sie Actions (Aktionen), Manage policy (Verwalten von Richtlinien).
5. Wählen Sie Full Access (Voller Zugriff), um vollen Zugriff auf den Service zu gewähren, oder wählen Sie Custom (Benutzerdefiniert), und fügen Sie eine benutzerdefinierte Richtlinie hinzu.
6. Wählen Sie Speichern.

So ändern Sie die Endpunktrichtlinie mithilfe der Befehlszeile

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Tools für Windows PowerShell)

Aktivieren von privaten DNS-Namen

Wir empfehlen Ihnen, private DNS-Namen für Ihre VPC-Endpunkte für zu aktivieren. AWS-Services Dadurch wird sichergestellt, dass Anfragen, die die Endpunkte des öffentlichen Dienstes verwenden, z. B. Anfragen, die über ein AWS SDK gestellt wurden, an Ihren VPC-Endpunkt weitergeleitet werden.

Um privates DNS zu verwenden, müssen Sie sowohl DNS-Hostnamen als auch die DNS-Auflösung für Ihre VPC aktivieren. Nachdem Sie private DNS-Namen aktiviert haben, kann es einige Minuten

dauern, bis die privaten IP-Adressen verfügbar sind. Die DNS-Einträge, die wir erstellen, wenn Sie private DNS-Namen aktivieren, sind privat. Daher kann der private DNS-Name nicht öffentlich aufgelöst werden.

So ändern Sie die Option für private DNS-Namen mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Schnittstellenendpunkt.
4. Wählen Sie Actions (Aktionen), Modify Private DNS names (Private DNS-Namen ändern).
5. Enable for this endpoint (Für diesen Endpunkt aktivieren) nach Bedarf auswählen oder löschen.
6. Wenn es sich bei dem Service um Amazon S3 handelt, wählen Sie im vorherigen Schritt Für diesen Endpunkt aktivieren auch Privates DNS nur für eingehenden Endpunkt aktivieren. Wenn Sie die standardmäßige private DNS-Funktionalität bevorzugen, deaktivieren Sie Privates DNS nur für eingehenden Endpunkt aktivieren. Wenn Sie zusätzlich zu einem Schnittstellenendpunkt für Amazon S3 keinen Gateway-Endpunkt für Amazon S3 haben und Sie Privates DNS nur für eingehenden Endpunkt aktivieren auswählen, erhalten Sie beim Speichern der Änderungen im nächsten Schritt eine Fehlermeldung. Weitere Informationen finden Sie unter the section called “Privates DNS”.
7. Wählen Sie Save Changes (Änderungen speichern).

So ändern Sie die Option für private DNS-Namen mithilfe der Befehlszeile

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Tools für Windows) PowerShell

Verwalten von Tags

Sie können Ihren Schnittstellenendpunkt markieren, um ihn zu identifizieren oder in Übereinstimmung mit den Anforderungen Ihrer Organisation kategorisieren zu können.

So verwalten Sie Tags mit der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Schnittstellenendpunkt.

4. Klicken Sie auf Actions (Aktionen), Manage tags (Markierungen verwalten).
5. Wählen Sie für jede Markierung Add new tag (Neue Markierung hinzufügen) und geben Sie den Schlüssel und Wert der Markierung ein.
6. Um eine Markierung zu entfernen, wählen Sie Remove (Entfernen) rechts neben dem Schlüssel und dem Wert der Markierung aus.
7. Wählen Sie Speichern.

So verwalten Sie Tags mit der Befehlszeile

- create-tags und delete-tags (AWS CLI)
- New-EC2Tagund Remove-EC2Tag(Tools für Windows PowerShell)

Empfangen von Warnmeldungen für Schnittstellen-Endpunkt-Ereignisse

Sie können eine Benachrichtigung erstellen, um Warnungen für bestimmte Ereignisse im Zusammenhang mit Ihrem Schnittstellenendpunkt zu erhalten. Beispielsweise können Sie eine E-Mail erhalten, wenn eine Verbindungsanfrage akzeptiert oder abgelehnt wird.

Aufgaben

- Eine SNS-Benachrichtigung erstellen
- Eine Zugriffsrichtlinie hinzufügen
- Eine Schlüsselrichtlinie hinzufügen

Eine SNS-Benachrichtigung erstellen

Gehen Sie folgendermaßen vor, um ein Amazon-SNS-Thema für die Benachrichtigungen zu erstellen und das Thema zu abonnieren.

So erstellen Sie mithilfe der Konsole eine Benachrichtigung für einen Schnittstellenendpunkt

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Schnittstellenendpunkt.

4. Wählen Sie aus der Registerkarte Notifications (Benachrichtigungen) die Option Create notification (Benachrichtigung erstellen) aus.
5. Wählen Sie für Notification ARN (Benachrichtigungs-ARN) den ARN für das SNS-Thema aus, das Sie erstellt haben.
6. Um ein Ereignis zu abonnieren, wählen Sie es aus Events (Ereignisse).
   - Connect (Verbinden) – Der Service-Verbraucher hat den Schnittstellenendpunkt erstellt. Dadurch wird eine Verbindungsanfrage an den Service-Anbieter gesendet.
   - Accept (Akzeptieren) – Der Service-Anbieter hat die Verbindungsanfrage akzeptiert.
   - Reject (Ablehnen) – Der Service-Anbieter hat die Verbindungsanfrage abgelehnt.
   - Delete (Löschen) – Der Service-Verbraucher hat den Schnittstellenendpunkt gelöscht.
7. Wählen Sie Benachrichtigung erstellen aus.

So erstellen Sie mithilfe der Befehlszeile eine Benachrichtigung für einen Schnittstellenendpunkt

- create-vpc-endpoint-connection-notification (AWS CLI)
- New-EC2VpcEndpointConnectionNotification(Tools für Windows PowerShell)

Eine Zugriffsrichtlinie hinzufügen

Fügen Sie dem Amazon SNS SNS-Thema eine Zugriffsrichtlinie hinzu, die es ermöglicht, Benachrichtigungen in Ihrem Namen AWS PrivateLink zu veröffentlichen, z. B. die folgenden. Weitere Informationen finden Sie unter Wie bearbeite ich die Zugriffsrichtlinie meines Amazon-SNS-Themas? Verwenden Sie die globalen Konditionsschlüssel `aws:SourceArn` und `aws:SourceAccount` zum Schutz vor dem Problem des verwirrten Stellvertreters.

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

Eine Schlüsselrichtlinie hinzufügen

Wenn Sie verschlüsselte SNS-Themen verwenden, muss die Ressourcenrichtlinie für den KMS-Schlüssel darauf vertrauen AWS PrivateLink , AWS KMS API-Operationen aufzurufen. Es folgt eine Beispielschlüsselrichtlinie.

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

Löschen eines Schnittstellenendpunkts

Wenn Sie einen VPC-Endpunkt nicht mehr benötigen, können Sie ihn löschen. Das Löschen eines Schnittstellenendpunkts löscht auch seine Endpunktnetzwerkschnittstellen.

So löschen Sie einen Schnittstellen-Endpunkt unter Verwendung der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Schnittstellenendpunkt.
4. Wählen Sie Actions (Aktionen), Delete VPC Endpoint (VPC-Endpunkte löschen).
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein.
6. Wählen Sie Löschen.

So löschen Sie einen Schnittstellen-Endpunkt unter Verwendung der Befehlszeile

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

Gateway-Endpunkte

Gateway-VPC-Endpunkte bieten zuverlässige Konnektivität zu Amazon S3 und DynamoDB, ohne dass ein Internet-Gateway oder ein NAT-Gerät für Ihre VPC erforderlich ist. Gateway-Endpunkte verwenden AWS PrivateLink im Gegensatz zu anderen Arten von VPC-Endpunkten nicht.

Amazon S3 und DynamoDB unterstützen sowohl Gateway-Endpunkte als auch Schnittstellenendpunkte. Einen Vergleich der Optionen finden Sie im Folgenden:

- Arten von VPC-Endpunkten für Amazon S3
- Arten von VPC-Endpunkten für Amazon DynamoDB

Preisgestaltung

Für die Nutzung von Gateway-Endpunkten fallen keine zusätzlichen Gebühren an.

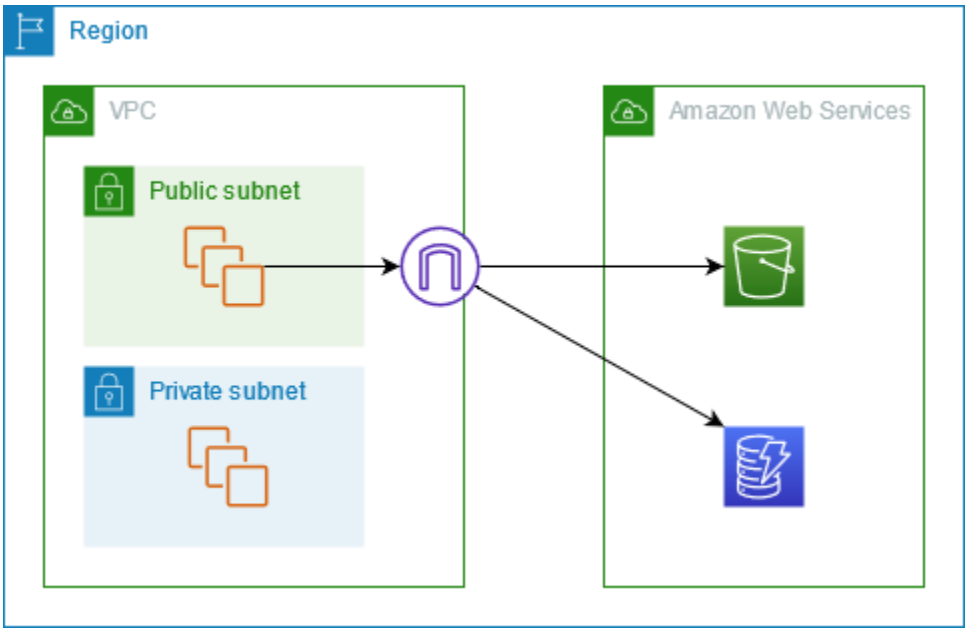
Inhalt

Übersicht

Sie können über ihre öffentlichen Service-Endpunkte oder über Gateway-Endpunkte auf Amazon S3 und DynamoDB zugreifen. In dieser Übersicht werden diese Methoden verglichen.

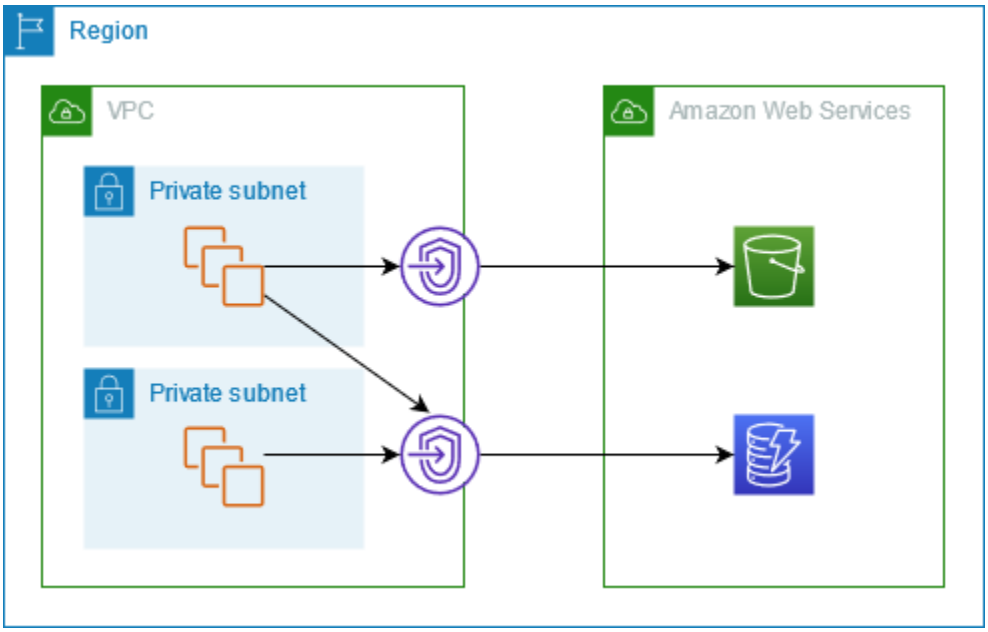
Zugriff über ein Internet-Gateway

Das folgende Diagramm zeigt, wie Instances über ihre Endpunkte des öffentlichen Services auf Amazon S3 und DynamoDB zugreifen. Datenverkehr zu Amazon S3 oder DynamoDB von einer Instance in einem öffentlichen Subnetz wird zum Internet-Gateway für die VPC und dann an den Service geroutet. Instances in einem privaten Subnetz können keinen Datenverkehr an Amazon S3 oder DynamoDB senden, da private Subnetze per Definition keine Routen zu einem Internet-Gateway haben. Damit Instances im privaten Subnetz Datenverkehr an Amazon S3 oder DynamoDB senden können, fügen Sie ein NAT-Gerät zum öffentlichen Subnetz hinzu und leiten den Datenverkehr im privaten Subnetz an das NAT-Gerät weiter. Der Datenverkehr zu Amazon S3 oder DynamoDB durchquert zwar das Internet-Gateway, verlässt aber das Netzwerk nicht. AWS



Zugriff über einen Gateway-Endpunkt

Das folgende Diagramm zeigt, wie Instances über einen Gateway-Endpunkt auf Amazon S3 und DynamoDB zugreifen. Datenverkehr von Ihrer VPC zu Amazon S3 oder DynamoDB wird an den Gateway-Endpunkt geleitet. Jede Subnetz-Routing-Tabelle muss über eine Route verfügen, die den für den Service bestimmten Datenverkehr mithilfe der Präfixliste für den Service an den Gateway-Endpunkt sendet. Weitere Informationen finden Sie im Abschnitt zur AWS-verwalteten Präfixliste im Amazon-VPC-Benutzerhandbuch.



Routing

Wenn Sie einen Gateway-Endpunkt erstellen, wählen Sie die VPC-Routing-Tabellen für die Subnetze aus, die Sie aktivieren. Die folgende Route wird automatisch zu jeder Routing-Tabelle hinzugefügt, die Sie auswählen. Das Ziel ist eine Präfixliste für den Dienst, dessen Eigentümer der Dienst ist, AWS und das Ziel ist der Gateway-Endpunkt.

Bestimmungsort	Ziel
prefix_list_id	*gateway_endpoint_id*

Überlegungen

- Sie können die Endpunktrouten überprüfen, die wir Ihrer Routing-Tabelle hinzufügen, aber Sie können sie nicht ändern oder löschen. Um einer Routing-Tabelle eine Endpunktroute

hinzuzufügen, ordnen Sie sie dem Gateway-Endpunkt zu. Wir löschen die Endpunktroute, wenn Sie die Routing-Tabelle vom Gateway-Endpunkt trennen oder wenn Sie den Gateway-Endpunkt löschen.

- Alle Instances in den Subnetzen, die einer Routing-Tabelle zugeordnet sind, die einem Gateway-Endpunkt zugeordnet ist, verwenden automatisch den Gateway-Endpunkt, um auf den Service zuzugreifen. Instances in Subnetzen, die diesen Routing-Tabellen nicht zugeordnet sind, verwenden den öffentlichen Service-Endpunkt, nicht den Gateway-Endpunkt.
- Eine Routing-Tabelle kann sowohl eine Endpunktroute zu Amazon S3 als auch eine Endpunktroute zu DynamoDB enthalten. Sie können Endpunktrouten an denselben Service (Amazon S3 oder DynamoDB) in mehreren Routing-Tabellen haben. Sie können nicht mehrere Endpunktrouten zum selben Service (Amazon S3 oder DynamoDB) in einer einzigen Routing-Tabelle haben.
- Wir verwenden die spezifischste mit dem Datenverkehr übereinstimmende Route, um Datenverkehr weiterzuleiten (Übereinstimmung mit längstem Präfix). Für Routing-Tabellen mit einer Endpunktroute bedeutet dies Folgendes:
  - Wenn es eine Route gibt, die den gesamten Internetdatenverkehr (0.0.0.0/0) an ein Internet-Gateway sendet, hat die Endpunktroute Vorrang für Datenverkehr, der für den Service (Amazon S3 oder DynamoDB) in der aktuellen Region bestimmt ist. Datenverkehr, der für einen anderen bestimmt ist, AWS-Service verwendet das Internet-Gateway.
  - Datenverkehr, der für den Service (Amazon S3 oder DynamoDB) in einer anderen Region bestimmt ist, geht an das Internet-Gateway, da Präfixlisten spezifisch für eine Region sind.
  - Wenn es eine Route gibt, die den genauen IP-Adressbereich für den Service (Amazon S3 oder DynamoDB) in derselben Region angibt, hat diese Route Vorrang vor der Endpunktroute.

Sicherheit

Wenn Ihre Instances über einen Gateway-Endpunkt auf Amazon S3 oder DynamoDB zugreifen, greifen sie über seinen öffentlichen Endpunkt auf den Service zu. Die Sicherheitsgruppen für diese Instances müssen den Datenverkehr aus dem Load Balancer zulassen. Es folgt ein Beispiel für eine Outbound-Regel. Es verweist auf die ID der Präfixliste für den Service.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich
prefix_list_id	TCP	443

Die Netzwerk-ACLs für die Subnetze dieser Instances müssen auch den Verkehr zum und vom Dienst zulassen. Es folgt ein Beispiel für eine Outbound-Regel. Sie können in Netzwerk-ACL-Regeln nicht auf Präfixlisten verweisen, aber Sie können die IP-Adresse für den Dienst aus der Präfixliste abrufen.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich
service_cidr_block_1	TCP	443
service_cidr_block_2	TCP	443
service_cidr_block_3	TCP	443

Gateway-Endpunkte für Amazon S3

Sie können über Gateway-VPC-Endpunkte von Ihrer VPC aus auf Amazon S3 zugreifen. Nachdem Sie den Gateway-Endpunkt erstellt haben, können Sie ihn als Ziel in Ihrer Routing-Tabelle für Datenverkehr hinzufügen, der von Ihrer VPC zu Amazon S3 bestimmt ist.

Für die Nutzung von Gateway-Endpunkten fallen keine zusätzlichen Gebühren an.

Amazon S3 unterstützt sowohl Gateway-Endpunkte als auch Schnittstellenendpunkte. Mit einem Gateway-Endpunkt können Sie von Ihrer VPC aus auf Amazon S3 zugreifen, ohne ein Internet-Gateway oder ein NAT-Gerät für Ihre VPC zu benötigen und ohne zusätzliche Kosten. Gateway-Endpunkte erlauben jedoch keinen Zugriff von lokalen Netzwerken, von Peer-VPCs in anderen AWS Regionen oder über ein Transit-Gateway. Für diese Szenarien müssen Sie einen Schnittstellenendpunkt verwenden, der gegen Aufpreis verfügbar ist. Weitere Informationen finden Sie unter VPC-Endpunkte für Amazon-S3 im Amazon-S3-Benutzerhandbuch.

Inhalt

Überlegungen

- Ein Gateway-Endpunkt ist nur in der Region verfügbar, in der Sie ihn erstellt haben. Stellen Sie sicher, dass Sie Ihren Gateway-Endpunkt in derselben Region wie Ihre S3-Buckets erstellen.
- Wenn Sie die Amazon-DNS-Server verwenden, müssen Sie sowohl DNS-Hostnamen als auch DNS-Auflösung für Ihre VPC aktivieren. Wenn Sie Ihren eigenen DNS-Server verwenden, stellen Sie sicher, dass Anforderungen an Amazon S3 korrekt in die von AWS verwalteten IP-Adressen erfüllt werden.
- Die ausgehenden Regeln für die Sicherheitsgruppe für Instances, die über den Gateway-Endpunkt auf Amazon S3 zugreifen, müssen Datenverkehr zu Amazon S3 zulassen. Sie können in den Regeln der Sicherheitsgruppe auf die ID der Präfixliste für Amazon S3 verweisen.
- Die Netzwerk-ACL für das Subnetz für Ihre Instances, die über einen Gateway-Endpunkt auf Amazon S3 zugreifen, müssen Datenverkehr zu und von Amazon S3 zulassen. Sie können in Netzwerk-ACL-Regeln nicht auf Präfixlisten verweisen, aber Sie können die IP-Adresse für Amazon S3 aus der Präfixliste für Amazon S3 abrufen.
- Prüfen Sie, ob Sie einen verwenden AWS-Service , der Zugriff auf einen S3-Bucket erfordert. Beispielsweise kann ein Dienst Zugriff auf Buckets benötigen, die Protokolldateien enthalten, oder Sie müssen Treiber oder Agenten auf Ihre EC2-Instances herunterladen. Wenn ja, stellen Sie sicher, dass Ihre Endpunktrichtlinie es der AWS-Service OR-Ressource erlaubt, mithilfe der `s3:GetObject` Aktion auf diese Buckets zuzugreifen.
- Sie können die Bedingung `aws:SourceIp` nicht in einer Identitätsrichtlinie oder einer Bucket-Richtlinie für Anforderungen an Amazon S3 verwenden, die einen VPC-Endpunkt durchlaufen. Verwenden Sie stattdessen die Bedingung `aws:VpcSourceIp`. Alternativ können Sie auch Routing-Tabellen verwenden, um zu steuern, welche EC2-Instanzen über den VPC-Endpunkt auf Amazon S3 zugreifen können.
- Gateway-Endpunkte unterstützen nur IPv4-Datenverkehr.
- Die von Amazon S3 empfangenen Quell-IPv4-Adressen von Instances in den betroffenen Subnetzen werden von öffentlichen IPv4-Adressen in die privaten IPv4-Adressen Ihrer VPC umgewandelt. Endpunkte wechseln zwischen Netzwerkrouten und trennen offene TCP-Verbindungen. Die vorherigen Verbindungen, die öffentliche IPv4-Adressen verwendet haben, werden nicht fortgesetzt. Wir empfehlen, während des Erstellens oder Änderns eines Endpunkts keine wichtigen Aufgaben auszuführen oder zu testen, ob Ihre Software nach der Verbindungstrennung automatisch erneut eine Verbindung zu Amazon S3 herstellt.
- Endpunktverbindungen können nicht auf einen Bereich außerhalb einer VPC erweitert werden. Ressourcen auf der anderen Seite einer VPN-Verbindung, VPC-Peering-Verbindung, eines Transit-

Gateways oder einer AWS Direct Connect Verbindung in Ihrer VPC können keinen Gateway-Endpunkt für die Kommunikation mit Amazon S3 verwenden.

- Ihr Konto hat ein Standardkontingent von 20 Gateway-Endpunkten pro Region, das anpassbar ist. Pro VPC sind auch höchstens 255 Gateway-Endpunkte zulässig.

Privates DNS

Sie können privates DNS zur Kostenoptimierung konfigurieren, wenn Sie sowohl einen Gateway-Endpunkt als auch einen Schnittstellenendpunkt für Amazon S3 erstellen.

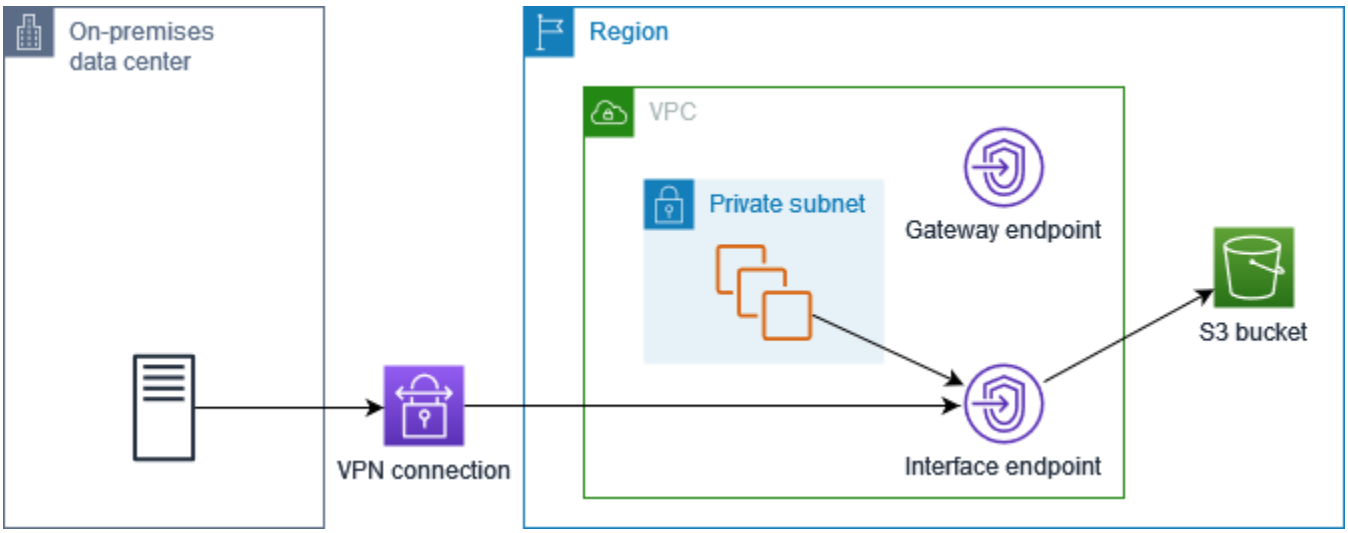
Route 53 Resolver

Amazon stellt einen DNS-Server den Route 53 Resolver für Ihre VPC zur Verfügung. Der Route 53 Resolver löst automatisch lokale VPC-Domainnamen und Datensätze in privaten gehosteten Zonen auf. Sie können den Route 53 Resolver jedoch nicht von außerhalb Ihrer VPC verwenden. Route 53 bietet Resolver-Endpunkte und Resolver-Regeln, so dass Sie den Route 53 Resolver von außerhalb Ihrer VPC nutzen können. Ein eingehender Resolver-Endpunkt leitet DNS-Abfragen vom On-Premises Netzwerk an Route 53 Resolver weiter. Ein ausgehender Resolver-Endpunkt leitet DNS-Abfragen vom Route 53 Resolver an das On-Premises Netzwerk weiter.

Wenn Sie Ihren Schnittstellenendpunkt für Amazon S3 so konfigurieren, dass nur privates DNS für den eingehenden Resolver-Endpunkt verwendet wird, erstellen wir einen eingehenden Resolver-Endpunkt. Der eingehende Resolver-Endpunkt löst DNS-Abfragen an Amazon S3 von On-Premises-Standorten an die privaten IP-Adressen des Schnittstellenendpunkts. Außerdem fügen wir der öffentlich gehosteten Zone für Amazon S3 ALIAS-Datensätze für den Route 53 Resolver hinzu, so dass DNS-Abfragen von Ihrer VPC an die öffentlichen IP-Adressen von Amazon S3 weitergeleitet werden, die den Datenverkehr zum Gateway-Endpunkt weiterleiten.

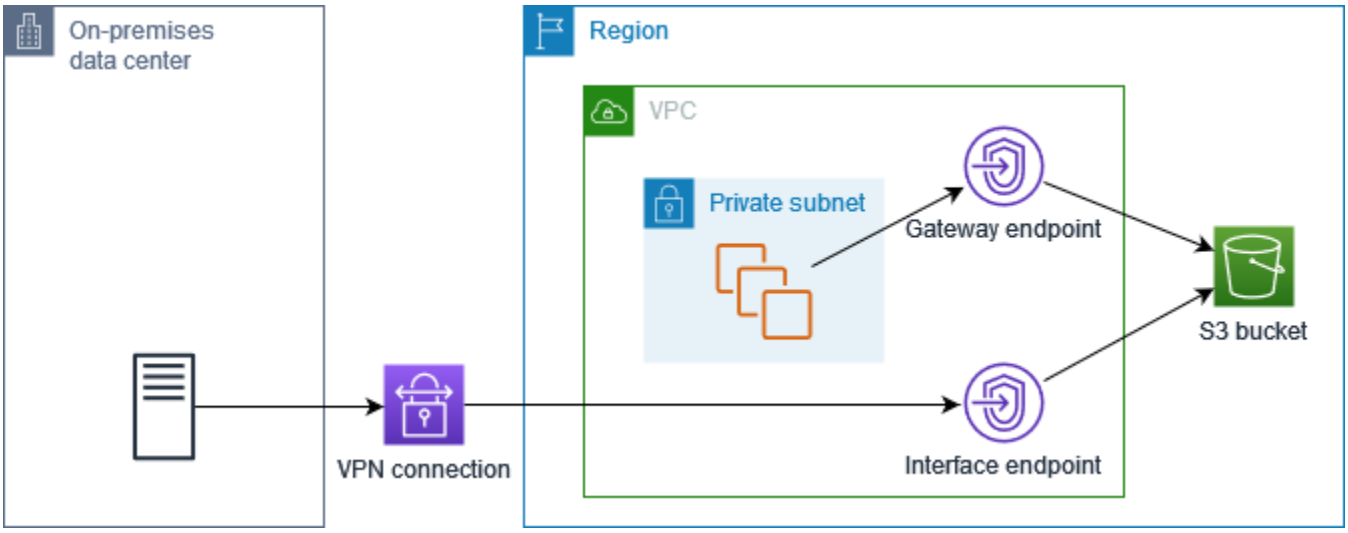
Privates DNS

Wenn Sie privates DNS für Ihren Schnittstellenendpunkt für Amazon S3 konfigurieren, aber nicht nur privates DNS für den eingehenden Resolver-Endpunkt konfigurieren, verwenden Anfragen sowohl aus Ihrem On-Premises-Netzwerk als auch aus Ihrer VPC den Schnittstellenendpunkt, um auf Amazon S3 zuzugreifen. Daher zahlen Sie für die Verwendung des Schnittstellenendpunkts für den Datenverkehr von der VPC, anstatt den Gateway-Endpunkt ohne zusätzliche Kosten zu verwenden.



Privates DNS nur für den eingehenden Resolver-Endpunkt

Wenn Sie privates DNS nur für den eingehenden Resolver-Endpunkt konfigurieren, verwenden Anfragen aus Ihrem On-Premises-Netzwerk den Schnittstellenendpunkt, um auf Amazon S3 zuzugreifen, und Anfragen aus Ihrer VPC verwenden den Gateway-Endpunkt, um auf Amazon S3 zuzugreifen. Daher optimieren Sie Ihre Kosten, da Sie für die Verwendung des Schnittstellenendpunkts nur für Datenverkehr zahlen, der den Gateway-Endpunkt nicht verwenden kann.



Privates DNS konfigurieren

Sie können privates DNS für einen Schnittstellenendpunkt für Amazon S3 konfigurieren, wenn Sie ihn erstellen oder nachdem Sie ihn erstellt haben. Weitere Informationen finden Sie unter the section called “Erstellen eines VPC-Endpunkts” (während der Erstellung konfigurieren) oder the section called “Aktivieren von privaten DNS-Namen” (nach der Erstellung konfigurieren).

Erstellen eines Gateway-Endpunkts

Gehen Sie wie folgt vor, um einen Gateway-Endpunkt zu erstellen, der eine Verbindung zu Amazon S3 herstellt.

So erstellen Sie ein Gateway-Endpunkt mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Wählen Sie für Servicekategorie die Option AWS-Services aus.
5. Fügen Sie für Services den Filter Type = Gateway hinzu und wählen Sie com.amazonaws aus. ***Region s.3.***
6. Wählen Sie für VPC eine VPC, in der der Endpunkt erstellt werden soll.
7. Wählen Sie für Route tables (Routing-Tabellen) die Routing-Tabellen, die von dem Endpunkt verwendet werden sollen. Wir fügen automatisch eine Route hinzu, die den für den Service bestimmten Datenverkehr auf die Netzwerkschnittstelle des Endpunkts verweist.
8. Wählen Sie für Policy (Richtlinie) Full access (Vollzugriff), um alle Operationen aller Prinzipale auf allen Ressourcen über den VPC-Endpunkt zuzulassen. Wählen Sie andernfalls Custom (Benutzerdefiniert), um eine VPC-Endpunktrichtlinie anzufügen, die die Berechtigungen steuert, die Prinzipale zum Ausführen von Aktionen für Ressourcen über den VPC-Endpunkt haben.
9. (Optional) Sie fügen ein Tag hinzu, indem Sie neuen Tag hinzufügen auswählen und den Schlüssel und den Wert für den Tag eingeben.
10. Wählen Sie Endpunkt erstellen.

So erstellen Sie ein Gateway-Endpunkt mithilfe der Befehlszeile

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Tools für Windows PowerShell)

Zugriffssteuerung mithilfe von Bucket-Richtlinien

Sie können Bucket-Richtlinien verwenden, um den Zugriff auf Buckets von bestimmten Endpunkten, VPCs, IP-Adressbereichen und aus zu steuern. AWS-Konten In diesen Beispielen wird davon

ausgegangen, dass es auch Richtlinienanweisungen gibt, die den für Ihre Anwendungsfälle erforderlichen Zugriff zulassen.

Example Beispiel: Beschränken des Zugriffs auf einen bestimmten Endpunkt

Sie können eine Bucket-Richtlinie mit dem aws:sourceVpce-Bedingungsschlüssel erstellen, um den Zugriff auf einen bestimmten Endpunkt zu beschränken. Die folgende Richtlinie lehnt Zugriff auf den angegebenen Bucket mit den angegebenen Aktionen ab, es sei denn, der angegebene Gateway-Endpunkt wird verwendet. Beachten Sie, dass diese Richtlinie den Zugriff auf den angegebenen Bucket mit den angegebenen Aktionen über die AWS Management Console blockiert.

```
{
  "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 Beispiel: Beschränken des Zugriffs auf eine bestimmte VPC

Sie können eine Bucket-Richtlinie mit dem aws:sourceVpc-Bedingungsschlüssel erstellen, um den Zugriff auf eine bestimmte VPC zu beschränken. Dies ist hilfreich, wenn Sie mehrere Endpunkte innerhalb derselben VPC konfiguriert haben. Die folgende Richtlinie lehnt Zugriff auf den angegebenen Bucket mit den angegebenen Aktionen ab, es sei denn, die Anforderung stammt von einer angegebenen VPC. Beachten Sie, dass diese Richtlinie den Zugriff auf den angegebenen Bucket mit den angegebenen Aktionen über die AWS Management Console blockiert.

```
{
  "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 Beispiel: Beschränken des Zugriffs auf einen bestimmten IP-Adressbereich

Mithilfe des Bedingungsschlüssels aws: VpcSource Ip können Sie eine Richtlinie erstellen, die den Zugriff auf bestimmte IP-Adressbereiche einschränkt. Die folgende Richtlinie verweigert den Zugriff auf den angegebenen Bucket, mit den angegebenen Aktionen, es sei denn, die Anforderung stammt von der angegebenen IP-Adresse. Beachten Sie, dass diese Richtlinie den Zugriff auf den angegebenen Bucket mit den angegebenen Aktionen über die AWS Management Console blockiert.

```
{
  "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 Beispiel: Beschränken Sie den Zugriff auf Buckets in einem bestimmten Bereich AWS-Konto

Sie können eine Richtlinie erstellen, die den Zugriff auf die S3-Buckets in einem bestimmten AWS-Konto einschränkt, indem Sie den Befehlsschlüssel `s3:ResourceAccount` verwenden. Die folgende Richtlinie verweigert den Zugriff auf S3-Buckets mit den angegebenen Aktionen, es sei denn, sie gehören dem angegebenen AWS-Konto an.

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

Zuordnen von Routing-Tabellen

Sie können die Routing-Tabellen ändern, die dem Gateway-Endpunkt zugeordnet sind. Wenn Sie eine Routing-Tabelle zuordnen, fügen wir automatisch eine Route hinzu, die den für den Service bestimmten Datenverkehr auf die Netzwerkschnittstelle des Endpunkts verweist. Wenn Sie die Zuordnung einer Routing-Tabelle aufheben, entfernen wir die Endpunktroute automatisch aus der Routing-Tabelle.

Zuordnen von Routing-Tabellen mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Erstellen des Gateway-Endpunkts.
4. Wählen Sie Aktionen und dann Verwalte Routing-Tabelle aus.
5. Aktivieren oder deaktivieren Sie die Auswahl von Routing-Tabellen nach Bedarf.

6. Wählen Sie Modify route tables (Ändern von Routing-Tabellen).

Zuordnen von Routing-Tabellen mithilfe der Befehlszeile

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Tools für Windows PowerShell)

Bearbeiten der VPC-Endpunktrichtlinie

Sie können die Endpunktrichtlinie für einen Gateway-Endpunkt bearbeiten, der den Zugriff auf Amazon S3 von der VPC über den Endpunkt steuert. Die Standardrichtlinie lässt Vollzugriff zu. Weitere Informationen finden Sie unter Endpunktrichtlinien.

So ändern Sie die Endpunktrichtlinie mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Erstellen des Gateway-Endpunkts.
4. Wählen Sie Aktionen, Verwalten von Richtlinien.
5. Wählen Sie Full Access (Voller Zugriff), um vollen Zugriff auf den Service zu gewähren, oder wählen Sie Custom (Benutzerdefiniert), und fügen Sie eine benutzerdefinierte Richtlinie hinzu.
6. Wählen Sie Speichern.

Nachfolgend sind Beispielendpunktrichtlinien für den Zugriff auf Amazon S3 aufgeführt.

Example Beispiel: Beschränken des Zugriffs auf einen bestimmten Bucket

Sie können eine Richtlinie erstellen, die den Zugriff auf bestimmte S3-Buckets beschränkt. Dies ist nützlich, wenn Sie andere AWS-Services in Ihrer VPC haben, die S3-Buckets verwenden.

```
{
  "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 Beispiel: Beschränken des Zugriffs auf eine bestimmte IAM-Rolle

Sie können eine Richtlinie erstellen, die den Zugriff auf eine bestimmte IAM-Rolle beschränkt. Sie müssen `aws:PrincipalArn` verwenden, um einem Prinzipal Zugriff zu gewähren.

```
{
  "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 Beispiel: Beschränken des Zugriffs auf Benutzer in einem bestimmten Konto

Sie können eine Richtlinie erstellen, die den Zugriff auf ein bestimmtes Konto beschränkt.

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

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

Löschen eines Gateway-Endpunkts

Wenn Sie einen Gateway-Endpunkt nicht mehr benötigen, können Sie ihn löschen. Wenn Sie einen Gateway-Endpunkt löschen, entfernen wir die Endpunktroute aus den Subnetz-Routing-Tabellen.

Ein Gateway-Endpunkt kann nicht gelöscht werden, wenn privates DNS aktiviert ist.

So löschen Sie ein Gateway-Endpunkt mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Erstellen des Gateway-Endpunkts.
4. Wählen Sie Actions (Aktionen), Delete VPC Endpoint (VPC-Endpunkte löschen).
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein.
6. Wählen Sie Löschen.

So löschen Sie ein Gateway-Endpunkt mithilfe der Befehlszeile

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

Gateway-Endpunkte für Amazon DynamoDB

Sie können über Gateway-VPC-Endpunkte von Ihrer VPC aus auf Amazon DynamoDB zugreifen. Nachdem Sie den Gateway-Endpunkt erstellt haben, können Sie ihn als Ziel in Ihrer Routing-Tabelle für Datenverkehr hinzufügen, der von Ihrer VPC zu DynamoDB bestimmt ist.

Für die Nutzung von Gateway-Endpunkten fallen keine zusätzlichen Gebühren an.

DynamoDB unterstützt sowohl Gateway-Endpunkte als auch Schnittstellenendpunkte. Mit einem Gateway-Endpunkt können Sie von Ihrer VPC aus auf DynamoDB zugreifen, ohne dass ein Internet-Gateway oder ein NAT-Gerät für Ihre VPC erforderlich ist, und ohne zusätzliche Kosten. Gateway-Endpunkte ermöglichen jedoch keinen Zugriff von lokalen Netzwerken, von Peer-VPCs in anderen AWS Regionen oder über ein Transit-Gateway. Für diese Szenarien müssen Sie einen Schnittstellenendpunkt verwenden, der gegen Aufpreis verfügbar ist. Weitere Informationen finden Sie unter Typen von VPC-Endpunkten für DynamoDB im Amazon DynamoDB Developer Guide.

Inhalt

Überlegungen

- Ein Gateway-Endpunkt ist nur in der Region verfügbar, in der Sie ihn erstellt haben. Stellen Sie sicher, dass Sie Ihren Gateway-Endpunkt in derselben Region wie Ihre DynamoDB-Tabellen erstellen.
- Wenn Sie die Amazon-DNS-Server verwenden, müssen Sie sowohl DNS-Hostnamen als auch DNS-Auflösung für Ihre VPC aktivieren. Wenn Sie Ihren eigenen DNS-Server verwenden, stellen Sie sicher, dass Anforderungen an DynamoDB korrekt in die von AWS verwalteten IP-Adressen erfüllt werden.
- Die ausgehenden Regeln für die Sicherheitsgruppe für Instances, die über den Gateway-Endpunkt auf DynamoDB zugreifen, müssen Datenverkehr zu DynamoDB zulassen. Sie können in den Regeln der Sicherheitsgruppe auf die ID der Präfixliste für DynamoDB verweisen.

- Die Netzwerk-ACL für das Subnetz für Ihre Instances, die über einen Gateway-Endpunkt auf DynamoDB zugreifen, muss Datenverkehr zu und von DynamoDB zulassen. Sie können in Netzwerk-ACL-Regeln nicht auf Präfixlisten verweisen, aber Sie können die IP-Adresse für DynamoDB aus der Präfixliste für DynamoDB abrufen.
- Wenn Sie AWS CloudTrail DynamoDB-Operationen protokollieren, enthalten die Protokolldateien die privaten IP-Adressen der EC2-Instances in der Service Consumer-VPC und die ID des Gateway-Endpunkts für alle Anfragen, die über den Endpunkt ausgeführt werden.
- Gateway-Endpunkte unterstützen nur IPv4-Datenverkehr.
- Die Quell-IPv4-Adressen von Instances in den betroffenen Subnetzen werden von öffentlichen IPv4-Adressen in private IPv4-Adressen Ihrer VPC umgewandelt. Endpunkte wechseln zwischen Netzwerkrouten und trennen offene TCP-Verbindungen. Die vorherigen Verbindungen, die öffentliche IPv4-Adressen verwendet haben, werden nicht fortgesetzt. Wir empfehlen, während des Erstellens oder Änderns eines Gateway-Endpunkts keine wichtigen Aufgaben auszuführen. Testen Sie alternativ, um sicherzustellen, dass Ihre Software automatisch wieder eine Verbindung zu DynamoDB herstellen kann, wenn eine Verbindung unterbrochen wird.
- Endpunktverbindungen können nicht auf einen Bereich außerhalb einer VPC erweitert werden. Ressourcen auf der anderen Seite einer VPN-Verbindung, VPC-Peering-Verbindung, eines Transit-Gateways oder einer AWS Direct Connect Verbindung in Ihrer VPC können keinen Gateway-Endpunkt für die Kommunikation mit DynamoDB verwenden.
- Ihr Konto hat ein Standardkontingent von 20 Gateway-Endpunkten pro Region, das anpassbar ist. Pro VPC sind auch höchstens 255 Gateway-Endpunkte zulässig.

Erstellen eines Gateway-Endpunkts

Gehen Sie wie folgt vor, um einen Gateway-Endpunkt zu erstellen, der eine Verbindung zu DynamoDB herstellt.

So erstellen Sie ein Gateway-Endpunkt mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Wählen Sie für Servicekategorie die Option AWS-Services aus.
5. Fügen Sie für Services den Filter Type = Gateway hinzu und wählen Sie com.amazonaws aus. ***region .dynamodb.***

6. Wählen Sie für VPC eine VPC, in der der Endpunkt erstellt werden soll.
7. Wählen Sie für Route tables (Routing-Tabellen) die Routing-Tabellen, die von dem Endpunkt verwendet werden sollen. Wir fügen automatisch eine Route hinzu, die den für den Service bestimmten Datenverkehr auf die Netzwerkschnittstelle des Endpunkts verweist.
8. Wählen Sie für Policy (Richtlinie) Full access (Vollzugriff), um alle Operationen aller Prinzipale auf allen Ressourcen über den VPC-Endpunkt zuzulassen. Wählen Sie andernfalls Custom (Benutzerdefiniert), um eine VPC-Endpunktrichtlinie anzufügen, die die Berechtigungen steuert, die Prinzipale zum Ausführen von Aktionen für Ressourcen über den VPC-Endpunkt haben.
9. (Optional) Sie fügen ein Tag hinzu, indem Sie neuen Tag hinzufügen auswählen und den Schlüssel und den Wert für den Tag eingeben.
10. Wählen Sie Endpunkt erstellen.

So erstellen Sie ein Gateway-Endpunkt mithilfe der Befehlszeile

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Tools für Windows) PowerShell

Zugriffssteuerung mit IAM-Richtlinien

Sie können IAM-Richtlinien erstellen, um zu steuern, welche IAM-Prinzipale über einen bestimmten VPC-Endpunkt auf DynamoDB-Tabellen zugreifen können.

Example Beispiel: Beschränken des Zugriffs auf einen bestimmten Endpunkt

Sie können eine Richtlinie mit dem aws:sourceVpce-Bedingungsschlüssel erstellen, um den Zugriff auf einen bestimmten VPC-Endpunkt zu beschränken. Die folgende Richtlinie verweigert den Zugriff auf DynamoDB-Tabellen im Konto, sofern der angegebene VPC-Endpunkt nicht verwendet wird. In diesem Beispiel wird davon ausgegangen, dass es auch eine Richtlinienanweisung gibt, die den für Ihre Anwendungsfälle erforderlichen Zugriff ermöglicht.

```
{
   "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 Beispiel: Erlauben des Zugriffs von einer bestimmten IAM-Rolle

Sie können eine Richtlinie erstellen, die den Zugriff mithilfe einer bestimmten IAM-Rolle zulässt. Die folgende Richtlinie gewährt Zugriff auf die angegebene IAM-Rolle.

```
{
   "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 Beispiel: Ermöglicht den Zugriff von einem bestimmten Konto aus

Sie können eine Richtlinie erstellen, die den Zugriff nur von einem bestimmten Konto aus zulässt. Die folgende Richtlinie gewährt Benutzern im angegebenen Konto Zugriff.

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

```
         "Sid": "Allow-access-from-account",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "aws:PrincipalAccount": "111122223333"
            }
         }
      }
   ]
}
```

Zuordnen von Routing-Tabellen

Sie können die Routing-Tabellen ändern, die dem Gateway-Endpunkt zugeordnet sind. Wenn Sie eine Routing-Tabelle zuordnen, fügen wir automatisch eine Route hinzu, die den für den Service bestimmten Datenverkehr auf die Netzwerkschnittstelle des Endpunkts verweist. Wenn Sie die Zuordnung einer Routing-Tabelle aufheben, entfernen wir die Endpunktroute automatisch aus der Routing-Tabelle.

Zuordnen von Routing-Tabellen mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Erstellen des Gateway-Endpunkts.
4. Wählen Sie Aktionen und dann Verwalte Routing-Tabelle aus.
5. Aktivieren oder deaktivieren Sie die Auswahl von Routing-Tabellen nach Bedarf.
6. Wählen Sie Modify route tables (Ändern von Routing-Tabellen).

Zuordnen von Routing-Tabellen mithilfe der Befehlszeile

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Tools für Windows PowerShell)

Bearbeiten der VPC-Endpunktrichtlinie

Sie können die Endpunktrichtlinie für einen Gateway-Endpunkt bearbeiten, der den Zugriff auf DynamoDB von der VPC über den Endpunkt steuert. Die Standardrichtlinie lässt Vollzugriff zu. Weitere Informationen finden Sie unter Endpunktrichtlinien.

So ändern Sie die Endpunktrichtlinie mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Erstellen des Gateway-Endpunkts.
4. Wählen Sie Aktionen, Verwalten von Richtlinien.
5. Wählen Sie Full Access (Voller Zugriff), um vollen Zugriff auf den Service zu gewähren, oder wählen Sie Custom (Benutzerdefiniert), und fügen Sie eine benutzerdefinierte Richtlinie hinzu.
6. Wählen Sie Speichern.

So ändern Sie ein Gateway-Endpunkt mithilfe der Befehlszeile

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Tools für Windows PowerShell)

Nachfolgend sind Beispielendpunktrichtlinien für den Zugriff auf DynamoDB aufgeführt.

Example Beispiel: Schreibgeschützten Zugriff zulassen

Sie können eine Richtlinie erstellen, die den Zugriff auf den schreibgeschützten Zugriff beschränkt. Die folgende Richtlinie erteilt die Berechtigung zum Auflisten und Beschreiben von DynamoDB-Tabellen.

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

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

Example Beispiel: Beschränken des Zugriffs auf eine bestimmte Tabelle

Sie können eine Richtlinie erstellen, die den Zugriff auf eine bestimmte DynamoDB-Tabelle beschränkt. Die folgende Richtlinie gewährt den Zugriff auf die angegebene DynamoDB-Tabelle.

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

Löschen eines Gateway-Endpunkts

Wenn Sie einen Gateway-Endpunkt nicht mehr benötigen, können Sie ihn löschen. Wenn Sie einen Gateway-Endpunkt löschen, entfernen wir die Endpunktroute aus den Subnetz-Routing-Tabellen.

So löschen Sie ein Gateway-Endpunkt mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Erstellen des Gateway-Endpunkts.
4. Wählen Sie Actions (Aktionen), Delete VPC Endpoint (VPC-Endpunkte löschen).

5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein.
6. Wählen Sie Löschen.

So löschen Sie ein Gateway-Endpunkt mithilfe der Befehlszeile

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

Zugriff auf SaaS-Produkte über AWS PrivateLink

Mit AWS PrivateLink dieser Option können Sie privat auf SaaS-Produkte zugreifen, als ob sie in Ihrer eigenen VPC laufen würden.

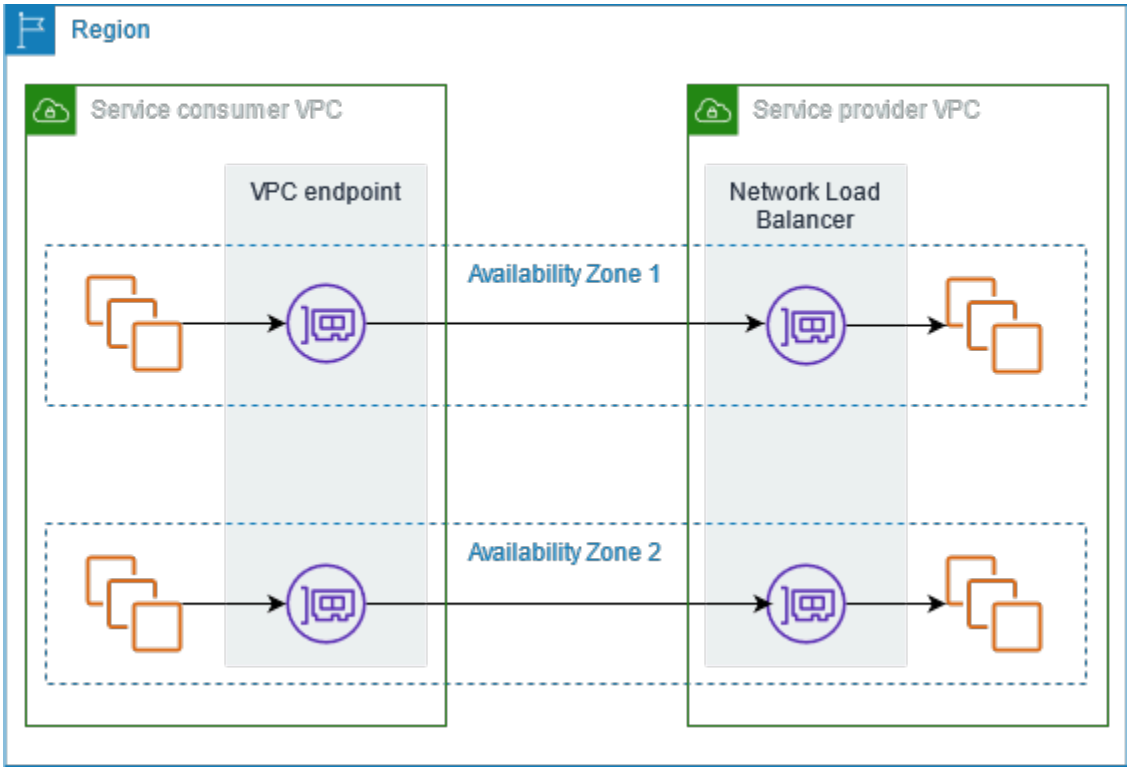
Inhalt

Übersicht

Sie können SaaS-Produkte, die von bereitgestellt werden, entdecken, kaufen und AWS PrivateLink bereitstellen AWS Marketplace. Weitere Informationen finden Sie unter AWS Marketplace: - PrivateLink.

Sie können auch SaaS-Produkte finden, die AWS PrivateLink von AWS Partnern bereitgestellt werden. Weitere Informationen finden Sie unter AWS PrivateLink -Partner.

Das folgende Diagramm zeigt, wie Sie VPC-Endpunkte verwenden, um eine Verbindung mit SaaS-Produkten herzustellen. Der Service-Anbieter erstellt einen Endpunkt-Service und gewährt seinen Kunden Zugriff auf den Endpunkt-Service. Als Service-Verbraucher erstellen Sie einen Schnittstellen-VPC-Endpunkt, der Verbindungen zwischen einem oder mehreren Subnetzen in Ihrer VPC und dem Endpunkt-Service herstellt.



Erstellen eines Schnittstellenendpunkts

Verwenden Sie das folgende Verfahren, um einen Schnittstellen-VPC-Endpunkt zu erstellen, der eine Verbindung mit dem SaaS-Produkt herstellt.

Anforderung

Den Service abonnieren.

So erstellen Sie einen Schnittstellenendpunkt zu einem Partnerservice

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Wenn Sie den Service bei gekauft haben AWS Marketplace, gehen Sie wie folgt vor:
    a. Wählen Sie bei Service category (Servicekategorie) die Option AWS Marketplace services (-Services) aus.
    b. Geben Sie den Namen des Services ein.

5. Wenn Sie einen Dienst mit der Bezeichnung AWS Service Ready abonniert haben, gehen Sie wie folgt vor:

   a. Wählen Sie als Servicekategorie die Option PrivateLink Ready-Partnerdienste aus.

   b. Geben Sie den Namen des Service ein und wählen Sie Verify service (Service überprüfen).

6. Wählen Sie für VPC die VPC aus, von der aus Sie auf das Produkt zugreifen.
7. Wählen Sie für Subnets (Subnetze) ein Subnetz pro Availability Zone aus, von dem aus Sie auf das Produkt zugreifen.
8. Für Sicherheitsgruppe wählen Sie die Sicherheitsgruppen aus, die den Endpunktnetzwerkschnittstellen zugeordnet werden sollen. Die Sicherheitsgruppenregeln müssen Datenverkehr zwischen den Ressourcen in der VPC und den Endpunktnetzwerkschnittstellen zulassen.
9. (Optional) Sie fügen ein Tag hinzu, indem Sie neuen Tag hinzufügen auswählen und den Schlüssel und den Wert für den Tag eingeben.
10. Wählen Sie Endpunkt erstellen.

So konfigurieren Sie einen Schnittstellen-Endpunkt

Informationen zum Konfigurieren des Schnittstellenendpunkts finden Sie unter the section called “Konfigurieren eines Schnittstellenendpunkts”.

Greifen Sie auf virtuelle Geräte zu über AWS PrivateLink

Sie können einen Gateway Load Balancer verwenden, um den Datenverkehr an eine Flotte virtueller Netzwerkgeräte zu verteilen. Die Appliances können für Sicherheitsinspektionen, Compliance, Richtlinienkontrollen und andere Netzwerkdienste verwendet werden. Sie geben den Gateway Load Balancer an, wenn Sie einen VPC-Endpunkt-Service erstellen. Sonstige AWS -Prinzipale greifen auf den Endpunkt-Service zu, indem sie einen Gateway-Load-Balancer-Endpunkt.

Preisgestaltung

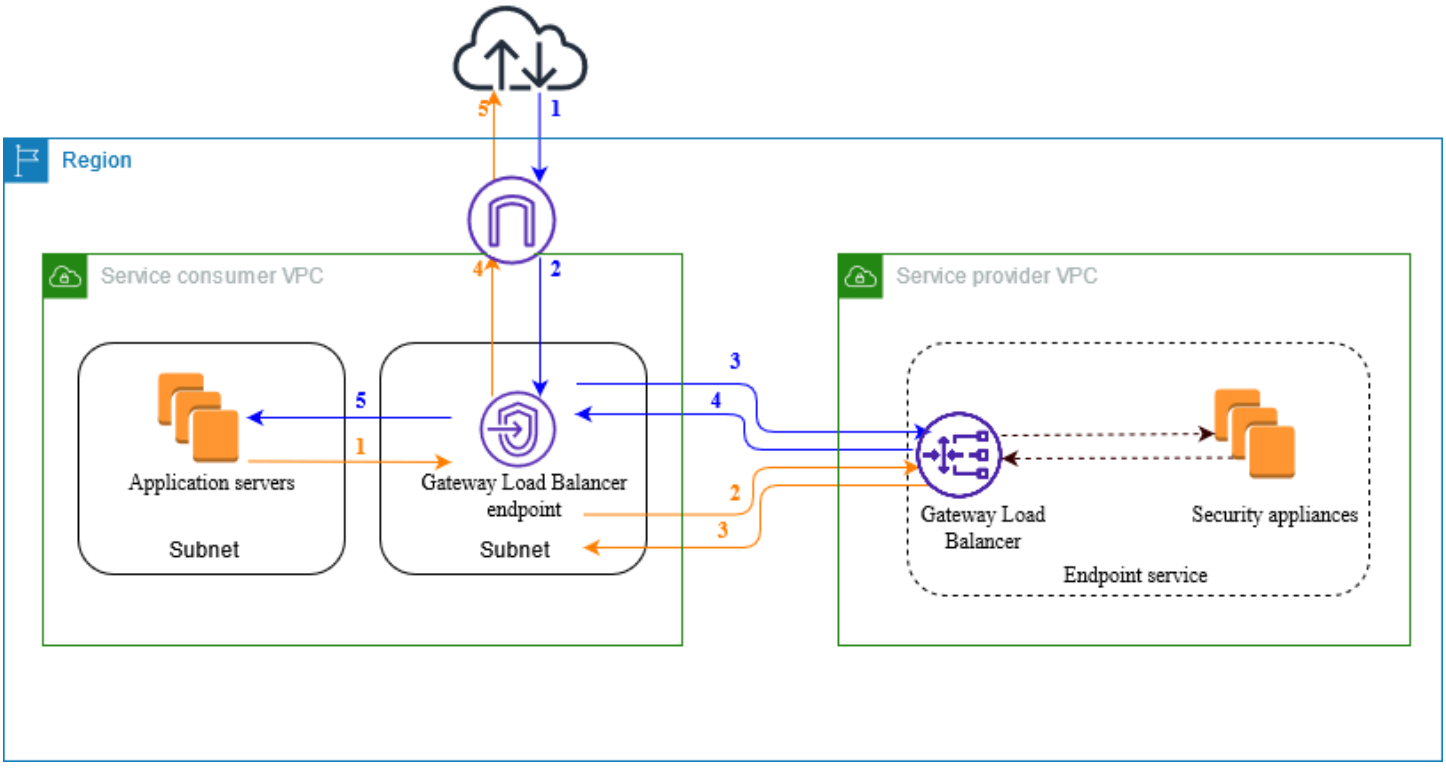
Ihnen wird jede Stunde in Rechnung gestellt, in der Ihr Gateway Load Balancer-Endpunkt in jeder Availability Zone bereitgestellt wird. Ihnen wird auch pro GB verarbeiteter Daten in Rechnung gestellt. Weitere Informationen finden Sie unter AWS PrivateLink -Preisgestaltung.

Inhalt

Weitere Informationen finden Sie unter Gateway Load Balancer.

Übersicht

Das folgende Diagramm zeigt, wie Anwendungsserver auf Sicherheits-Appliances zugreifen AWS PrivateLink. Die Anwendungsserver werden in einem Subnetz der Service-Verbraucher-VPC ausgeführt. Sie erstellen einen Gateway-Load-Balancer-Endpunkt in einem anderen Subnetz derselben VPC. Der gesamte Datenverkehr, der über das Internet-Gateway in die Service-Verbraucher-VPC gelangt, wird zunächst zur Überprüfung an den Gateway-Load-Balancer-Endpunkt weitergeleitet und dann an das Zielsubnetz. Ebenso wird der gesamte Datenverkehr, der die Anwendungsserver verlässt, zur Überprüfung an den Gateway-Load-Balancer-Endpunkt geleitet, bevor er über das Internet-Gateway zurückgeleitet wird.



Datenverkehr vom Internet zu den Anwendungsservern (blaue Pfeile):

1. Der Datenverkehr gelangt über das Internet-Gateway in die Service-Verbraucher-VPC.
2. Der Datenverkehr wird basierend auf der Routingtabellenkonfiguration an den Gateway-Load-Balancer-Endpunkt gesendet.
3. Der Datenverkehr wird zur Überprüfung durch die Sicherheits-Appliance an den Gateway Load Balancer gesendet.
4. Der Datenverkehr wird nach der Überprüfung an den Gateway-Load-Balancer-Endpunkt zurückgesendet
5. Der Datenverkehr wird basierend auf der Konfiguration der Routing-Tabelle an die Anwendungsserver gesendet.

Datenverkehr von den Anwendungsservern ins Internet (orangefarbene Pfeile):

1. Der Datenverkehr wird basierend auf der Routingtabellenkonfiguration an den Gateway-Load-Balancer-Endpunkt gesendet.
2. Der Datenverkehr wird zur Überprüfung durch die Sicherheits-Appliance an den Gateway Load Balancer gesendet.

3. Der Datenverkehr wird nach der Überprüfung an den Gateway-Load-Balancer-Endpunkt zurückgesendet
4. Der Datenverkehr wird basierend auf der Routingtabellenkonfiguration an das Internet-Gateway gesendet.
5. Der Datenverkehr wird zurück ins Internet geleitet.

IP-Adresstypen

Serviceanbieter können ihre Service-Endpunkte den Servicenutzern über IPv4, IPv6 oder sowohl IPv4 als auch IPv6 zur Verfügung stellen, auch wenn ihre Sicherheitsanwendungen nur IPv4 unterstützen. Wenn Sie die Dualstack-Support aktivieren, können bestehende Verbraucher weiterhin IPv4 verwenden, um auf Ihren Service zuzugreifen, und neue Verbraucher können IPv6 für den Zugriff auf Ihren Service verwenden.

Wenn ein Endpunkt des Gateway-Load-Balancers IPv4 unterstützt, verfügen die Endpunkt-Netzwerkschnittstellen über IPv4-Adressen. Wenn ein Endpunkt des Gateway-Load-Balancers IPv6 unterstützt, verfügen die Endpunkt-Netzwerkschnittstellen über IPv6-Adressen. Die IPv6-Adresse für eine Endpunkt-Netzwerkschnittstelle ist aus dem Internet nicht erreichbar. Wenn Sie eine Endpunktnetzwerkschnittstelle mit einer IPv6-Adresse beschreiben, beachten Sie, dass `denyAllIgwTraffic` aktiviert ist.

Anforderungen zum Aktivieren von IPv6 für einen Endpunkt-Service

- Die VPC und Subnetze für den Endpunkt-Service müssen IPv6-CIDR-Blöcke haben.
- Der Gateway-Load-Balancer für den Endpunktservice muss den IP-Adresstyp Dualstack verwenden. Die Sicherheits-Appliances müssen keinen IPv6-Datenverkehr unterstützen.

Anforderungen zum Aktivieren von IPv6 für einen Endpunkt des Gateway-Load-Balancers

- Der Endpunktservice muss über einen IP-Adresstyp verfügen, der IPv6-Unterstützung beinhaltet.
- Der IP-Adresstyp eines Endpunkts des Gateway-Load-Balancers muss mit dem Subnetz für den Endpunkt des Gateway-Load-Balancers kompatibel sein, wie hier beschrieben:
  - IPv4 – Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv4-Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze über IPv4-Adressbereiche verfügen.
  - IPv6 – Weisen Sie Ihren Endpunktnetzwerkschnittstellen IPv6-Adressen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze reine IPv6-Subnetze sind.

- Dualstack – Zuweisen von IPv4- und IPv6-Adressen zu Ihren Endpunktnetzwerkschnittstellen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze sowohl IPv4- als auch IPv6-Adressbereiche aufweisen.
- Die Routing-Tabellen für die Subnetze in der Servicenutzer-VPC müssen IPv6-Datenverkehr weiterleiten und die Netzwerk-ACLs für diese Subnetze müssen IPv6-Datenverkehr zulassen.

Routing

Um den Datenverkehr an den Endpunkt-Service weiterzuleiten, geben Sie den Gateway-Load-Balancer-Endpunkt als Ziel in Ihren Routingtabellen an, indem Sie seine ID verwenden. Fügen Sie für das obige Diagramm wie folgt Routen zu den Routing-Tabellen hinzu. Beachten Sie, dass IPv6-Routen für eine Dualstack-Konfiguration enthalten sind.

Routing-Tabelle für das Internet-Gateway

Diese Routing-Tabelle muss über eine Route verfügen, die Datenverkehr für die Anwendungsserver an den Gateway-Load-Balancer-Endpunkt sendet.

Bestimmungsort	Ziel
VPC – IPv4 CIDR	Local
VPC – IPv6 CIDR	Local
Anwendungs-Subnetz – IPv4 CIDR	*vpc-endpoint-id*
Anwendungs-Subnetz – IPv6 CIDR	*vpc-endpoint-id*

Routing-Tabelle für das Subnetz mit den Anwendungsservern

Diese Routing-Tabelle muss eine Route enthalten, die den gesamten Datenverkehr von den Anwendungsservern an den Endpunkt des Gateway-Load-Balancers sendet.

Bestimmungsort	Ziel
VPC – IPv4 CIDR	Local
VPC – IPv6 CIDR	Local

Bestimmungsort	Ziel
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Routing-Tabelle für das Subnetz mit dem Gateway-Load-Balancer-Endpunkt

Diese Routing-Tabelle muss Datenverkehr, der von der Überprüfung zurückgegeben wird, an sein Endziel senden. Für Datenverkehr aus dem Internet sendet die lokale Route den Datenverkehr an die Anwendungsserver. Fügen Sie für Datenverkehr, der von den Anwendungsservern ausgeht, eine Route hinzu, die den gesamten Datenverkehr an das Internet-Gateway sendet.

Bestimmungsort	Ziel
VPC – IPv4 CIDR	Local
VPC – IPv6 CIDR	Local
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

Erstellen eines Inspektionssystems als Gateway-Load-Balancer-Endpunkt-Service

Sie können Ihren eigenen Dienst erstellen AWS PrivateLink, der als Endpunktdienst bezeichnet wird. Sie sind der Dienstanbieter, und die AWS Principals, die Verbindungen zu Ihrem Service herstellen, sind die Dienstnutzer.

Endpunkt-Services erfordern entweder einen Network Load Balancer oder einen Gateway Load Balancer. In diesem Fall erstellen Sie einen Endpunkt-Service mit einem Gateway Load Balancer. Weitere Informationen zum Erstellen eines Endpunkt-Service mit einem Network Load Balancer finden Sie unter Erstellen eines Endpunkt-Service.

Inhalt

- Voraussetzungen
- Erstellen Sie den Endpunktservice
- Stellen Sie Ihren Endpunkt-Service zur Verfügung

Überlegungen

- Ein Endpunktservice ist in der Region verfügbar, in der Sie ihn erstellt haben.
- Wenn Service-Verbraucher Informationen zu einem Endpunkt-Service abrufen, können sie nur die Availability Zones sehen, die sie mit dem Service-Anbieter gemeinsam haben. Wenn sich der Service-Anbieter und der Service-Verbraucher in verschiedenen Konten befinden, kann ein Name der Availability Zone, z. B. `us-east-1a`, in jedem AWS-Konto einer anderen physischen Verfügbarkeitszone zugeordnet werden. Mithilfe von AZ-IDs können Sie die Availability Zones für Ihren Service einheitlich identifizieren. Weitere Informationen finden Sie unter AZ-IDs im Amazon EC2 EC2-Benutzerhandbuch.
- Es gibt Kontingente für Ihre AWS PrivateLink Ressourcen. Weitere Informationen finden Sie unter AWS PrivateLink -Kontingente.

Voraussetzungen

- Erstellen Sie eine Service-Verbraucher-VPC mit mindestens zwei Subnetzen in der Availability Zone, in der der Service zur Verfügung stehen soll. Ein Subnetz ist für die Security-Appliance-Instances und das andere für den Gateway Load Balancer vorgesehen.
- Erstellen Sie einen Gateway Load Balancer in Ihrer Service-Verbraucher-VPC. Wenn Sie planen, IPv6-Unterstützung auf Ihrem Endpunktservice zu aktivieren, müssen Sie Dualstack-Unterstützung auf Ihrem Gateway-Load-Balancer aktivieren. Weitere Informationen finden Sie unter Erste Schritte mit Gateway Load Balancern.
- Starten Sie Sicherheits-Appliances in der Service-Verbraucher-VPC und registrieren Sie sie bei einer Load-Balancer-Zielgruppe.

Erstellen Sie den Endpunktservice

Verwenden Sie das folgende Verfahren, um einen Endpunkt-Service mit einem Gateway Load Balancer zu erstellen.

So erstellen Sie einen Endpunktservice unter Verwendung der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie Create Endpoint Service (Endpunkt-Service erstellen) aus.
4. Wählen Sie für Load-Balancer-Typ Gateway aus.
5. Wählen Sie für Available load balancers (verfügbare Load Balancer) Ihren Gateway-Load-Balancer aus.
6. Wählen Sie für Require acceptance for endpoint (Akzeptanz für Endpunkt erforderlich) Acceptance required (Akzeptanz erforderlich), um zu verlangen, dass Verbindungsanforderungen an Ihren Endpunkt-Service manuell akzeptiert werden. Andernfalls werden sie automatisch akzeptiert.
7. Führen Sie für Unterstützte IP-Adresstyp einen der folgenden Schritte aus:
   - Wählen Sie IPv4 – Aktivieren Sie den Endpunkt-Service, um IPv4-Anfragen anzunehmen.
   - Wählen Sie IPv6 – Aktivieren Sie den Endpunkt-Service, um IPv6-Anfragen zu akzeptieren.
   - Wählen Sie IPv4 und IPv6 – Aktivieren Sie den Endpunkt-Service, um IPv4- und IPv6-Anfragen zu akzeptieren.
8. (Optional) Sie fügen ein Tag hinzu, indem Sie Add new tag (neuen Tag hinzufügen) auswählen und den Schlüssel und den Wert für den Tag eingeben.
9. Wählen Sie Erstellen.

So erstellen Sie einen Endpunktservice unter Verwendung der Befehlszeile

- create-vpc-endpoint-service-configuration (AWS CLI)
- New-EC2VpcEndpointServiceConfiguration(Tools für Windows PowerShell)

Stellen Sie Ihren Endpunkt-Service zur Verfügung

Service-Anbieter müssen Folgendes tun, um ihre Services den Service-Verbrauchern zur Verfügung zu stellen.

- Fügen Sie Berechtigungen hinzu, die es jedem Service-Verbraucher ermöglichen, eine Verbindung mit Ihrem Endpunkt-Service herzustellen. Weitere Informationen finden Sie unter the section called “Verwalten von Berechtigungen”.

- Geben Sie dem Service-Verbraucher den Namen Ihres Service und der unterstützten Availability Zonen, damit er einen Schnittstellenendpunkt erstellen kann, um eine Verbindung mit dem Service herzustellen. Weitere Informationen finden Sie im folgenden Verfahren.
- Akzeptieren Sie die Endpunktverbindungsanforderung vom Service-Verbraucher. Weitere Informationen finden Sie unter the section called “Annehmen oder Ablehnen von Verbindungsanforderungen”.

AWS Principals können sich privat mit Ihrem Endpoint Service verbinden, indem sie einen Gateway Load Balancer-Endpunkt erstellen. Weitere Informationen finden Sie unter Erstellen eines Gateway-Load-Balancer-Endpunkts.

Zugriff auf ein Inspektionssystem per Gateway-Load-Balancer-Endpunkt

Sie können einen Gateway-Load-Balancer-Endpunkt erstellen, um eine Verbindung mit Endpunkt-Services herzustellen, die von AWS PrivateLink unterstützt werden.

Für jedes Subnetz, das Sie in Ihrer VPC angeben, erstellen wir eine Endpunkt-Netzwerkschnittstelle im Subnetz und weisen ihr eine private IP-Adresse aus dem Subnetz-Adressbereich zu. Eine Endpunkt-Netzwerkschnittstelle ist eine vom Anforderer verwaltete Netzwerkschnittstelle. Sie können sie in Ihrem anzeigen AWS-Konto, aber nicht selbst verwalten.

Die stündliche Nutzung und Datenverarbeitungsgebühren werden Ihnen in Rechnung gestellt. Weitere Informationen finden Sie auf Preise zu Gateway-Load-Balancer-Endpunkte.

Inhalt

Überlegungen

- Sie können nur eine Availability Zone in der Service-Verbraucher-VPC auswählen. Sie können dieses Subnetz später nicht mehr ändern. Um einen Gateway-Load-Balancer-Endpunkt in einem anderen Subnetz zu verwenden, müssen Sie einen neuen Gateway-Load-Balancer-Endpunkt erstellen.
- Sie können je Service einen Gateway-Load-Balancer-Endpunkt pro Availability Zone erstellen und müssen die Availability Zone auswählen, die vom Gateway Load Balancer unterstützt wird. Wenn sich der Service-Anbieter und der Service-Verbraucher in verschiedenen Konten befinden, kann ein Name der Availability Zone, z. B. `us-east-1a`, in jedem AWS-Konto einer anderen physischen Verfügbarkeitszone zugeordnet werden. Mithilfe von AZ-IDs können Sie die Availability Zones für Ihren Service einheitlich identifizieren. Weitere Informationen finden Sie unter AZ-IDs im Amazon EC2 EC2-Benutzerhandbuch.
- Bevor Sie den Endpunkt-Service verwenden können, muss der Service-Anbieter die Verbindungsanforderungen akzeptieren. Der Service kann keine Anfragen an Ressourcen in Ihrer VPC über den VPC-Endpunkt veranlassen. Der Endpunkt gibt nur Antworten auf Datenverkehr zurück, der von Ressourcen in Ihrer VPC initiiert wurde.
- Jeder Gateway Load Balancer-Endpunkt kann eine Bandbreite von bis zu 10 GBit/s pro Availability Zone unterstützen und skaliert automatisch auf bis zu 100 Gbit/s.
- Wenn ein Endpunktservice mehreren Gateway Load Balancers zugeordnet ist, richtet ein Gateway-Load-Balancer-Endpunkt eine Verbindung mit nur einem Load Balancer pro Availability Zone ein.
- Um den Datenverkehr innerhalb derselben Availability Zone zu halten, empfehlen wir Ihnen, in jeder Availability Zone, an die Sie Datenverkehr senden, einen Gateway-Load-Balancer-Endpunkt zu erstellen.
- Die IP-Beibehaltung des Network-Load-Balancer-Clients wird nicht unterstützt, wenn der Datenverkehr über einen Gateway-Load-Balancer-Endpunkt weitergeleitet wird, selbst wenn sich das Ziel in derselben VPC wie der Network Load Balancer befindet.
- Es gibt Kontingente für Ihre AWS PrivateLink Ressourcen. Weitere Informationen finden Sie unter AWS PrivateLink -Kontingente.

Voraussetzungen

- Erstellen Sie eine Service-Verbraucher-VPC mit mindestens zwei Subnetzen in der Availability Zone, von der aus Sie auf den Service zugreifen. Ein Subnetz ist für die Anwendungsserver und das andere für den Gateway-Load-Balancer-Endpunkt.

- Um zu überprüfen, welche Availability Zones vom Endpunkt-Service unterstützt werden, beschreiben Sie den Endpunkt-Service mithilfe der Konsole oder des Befehls describe-vpc-endpoint-services.
- Wenn sich Ihre Ressourcen in einem Subnetz mit einer Netzwerk-ACL befinden, stellen Sie sicher, dass die Netzwerk-ACL Datenverkehr zwischen den Netzwerkschnittstellen des Endpunkts und den Ressourcen in der VPC zulässt.

Endpunkt erstellen

Verwenden Sie das folgende Verfahren, um einen Gateway-Load-Balancer-Endpunkt zu erstellen, der eine Verbindung mit dem Endpunkt-Service für das Inspektionssystem herstellt.

So erstellen Sie einen Gateway-Load-Balancer-Endpunkt mit der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Wählen Sie für Service category (Servicekategorie) Other endpoint services (Andere Endpunkt-Services).
5. Geben Sie für Service Name (Servicename) den Namen des Service ein und wählen Sie Verify service (Service überprüfen) aus.
6. Wählen Sie für VPC eine VPC, in der der Endpunkt erstellt werden soll.
7. Wählen Sie für Subnets (Subnetze) das Subnetz aus, in dem der Endpunkt erstellt werden soll.
8. Wählen Sie für IP address type (IP-Adressentyp) eine der folgenden Optionen aus:
   - IPv4 – Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv4-Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze über IPv4-Adressbereiche verfügen.
   - IPv6 – Weisen Sie Ihren Endpunktnetzwerkschnittstellen IPv6-Adressen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze reine IPv6-Subnetze sind.
   - Dualstack – Zuweisen von IPv4- und IPv6-Adressen zu Ihren Endpunktnetzwerkschnittstellen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze sowohl IPv4- als auch IPv6-Adressbereiche aufweisen.
9. (Optional) Sie fügen ein Tag hinzu, indem Sie neuen Tag hinzufügen auswählen und den Schlüssel und den Wert für den Tag eingeben.
10. Wählen Sie Endpunkt erstellen. Der ursprüngliche Status ist `pending acceptance`.

So erstellen Sie einen Gateway-Load-Balancer-Endpunkt mit der Befehlszeile

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Tools für Windows PowerShell)

Routing konfigurieren

Gehen Sie wie folgt vor, um Routing-Tabellen für die Service-Verbraucher-VPC zu konfigurieren. Auf diese Weise können die Sicherheits-Appliances eine Sicherheitsüberprüfung für eingehenden Datenverkehr durchführen, der für die Anwendungsserver bestimmt ist. Weitere Informationen finden Sie unter the section called “Routing”.

So konfigurieren Sie Routing mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Wählen Sie die Routing-Tabelle für den Internet-Gateway aus, und führen Sie die folgenden Schritte aus:
   a. Wählen Sie Aktionen und dann Routen bearbeiten.
   b. Wenn Sie IPv4 unterstützen, wählen Sie Add route (Route hinzufügen). Geben Sie für Destination (Ziel) den IPv4-CIDR-Block des Subnetzes für die Anwendungsserver ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.
   c. Wenn Sie IPv6 unterstützen, wählen Sie Add route (Route hinzufügen). Geben Sie für Destination (Ziel) den IPv6-CIDR-Block des Subnetzes für die Anwendungsserver ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.
   d. Wählen Sie Änderungen speichern.
4. Wählen Sie die Routing-Tabelle für das Subnetz mit den Anwendungsservern aus, und führen Sie folgende Schritte aus:
   a. Wählen Sie Aktionen und dann Routen bearbeiten.
   b. Wenn Sie IPv4 unterstützen, wählen Sie Add route (Route hinzufügen). Geben Sie für Destination **`0.0.0.0/0`** ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.
   c. Wenn Sie IPv6 unterstützen, wählen Sie Add route (Route hinzufügen). Geben Sie für Destination **`::/0`** ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.
   d. Wählen Sie Änderungen speichern.

5. Wählen Sie die Routing-Tabelle für das Subnetz mit dem Gateway-Load-Balancer-Endpunkt aus und tun Sie Folgendes:

   a. Wählen Sie Aktionen und dann Routen bearbeiten.

   b. Wenn Sie IPv4 unterstützen, wählen Sie Add route (Route hinzufügen). Geben Sie für Destination **`0.0.0.0/0`** ein. Wählen Sie für Target (Ziel) das Internet-Gateway aus.

   c. Wenn Sie IPv6 unterstützen, wählen Sie Add route (Route hinzufügen). Geben Sie für Destination **`::/0`** ein. Wählen Sie für Target (Ziel) das Internet-Gateway aus.

   d. Wählen Sie Änderungen speichern aus.

So konfigurieren Sie das Routing mithilfe der Befehlszeile

- create-route (AWS CLI)
- New-EC2Route(Tools für Windows PowerShell)

Verwalten von Tags

Sie können Ihren Gateway-Load-Balancer-Endpunkt markieren, um ihn identifizieren oder in Übereinstimmung mit den Anforderungen Ihrer Organisation kategorisieren zu können.

So verwalten Sie Tags mit der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Schnittstellenendpunkt.
4. Klicken Sie auf Actions (Aktionen), Manage tags (Markierungen verwalten).
5. Wählen Sie für jede Markierung Add new tag (Neue Markierung hinzufügen) und geben Sie den Schlüssel und Wert der Markierung ein.
6. Um eine Markierung zu entfernen, wählen Sie Remove (Entfernen) rechts neben dem Schlüssel und dem Wert der Markierung aus.
7. Wählen Sie Speichern.

So verwalten Sie Tags mit der Befehlszeile

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

- New-EC2Tagund Remove-EC2Tag(Tools für Windows PowerShell)

Löschen eines Gateway-Load-Balancer-Endpunkts

Wenn Sie einen Endpunkt nicht mehr benötigen, können Sie ihn löschen. Durch das Löschen eines Gateway-Load-Balancer-Endpunkts werden auch die Endpunkt-Netzwerkschnittstellen gelöscht. Sie können einen Gateway-Load-Balancer-Endpunkt nicht löschen, wenn es Routen in Ihren Routingtabellen gibt, die auf den Endpunkt verweisen.

So löschen Sie einen Gateway-Load-Balancer-Endpunkt

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Endpoints und wählen Sie Ihren Endpunkt aus.
3. Wählen Sie Actions, Delete Endpoint.
4. Wählen Sie auf dem Bestätigungsbildschirm Yes, Delete aus.

So löschen Sie einen Gateway-Load-Balancer-Endpunkt

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

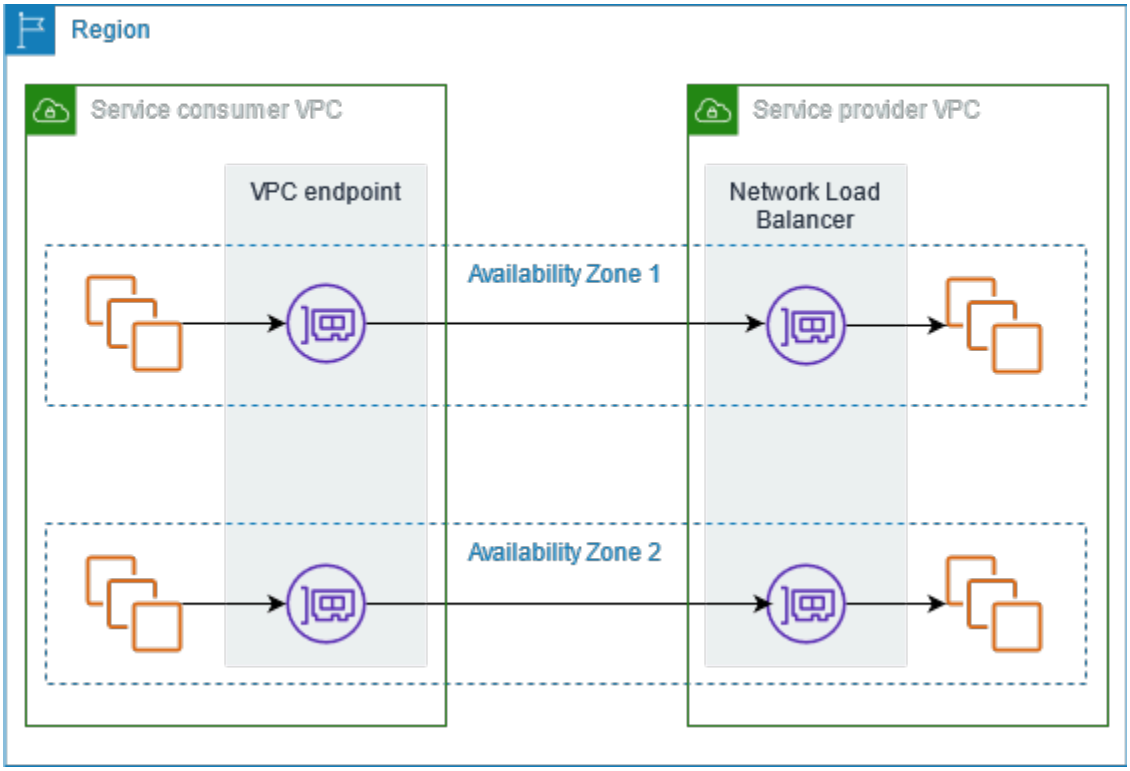
Teilen Sie Ihre Dienste über AWS PrivateLink

Sie können Ihren eigenen Dienst AWS PrivateLink , einen sogenannten Endpunktdienst, hosten und ihn mit anderen AWS Kunden teilen.

Inhalt

Übersicht

Das folgende Diagramm zeigt, wie Sie Ihren gehosteten Dienst AWS mit anderen AWS Kunden teilen und wie diese Kunden eine Verbindung zu Ihrem Dienst herstellen. Als Service-Anbieter erstellen Sie in Ihrer VPC einen Network Load Balancer als Service-Frontend. Anschließend wählen Sie diesen Load Balancer aus, wenn Sie die VPC-Endpunkt-Servicekonfiguration erstellen. Sie erteilen bestimmten AWS -Prinzipalen eine Berechtigung, damit diese eine Verbindung mit Ihrem Service herstellen können. Als Service-Verbraucher erstellt der Kunde einen Schnittstellen-VPC-Endpunkt, der Verbindungen zwischen den Subnetzen, die er aus seiner VPC auswählt, und Ihrem Endpunktservice herstellt. Der Load Balancer empfängt Anforderungen vom Service-Verbraucher und leitet sie an die Ziele weiter, die Ihren Service hosten.



Für niedrige Latenz und Hochverfügbarkeit empfehlen wir, dass Sie Ihren Service in mindestens zwei Availability Zones zur Verfügung stellen.

DNS-Hostnamen

Wenn ein Dienstanbieter einen VPC-Endpunktdienst erstellt, AWS generiert er einen endpunktspezifischen DNS-Hostnamen für den Dienst. Diese Namen haben die folgende Syntax:

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

Das folgende Beispiel zeigt einen DNS-Hostnamen für einen VPC-Endpunkt-Service in der Region us-east-2:

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

Wenn ein Service-Verbraucher einen VPC-Schnittstellen-Endpunkt erstellt, erstellen wir regionale und zonale DNS-Namen, die der Service-Verbraucher für die Kommunikation mit dem Endpunkt-Service verwenden kann. Regionale Namen haben die folgende Syntax:

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

Zonale Namen haben die folgende Syntax:

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

Privates DNS

Ein Service-Anbieter kann seinem Endpunkt-Service auch einen privaten DNS-Namen zuordnen, sodass Service-Verbraucher weiterhin mit ihrem vorhandenen DNS-Namen auf den Service zugreifen können. Wenn ein Service-Anbieter einen privaten DNS-Namen mit einem Endpunkt-Service verknüpft, können Service-Nutzer private DNS-Namen für den Schnittstellenendpunkt aktivieren. Wenn ein Service-Anbieter kein privates DNS aktiviert, müssen die Service-Nutzer möglicherweise die Anwendungen aktualisieren, um den öffentlichen DNS-Namen für den VPC-Endpunkt-Service zu verwenden. Weitere Informationen finden Sie unter DNS-Namen verwalten.

IP-Adresstypen

Service-Anbieter können ihre Service-Endpunkte Service-Verbrauchern über IPv4, IPv6 oder IPv4 und IPv6 sowohl IPv4 als auch IPv6 zur Verfügung stellen, auch wenn ihre Back-End-Server nur IPv4 unterstützen. Wenn Sie die Dualstack-Support aktivieren, können bestehende Verbraucher weiterhin IPv4 verwenden, um auf Ihren Service zuzugreifen, und neue Verbraucher können IPv6 für den Zugriff auf Ihren Service verwenden.

Wenn ein Schnittstellen-VPC-Endpunkt IPv4 unterstützt, verfügen die Endpunkt-Netzwerkschnittstellen über IPv4-Adressen. Wenn ein Schnittstellen-VPC-Endpunkt IPv6 unterstützt, verfügen die Endpunkt-Netzwerkschnittstellen über IPv6-Adressen. Die IPv6-Adresse für eine Endpunkt-Netzwerkschnittstelle ist aus dem Internet nicht erreichbar. Wenn Sie eine Endpunktnetzwerkschnittstelle mit einer IPv6-Adresse beschreiben, beachten Sie, dass `denyAllIgwTraffic` aktiviert ist.

Anforderungen zum Aktivieren von IPv6 für einen Endpunkt-Service

- Die VPC und Subnetze für den Endpunkt-Service müssen IPv6-CIDR-Blöcke haben.
- Alle Network Load Balancer für den Endpunkt-Service müssen den Dualstack-IP-Adresstyp verwenden. Die Ziele müssen keinen IPv6-Datenverkehr unterstützen. Wenn der Service Quell-IP-Adressen aus dem Header der Version 2 des Proxyprotokolls verarbeitet, muss er IPv6-Adressen verarbeiten.

Anforderungen zum Aktivieren von IPv6 für einen Schnittstellenendpunkt

- Der Endpunkt-Service muss IPv6-Anfragen unterstützen.
- Der IP-Adresstyp eines Schnittstellenendpunkts muss mit den Subnetzen für den Schnittstellenendpunkt kompatibel sein, wie hier beschrieben:
  - IPv4 – Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv4-Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze über IPv4-Adressbereiche verfügen.
  - IPv6 – Weisen Sie Ihren Endpunktnetzwerkschnittstellen IPv6-Adressen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze reine IPv6-Subnetze sind.
  - Dualstack – Zuweisen von IPv4- und IPv6-Adressen zu Ihren Endpunktnetzwerkschnittstellen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze sowohl IPv4- als auch IPv6-Adressbereiche aufweisen.

IP-Adresstyp des DNS-Eintrags für einen Schnittstellenendpunkt

Der IP-Adresstyp des DNS-Eintrags, den ein Schnittstellenendpunkt unterstützt, bestimmt die von uns erstellten DNS-Einträge. Der IP-Adresstyp des DNS-Eintrags eines Schnittstellenendpunkts muss mit dem IP-Adresstypen für den Schnittstellenendpunkt kompatibel sein, wie hier beschrieben:

- IPv4 – Erstellen Sie A-Datensätze für die privaten, regionalen und zonalen DNS-Namen. Der IP-Adresstyp muss IPv4 oder Dualstack sein.
- IPv6 – Erstellen Sie AAAA-Datensätze für die privaten, regionalen und zonalen DNS-Namen. Der IP-Adresstyp muss IPv6 oder Dualstack sein.
- Dualstack – Erstellen Sie A- und AAAA-Datensätze für die privaten, regionalen und zonalen DNS-Namen. Der IP-Adresstyp muss Dualstack sein.

Erstellen Sie einen Dienst, der unterstützt wird von AWS PrivateLink

Sie können Ihren eigenen Dienst erstellen AWS PrivateLink, der als Endpunktdienst bezeichnet wird. Sie sind der Service-Anbieter, und die AWS -Prinzipale, die Verbindungen zu Ihrem Service einrichten, sind die Service-Verbraucher.

Endpunkt-Services erfordern entweder einen Network Load Balancer oder einen Gateway Load Balancer. Der Load Balancer erhält Anfragen von Service-Verbrauchern und leitet sie an Ihren

Service weiter. In diesem Fall erstellen Sie einen Endpunkt-Service mit einem Network Load Balancer. Weitere Informationen zum Erstellen eines Endpunktservice mit einem Gateway Load Balancer finden Sie unter Zugriff auf virtuelle Appliances.

Inhalt

Überlegungen

- Ein Endpunktservice ist in der Region verfügbar, in der Sie ihn erstellt haben. Sie können mithilfe von VPC-Peering von anderen Regionen aus auf den Endpunkt-Service zugreifen.
- Ein Endpunktservice unterstützt nur Datenverkehr über TCP.
- Wenn Service-Verbraucher Informationen zu einem Endpunkt-Service abrufen, können sie nur die Availability Zones sehen, die sie mit dem Service-Anbieter gemeinsam haben. Wenn sich der Service-Anbieter und der Service-Verbraucher in verschiedenen Konten befinden, kann ein Name der Availability Zone, z. B. `us-east-1a`, in jedem AWS-Konto einer anderen physischen Verfügbarkeitszone zugeordnet werden. Mithilfe von AZ-IDs können Sie die Availability Zones für Ihren Service einheitlich identifizieren. Weitere Informationen finden Sie unter AZ-IDs im Amazon EC2 EC2-Benutzerhandbuch.
- Wenn Service-Verbraucher Datenverkehr über einen Schnittstellenendpunkt an einen Service senden, sind die der Anwendung bereitgestellten Quell-IP-Adressen die privaten IP-Adressen der Load-Balancer-Knoten, nicht die IP-Adressen der Service-Verbraucher. Wenn Sie das Proxyprotokoll auf dem Load Balancer aktivieren, können Sie die Adressen der Service-Verbraucher und die IDs der Schnittstellenendpunkte aus dem Proxyprotokoll-Header abrufen. Weitere Informationen finden Sie unter Proxy-Protokoll im Benutzerhandbuch für Network Load Balancers.
- Wenn ein Endpunktservice mehreren Network Load Balancern zugeordnet ist, ist jede Endpunkt-Netzwerkschnittstelle einem Load Balancer zugeordnet. Wenn die erste Verbindung von einer Endpunkt-Netzwerkschnittstelle aus initiiert wird, wählen wir nach dem Zufallsprinzip einen der Network Load Balancer in derselben Availability Zone wie die Endpunkt-Netzwerkschnittstelle aus. Alle nachfolgenden Verbindungsanfragen von dieser Endpunkt-Netzwerkschnittstelle verwenden den ausgewählten Load Balancer. Wir empfehlen, für einen Endpunktservice dieselbe Listener-

und Zielgruppenkonfiguration für alle Load Balancer zu verwenden, damit Verbraucher den Endpunktservice unabhängig von der Wahl des Load Balancers erfolgreich nutzen können.

- Es gibt Kontingente für Ihre AWS PrivateLink Ressourcen. Weitere Informationen finden Sie unter AWS PrivateLink -Kontingente.

Voraussetzungen

- Erstellen Sie eine VPC für Ihren Endpunktservice mit mindestens einem Subnetz in jeder Availability Zone, in der der Service verfügbar sein soll.
- Damit Service-Verbraucher IPv6-Schnittstellen-VPC-Endpunkte für Ihren Endpunkt-Service erstellen können, müssen die VPC und die Subnetze über zugeordnete IPv6-CIDR-Blöcke verfügen.
- Erstellen eines Network Load Balancers in Ihrer VPC. Wählen Sie pro Availability Zone ein Subnetz aus, in dem der Service für Service-Verbraucher verfügbar sein soll. Für niedrige Latenz und Fehlertoleranz empfehlen wir, dass Sie Ihren Service in mindestens zwei Availability Zones der Region zur Verfügung stellen.
- Wenn Ihr Network Load Balancer über eine Sicherheitsgruppe verfügt, muss er eingehenden Datenverkehr von den IP-Adressen der Clients zulassen. Alternativ können Sie die Auswertung der Regeln für eingehende Sicherheitsgruppen für den durchgehenden Datenverkehr deaktivieren. AWS PrivateLink Weitere Informationen finden Sie unter Sicherheitsgruppen im Benutzerhandbuch für Network Load Balancers.
- Damit Ihr Endpunkt-Service IPv6-Anfragen akzeptieren kann, müssen seine Network Load Balancer den Dualstack-IP-Adresstypen verwenden. Die Ziele müssen keinen IPv6-Datenverkehr unterstützen. Weitere Informationen finden Sie unter IP-Adresstyp im Benutzerhandbuch für Network Load Balancer.

  Wenn Sie Quell-IP-Adressen aus dem Header des Proxyprotokolls Version 2 verarbeiten, stellen Sie sicher, dass Sie IPv6-Adressen verarbeiten können.
- Starten Sie Instances in jeder Availability Zone, in der der Service verfügbar sein soll, und registrieren Sie sie bei einer Load-Balancer-Zielgruppe. Wenn Sie Instances nicht in allen aktivierten Availability Zones starten, können Sie den zonenübergreifenden Lastenausgleich aktivieren, um Service-Verbraucher zu unterstützen, die zonale DNS-Hostnamen für den Zugriff auf den Service verwenden. Gebühren für regionale Datenübertragungen fallen an, wenn Sie den zonenübergreifenden Lastausgleich aktivieren. Weitere Informationen finden Sie unter Zonenübergreifendes Load Balancing im Benutzerhandbuch für Network Load Balancers.

Erstellen eines Endpunktservice

Verwenden Sie das folgende Verfahren, um einen Endpunkt-Service mit einem Network Load Balancer zu erstellen.

So erstellen Sie einen Endpunktservice unter Verwendung der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie Create Endpoint Service (Endpunkt-Service erstellen) aus.
4. Wählen Sie für Load balancer type (Load-Balancer-Typ) die Option Network (Netzwerk) aus.
5. Wählen Sie für Available load balancers (verfügbare Load Balancer) die Network Load Balancer aus, die dem Endpunktservice zugeordnet werden sollen. Unter Included Availability Zones sind die Availability Zones aufgeführt, die für die ausgewählten Network Load Balancer aktiviert sind. Ihr Endpunktdienst wird in diesen Availability Zones verfügbar sein.
6. Wählen Sie für Require acceptance for endpoint (Akzeptanz für Endpunkt erforderlich) Acceptance required (Akzeptanz erforderlich), um zu verlangen, dass Verbindungsanforderungen an Ihren Endpunkt-Service manuell akzeptiert werden. Andernfalls werden diese Anfragen automatisch akzeptiert.
7. Wählen Sie für Enable private DNS (Privates DNS aktivieren) Associate a private DNS name with the service (Zuordnen eines privaten DNS-Namens zum Service), um einen privaten DNS-Namen zuzuordnen, den Service-Verbraucher für den Zugriff auf Ihren Service verwenden können, und geben Sie dann den privaten DNS-Namen ein. Andernfalls können Dienstnutzer den endpunktspezifischen DNS-Namen verwenden, der von bereitgestellt wird. AWS Bevor Service-Verbraucher den privaten DNS-Namen verwenden können, muss der Service-Anbieter überprüfen, ob er Eigentümer der Domain ist. Weitere Informationen finden Sie unter DNS-Namen verwalten.
8. Führen Sie für Supported IP address types (Unterstützte IP-Adresstyp) einen der folgenden Schritte aus:

   - Wählen Sie IPv4 – Aktivieren Sie den Endpunkt-Service, um IPv4-Anfragen anzunehmen.
   - Wählen Sie IPv6 – Aktivieren Sie den Endpunkt-Service, um IPv6-Anfragen zu akzeptieren.
   - Wählen Sie IPv4 und IPv6 – Aktivieren Sie den Endpunkt-Service, um IPv4- und IPv6-Anfragen zu akzeptieren.
9. (Optional) Sie fügen ein Tag hinzu, indem Sie Add new tag (neuen Tag hinzufügen) auswählen und den Schlüssel und den Wert für den Tag eingeben.

10. Wählen Sie Erstellen.

So erstellen Sie einen Endpunktservice unter Verwendung der Befehlszeile

- create-vpc-endpoint-service-configuration (AWS CLI)
- New-EC2VpcEndpointServiceConfiguration(Tools für Windows) PowerShell

Bereitstellen des Endpunkt-Service für Service-Verbraucher

AWS Principals können sich privat mit Ihrem Endpunktdienst verbinden, indem sie einen VPC-Schnittstellen-Endpunkt erstellen. Service-Anbieter müssen Folgendes tun, um ihre Services den Service-Verbrauchern zur Verfügung zu stellen.

- Fügen Sie Berechtigungen hinzu, die es jedem Service-Verbraucher ermöglichen, eine Verbindung mit Ihrem Endpunkt-Service herzustellen. Weitere Informationen finden Sie unter the section called “Verwalten von Berechtigungen”.
- Geben Sie dem Service-Verbraucher den Namen Ihres Service und der unterstützten Availability Zonen, damit er einen Schnittstellenendpunkt erstellen kann, um eine Verbindung mit dem Service herzustellen. Weitere Informationen finden Sie im folgenden Verfahren.
- Akzeptieren Sie die Endpunktverbindungsanforderung vom Service-Verbraucher. Weitere Informationen finden Sie unter the section called “Annehmen oder Ablehnen von Verbindungsanforderungen”.

Herstellen einer Verbindung mit einem Endpunkt-Service als Service-Verbraucher

Ein Service-Verbraucher verwendet das folgende Verfahren, um einen Schnittstellenendpunkt zu erstellen, um eine Verbindung mit dem Endpunkt-Service herzustellen.

So erstellen Sie einen Schnittstellenendpunkt mit der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Wählen Sie für Service category (Servicekategorie) Other endpoint services (Andere Endpunkt-Services).

5. Geben Sie für Service name (Servicenamen) den Namen des Service ein (z. B. `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`) und wählen Sie Verify service (Service verifizieren).
6. Für VPC wählen Sie eine VPC, in der der Endpunkt erstellt werden soll.
7. Wählen Sie für Subnets (Subnetze) die Subnetze (Availability Zones) aus, von denen aus Sie auf den Endpunktservice zugreifen.
8. Wählen Sie für IP address type (IP-Adressentyp) eine der folgenden Optionen aus:

   - IPv4 – Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv4-Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4-Adressbereiche haben und der Endpunkt-Dienst IPv4-Anfragen akzeptiert.
   - IPv6 – Weisen Sie Ihren Endpunktnetzwerkschnittstellen IPv6-Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze reine IPv6-Subnetze sind und der Endpunkt-Dienst IPv6-Anfragen akzeptiert.
   - Dualstack – Zuweisen von IPv4- und IPv6-Adressen zu Ihren Endpunktnetzwerkschnittstellen. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze sowohl IPv4- als auch IPv6-Adressbereiche haben und der Endpunkt-Dienst sowohl IPv4- als auch IPv6-Anfragen akzeptiert.
9. Wählen Sie für DNS record IP type (IP-Typ des DNS-Eintrags) eine der folgenden Optionen aus:

   - IPv4 – Erstellen Sie A-Datensätze für die privaten, regionalen und zonalen DNS-Namen. Der IP-Adresstyp muss IPv4 oder Dualstack sein.
   - IPv6 – Erstellen Sie AAAA-Datensätze für die privaten, regionalen und zonalen DNS-Namen. Der IP-Adresstyp muss IPv6 oder Dualstack sein.
   - Dualstack – Erstellen Sie A- und AAAA-Datensätze für die privaten, regionalen und zonalen DNS-Namen. Der IP-Adresstyp muss Dualstack sein.
   - Service defined (Service definiert) – Erstellen Sie A-Datensätze für die privaten, regionalen und zonalen DNS-Namen und AAAA-Einträge für die regionalen und zonalen DNS-Namen. Der IP-Adresstyp muss Dualstack sein.
10. Für Sicherheitsgruppe wählen Sie die Sicherheitsgruppen aus, die den Endpunktnetzwerkschnittstellen zugeordnet werden sollen.
11. Wählen Sie Endpunkt erstellen.

So erstellen Sie einen Schnittstellenendpunkt mithilfe der Befehlszeile

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Tools für Windows) PowerShell

Konfigurieren eines Endpunkt-Service

Nachdem Sie einen Endpunktservice erstellt haben, können Sie dessen Konfiguration aktualisieren.

Aufgaben

- Verwalten von Berechtigungen
- Annehmen oder Ablehnen von Verbindungsanforderungen
- Load Balancer verwalten
- Zuordnen eines privaten DNS-Namens
- Ändern der unterstützten IP-Adresstypen
- Verwalten von Tags

Verwalten von Berechtigungen

Mithilfe der Kombination aus Berechtigungen und Akzeptanzeinstellungen können Sie steuern, welche Dienstnutzer (AWS Prinzipale) auf Ihren Endpunktdienst zugreifen können. Beispielsweise können Sie bestimmten Prinzipalen, denen Sie vertrauen, Berechtigungen erteilen und alle Verbindungsanforderungen automatisch akzeptieren, oder einer allgemeineren Prinzipalgruppe Berechtigungen erteilen und nur bestimmte vertrauenswürdige Verbindungsanfragen manuell akzeptieren.

Standardmäßig ist Ihr Endpunkt-Service für Service-Verbraucher nicht verfügbar. Sie müssen Berechtigungen hinzufügen, die es bestimmten AWS Prinzipalen ermöglichen, einen VPC-Schnittstellen-Endpunkt zu erstellen, um eine Verbindung zu Ihrem Endpunktdienst herzustellen. Um Berechtigungen für einen AWS Prinzipal hinzuzufügen, benötigen Sie dessen Amazon-Ressourcennamen (ARN). Die folgende Liste enthält Beispiel-ARNs für unterstützte AWS -Prinzipale.

ARNs für AWS Principals

AWS-Konto (beinhaltet alle Principals im Konto)

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

Rolle

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

Benutzer

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

Insgesamt alle Schulleiter AWS-Konten

*

Überlegungen

- Wenn Sie allen Benutzern die Berechtigung erteilen, auf den Endpunkt-Service zuzugreifen, und den Endpunkt-Service so konfigurieren, dass er alle Anforderungen akzeptiert, ist Ihr Load Balancer auch dann öffentlich, wenn er keine öffentliche IP-Adresse hat.
- Wenn Sie Berechtigungen entfernen, hat dies keine Auswirkungen auf bestehende Verbindungen zwischen dem Endpunkt und dem Dienst, die zuvor akzeptiert wurden.

So verwalten Sie Berechtigungen für den Endpunkt-Service mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie Ihren Endpunktservice aus und wählen Sie dann die Registerkarte Allow principals (Prinzipale zulassen).
4. Um Berechtigungen hinzuzufügen, wählen Sie Allow principals (Prinzipale zulassen). Geben Sie für Principals to add (Prinzipale zum Hinzufügen) den ARN des Prinzipals ein. Um einen weiteren Prinzipal hinzuzufügen, wählen Sie Add principal (Prinzipal hinzufügen. Wenn Sie mit dem Hinzufügen der Prinzipale fertig sind, wählen Allow principals (Prinzipale zulassen).
5. Um Berechtigungen zu entfernen, wählen Sie den Prinzipal aus und wählen Sie unter Actions (Aktionen) Delete (Löschen) aus. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.

So fügen Sie Berechtigungen für Ihren Endpunkt-Service mithilfe der Befehlszeile hinzu

- modify-vpc-endpoint-service-permissions (AWS CLI)
- Edit-EC2EndpointServicePermission(Tools für Windows PowerShell)

Annehmen oder Ablehnen von Verbindungsanforderungen

Mithilfe der Kombination aus Berechtigungen und Akzeptanzeinstellungen können Sie steuern, welche Dienstnutzer (AWS Prinzipale) auf Ihren Endpunktdienst zugreifen können. Beispielsweise können Sie bestimmten Prinzipalen, denen Sie vertrauen, Berechtigungen erteilen und alle Verbindungsanforderungen automatisch akzeptieren, oder einer allgemeineren Prinzipalgruppe Berechtigungen erteilen und nur bestimmte vertrauenswürdige Verbindungsanfragen manuell akzeptieren.

Sie können Ihren Endpunkt-Service so konfigurieren, dass Verbindungsanforderungen automatisch akzeptiert werden. Andernfalls müssen Sie sie manuell akzeptieren oder ablehnen. Wenn Sie eine Verbindungsanforderung nicht akzeptieren, kann der Service-Verbraucher nicht auf Ihren Endpunkt-Service zugreifen.

Sie können eine Benachrichtigung erhalten, wenn eine Verbindungsanfrage akzeptiert oder abgelehnt wird. Weitere Informationen finden Sie unter the section called “Empfangen von Warnmeldungen für Endpunkt-Serviceereignisse”.

Überlegungen

- Wenn Sie allen Benutzern die Berechtigung erteilen, auf den Endpunkt-Service zuzugreifen, und den Endpunkt-Service so konfigurieren, dass er alle Anforderungen akzeptiert, ist Ihr Load Balancer auch dann öffentlich, wenn er keine öffentliche IP-Adresse hat.
- Wenn Sie eine Anfrage ablehnen, die bereits akzeptiert wurde, hat dies keine Auswirkungen auf die Verbindung zwischen dem Endpunkt und dem Dienst.

So ändern Sie die Akzeptanzeinstellung mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den Endpunktservice aus.
4. Wählen Sie Actions, Modify endpoint acceptance setting.
5. Acceptance required (Akzeptanz erforderlich) auswählen oder löschen.
6. Wählen Sie Save Changes (Änderungen speichern)

So ändern Sie die Akzeptanzeinstellung mithilfe der Befehlszeile

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Tools für Windows PowerShell)

So akzeptieren Sie eine Verbindungsanfrage mit Hilfe der Konsole oder lehnen diese ab

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den Endpunktservice aus.
4. Wählen Sie die Endpunktverbindung auf der Registerkarte Endpoint connections (Endpunktverbindungen) aus.
5. Um die Verbindungsanforderung zu akzeptieren, wählen Sie Actions (Aktionen), Accept endpoint connection request (Endpunkt-Verbindungsanforderung akzeptieren). Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`accept`** ein und wählen Sie dann Accept (Akzeptieren).
6. Um die Verbindungsanforderung abzulehnen, wählen Sie Actions (Aktionen), Reject endpoint connection request (Endpunkt-Verbindungsanforderung ablehnen). Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`reject`** ein und wählen Sie dann Reject (Ablehnen).

So akzeptieren Sie eine Verbindungsanfrage mit Hilfe der Befehlszeile oder lehnen diese ab

- accept-vpc-endpoint-connections oder reject-vpc-endpoint-connections (AWS CLI)
- Approve-EC2EndpointConnectionoder Deny-EC2EndpointConnection(Tools für Windows PowerShell)

Load Balancer verwalten

Sie können die Load Balancer verwalten, die Ihrem Endpoint Service zugeordnet sind. Sie können einen Load Balancer nicht trennen, wenn Ihrem Endpunktservice Endpunkte zugeordnet sind.

Wenn Sie eine andere Availability Zone für einen Network Load Balancer aktivieren, können Sie auch die Availability Zone für Ihren Endpoint Service aktivieren. Nachdem Sie eine Availability Zone für den Endpoint Service aktiviert haben, können Service Consumer ein Subnetz aus dieser Availability Zone zu ihren Schnittstellen-VPC-Endpunkten hinzufügen.

Um die Load Balancer für Ihren Endpoint Service mithilfe der Konsole zu verwalten

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den Endpunktservice aus.
4. Wählen Sie Actions (Aktionen), Associate or disassociate load balancers (Load Balancer zuordnen oder trennen).
5. Ändern Sie die Konfiguration des Endpunktdienstes nach Bedarf. Beispielsweise:
   - Aktivieren Sie das Kontrollkästchen für einen Load Balancer, um ihn mit dem Endpunktdienst zu verknüpfen.
   - Deaktivieren Sie das Kontrollkästchen für einen Load Balancer, um ihn vom Endpunktdienst zu trennen. Sie müssen mindestens einen Load Balancer ausgewählt lassen.
   - Wenn Sie kürzlich eine andere Availability Zone für Ihren Load Balancer aktiviert haben, wird diese unter Inbegriffene Availability Zones angezeigt. Wenn Sie im nächsten Schritt Änderungen speichern, wird dadurch der Endpunktdienst für die neue Availability Zone aktiviert.
6. Wählen Sie Save Changes (Änderungen speichern)

Um die Load Balancer für Ihren Endpoint Service über die Befehlszeile zu verwalten

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Tools für Windows PowerShell)

Um den Endpunktdienst in einer Availability Zone zu aktivieren, die kürzlich für den Load Balancer aktiviert wurde, rufen Sie einfach den Befehl mit der ID des Endpunktdienstes auf.

Zuordnen eines privaten DNS-Namens

Sie können einen privaten DNS-Namen mit Ihrem Endpunkt-Service verknüpfen. Nachdem Sie einen privaten DNS-Namen zugeordnet haben, müssen Sie den Eintrag für die Domain auf Ihrem DNS-Server aktualisieren. Bevor Service-Verbraucher den privaten DNS-Namen verwenden können, muss der Service-Anbieter überprüfen, ob er Eigentümer der Domain ist. Weitere Informationen finden Sie unter DNS-Namen verwalten.

So ändern Sie den privaten DNS-Namen eines Endpunktservice mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den Endpunktservice aus.
4. Wählen Sie Actions (Aktionen), Modify Private DNS names (Private DNS-Namen ändern).
5. Wählen Sie Associate a private DNS name with the service (dem Service einen privaten DNS-Namen zuordnen) aus und geben Sie den privaten DNS-Namen ein.
   - Domain-Namen müssen Kleinbuchstaben benutzen.
   - Sie können Platzhalter in Domain-Namen verwenden (z. B. **`*.myexampleservice.com`**).
6. Wählen Sie Änderungen speichern aus.
7. Der private DNS-Name kann von Service-Verbrauchern verwendet werden, wenn der Überprüfungsstatus verified (verifiziert) lautet. Wenn sich der Überprüfungsstatus ändert, werden neue Verbindungsanforderungen abgelehnt, bestehende Verbindungen sind jedoch nicht betroffen.

So ändern Sie den privaten DNS-Namen eines Endpunktservice mithilfe der Befehlszeile

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Tools für Windows PowerShell)

So initiieren Sie den Domain-Überprüfungsprozess mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den Endpunktservice aus.
4. Wählen Sie Actions (Aktionen),Verify domain ownership for private DNS name (Domain-Besitz für privaten DNS-Namen verifizieren).
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`verify`** ein und wählen Sie dann Verify (Verifizieren).

So initiieren Sie den Domain-Überprüfungsprozess mithilfe der Befehlszeile

- start-vpc-endpoint-service-private-dns-verification (AWS CLI)

- Start-EC2VpcEndpointServicePrivateDnsVerification(Tools für Windows PowerShell)

Ändern der unterstützten IP-Adresstypen

Sie können die IP-Adresstypen ändern, die von Ihrem Endpunkt-Service unterstützt werden.

Überlegungen

Damit Ihr Endpunkt-Service IPv6-Anfragen akzeptieren kann, müssen seine Network Load Balancer den Dualstack-IP-Adresstypen verwenden. Die Ziele müssen keinen IPv6-Datenverkehr unterstützen. Weitere Informationen finden Sie unter IP-Adresstyp im Benutzerhandbuch für Network Load Balancer.

So ändern Sie die unterstützten IP-Adresstypen mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den VPC-Endpunktservice aus.
4. Wählen Sie Actions (Aktionen), Modify supported IP address types (Unterstützte IP-Adresstypen ändern).
5. Führen Sie für Supported IP address types (Unterstützte IP-Adresstyp) einen der folgenden Schritte aus:
   - Wählen Sie IPv4 – Aktivieren Sie den Endpunkt-Service, um IPv4-Anfragen anzunehmen.
   - Wählen Sie IPv6 – Aktivieren Sie den Endpunkt-Service, um IPv6-Anfragen zu akzeptieren.
   - Wählen Sie IPv4 und IPv6 – Aktivieren Sie den Endpunkt-Service, um IPv4- und IPv6-Anfragen zu akzeptieren.
6. Wählen Sie Änderungen speichern aus.

So ändern Sie die unterstützten IP-Adresstypen mithilfe der Befehlszeile

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Tools für Windows PowerShell)

Verwalten von Tags

Sie können Ihre Ressourcen markieren, um sie zu identifizieren oder in Übereinstimmung mit den Anforderungen Ihrer Organisation kategorisieren zu können.

So verwalten Sie Tags für den Endpunkt-Service mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den VPC-Endpunktservice aus.
4. Klicken Sie auf Actions (Aktionen), Manage tags (Markierungen verwalten).
5. Wählen Sie für jede Markierung Add new tag (Neue Markierung hinzufügen) und geben Sie den Schlüssel und Wert der Markierung ein.
6. Um eine Markierung zu entfernen, wählen Sie Remove (Entfernen) rechts neben dem Schlüssel und dem Wert der Markierung aus.
7. Wählen Sie Speichern.

So verwalten Sie Tags für Ihre Endpunktverbindungen mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den VPC-Endpunktservice und dann die Registerkarte Endpoint-Verbindungen.
4. Wählen Sie die Endpunktverbindung und dann Actions (Aktionen), Manage tags (Tags verwalten) aus.
5. Wählen Sie für jede Markierung Add new tag (Neue Markierung hinzufügen) und geben Sie den Schlüssel und Wert der Markierung ein.
6. Um eine Markierung zu entfernen, wählen Sie Remove (Entfernen) rechts neben dem Schlüssel und dem Wert der Markierung aus.
7. Wählen Sie Speichern.

So verwalten Sie Tags für Ihre Endpunkt-Serviceberechtigungen mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.

3. Wählen Sie den VPC-Endpunktservice und dann die Registerkarte Allow principals (Prinzipale zulassen) aus.
4. Wählen Sie den Prinzipal aus und wählen Sie dann Actions (Aktionen), Manage tags (Tags verwalten) aus.
5. Wählen Sie für jede Markierung Add new tag (Neue Markierung hinzufügen) und geben Sie den Schlüssel und Wert der Markierung ein.
6. Um eine Markierung zu entfernen, wählen Sie Remove (Entfernen) rechts neben dem Schlüssel und dem Wert der Markierung aus.
7. Wählen Sie Speichern.

So fügen Sie Tags über die Befehlszeile hinzu und entfernen sie

- create-tags und delete-tags (AWS CLI)
- New-EC2Tagund Remove-EC2Tag(Tools für Windows PowerShell)

DNS-Namen für VPC-Endpunktservices verwalten

Service-Anbieter können private DNS-Namen für ihre Endpunkt-Services konfigurieren. Wenn ein Service-Anbieter einen vorhandenen öffentlichen DNS-Namen als privaten DNS-Namen für seinen Endpunkt-Service verwendet, müssen Service-Verbraucher keine Anwendungen ändern, die den vorhandenen öffentlichen DNS-Namen verwenden. Bevor Sie einen privaten DNS-Namen für den Endpunkt-Service konfigurieren können, müssen Sie nachweisen, dass Sie Eigentümer der Domain sind, indem Sie eine Überprüfung des Domain-Besitzes durchführen.

Überlegungen

- Ein Endpunktservice kann nur einen privaten DNS-Namen haben.
- Sie dürfen keinen A-Datensatz für den privaten DNS-Namen erstellen, sodass nur Server in der Service-Verbraucher-VPC den privaten DNS-Namen auflösen können.
- Private DNS-Namen werden für Gateway-Load-Balancer-Endpunkte nicht unterstützt.
- Um eine Domain zu überprüfen, benötigen Sie einen öffentlichen Hostnamen oder einen öffentlichen DNS-Anbieter.
- Sie können die Domain einer Sub-Domain überprüfen. Beispielsweise können Sie example.com anstelle von a.example.com überprüfen. Jedes DNS-Label kann bis zu 63 Zeichen lang sein und der gesamte Domainname darf eine Gesamtlänge von 255 Zeichen nicht überschreiten.

Wenn Sie eine zusätzliche Sub-Domain hinzufügen, müssen Sie die Sub-Domain oder die Domain überprüfen. Angenommen, Sie hatten a.example.com und haben example.com überprüft. Sie fügen nun b.example.com als privaten DNS-Namen hinzu. Sie müssen example.com oder b.example.com überprüfen, bevor Service-Verbraucher den Namen verwenden können.

Domain-Verifizierungsname

Ihre Domain ist mit einer Reihe von DNS (Domain Name System)-Datensätzen verknüpft, die Sie über Ihren DNS-Anbieter verwalten. Ein TXT-Datensatz ist eine Art von DNS-Datensatz, der zusätzliche Informationen zu Ihrer Domain bereitstellt. Sie besteht aus einem Namen und einem Wert. Im Rahmen des Überprüfungsprozesses müssen Sie dem DNS-Server einen TXT-Eintrag für Ihre öffentliche Domain hinzufügen.

Domain-Eigentumsüberprüfung ist abgeschlossen, wenn wir erkennen, dass der TXT-Datensatz in den DNS-Einstellungen Ihrer Domain vorhanden ist.

Nachdem Sie einen Datensatz hinzugefügt haben, können Sie den Status des Domainverifizierungsprozesses über die Amazon-VPC-Konsole überprüfen. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus. Wählen Sie den Endpunkt-Service aus und überprüfen Sie den Wert von Domain verification status (Domain-Verifizierungsstatus) im Tab Details. Wenn die Domain-Überprüfung aussteht, warten Sie einige Minuten und aktualisieren Sie den Bildschirm. Bei Bedarf können Sie den Überprüfungsprozess manuell einleiten. Wählen Sie Actions (Aktionen),Verify domain ownership for private DNS name (Domain-Besitz für privaten DNS-Namen verifizieren).

Der private DNS-Name kann von Service-Verbrauchern verwendet werden, wenn der Überprüfungsstatus verified (verifiziert) lautet. Wenn sich der Überprüfungsstatus ändert, werden neue Verbindungsanforderungen abgelehnt, bestehende Verbindungen sind jedoch nicht betroffen.

Wenn der Überprüfungsstatus failed (fehlgeschlagen) lautet, siehe the section called “Probleme mit der Domain-Verifizierung beheben”.

Abrufen des Namens und des Werts

Wir geben Ihnen den Namen und Wert, den Sie im TXT-Datensatz verwenden. Beispielsweise sind die Informationen im AWS Management Console verfügbar. Wählen Sie den Endpunkt-Service aus und siehe Domain verification nameDomain-Verifizierungsname) und Domain verification value on the

Details tab for the endpoint service (Domain-Verifizierungswert) auf der Details-Registerkarte für den Endpunkt-Service. Sie können auch den folgenden AWS CLI Befehl describe-vpc-endpoint-service-configurations verwenden, um Informationen über die Konfiguration des privaten DNS-Namens für den angegebenen Endpunktdienst abzurufen.

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

Es folgt eine Beispielausgabe. Sie verwenden `Value` und `Name`, wenn Sie den TXT-Eintrag erstellen.

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

Angenommen, Ihr Domainname ist beispielsweise example.com und `Value` und `Name` sind wie in der obigen Beispielausgabe gezeigt. Die folgende Tabelle ist ein Beispiel für die TXT-Datensatzeinstellungen.

Name	Typ	Wert
_6e86v84tqgqubxbwi i1m.example.com	TXT	vpce: L6P0E 45JEVFWOCP RxlTt

Es wird empfohlen, `Name` als Datensatz-Unter-Domain zu verwenden, da der Basis-Domain-Name möglicherweise bereits verwendet wird. Wenn Ihr DNS-Anbieter jedoch nicht zulässt, dass DNS-Datensatznamen Unterstriche enthalten, können Sie den Wert „_6e86v84tqgqubxbwii1m“ weglassen und einfach „example.com“ im TXT-Eintrag verwenden.

Nachdem wir „_6e86v84tqgqubxbwii1m.example.com“ verifiziert haben, können Service-Verbraucher „example.com“ oder eine Subdomain (z. B. „service.example.com“ oder „my.service.example.com“) verwenden.

Fügen Sie einen TXT-Datensatz zum DNS-Server der Domain hinzu

Die Schritte zum Hinzufügen von TXT-Datensätzen zum DNS-Server Ihrer Domain hängen davon ab, wer den DNS-Service bereitstellt. Ihr DNS-Anbieter kann Amazon Route 53 oder eine andere Domain-Namen-Vergabestelle sein.

Amazon Route 53

Erstellen Sie einen Datensatz für Ihre öffentlich gehostete Zone. Verwenden Sie die folgenden Werte:

- Wählen Sie für den Record type (Datensatztyp) TXT.
- Geben Sie für TLL (Seconds) (TTL (Sekunden)) den Wert **`1800`** ein.
- Wählen Sie als Routing-Richtlinie Einfaches Routing aus.
- Geben Sie für Record name (Datensatzname) die Domain oder Subdomain ein.
- Geben Sie für Value/Route traffic to (Wert/Datenverkehr weiterleiten an) den Domain-Verifizierungswert ein.

Für weitere Informationen finden Sie unter Erstellen von Datensätzen mithilfe der Konsole im Amazon-Route-53-Entwicklerhandbuch.

Allgemeines Verfahren

Gehen Sie zur Website Ihres DNS-Anbieters und melden Sie sich bei Ihrem Konto an. Suchen Sie die Seite zum Aktualisieren der DNS-Einträge für Ihre Domain. Fügen Sie einen TXT-Eintrag mit dem angegebenen Namen und Wert hinzu. Es kann bis zu 48 Stunden dauern, bis DNS-Eintragsaktualisierungen wirksam werden, aber sie werden oft viel früher wirksam.

Genauere Anweisungen finden Sie in der Dokumentation Ihres DNS-Anbieters. Dieser Abschnitt enthält Links zur Dokumentation für mehrere gängige DNS-Anbieter. Diese Liste erhebt keinen Anspruch auf Vollständigkeit und ist auch nicht als Empfehlung der von diesen Unternehmen angebotenen Produkte oder Services gedacht.

DNS/Hosting-Anbieter	Link zur Dokumentation
GoDaddy	Einen TXT-Datensatz hinzufügen
Dreamhost	Hinzufügen von benutzerdefinierten DNS-Datensätzen
Cloudflare	DNS-Datensätze verwalten

DNS/Hosting-Anbieter	Link zur Dokumentation
HostGator	DNS-Einträge mit /eNom verwalten HostGator
Namecheap	Wie füge ich TXT/SPF/DKIM/DMARC-Datensätze für meine Domain hinzu?
Names.co.uk	Ändern der DNS-Einstellungen für Domain
Wix	Hinzufügen oder Aktualisieren von TXT-Datensätzen in Ihrem Wix-Konto

Prüfen Sie, ob der TXT-Datensatz veröffentlicht ist

Sie können mit den folgenden Schritten überprüfen, ob der TXT-Datensatz der Domain-Eigentumsüberprüfung Ihres privaten DNS-Namens ordnungsgemäß auf Ihrem DNS-Server veröffentlicht wird. Sie führen den nslookup Befehl aus, der für Windows und Linux verfügbar ist.

Sie fragen die DNS-Server ab, die Ihre Domain bedienen, da diese Server die meisten up-to-date Informationen für Ihre Domain enthalten. Es dauert einige Zeit, bis Ihre Domain-Informationen an andere DNS-Server weitergegeben werden.

So überprüfen Sie, ob Ihr TXT-Datensatz auf Ihrem DNS-Server veröffentlicht wird

1. Suchen Sie die Nameserver für Ihre Domain mit dem folgenden Befehl.

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

   In der Ausgabe werden alle Nameserver für Ihre Domain aufgelistet. Im nächsten Schritt werden Sie einen dieser Server abfragen.
2. Überprüfen Sie, ob der TXT-Eintrag ordnungsgemäß veröffentlicht wurde, indem Sie den folgenden Befehl verwenden, wobei *name_server* einer der Namenserver ist, die Sie im vorherigen Schritt gefunden haben.

   ```
   nslookup -type=TXT  _6e86v84tqgqubxbwii1m.example.com name_server
   ```
3. Überprüfen Sie in der Ausgabe des vorherigen Schritts, ob die Zeichenfolge, die auf `text =` folgt, mit dem TXT-Wert übereinstimmt.

In unserem Beispiel enthält die Ausgabe Folgendes, wenn der Datensatz korrekt veröffentlicht wurde.

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

Probleme mit der Domain-Verifizierung beheben

Wenn der Domain-Verifizierungsprozess fehlschlägt, können die folgenden Informationen Ihnen helfen, Probleme zu beheben.

- Überprüfen Sie, ob Ihr DNS-Anbieter Unterstriche in TXT-Eintragsnamen zulässt. Wenn Ihr DNS-Anbieter keine Unterstriche zulässt, können Sie den Domain-Überprüfungsnamen (z. B. „_6e86v84tqgqubxbwii1m“) im TXT-Eintrag weglassen.
- Überprüfen Sie, ob Ihr DNS-Anbieter den Domain-Namen an das Ende des TXT-Eintrags angehängt hat. Einige DNS-Anbieter hängen den Namen Ihrer Domain automatisch an den Attributnamen des TXT-Datensatzes an. Um diese Duplizierung des Domain-Namens zu vermeiden, fügen Sie beim Erstellen des TXT-Eintrags einen Punkt am Ende des Domain-Namens hinzu. Dies gibt Ihrem DNS-Anbieter zu verstehen, dass es nicht erforderlich ist, den Domain-Namen an den TXT-Datensatz anzuhängen.
- Überprüfen Sie, ob Ihr DNS-Anbieter den DNS-Datensatzwert geändert hat, um nur Kleinbuchstaben zu verwenden. Wir verifizieren Ihre Domain nur, wenn es einen Bestätigungsdatensatz mit einem Attributwert gibt, der genau mit dem von uns angegebenen Wert übereinstimmt. Wenn der DNS-Anbieter Ihre TXT-Eintragswerte so geändert hat, dass nur Kleinbuchstaben verwendet werden, wenden Sie sich an ihn, um Unterstützung zu erhalten.
- Möglicherweise müssen Sie Ihre Domain mehr als einmal überprüfen, da Sie mehrere Regionen oder mehrere AWS-Konten unterstützen. Wenn Ihr DNS-Anbieter nicht mehr als einen TXT-Datensatz mit demselben Attributnamen zulässt, überprüfen Sie, ob Ihr DNS-Anbieter Ihnen gestattet, demselben TXT-Datensatz mehrere Attributwerte mit demselben Attributnamen zuzuweisen. Wenn Ihr DNS von Amazon Route 53 verwaltet wird, können Sie das folgende Verfahren verwenden.
  1. Wählen Sie in der Route 53-Konsole den TXT-Datensatz aus, den Sie bei der Verifizierung Ihrer Domain in der ersten Region erstellt haben.
  2. Navigieren Sie im Feld Value (Wert) zum Ende des vorhandenen Attributwertes und drücken Sie dann die Eingabetaste.

3. Fügen Sie den Attributwert für die zusätzliche Region hinzu und speichern Sie dann den Datensatz.

Wenn Ihr DNS-Anbieter Ihnen nicht gestattet, demselben TXT-Datensatz mehrere Werte zuzuweisen, können Sie die Domain einmal mit dem Wert im Attributnamen des TXT-Datensatzes und ein weiteres Mal ohne den Wert im Attributnamen verifizieren. Sie können dieselbe Domain jedoch nur zweimal verifizieren.

Empfangen von Warnmeldungen für Endpunkt-Serviceereignisse

Sie können eine Benachrichtigung erstellen, um Warnungen für bestimmte Ereignisse im Zusammenhang mit Ihrem Endpunkt-Service zu erhalten. Beispielsweise können Sie eine E-Mail erhalten, wenn eine Verbindungsanfrage akzeptiert oder abgelehnt wird.

Aufgaben

- Eine SNS-Benachrichtigung erstellen
- Eine Zugriffsrichtlinie hinzufügen
- Eine Schlüsselrichtlinie hinzufügen

Eine SNS-Benachrichtigung erstellen

Gehen Sie folgendermaßen vor, um ein Amazon-SNS-Thema für die Benachrichtigungen zu erstellen und das Thema zu abonnieren.

So erstellen Sie mithilfe der Konsole eine Benachrichtigung für einen Endpunkt-Service

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den Endpunktservice aus.
4. Wählen Sie aus der Registerkarte Notifications (Benachrichtigungen) die Option Create notification (Benachrichtigung erstellen) aus.
5. Wählen Sie für Notification ARN (Benachrichtigungs-ARN) den ARN für das SNS-Thema aus, das Sie erstellt haben.
6. Um ein Ereignis zu abonnieren, wählen Sie es aus Events (Ereignisse).

- Connect (Verbinden) – Der Service-Verbraucher hat den Schnittstellenendpunkt erstellt. Dadurch wird eine Verbindungsanfrage an den Service-Anbieter gesendet.
- Accept (Akzeptieren) – Der Service-Anbieter hat die Verbindungsanfrage akzeptiert.
- Reject (Ablehnen) – Der Service-Anbieter hat die Verbindungsanfrage abgelehnt.
- Delete (Löschen) – Der Service-Verbraucher hat den Schnittstellenendpunkt gelöscht.

7. Wählen Sie Benachrichtigung erstellen aus.

So erstellen Sie mithilfe der Befehlszeile eine Benachrichtigung für einen Endpunkt-Service

- create-vpc-endpoint-connection-notification (AWS CLI)
- New-EC2VpcEndpointConnectionNotification(Tools für Windows PowerShell)

Eine Zugriffsrichtlinie hinzufügen

Fügen Sie dem SNS-Thema eine Zugriffsrichtlinie hinzu, die es ermöglicht, Benachrichtigungen in Ihrem Namen AWS PrivateLink zu veröffentlichen, z. B. die folgenden. Weitere Informationen finden Sie unter Wie bearbeite ich die Zugriffsrichtlinie meines Amazon-SNS-Themas? Verwenden Sie die globalen Konditionsschlüssel `aws:SourceArn` und `aws:SourceAccount` zum Schutz vor dem Problem des verwirrten Stellvertreters.

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

Eine Schlüsselrichtlinie hinzufügen

Wenn Sie verschlüsselte SNS-Themen verwenden, muss die Ressourcenrichtlinie für den KMS-Schlüssel darauf vertrauen AWS PrivateLink , AWS KMS API-Operationen aufzurufen. Es folgt eine Beispielschlüsselrichtlinie.

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

Löschen eines Endpunktservice

Wenn Sie einen Endpunkt-Service nicht mehr benötigen, können Sie ihn löschen. Sie können einen Endpunkt-Service nicht löschen, wenn Endpunkte vorhanden sind, die mit dem Endpunkt-Service verbunden sind, die sich im `available`- oder `pending-acceptance`-Status befinden.

Das Löschen eines Endpunkt-Services löscht nicht den zugehörigen Load Balancer und wirkt sich nicht auf die Anwendungsserver aus, die bei den Load-Balancer-Zielgruppen registriert sind.

So löschen Sie einen Endpunktservice unter Verwendung der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den Endpunktservice aus.
4. Wählen Sie Actions (Aktionen), Delete endpoint service (Endpunktservice löschen).
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.

So löschen Sie einen Endpunktservice unter Verwendung der Befehlszeile

- delete-vpc-endpoint-service-configurations (AWS CLI)
- Remove-EC2EndpointServiceConfiguration(Tools für Windows PowerShell)

Identitäts- und Zugriffsmanagement für AWS PrivateLink

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS PrivateLink IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Inhalt

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. AWS PrivateLink

Dienstbenutzer — Wenn Sie den AWS PrivateLink Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS PrivateLink Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS PrivateLink Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS PrivateLink. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS PrivateLink Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen.

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS PrivateLink verfassen können.

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon

ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche

Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden

Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe

oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer

IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS PrivateLink funktioniert mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf zu verwalten AWS PrivateLink, sollten Sie sich darüber informieren, mit welchen IAM-Funktionen Sie verwenden können. AWS PrivateLink

IAM-Funktionen, die Sie mit verwenden können AWS PrivateLink

IAM-Feature	AWS PrivateLink Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie AWS PrivateLink und wie die meisten IAM-Funktionen AWS-Services funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für AWS PrivateLink

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen

ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS PrivateLink

Beispiele für AWS PrivateLink identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS PrivateLink

Ressourcenbasierte Richtlinien finden Sie in AWS PrivateLink

Unterstützt ressourcenbasierte Richtlinien	Ja

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen

finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

AWS PrivateLink Der Dienst unterstützt eine Art von ressourcenbasierter Richtlinie, die als Endpunktrichtlinie bezeichnet wird. Eine Endpunktrichtlinie steuert, welche AWS -Prinzipale den Endpunkt für den Zugriff auf den Endpunktservice verwenden können. Weitere Informationen finden Sie unter the section called “Endpunktrichtlinien”.

Politische Aktionen für AWS PrivateLink

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

AWS PrivateLink teilt seinen API-Namespace mit Amazon EC2. Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS PrivateLink verwendet:

```
ec2
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

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

Eine Liste der AWS PrivateLink Aktionen finden Sie unter AWS PrivateLink Aktionen in der Amazon EC2 API-Referenz. Weitere Informationen finden Sie unter Von Amazon EC2 definierte Aktionen in der Service-Authorization-Referenz.

Politische Ressourcen für AWS PrivateLink

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Richtlinien-Bedingungsschlüssel für AWS PrivateLink

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Die folgenden Bedingungsschlüssel sind spezifisch für: AWS PrivateLink

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

Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon EC2 definierte Aktionen.

ACLs in AWS PrivateLink

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS PrivateLink

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit AWS PrivateLink

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären

Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipalberechtigungen für AWS PrivateLink

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS PrivateLink

Unterstützt Servicerollen	Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern

und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

Mit Diensten verknüpfte Rollen für AWS PrivateLink

Unterstützt serviceverknüpfte Rollen	Nein

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Beispiele für identitätsbasierte Richtlinien für AWS PrivateLink

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS PrivateLink -Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden AWS PrivateLink, einschließlich des Formats der ARNs für jeden der Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 in der Service Authorization Reference.

Beispiele

- Steuern der Nutzung von VPC-Endpunkten
- Steuern der Erstellung von VPC-Endpunkten auf Grundlage des Servicebesitzers
- Steuern der privaten DNS-Namen, die für VPC-Endpunktservices angegeben werden können
- Steuern der Servicenamen, die für VPC-Endpunktservices angegeben werden können

Steuern der Nutzung von VPC-Endpunkten

Standardmäßig haben -Benutzer keine Berechtigungen zum Arbeiten mit Endpunkten. Sie können eine identitätsbasierte Richtlinie erstellen, die Benutzern die Berechtigung zum Erstellen, Ändern, Beschreiben und Löschen von Endpunkten erteilt. Im Folgenden wird ein Beispiel gezeigt.

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

Informationen zur Steuerung des Zugriffs aus Services mit VPC-Endpunkten vgl. the section called “Endpunktrichtlinien”.

Steuern der Erstellung von VPC-Endpunkten auf Grundlage des Servicebesitzers

Mit dem `ec2:VpceServiceOwner`-Bedingungsschlüssel können Sie steuern, welcher VPC-Endpunkt basierend auf dem Eigentümer des Services (`amazon`, `aws-marketplace` oder die Konto-ID) erstellt werden kann. Im folgenden Beispiel wird die Berechtigung zum Erstellen von VPC-Endpunkten mit dem angegebenen Servicebesitzer erteilt. Um dieses Beispiel zu verwenden, ersetzen Sie die Region, die Konto-ID und den Servicebesitzer.

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

Steuern der privaten DNS-Namen, die für VPC-Endpunktservices angegeben werden können

Mit dem `ec2:VpceServicePrivateDnsName`-Bedingungsschlüssel können Sie steuern, welcher VPC-Endpunktservice basierend auf dem privaten DNS-Namen geändert oder erstellt werden kann, der dem VPC-Endpunktservice zugeordnet ist. Im folgenden Beispiel wird die Berechtigung zum Erstellen eines VPC-Endpunktservices mit dem angegebenen privaten DNS-Namen erteilt. Um dieses Beispiel zu verwenden, ersetzen Sie die Region, die Konto-ID und den privaten DNS-Namen.

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

Steuern der Servicenamen, die für VPC-Endpunktservices angegeben werden können

Mit dem Bedingungsschlüssel `ec2:VpceServiceName` können Sie steuern, welcher VPC-Endpunkt basierend auf dem Namen des VPC-Endpunktservice erstellt werden kann. Im folgenden Beispiel wird die Berechtigung zum Erstellen eines VPC-Endpunkts mit dem angegebenen Servicenamen erteilt. Um dieses Beispiel zu verwenden, ersetzen Sie die Region, die Konto-ID und den Servicenamen.

```
{
    "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"
                    ]
                }
```

```
            }
        }
    ]
}
```

Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien

Eine Endpunktrichtlinie ist eine ressourcenbasierte Richtlinie, die Sie an einen VPC-Endpunkt anhängen, um zu steuern, welche AWS Prinzipale den Endpunkt für den Zugriff auf einen verwenden können. AWS-Service

Eine Endpunktrichtlinie setzt keine identitätsbasierten Richtlinien oder ressourcenbasierten Richtlinien außer Kraft oder ersetzt sie. Beispiel: Wenn Sie einen Schnittstellenendpunkt verwenden, um eine Verbindung zu Amazon S3 herzustellen, können Sie auch Amazon-S3-Bucket-Richtlinien verwenden, um den Zugriff auf Buckets von bestimmten Endpunkten oder VPCs zu steuern.

Inhalt

Überlegungen

- Eine Endpunktrichtlinie ist ein JSON-Richtliniendokument, das die IAM-Richtliniensprache verwendet. Sie muss ein Prinzipal-Element enthalten. Die Größe einer Endpunktrichtlinie darf 20.480 Zeichen (einschließlich Leerzeichen) nicht überschreiten.
- Wenn Sie eine Schnittstelle oder einen Gateway-Endpunkt für einen erstellen AWS-Service, können Sie dem Endpunkt eine einzelne Endpunktrichtlinie zuordnen. Sie können die Endpunktrichtlinie jederzeit aktualisieren. Wenn Sie keine Endpunktrichtlinie anfügen, fügen wir die Standard-Endpunktrichtlinie hinzu.
- Nicht alle AWS-Services unterstützen Endpunktrichtlinien. Wenn an AWS-Service keine Endpunktrichtlinien unterstützt, gewähren wir vollen Zugriff auf jeden Endpunkt für den Service.

Weitere Informationen finden Sie unter the section called “Anzeigen der Unterstützung für Endpunkt-Richtlinien”.

- Wenn Sie einen VPC-Endpunkt für einen anderen Endpunktservice als einen AWS-Service erstellen, lassen wir vollen Zugriff auf den Endpunkt zu.

Standard-Endpunktrichtlinie

Die Standard-Endpunktrichtlinie lässt vollen Zugriff auf den Endpunkt zu.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Richtlinien für Schnittstellenendpunkte

Beispiele für Endpunktrichtlinien für AWS-Services finden Sie unterthe section called “Services, die integrieren”. Die erste Spalte der Tabelle enthält Links zur jeweiligen AWS PrivateLink Dokumentation AWS-Service. Wenn ein AWS-Service Endpunktrichtlinien unterstützt, enthält seine Dokumentation Beispiele für Endpunktrichtlinien.

Prinzipale für Gateway-Endpunkte

Bei Gateway-Endpunkten muss das `Principal` Element auf eingestellt sein`*`. Verwenden Sie den `aws:PrincipalArn` Bedingungsschlüssel, um einen Prinzipal anzugeben.

```
"Condition": {
    "StringEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
    }
}
```

Wenn Sie den Prinzipal im folgenden Format angeben, wird der Zugriff Root-Benutzer des AWS-Kontos nur, nicht allen Benutzern und Rollen für das Konto gewährt.

```
"AWS": "account_id"
```

Beispiele für Endpunktrichtlinien für Gateway-Endpunkte finden Sie in den folgenden Themen:

- Endpunkte für Amazon S3
- Endpunkte für DynamoDB

Aktualisieren einer VPC-Endpunktrichtlinie

Gehen Sie wie folgt vor, um eine Endpunktrichtlinie für einen AWS-Service zu aktualisieren. Nachdem Sie eine Endpunktrichtlinie aktualisiert haben, kann es einige Minuten dauern, bis die Änderungen wirksam werden.

Ändern einer Endpunktrichtlinie mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den VPC-Endpunkt.
4. Wählen Sie Actions (Aktionen), Manage policy (Verwalten von Richtlinien).
5. Wählen Sie Full Access (Voller Zugriff), um vollen Zugriff auf den Service zu gewähren, oder wählen Sie Custom (Benutzerdefiniert), und fügen Sie eine benutzerdefinierte Richtlinie hinzu.
6. Wählen Sie Speichern.

Ändern einer Endpunktrichtlinie mithilfe der Befehlszeile

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Tools für Windows PowerShell)

CloudWatch-Metriken für AWS PrivateLink

AWS PrivateLink veröffentlicht Datenpunkte für Ihre Interface-Endpunkte, Gateway-Load-Balancer-Endpunkte und Endpunktservices auf Amazon CloudWatch. CloudWatch ermöglicht Ihnen, Statistiken zu diesen Datenpunkten als geordneten Satz von Zeitreihendaten, als Metriken bezeichnet, abzurufen. Sie können sich eine Metrik als eine zu überwachende Variable und die Datenpunkte als die Werte dieser Variable im Laufe der Zeit vorstellen. Jeder Datenpunkt verfügt über einen zugewiesenen Zeitstempel und eine optionale Maßeinheit.

Mit den Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Sie können z. B. einen CloudWatch-Alarm erstellen, um eine bestimmte Metrik zu überwachen, und eine Aktion einleiten (z. B. Senden einer Benachrichtigung an eine E-Mail-Adresse), wenn die Metrik außerhalb eines für Sie akzeptablen Bereichs liegt.

Metriken werden für alle Interface-Endpunkte, Gateway-Load-Balancer-Endpunkte und Endpunktservices veröffentlicht. Sie werden nicht für Gateway-Endpunkte veröffentlicht. Standardmäßig sendet AWS PrivateLink Metriken ohne zusätzliche Kosten in Intervallen von einer Minute an CloudWatch.

Weitere Informationen finden Sie im Amazon-CloudWatch-Benutzerhandbuch.

Inhalt

Endpunkt-Metriken und -Dimensionen

Der `AWS/PrivateLinkEndpoints`-Namespace enthält die folgenden Metriken für Interface-Endpunkte und Gateway-Load-Balancer-Endpunkte.

Metrik	Beschreibung
`ActiveConnections`	Die Anzahl der aktiven gleichzeitigen Verbindungen. Diese Metrik enthält Verbindungen im Zustand SYN_SENT und ESTABLISHED.

Metrik	Beschreibung
	Berichtkriterien: Der Endpunkt erhielt Datenverkehr während des Zeitraums von einer Minute. Statistiken: Die nützlichsten Statistiken sind `Average`, `Maximum` und `Minimum`. Dimensionen • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`BytesProcessed`	Die Anzahl der Bytes, die zwischen Endpunkten und Endpunkts ervices ausgetauscht wurden, und zwar aggregiert in beide Richtungen. Dies ist die Anzahl der Bytes, die dem Besitzer des Endpunkts in Rechnung gestellt werden. Dieser Wert wird in der Rechnung in GB angezeigt. Berichtkriterien: Der Endpunkt erhielt Datenverkehr während des Zeitraums von einer Minute. Statistiken: Die nützlichsten Statistiken sind `Average`, `Sum`, `Maximum` und `Minimum`. Dimensionen • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Metrik	Beschreibung
`NewConnections`	Die Anzahl der durch den Endpunkt eingerichteten Verbindungen. Berichtkriterien: Der Endpunkt erhielt Datenverkehr während des Zeitraums von einer Minute. Statistiken: Die nützlichsten Statistiken sind `Average`, `Sum`, `Maximum` und `Minimum`. Dimensionen • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`PacketsDropped`	Die Anzahl der vom Endpunkt abgeladenen Pakete. Diese Metrik erfasst möglicherweise nicht alle Paketabladungen. Steigende Werte könnten darauf hinweisen, dass der Endpunkt oder Endpunktservice in einem ungesunden Zustand ist. Berichtkriterien: Der Endpunkt erhielt Datenverkehr während des Zeitraums von einer Minute. Statistiken: Die nützlichsten Statistiken sind `Average`, `Sum` und `Maximum`. Dimensionen • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Metrik	Beschreibung
`RstPacketsReceived`	Die Anzahl der vom Endpunkt empfangenen RST-Pakete. Steigende Werte könnten darauf hinweisen, dass der Endpunktservice in einem ungesunden Zustand ist. Berichtkriterien: Der Endpunkt erhielt Datenverkehr während des Zeitraums von einer Minute. Statistiken: Die nützlichsten Statistiken sind `Average`, `Sum` und `Maximum`. Dimensionen • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Verwenden Sie die nachstehenden Dimensionen, um die Metriken zu filtern.

Dimension	Beschreibung
`Endpoint Type`	Filtert die Metrikdaten nach Endpunkttyp (`Interface` | `GatewayLoadBalancer`).
`Service Name`	Filtert die Metrikdaten nach Servicenamen.
`Subnet Id`	Filtert die Metrikdaten nach Subnetz.
`VPC Endpoint Id`	Filtert die Metrikdaten nach VPC-Endpunkt.
`VPC Id`	Filtert die Metrikdaten nach VPC.

Endpunktservicemetriken und -dimensionen

Der `AWS/PrivateLinkServices`-Namespace enthält die folgenden Metriken für Endpunktservices.

Metrik	Beschreibung
`ActiveConnections`	Die maximale Anzahl von aktiven Verbindungen von Clients zu Zielen über die Endpunkte. Steigende Werte könnten darauf hinweisen, dass der Load Balancer Ziele hinzugefügt werden müssen. Berichtkriterien: Ein mit dem Endpunktservice verbundener Endpunkt hat während eines Zeitraums von einer Minute Datenverkehr gesendet. Statistiken: Die nützlichsten Statistiken sind `Average` und `Maximum`. Dimensionen • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`BytesProcessed`	Die Anzahl der Bytes, die zwischen Endpunktservices und Endpunkten ausgetauscht wurden, und zwar in beide Richtungen. Berichtkriterien: Ein mit dem Endpunktservice verbundener Endpunkt hat während eines Zeitraums von einer Minute Datenverkehr gesendet. Statistiken: Die nützlichsten Statistiken sind `Average`, `Sum` und `Maximum`. Dimensionen • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`EndpointsCount`	Die Anzahl der Endpunkte, die mit dem Endpunktservice verbunden sind.

Metrik	Beschreibung
	Berichtkriterien: Im Fünf-Minuten-Zeitraum gibt es einen Wert ungleich Null. Statistiken: Die nützlichsten Statistiken sind `Average` und `Maximum`. Dimensionen • `Service Id`
`NewConnections`	Die Anzahl von neuen Verbindungen von Clients zu Zielen über die Endpunkte. Steigende Werte könnten darauf hinweisen, dass der Load Balancer Ziele hinzugefügt werden müssen. Berichtkriterien: Ein mit dem Endpunktservice verbundener Endpunkt hat während eines Zeitraums von einer Minute Datenverkehr gesendet. Statistiken: Die nützlichsten Statistiken sind `Average`, `Sum` und `Maximum`. Dimensionen • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Metrik	Beschreibung
`RstPacketsSent`	Die Anzahl der RST-Pakete, die vom Endpunktservice an Endpunkte gesendet wurden. Steigende Werte könnten darauf hindeuten, dass es Ziele im ungesunden Zustand gibt. Berichtkriterien: Ein mit dem Endpunktservice verbundener Endpunkt hat während eines Zeitraums von einer Minute Datenverkehr gesendet. Statistiken: Die nützlichsten Statistiken sind `Average`, `Sum` und `Maximum`. Dimensionen • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Verwenden Sie die nachstehenden Dimensionen, um die Metriken zu filtern.

Dimension	Beschreibung
`Az`	Filtert die Metrikdaten nach Availability Zone.
`Load Balancer Arn`	Filtert die Metrikdaten nach Load Balancer.
`Service Id`	Filtert die Metrikdaten nach Endpunktservice.
`VPC Endpoint Id`	Filtert die Metrikdaten nach VPC-Endpunkt.

CloudWatch-Metriken anzeigen

Sie können diese Metriken mit der CloudWatch-Konsole, der Amazon-VPC-Konsole oder der AWS CLI anzeigen.

So zeigen Sie Metriken mithilfe der Amazon-VPC-Konsole an

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus. Wählen Sie Ihren Endpunkt und dann die Registerkarte Monitoring (Überwachung) aus.
3. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus. Wählen Sie Ihren Endpunktservice und dann die Registerkarte Monitoring (Überwachung) aus.

So zeigen Sie Metriken mit der CloudWatch-Konsole an:

1. Öffnen Sie die CloudWatch-Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den AWS/PrivateLinkendPoints-Namespace aus.
4. Wählen Sie den AWS/PrivateLinkServices-Namespace aus.

So zeigen Sie Metriken mit der a AWS CLI

Verwenden Sie den folgenden lsit-metrics-Befehl zum Auflisten der verfügbaren Metriken für Interface-Endpunkte und Gateway-Load-Balancer-Endpunkte:

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkEndpoints
```

Verwenden Sie den folgenden list-metrics-Befehl zum Auflisten der verfügbaren Metriken für Endpunktservices:

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkServices
```

Verwenden von integrierten Regeln für Contributor Insights

AWS PrivateLink stellt integrierte Contributor-Insights-Regeln für Ihre Endpunktservices bereit, um herauszufinden, welche Endpunkte die größten Beiträge zu jeder unterstützten Metrik sind. Weitere Informationen finden Sie unter Contributor Insights im Amazon-CloudWatch-Benutzerhandbuch.

AWS PrivateLink bietet folgende Regeln:

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1` – Ordnet die Endpunkte nach der Anzahl der aktiven Verbindungen.

- `VpcEndpointService-BytesByEndpointId-v1` – Ordnet die Endpunkte nach der Anzahl der verarbeiteten Bytes.
- `VpcEndpointService-NewConnectionsByEndpointId-v1` – Ordnet die Endpunkte nach der Anzahl der neuen Verbindungen.
- `VpcEndpointService-RstPacketsByEndpointId-v1` – Ordnet die Endpunkte nach der Anzahl der an die Endpunkte gesendeten RST-Pakete.

Bevor Sie eine integrierte Regel verwenden können, müssen Sie sie aktivieren. Nachdem Sie eine Regel aktiviert haben, beginnt sie mit dem Sammeln von Teilnehmerdaten. Weitere Informationen zu den Gebühren für Contributor Insights finden Sie unter Amazon CloudWatch – Preise.

Sie müssen über die folgenden Berechtigungen verfügen, um Contributor Insights zu verwenden:

- `cloudwatch:DeleteInsightRules` – um Contributor-Insights-Regeln zu löschen.
- `cloudwatch:DisableInsightRules` – um Contributor-Insights-Regeln zu deaktivieren.
- `cloudwatch:GetInsightRuleReport` – um die Daten abzurufen.
- `cloudwatch:ListManagedInsightRules` – um die verfügbaren Contributor-Insights-Regeln aufzulisten.
- `cloudwatch:PutManagedInsightRules` – um Contributor-Insights-Regeln zu aktivieren.

Aufgaben

- Contributor-Insights-Regeln aktivieren
- Contributor-Insights-Regeln deaktivieren
- Contributor-Insights-Regeln löschen

Contributor-Insights-Regeln aktivieren

Verwenden Sie die folgenden Verfahren, um die integrierten Regeln fürAWS PrivateLink entweder mit der AWS Management Console oder der AWS CLI zu aktivieren.

So aktivieren Sie die Contributor-Insights-Regeln für AWS PrivateLink unter Verwendung der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie Ihren Endpunktservice aus.

4. Auf der Registerkarte Contributor Insights, wählen Sie Aktivieren aus.
5. (Optional) Standardmäßig sind alle Regeln aktiviert. Um nur bestimmte Regeln zu aktivieren, wählen Sie die Regeln aus, die nicht aktiviert werden sollen, und wählen Sie dann Aktionen, Regel deaktivieren aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie deaktivieren aus.

So aktivieren Sie die Contributor-Insights-Regeln für AWS PrivateLink unter Verwendung der AWS CLI

1. Verwenden Sie den Befehl list-managed-insight-rules wie folgt, um die verfügbaren Regeln aufzuzählen. Geben Sie für die `--resource-arn`-Option den ARN Ihres Endpunktdienstes an.

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

2. Kopieren Sie in der Ausgabe des `list-managed-insight-rules`-Befehls den Namen der Vorlage aus dem Feld `TemplateName`. Es folgt ein Beispiel dieses Feldes.

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

3. Verwenden Sie den Befehl put-managed-insight-rules wie folgt, um die Regel zu aktivieren. Sie müssen den Vorlagennamen und den ARN Ihres Endpunktdienstes angeben.

```
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
```

Contributor-Insights-Regeln deaktivieren

Sie können die integrierten Regeln für AWS PrivateLink jeder Zeit deaktivieren. Nachdem Sie eine Regel deaktiviert haben, werden keine Leistungsträgerdaten mehr erfasst, aber vorhandene Leistungsträgerdaten bleiben erhalten, bis sie 15 Tage alt sind. Nachdem Sie eine Regel deaktiviert haben, können Sie sie erneut aktivieren, um die Erfassung von Leistungsträgerdaten fortzusetzen.

So deaktivieren Sie die Contributor-Insights-Regeln für AWS PrivateLink unter Verwendung der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie Ihren Endpunktservice aus.
4. Wählen Sie auf der Registerkarte Contributor Insights Alle Deaktivieren aus, um alle Regeln zu deaktivieren. Als alternative Vorgehensweise können Sie das Panel Regelnerweitern, dann die Regeln auswählen, die Sie deaktivieren möchten, und anschließend in Aktionen Regel deaktivieren auswählen
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie deaktivieren aus.

So deaktivieren Sie die Contributor-Insights-Regeln für AWS PrivateLink unter Verwendung der AWS CLI

Verwenden Sie den Befehl disable-insight-rules, um eine Regel zu deaktivieren.

Contributor-Insights-Regeln löschen

Verwenden Sie die folgenden Verfahren, um die integrierten Regeln für AWS PrivateLink entweder mit der AWS Management Console oder der AWS CLI zu löschen. Nachdem Sie eine Regel gelöscht haben, werden keine Leistungsträgerdaten mehr erfasst, und wir löschen die vorhandenen Leistungsträgerdaten.

Löschen von Contributor-Insights-Regeln für AWS PrivateLink unter Verwendung der Konsole

1. Öffnen Sie die CloudWatch-Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Instances und anschließend Contributor Insights aus.
3. Erweitern Sie das Panel Rules (Regeln) und wählen Sie die Regeln aus.
4. Klicken Sie bei Actions (Aktionen) auf Delete rule (Regel löschen).
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Löschen von Contributor-Insights-Regeln für AWS PrivateLink unter Verwendung der AWS CLI

Verwenden Sie den Befehl delete-insight-rules zum Löschen einer Regel.

AWS PrivateLink -Kontingente

Die folgenden Tabellen führen die Kontingente, ehemals als Limits bezeichnet, für die AWS PrivateLink -Ressourcen pro Region für Ihr Konto auf. Sofern nicht anders angegeben, können Sie eine Erhöhung dieser Kontingente beantragen. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Wenn Sie eine Erhöhung des pro Ressource geltenden Kontingents beantragen, erhöhen wir das Kontingent für alle Ressourcen in der Region.

Name	Standard	Anpassbar	Kommentare
Schnittstellen- und Gateway Load Balancer-Endpunkte pro VPC	50	Ja	Dies ist ein kombiniertes Kontingent für Schnittstellenendpunkte und Gateway-Load-Balancer-Endpunkte
Gateway VPC-Endpunkte pro Region	20	Ja	Sie können bis zu 255 Gateway-Endpunkte pro VPC erstellen
Richtlinie für Zeichen pro VPC-Endpunkt	20 480	Nein	Die maximale Größe einer VPC-Endpunktrichtlinie, mit Leerzeichen

Die folgenden Überlegungen gelten für Datenverkehr, der einen VPC-Endpunkt durchläuft:

- Jeder VPC-Endpunkt kann standardmäßig eine Bandbreite von bis zu 10 GB/s pro Availability Zone unterstützen und skaliert automatisch auf bis zu 100 GB/s. Die maximale Bandbreite für einen VPC-Endpunkt bei der Verteilung der Last auf alle Availability Zones ist die Anzahl der Availability Zones multipliziert mit 100 GB/s. Wenn Ihre Anwendung einen höheren Durchsatz benötigt, wenden Sie sich an den AWS -Support.
- Die Maximum Transmission Unit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das einen VPC-Endpunkt durchläuft. Je größer die MTU, desto mehr Daten können in einem einzelnen Paket übergeben werden. Ein VPC-Endpunkt unterstützt eine MTU von 8.500 Byte. Pakete mit einer Größe von mehr als 8.500 Byte, die am VPC-Endpunkt ankommen, werden verworfen.

- Path MTU Discovery (PMTUD) wird nicht unterstützt. VPC-Endpunkte generieren nicht die folgende ICMP-Meldung: `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (Typ 3, Code 4).
- VPC-Endpunkte erzwingen das Klemmen der Maximum Segment Size (MSS) für alle Pakete. Weitere Informationen finden Sie unter RFC879

Dokumentenverlauf für AWS PrivateLink

In der folgenden Tabelle werden die Versionen für beschrieben AWS PrivateLink.

Änderung	Beschreibung	Datum
Vorgegebene IP-Adressen	Sie können die IP-Adressen für Ihre Endpunkt-Netzwerks chnittstellen angeben, wenn Sie Ihren VPC-Endpunkt erstellen oder ändern.	17. August 2023
IPv6-Support	Sie können Ihre Endpunkts ervices für Gateway-Load-Balancer und Endpunkte für Gateway-Load-Balancer so konfigurieren, dass sie sowohl IPv4- als auch IPv6-Adre ssen oder nur IPv6-Adressen unterstützen.	12. Dezember 2022
Contributor Insights	Sie können die integrier ten Contributor Insights-Regeln verwenden, um bestimmte Endpunkte zu identifizieren, die am meisten zu den CloudWatch Metriken beigetragen haben. AWS PrivateLink	18. August 2022
IPv6-Support	Service-Anbieter können es ihrem Endpunkt-Service ermöglichen, IPv6-Anfragen zu akzeptieren, auch wenn ihre Back-End-Dienste nur IPv4 unterstützen. Wenn ein Endpunkt-Service IPv6-	11. Mai 2022

	Anfragen akzeptiert, können Service-Verbraucher die IPv6-Unterstützung für ihre Schnittstellenendpunkte aktivieren, sodass sie über IPv6 auf den Endpunkt-Service zugreifen können.	
CloudWatch Metriken	AWS PrivateLink veröffentlicht CloudWatch Metriken für Ihre Schnittstellenendpunkte, Gateway Load Balancer-Endpunkte und Endpunktdienste.	27. Januar 2022
Gateway Load Balancer-Endpunkte	Sie können einen Gateway Load Balancer-Endpunkt in Ihrer VPC erstellen, um den Datenverkehr an einen VPC-Endpunktdienst zu leiten, den Sie mit einem Gateway Load Balancer konfiguriert haben.	10. November 2020
VPC-Endpunktrichtlinien	Sie können eine IAM-Richtlinie an einen Schnittstellen-VPC-Endpunkt für einen AWS -Service zur Steuerung des Zugriffs auf den Service anfügen.	23. März 2020
Bedingungsschlüssel für VPC-Endpunkte und Endpunktservices	Sie können EC2-Bedingungsschlüssel verwenden, um den Zugriff auf VPC-Endpunkte und -Endpunktservices zu steuern.	6. März 2020

Markierung von VPC-Endpunkt- und VPC-Endpunktservices bei der Erstellung	Sie können eine Markierung hinzufügen, wenn Sie VPC-Endpunkte und -Endpunktservices erstellen.	5. Februar 2020
Private DNS-Namen	Sie können von Ihrer VPC aus mithilfe von privaten DNS-Namen auf AWS PrivateLink basierte Dienste zugreifen.	6. Januar 2020
VPC-Endpunkt-Services	Sie können Ihre eigenen Endpunktservices erstellen und anderen AWS-Konten und Benutzern ermöglichen, über einen Schnittstellen-VPC-Endpunkt eine Verbindung zu Ihrem Service herzustellen. Sie können Ihre Endpunktservices für ein Abonnement im AWS Marketplace anbieten.	28. November 2017
Schnittstelle VPC-Endpunkte für AWS-Services	Sie können einen Schnittstellenendpunkt erstellen, um eine Verbindung zu AWS-Services diesem Integrationspunkt herzustellen, AWS PrivateLink ohne ein Internet-Gateway oder ein NAT-Gerät zu verwenden.	8. November 2017
VPC-Endpunkte für DynamoDB	Sie können einen Gateway-VPC-Endpunkt erstellen, um von Ihrer VPC aus auf Amazon DynamoDB zuzugreifen, ohne ein Internet-Gateway oder ein NAT-Gerät zu verwenden.	16. August 2017

VPC-Endpunkte für Amazon S3	Sie können einen Gateway-VPC-Endpunkt erstellen, um von Ihrer VPC aus auf Amazon S3 zuzugreifen, ohne ein Internet-Gateway oder ein NAT-Gerät zu verwenden.	11. Mai 2015

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.