AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

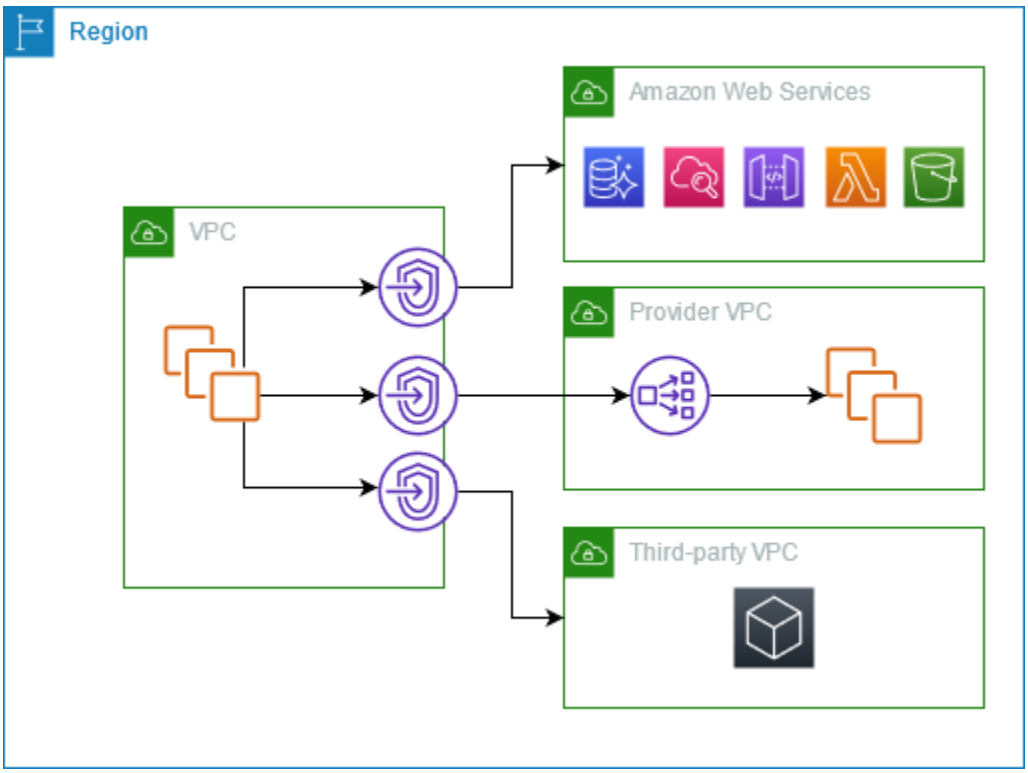
Was ist AWS PrivateLink?

AWS PrivateLink ist eine hochverfügbare, skalierbare Technologie, mit der Sie sich privat mit Diensten und Ressourcen verbinden könnenVPC, als ob sie sich in Ihren eigenen befinden würdenVPC. Sie müssen kein Internet-Gateway, NAT Gerät, öffentliche IP-Adresse, Verbindung oder AWS Direct Connect Verbindung verwenden, um die Kommunikation mit dem Dienst oder AWS Site-to-Site VPN der Ressource von Ihren privaten Subnetzen aus zu ermöglichen. Daher kontrollieren Sie die spezifischen API Endpunkte, Standorte, Dienste und Ressourcen, die von Ihrem aus erreichbar sind. VPC

Anwendungsfälle

Sie können VPC Endpunkte erstellen, um Clients in Ihrem System mit Diensten und Ressourcen VPC zu verbinden, in die Sie integriert werden können. 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 befinden sich VPC auf der linken Seite mehrere EC2 Amazon-Instances in einem privaten Subnetz und fünf VPC Endpunkte — drei VPC Schnittstellenendpunkte, ein VPC Ressourcenendpunkt und ein Servicenetzwerk-Endpunkt. VPC Der erste VPC Schnittstellenendpunkt stellt eine Verbindung zu einem Dienst her. AWS Der zweite VPC Schnittstellenendpunkt stellt eine Verbindung zu einem Dienst her, der von einem anderen AWS Konto (einem VPC Endpunktdienst) gehostet wird. Der dritte VPC Schnittstellenendpunkt stellt eine Verbindung zu einem AWS Marketplace-Partnerdienst her. Der VPC Ressourcenendpunkt stellt eine Verbindung zu einer Datenbank her. Der VPC Dienstnetzwerkendpunkt stellt eine Verbindung zu einem Dienstnetzwerk her.



Weitere Informationen

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

Arbeiten Sie mit VPC Endpunkten

Sie können VPC Endpoints mit einer der folgenden Methoden erstellen, darauf zugreifen und sie verwalten:

- AWS Management Console— Stellt eine Weboberfläche bereit, über die Sie auf Ihre AWS PrivateLink Ressourcen zugreifen können. Öffnen Sie die VPC Amazon-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::VPCEndpointConnectionNotification
  - AWS::EC2::VPCEndpointService
  - AWS::EC2::VPCEndpointServicePermissions
  - AWS:: ElasticLoadBalancing V2:: LoadBalancer
- AWS SDKs— APIs Sprachspezifisch angeben. SDKsSie kümmern sich um viele Verbindungsdetails, z. B. um die Berechnung von Signaturen, die Bearbeitung von Wiederholungsversuchen von Anfragen und die Behandlung von Fehlern. Weitere Informationen finden Sie unter Tools für AWS.
- Abfrage API — Stellt API Aktionen auf niedriger Ebene bereit, die Sie mithilfe von HTTPS Anfragen aufrufen. Die Verwendung der Query API ist der direkteste Weg, um auf Amazon zuzugreifenVPC. 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 EC2APIAmazon-Referenz.

Preisgestaltung

Informationen zu den Preisen für VPC Endgeräte finden Sie unter AWS PrivateLink Preisgestaltung.

AWS PrivateLink Konzepte

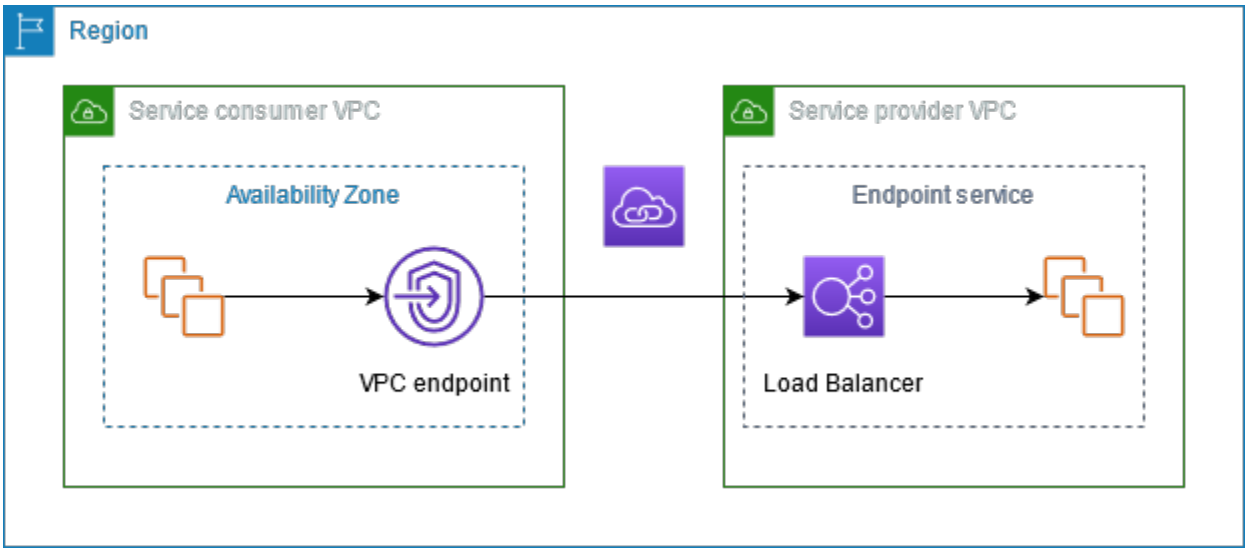
Sie können Amazon verwendenVPC, um eine virtuelle private Cloud (VPC) zu definieren, bei der es sich um ein logisch isoliertes virtuelles Netzwerk handelt. Sie können den Clients in Ihrem Netzwerk erlaubenVPC, sich mit Zielen außerhalb dieses VPC Bereichs zu verbinden. Fügen Sie dem beispielsweise ein Internet-Gateway hinzu, VPC um den Zugriff auf das Internet zu ermöglichen, oder fügen Sie eine VPN Verbindung hinzu, um den Zugriff auf Ihr lokales Netzwerk zu ermöglichen. Verwenden Sie diese Option auch, AWS PrivateLink um Ihren Clients die Möglichkeit VPC zu geben, VPCs über private IP-Adressen eine Verbindung zu Diensten und Ressourcen in anderen Ländern herzustellen, als ob diese Dienste und Ressourcen direkt in Ihrem 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 AWS PrivateLink Funktionsweise. Verbraucher erstellen VPC Endgeräte, um eine Verbindung zu Endpunktdiensten und Ressourcen herzustellen, die von Anbietern gehostet werden.



Anbieter

Machen Sie sich mit den Konzepten eines Anbieters vertraut.

Dienstanbieter

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 Instanzen oder mithilfe von lokalen Servern hosten.

Ressourcenanbieter

Der Besitzer einer Ressource, beispielsweise einer Datenbank, eines Knotenclusters oder einer Instanz, ist der Ressourcenanbieter. Zu den Ressourcenanbietern gehören AWS Dienste, AWS Partner und andere AWS Konten. Ressourcenanbieter können ihre Ressourcen vor Ort VPCs oder vor Ort hosten.

Konzepte

- Endpunkt-Services
- Service-Namen
- Service-Zustände
- Ressourcenkonfiguration
- Ressourcen-Gateway

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 Dienstnutzer muss bei der Erstellung eines VPC Endpunkts den Namen des Dienstes angeben. Dienstnutzer können die Dienstnamen für abfragen AWS-Services. 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.

Ressourcenkonfiguration

Der Ressourcenanbieter erstellt eine Ressourcenkonfiguration, um eine Ressource gemeinsam zu nutzen. Eine Ressourcenkonfiguration ist ein logisches Objekt, das entweder eine einzelne Ressource wie eine Datenbank oder eine Gruppe von Ressourcen wie einen Knotencluster darstellt. Eine Ressource kann eine IP-Adresse, ein Domainnamenziel oder eine RDS Amazon-Datenbank sein.

Bei der gemeinsamen Nutzung mit anderen Konten muss der Ressourcenanbieter die Ressource über eine AWS RAM Ressourcenfreigabe gemeinsam nutzen, damit bestimmte AWS Hauptbenutzer des anderen Kontos über einen Ressourcenendpunkt eine Verbindung mit der Ressource herstellen können. VPC

Ressourcenkonfigurationen können einem Servicenetzwerk zugeordnet werden, mit dem Principals über einen Servicenetzwerk-Endpunkt eine Verbindung herstellen. VPC

Ressourcen-Gateway

Ein Ressourcen-Gateway ist ein Zugangspunkt in einen Bereich, VPC von dem aus eine Ressource gemeinsam genutzt wird. Der Anbieter erstellt ein Ressourcengateway, um Ressourcen aus dem VPC gemeinsam zu nutzen.

Service- oder Ressourcenverbraucher

Der Benutzer eines Dienstes oder einer Ressource ist ein Verbraucher. Verbraucher können von ihren eigenen VPCs oder lokalen Standorten aus auf Endpunktdienste und -ressourcen zugreifen.

Konzepte

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

VPC-Endpunkte

Ein Verbraucher erstellt einen VPCEndpunkt, VPC um seinen Dienst oder eine Ressource mit einem Endpunkt zu verbinden. Ein Verbraucher muss bei der Erstellung eines Endpunkts den Endpunktdienst, die Ressource oder das Dienstnetzwerk angeben. VPC Es gibt mehrere Arten von VPC Endpunkten. Sie müssen den VPC Endpunkttyp erstellen, den Sie benötigen.

- `Interface`- Erstellen Sie einen Schnittstellenendpunkt, um UDP Datenverkehr TCP oder Datenverkehr an einen Endpunktdienst zu senden. Der für den Endpunktdienst 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 leiten den Verkehr mithilfe von Routentabellen von Ihrem VPC zum Gateway Load Balancer-Endpunkt weiter. Der Gateway Load Balancer verteilt den Datenverkehr an die virtuellen Appliances und kann je nach Bedarf skalieren.
- `Resource`- Erstellen Sie einen Ressourcenendpunkt, um auf eine Ressource zuzugreifen, die mit Ihnen gemeinsam genutzt wurde und sich auf einer anderen befindet. VPC Mit einem Ressourcenendpunkt können Sie privat und sicher auf Ressourcen wie eine Datenbank, einen Knotencluster, eine Instanz, einen Anwendungsendpunkt, ein Domainnamenziel oder eine IP-Adresse zugreifen, die sich in einem privaten Subnetz in einer anderen VPC oder in einer lokalen Umgebung befinden kann. Für Ressourcenendpunkte ist kein Load Balancer erforderlich, sodass Sie direkt auf die Ressource zugreifen können.
- `Service network`- Erstellen Sie einen Servicenetzwerk-Endpunkt, um auf ein Servicenetzwerk zuzugreifen, das Sie erstellt haben oder das für Sie freigegeben wurde. Sie können einen einzelnen Servicenetzwerk-Endpunkt verwenden, um privat und sicher auf mehrere Ressourcen und Dienste zuzugreifen, die einem Servicenetzwerk zugeordnet sind.

Es gibt einen anderen VPC Endpunkttyp`Gateway`, der einen Gateway-Endpunkt erstellt, um Datenverkehr an Amazon S3 oder DynamoDB zu senden. Gateway-Endpunkte verwenden AWS PrivateLink im Gegensatz zu den anderen Arten von Endpunkten nicht. VPC 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 an einen Endpunktdienst, eine Ressource oder ein

Dienstnetzwerk gerichtet ist. Für jedes Subnetz, das Sie bei der Erstellung eines Endpunkts angeben, erstellen wir eine VPC Endpunkt-Netzwerkschnittstelle im Subnetz.

Wenn ein VPC Endpunkt dies unterstütztIPv4, haben IPv4 seine Endpunkt-Netzwerkschnittstellen Adressen. Wenn ein VPC Endpunkt dies unterstütztIPv6, haben seine Endpunkt-Netzwerkschnittstellen IPv6 Adressen. Die IPv6 Adresse für eine Endpunkt-Netzwerkschnittstelle ist vom Internet aus nicht erreichbar. Wenn Sie eine Endpunkt-Netzwerkschnittstelle mit einer IPv6 Adresse beschreiben, beachten Sie, dass diese aktiviert `denyAllIgwTraffic` ist.

Endpunktrichtlinien

Eine VPCEndpunktrichtlinie ist eine IAM Ressourcenrichtlinie, die Sie einem VPC Endpunkt zuordnen. Sie bestimmt, welche Prinzipale den Endpunkt für den Zugriff auf den VPC Endpunktdienst verwenden können. Die standardmäßige VPC Endpunktrichtlinie erlaubt alle Aktionen aller Prinzipale auf allen Ressourcen über den VPC Endpunkt.

Endpunktzustände

Wenn Sie einen VPC Schnittstellenendpunkt erstellen, erhält der Endpunktdienst eine Verbindungsanforderung. Der Service-Anbieter kann die Anfrage annehmen oder ablehnen. Wenn der Dienstanbieter die Anfrage akzeptiert, kann der Dienstnutzer den VPC Endpunkt verwenden, nachdem dieser den `Available` Status erreicht hat.

Im Folgenden sind die möglichen Zustände für einen VPC Endpunkt aufgeführt:

- `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 Dienstnutzer den VPC Endpunkt ändert.
- `Available`- Der VPC Endpunkt kann verwendet werden.
- `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 Servicebenutzer hat den VPC Endpunkt gelöscht und der Löschvorgang ist im Gange.
- `Deleted`- Der VPC Endpunkt wurde gelöscht.

AWS PrivateLink Verbindungen

Der Datenverkehr von Ihrem VPC wird über eine Verbindung zwischen dem Endpunkt und dem Endpunktdienst oder der VPC Endpunktressource an einen Endpunktdienst oder eine Endpunktressource gesendet. Der Verkehr zwischen einem VPC Endpunkt und einem Endpunktdienst oder einer Endpunktressource 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. Ein Ressourcenbesitzer oder ein Dienstnetzwerkbesitzer teilt eine Ressourcenkonfiguration oder ein Dienstnetzwerk mit Verbrauchern, AWS Resource Access Manager sodass Verbraucher auf die Ressource oder das Dienstnetzwerk zugreifen können.

Bei VPC Schnittstellenendpunkten können Verbraucher mithilfe von Endpunktrichtlinien steuern, welche IAM Prinzipale einen Endpunkt für den Zugriff auf einen Endpunktdienst VPC oder eine Endpunktressource verwenden können.

Private gehostete Zonen

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

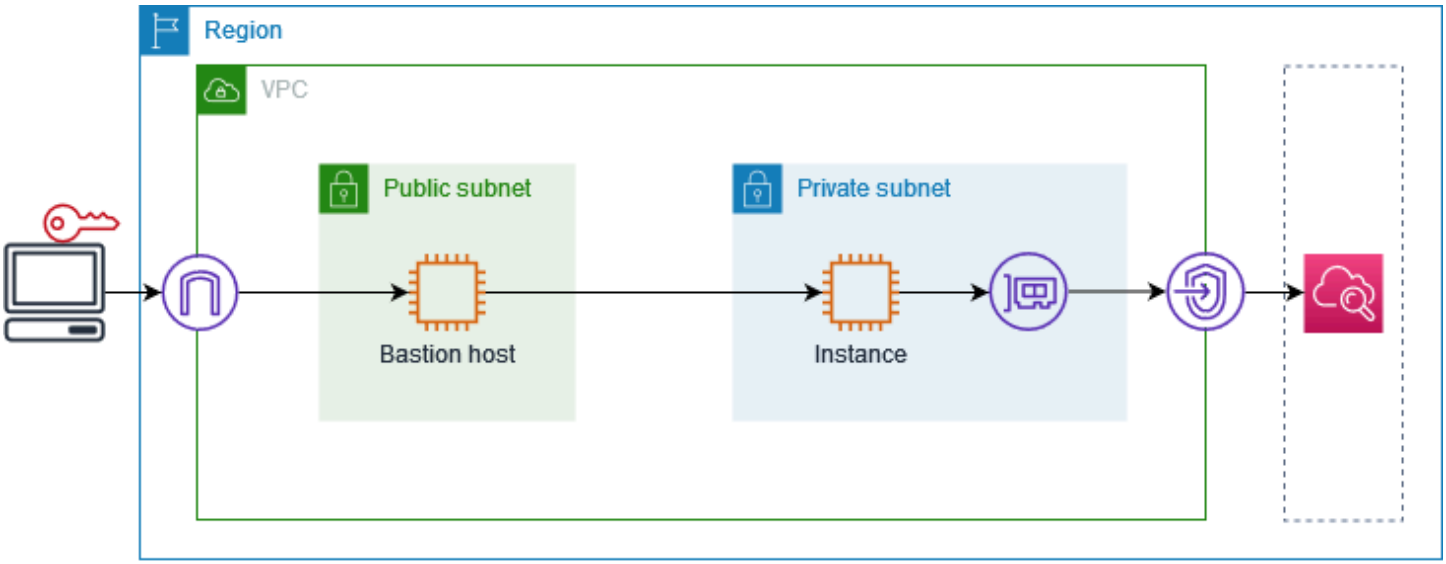
Sie können Amazon Route 53 so konfigurieren, dass Domain-Traffic an einen VPC Endpunkt weitergeleitet wird. Weitere Informationen finden Sie unter Weiterleiten von Datenverkehr zu einem VPC Endpunkt mithilfe Ihres Domainnamens.

Sie können Route 53 verwenden, um Split-Horizon zu konfigurierenDNS, wobei Sie denselben Domainnamen sowohl für eine öffentliche Website als auch für einen Endpunktdienst verwenden, der von bereitgestellt wird. AWS PrivateLink DNSAnfragen des Verbrauchers nach dem öffentlichen Hostnamen werden an VPC die privaten IP-Adressen der Endpunkt-Netzwerkschnittstellen weitergeleitet, Anfragen von außerhalb werden jedoch VPC weiterhin an die öffentlichen Endpunkte weitergeleitet. Weitere Informationen finden Sie unter DNSMechanismen für das Routing des Datenverkehrs und die Aktivierung von Failover für Bereitstellungen. AWS PrivateLink

Fangen Sie an mit AWS PrivateLink

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

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 Instanz, für die bestimmt CloudWatch ist, zur Netzwerkschnittstelle des Endpunkts aufgelöst und dann an CloudWatch den VPC Endpunkt weitergeleitet.



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

- Schritt 4: Erstellen Sie einen VPC Endpunkt für den Zugriff CloudWatch
- Schritt 5: Testen Sie den Endpunkt VPC
- Schritt 6: Bereinigen

Schritt 1: Erstellen Sie eine mit Subnetzen VPC

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

So erstellen Sie das VPC

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie Create (Erstellen)VPC aus.
3. Wählen Sie unter Ressourcen zum Erstellen aus VPCund mehr.
4. Geben Sie unter Automatische Generierung von Namenstags einen Namen für das 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 Create (Erstellen)VPC aus.

Schritt 2: Starten der Instances

Starten Sie mit demVPC, was Sie im vorherigen Schritt erstellt haben, 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 Datenverkehr aus dem CIDR Block für Ihren Computer zulässt.

- Erstellen Sie eine Sicherheitsgruppe für die Instanz, die eingehenden SSH Datenverkehr von der Sicherheitsgruppe für den Bastion-Host zulässt.
- Erstellen Sie ein IAM Instanzprofil und fügen Sie die CloudWatchReadOnlyAccessRichtlinie an.

Starten des Bastion-Hosts

1. Öffnen Sie die EC2 Amazon-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. Für VPC, wählen Sie IhreVPC.
    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 EC2 Amazon-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. Für VPC, wählen Sie IhreVPC.
    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 zum IAMBeispiel Instanzprofil Ihr IAM Instanzprofil aus.
8. Wählen Sie Launch Instance (Instance starten) aus.

Schritt 3: Testen Sie CloudWatch 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 von Ihrem Computer aus das key pair mit dem folgenden Befehl zum SSH Agenten hinzu, wobei der Name Ihrer PEM-Datei *key.pem* steht.

   ```
   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 `--region` Option die Region an, in der Sie die erstellt haben. VPC

```
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 mit der aktuellen VPC Konfiguration CloudWatch von der Instanz aus 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, versuchen Sie es erneut mit diesem list-metrics Befehl.

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 der Datenverkehr zugelassen wird CloudWatch. Fügen Sie beispielsweise eine Regel hinzu, die den HTTPS Datenverkehr aus dem VPC CIDR Block zulässt.

Um einen VPC Endpunkt zu erstellen für CloudWatch

1. Öffnen Sie die VPC Amazon-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 für Service die Option com.amazonaws aus. ***region***. Überwachung.
7. Wählen Sie für VPCIhreVPC.
8. Wählen Sie unter Subnets (Subnetze) die Availability Zone und dann das private Subnetz aus.
9. Wählen Sie unter Sicherheitsgruppe die Sicherheitsgruppe für den VPC Endpunkt aus.

10. Wählen Sie für Richtlinie die Option Vollzugriff aus, 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 Sie den Endpunkt VPC

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

Um den VPC Endpunkt zu testen

Führen Sie den folgenden Befehl auf Ihrer Instance aus. Geben Sie für die `--region` Option 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 verbunden AWS PrivateLink.

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

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

- Die Sicherheitsgruppe für den Endpunkt ermöglicht den Datenverkehr zu CloudWatch.
- Die `--region` Option 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 EC2 Amazon-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.

Um den VPC Endpunkt zu löschen

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den VPC Endpunkt aus.
4. Wählen Sie Aktionen, VPCEndpunkte löschen aus.
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. Bei den standardmäßigen Dienstendpunkten handelt es sich um öffentliche Schnittstellen. Sie müssen VPC also ein Internet-Gateway zu Ihrem hinzufügen, damit der Datenverkehr von VPC zu den AWS-Service Wenn diese Konfiguration Ihren Anforderungen an die Netzwerksicherheit nicht entspricht, können Sie Ihre Geräte so AWS PrivateLink verbinden, AWS-Services als ob sie sich in Ihrem befinden würdenVPC, ohne ein Internet-Gateway verwenden VPC zu müssen.

Sie können privat auf die Geräte zugreifen AWS-Services , die mit AWS PrivateLink VPC Endgeräten 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 VPC Schnittstellenendpunkt in jeder Availability Zone bereitgestellt wird. Ihnen wird auch pro GB verarbeiteter Daten in Rechnung gestellt. Weitere Informationen finden Sie unter AWS PrivateLink -Preisgestaltung.

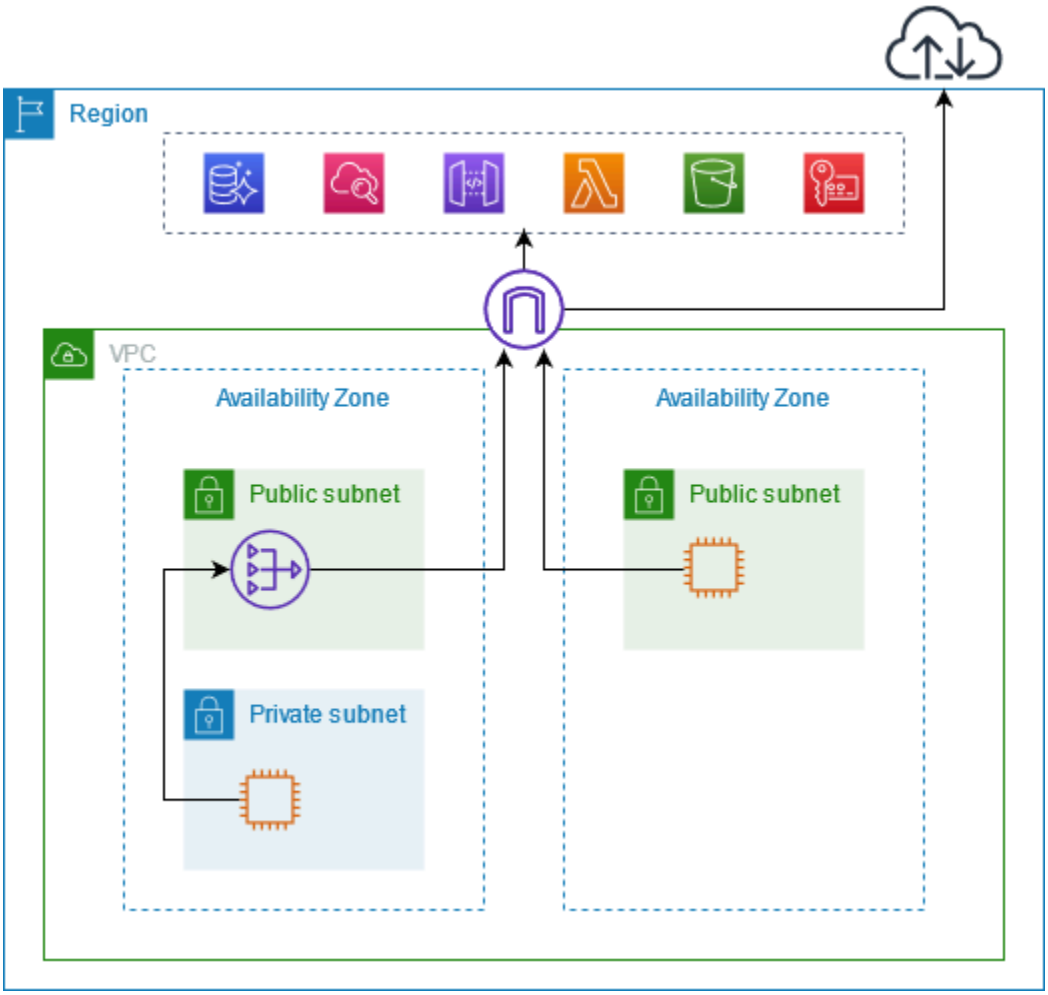
Inhalt

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.

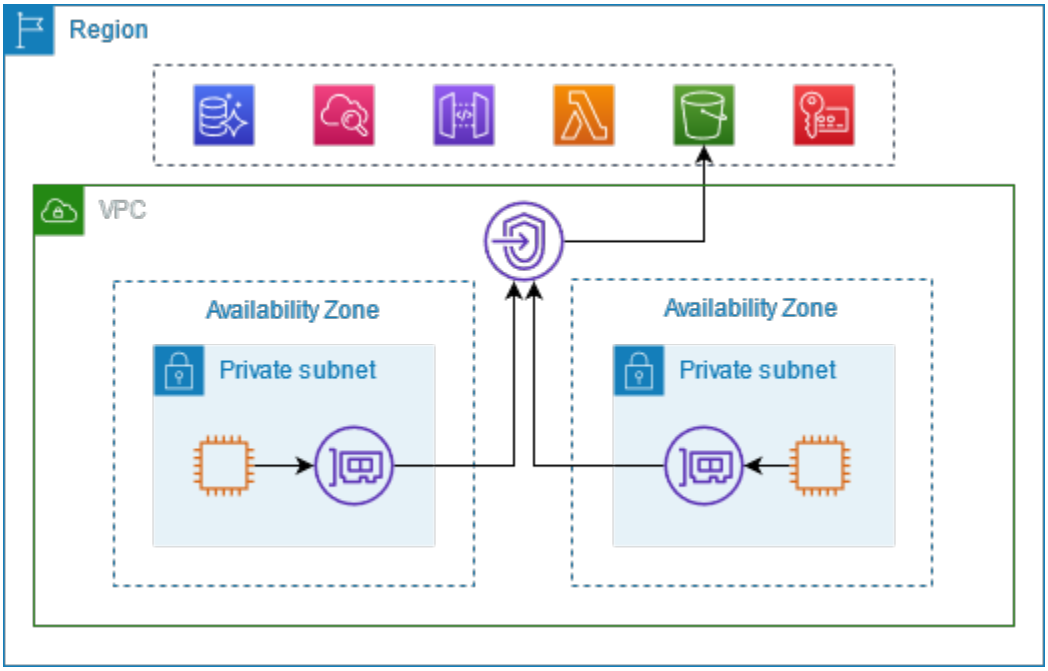
Zugang über Endpunkte für öffentliche Services

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 VPC und dann an die weitergeleitet. AWS-Service Der Datenverkehr zu und AWS-Service von einer Instance in einem privaten Subnetz wird an ein NAT Gateway weitergeleitet, dann an das Internet-Gateway für die und dann an denVPC. AWS-Service 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 Schnittstellenendpunkt, der Verbindungen zwischen den Subnetzen in Ihren VPC und den AWS-Service verwendeten Netzwerkschnittstellen herstellt. Der Datenverkehr, der für die bestimmt AWS-Service ist, wird mithilfe DNS der Netzwerkschnittstellen an die privaten IP-Adressen der Endpunkt-Netzwerkschnittstellen aufgelöst und dann an die AWS-Service Verbindung zwischen dem VPC Endpunkt und dem gesendet. AWS-Service



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

DNSHostnamen

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 Schnittstellenendpunkt erstellen, erstellen wir regionale und zonale DNS Namen, die Sie für die AWS-Service Kommunikation mit Ihrem Endgerät verwenden können. VPC

Der regionale DNS Name für Ihren VPC Schnittstellenendpunkt 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 Schnittstellenendpunkt für einen erstellen AWS-Service, können Sie private DNS aktivieren. Mit Private können Sie weiterhin Anfragen an einen Dienst stellenDNS, indem Sie den DNS Namen seines öffentlichen Endpunkts verwenden und gleichzeitig die private Konnektivität über den VPC Schnittstellenendpunkt nutzen. Weitere Informationen finden Sie unter the section called “DNSAuflösung”.

Der folgende describe-vpc-endpointsBefehl 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"
        }
    ]
]
```

DNSAuflösung

Die DNS Datensätze, die wir für Ihren VPC Schnittstellenendpunkt erstellen, sind öffentlich. Daher sind diese DNS Namen öffentlich auflösbar. DNSAnfragen von außerhalb geben jedoch VPC immer noch die privaten IP-Adressen der Endpunkt-Netzwerkschnittstellen zurück, sodass diese IP-Adressen nicht für den Zugriff auf den Endpunktdienst verwendet werden können, es sei denn, Sie haben Zugriff auf dieVPC.

Privat DNS

Wenn Sie Private DNS für Ihren VPC Schnittstellenendpunkt aktivieren und bei Ihrem VPC sowohl DNSHostnamen als auch DNS Auflösung aktiviert sind, erstellen wir eine versteckte, AWS verwaltete private Hosting-Zone für Sie. Die gehostete Zone enthält einen Datensatz für den DNS Standardnamen für den Dienst, der ihn in die privaten IP-Adressen der Endpunkt-Netzwerkschnittstellen in Ihrem auflöst. VPC 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 Endgeräte für zu aktivieren. AWS-Services Dadurch wird sichergestellt, dass Anfragen, die die Endpunkte des öffentlichen Dienstes verwenden, wie Anfragen, die über einen gestellt werden AWS SDK, an Ihren VPC Endpunkt weitergeleitet werden.

Amazon stellt für Sie einen DNS Server bereitVPC, den sogenannten Route 53 Resolver. Der Route 53 Resolver löst automatisch lokale VPC Domainnamen auf und zeichnet in privaten Hosting-Zonen auf. Sie können den Route 53 Resolver jedoch nicht von außerhalb Ihres verwenden. VPC Wenn Sie von Ihrem lokalen Netzwerk aus auf Ihren VPC Endpunkt zugreifen möchten, können Sie Route 53 Resolver-Endpunkte und Resolver-Regeln verwenden. Weitere Informationen finden Sie unter Integration mit und. AWS Transit GatewayAWS PrivateLinkAmazon Route 53 Resolver

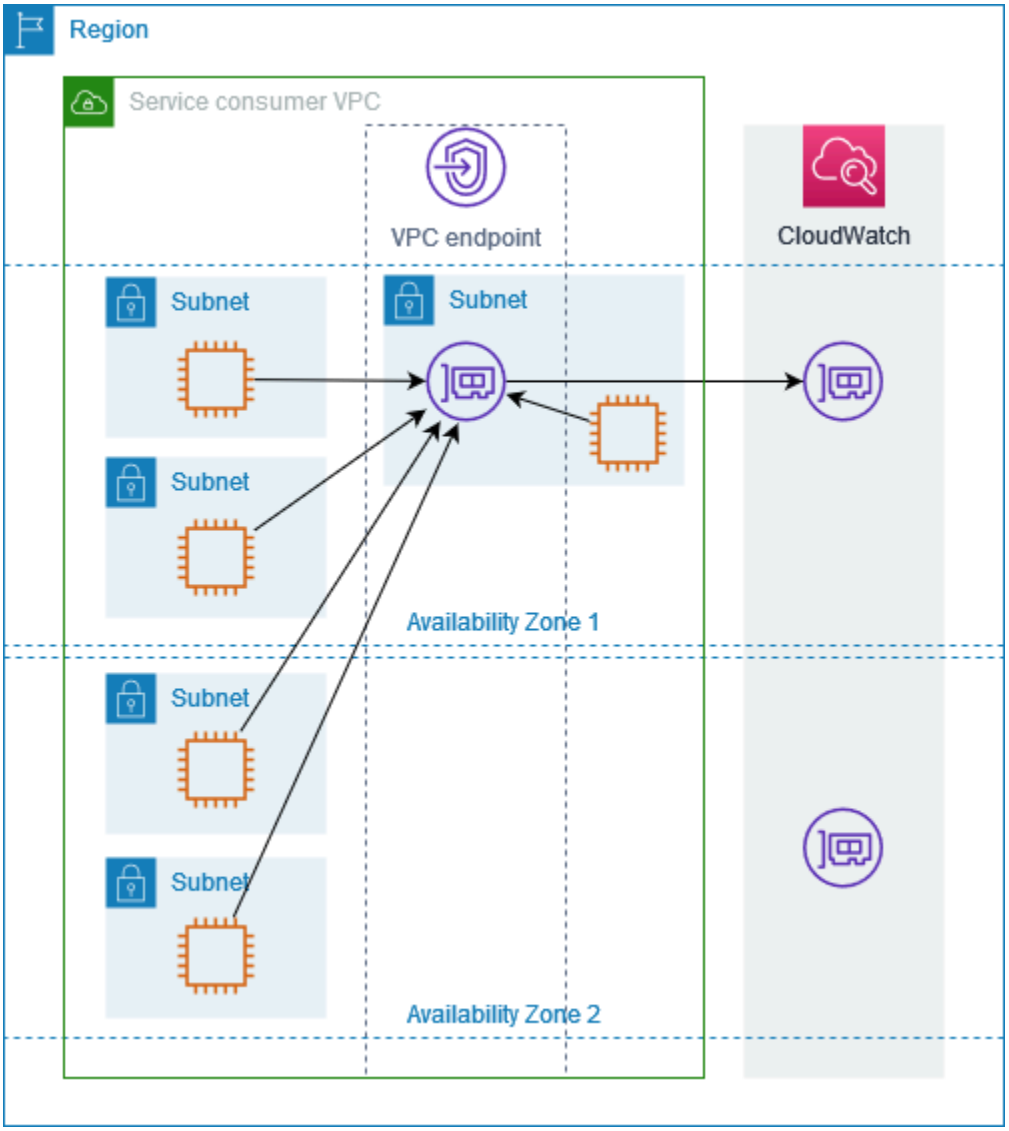
Subnetze und Availability Zones

Sie können Ihren VPC Endpunkt 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.

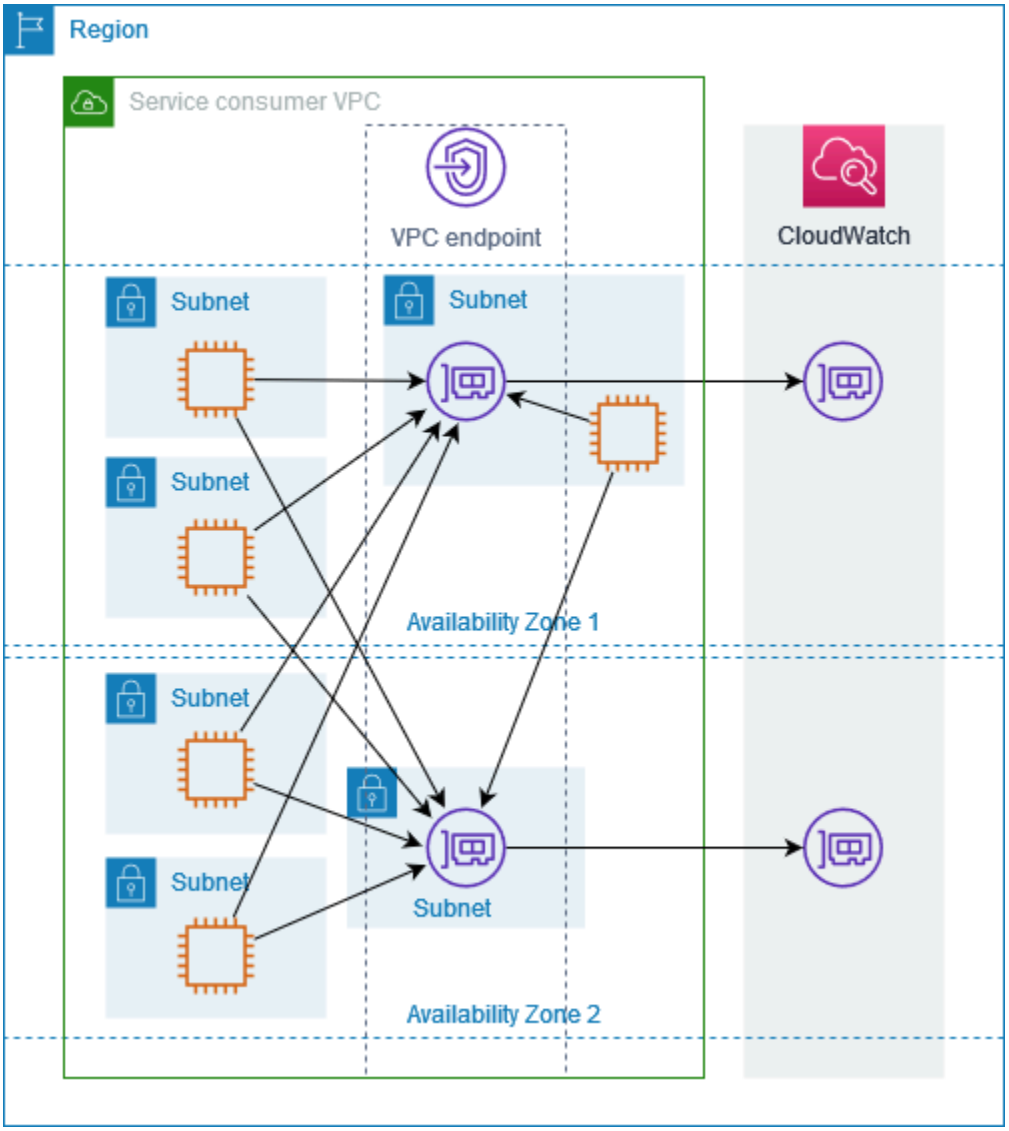
In einer Produktionsumgebung empfehlen wir für hohe Verfügbarkeit und Ausfallsicherheit Folgendes:

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

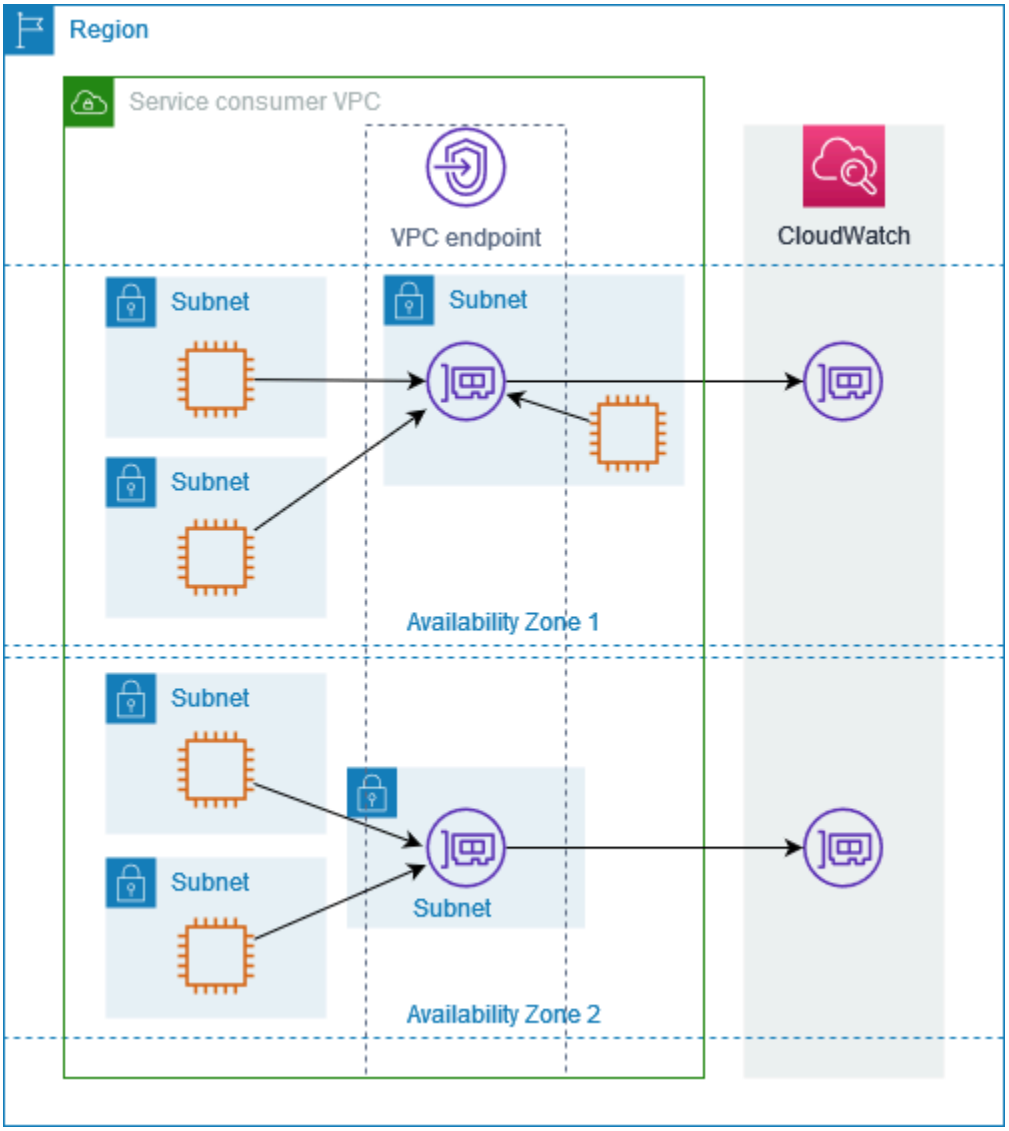
Das folgende Diagramm zeigt einen VPC Endpunkt für Amazon CloudWatch mit einer Endpunkt-Netzwerkschnittstelle in einer einzigen Availability Zone. Wenn eine Ressource in einem beliebigen Subnetz CloudWatch über ihren öffentlichen Endpunkt auf Amazon VPC zugreift, lösen wir den Datenverkehr an die IP-Adresse 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 über ihren öffentlichen Endpunkt auf Amazon VPC CloudWatch zugreift, wählen wir eine fehlerfreie 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 Support bieten, auch wenn sie keinen Support IPv6 über ihre öffentlichen Endpunkte anbieten. Endgeräte, die Support anbieten, IPv6 können DNS Anfragen mit Datensätzen beantworten. AAAA

Anforderungen zur Aktivierung IPv6 für einen Schnittstellenendpunkt

- Der AWS-Service muss seine Dienstendpunkte über IPv6 verfügbar machen. Weitere Informationen finden Sie unter the section called “IPv6Support anzeigen”.
- 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 IPv4 Adressbereiche haben.
- IPv6— Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv6 nur Subnetze sind.
- Dualstack — Weisen Sie Ihren IPv4 Endpunkt-Netzwerkschnittstellen sowohl IPv6 Adressen als auch Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 sowohl IPv6 als auch Adressbereiche haben.

Wenn ein VPC Schnittstellenendpunkt dies unterstütztIPv4, haben die Endpunkt-Netzwerkschnittstellen IPv4 Adressen. Wenn ein VPC Schnittstellenendpunkt diese unterstütztIPv6, haben die Endpunkt-Netzwerkschnittstellen IPv6 Adressen. Die IPv6 Adresse für eine Endpunkt-Netzwerkschnittstelle ist vom Internet aus nicht erreichbar. Wenn Sie eine Endpunkt-Netzwerkschnittstelle mit einer IPv6 Adresse beschreiben, beachten Sie, dass diese aktiviert `denyAllIgwTraffic` ist.

AWS-Services die sich integrieren mit AWS PrivateLink

Die folgenden AWS-Services lassen sich in integrieren AWS PrivateLink. Sie können einen VPC Endpunkt erstellen, um eine private Verbindung zu diesen Diensten herzustellen, als ob sie auf Ihrem eigenen Server laufen würdenVPC.

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 bei der Erstellung des VPC Schnittstellenendpunkts angeben, 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*.konto
APIAmazon-Gateway	com.amazonaws. *region*.execute-api
AWS AppConfig	com.amazonaws. *region*.appconfig
	com.amazonaws. *region*.appconfig-Daten

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.anfragen
Application Auto Scaling	com.amazonaws. *region*.automatische Skalierung von Anwendungen
AWS Application Discovery Service	com.amazonaws. *region*.discovery
	com.amazonaws. *region*.arsenal-discovery
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*. Prüfungsleiter
Amazon Aurora	com.amazonaws. *region*.rds
AWS Auto Scaling	com.amazonaws. *region*.autoscaling-Pläne
AWS B2B-Datenaustausch	com.amazonaws. *region*.b2bi
AWS Backup	com.amazonaws. *region*. Sicherungskopie
	com.amazonaws. *region*.backup-gateway
AWS Batch	com.amazonaws. *region*.stapel

AWS-Service	Service-Name
Amazon Bedrock	com.amazonaws. *region*. Grundgestein
	com.amazonaws. *region*. Bedrock-Agent
	com.amazonaws. *region*. bedrock-agent-runtime
	com.amazonaws. *region*.bedrock-Laufzeit
AWS Billing and Cost Management	com.amazonaws. *region*. Abrechnung
	com.amazonaws. *region*.kostenloser Tarif
	com.amazonaws. *region*.steuer
AWS Billing Conductor	com.amazonaws. *region*. Abrechnungsleiter
Amazon Braket	com.amazonaws. *region*. Klammer
AWS Clean Rooms	com.amazonaws. *region*. saubere Räume
AWS Saubere Räume ML	com.amazonaws. *region*.cleanrooms-ml
AWS Cloud Control API	com.amazonaws. *region*.cloudcontrol-API
	com.amazonaws. *region*.cloudcontrol api-fips
Amazon Cloud Directory	com.amazonaws. *region*.cloud-Verzeichnis
AWS CloudFormation	com.amazonaws. *region*. Wolkenbildung
AWS CloudHSM	com.amazonaws. *region*.cloudhsmv2
AWS Cloud Map	com.amazonaws. *region*.servicediscovery
	com.amazonaws. *region*.servicediscovery-fips
	com.amazonaws. *region*.datenservicediscovery
	com.amazonaws. *region*. data-servicediscovery-fips

AWS-Service	Service-Name
AWS CloudTrail	com.amazonaws. *region*. Wolkenpfad
Amazon CloudWatch	com.amazonaws. *region*.Anwendungssignale
	com.amazonaws. *region*. Einblicke in die Anwendung
	com.amazonaws. *region*. offensichtlich
	com.amazonaws. *region*. offensichtlich - Datenebene
	com.amazonaws. *region*. Internetmonitor
	com.amazonaws. *region*.internetmonitor-fips
	com.amazonaws. *region*. Überwachung
	com.amazonaws. *region*. Netzwerkflussmonitor
	com.amazonaws. *region*.networkflowmonitor-Berichte
	com.amazonaws. *region*. Netzwerkmonitor
	com.amazonaws. *region*.beobachtbarkeit/admin
	com.amazonaws. *region*. rum
	com.amazonaws. *region*.rum-Datenebene
	com.amazonaws. *region*. Kunststoffe
	com.amazonaws. *region*.synthetik-fips
CloudWatch Amazon-Protokolle	com.amazonaws. *region*.protokolle
AWS CodeArtifact	com.amazonaws. *region*.codeartifact.api
	com.amazonaws. *region*.codeartifact.repositorien
AWS CodeBuild	com.amazonaws. *region*.codebuild

AWS-Service	Service-Name
	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-verbindungen.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-gutachter
AWS CodePipeline	com.amazonaws. *region*.code-Pipeline
Amazon Comprehend	com.amazonaws. *region*.com verstehen
Amazon Comprehend Medical	com.amazonaws. *region*.com prehend medizinisch
AWS Compute Optimizer	com.amazonaws. *region*.compute-optimierer
AWS Config	com.amazonaws. *region*.config
Amazon Connect	com.amazonaws. *region*.app-Integrationen
	com.amazonaws. *region*.fälle
	com.amazonaws. *region*.connect-kampagnen
	com.amazonaws. *region*.profil

AWS-Service	Service-Name
	com.amazonaws. *region*. Stimmen-ID
	com.amazonaws. *region*. Weisheit
AWS Connector Service	com.amazonaws. *region*.aws-Anschluss
AWS Control Catalog	com.amazonaws. *region*.control-Katalog
AWS Cost Explorer	com.amazonaws. *region*.ce
AWS Cost Optimization Hub	com.amazonaws. *region*. cost-optimization-hub
AWS Data Exchange	com.amazonaws. *region*. Datenaustausch
AWS Data Exports	com.amazonaws. *region*. bcm-data-exports
Amazon Data Firehose	com.amazonaws. *region*.kinesis-Feuerwehrhose
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*.termin.management
	com.amazonaws. *region*.Deadline.Terminplanung
DevOpsAmazon-Guru	com.amazonaws. *region*.devops-guru
AWS Directory Service	com.amazonaws. *region*.ds
	com.amazonaws. *region*.ds-Daten
Amazon DocumentDB	com.amazonaws. *region*.rds
Amazon-DynamoDB	com.amazonaws. *region*.dynamodb

AWS-Service	Service-Name
	com.amazonaws. *region*.dynamodb-fips
Amazon EBS direkt APIs	com.amazonaws. *region*.ebs
Amazon EC2	com.amazonaws. *region*.ec2
Amazon EC2 Auto Scaling	com.amazonaws. *region*.automatische Skalierung
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-Telemetrie
Amazon EKS	com.amazonaws. *region*.eks
	com.amazonaws. *region*.eks-auth
AWS Elastic Beanstalk	com.amazonaws. *region*. elastische Bohnenstange
	com.amazonaws. *region*.elasticbeanstalk-gesundheit
AWS Elastic Disaster Recovery	com.amazonaws. *region*.drs
Amazon Elastic File System	com.amazonaws. *region*.elastisches Dateisystem
	com.amazonaws. *region*.elastisches Dateisystem-Fips
Elastic Load Balancing	com.amazonaws. *region*.elastischer Lastenausgleich
Amazon ElastiCache	com.amazonaws. *region*. elastischer Cache
	com.amazonaws. *region*.elasticache-fips

AWS-Service	Service-Name
AWS Elemental MediaConnect	com.amazonaws. *region*.mediaconnect
Amazon EMR	com.amazonaws. *region*.elasticmapreduce
Amazon EMR auf EKS	com.amazonaws. *region*.emr-Behälter
Amazon EMR Serverlos	com.amazonaws. *region*.emr-serverlos
	com.amazonaws. *region*. emr-serverless-services. Livius
Amazon EMR WAL	com.amazonaws. *region*.emrwal.prod
AWS Nachrichten für Endbenutzer in sozialen Netzwerken	com.amazonaws. *region*.soziale Nachrichtenübermittlung
AWS Entity Resolution	com.amazonaws. *region*. Entitätsauflösung
Amazon EventBridge	com.amazonaws. *region*.veranstaltungen
	com.amazonaws. *region*. Rohre
	com.amazonaws. *region*.pipes-Daten
	com.amazonaws. *region*.pipes-fips
	com.amazonaws. *region*.schemas
AWS Fault Injection Service	com.amazonaws. *region*.fis
Amazon FinSpace	com.amazonaws. *region*.finspace
	com.amazonaws. *region*.finspace-api
Amazon Forecast	com.amazonaws. *region*. Prognose
	com.amazonaws. *region*. Prognoseabfrage
	com.amazonaws. *region*.Forecast-Fips

AWS-Service	Service-Name
	com.amazonaws. *region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws. *region*. Betrugsdetektor
Amazon FSx	com.amazonaws. *region*.fsx
	com.amazonaws. *region*.fsx-fips
AWS Glue	com.amazonaws. *region*. kleben
	com.amazonaws. *region*.glue.dashboard
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*. Bodenstation
Amazon GuardDuty	com.amazonaws. *region*. Wachdienst
	com.amazonaws. *region*.guardduty-Daten
	com.amazonaws. *region*. guardduty-data-fips
	com.amazonaws. *region*.guardduty-fips
AWS HealthImaging	com.amazonaws. *region*. dicom-medical-imaging
	com.amazonaws. *region*.medizinische Bildgebung
	com.amazonaws. *region*. runtime-medical-imaging
AWS HealthLake	com.amazonaws. *region*. Gesundheitssee
AWS HealthOmics	com.amazonaws. *region*.analytics-Comics
	com.amazonaws. *region*. control-storage-omics

AWS-Service	Service-Name
	com.amazonaws. *region*.storage-comics
	com.amazonaws. *region*.tags-Comics
	com.amazonaws. *region*.workflows-Comics
AWS Identity and Access Management (IAM)	com.amazonaws.iam
IAMIdentitätszentrum	com.amazonaws. *region*. Identitätsspeicher
IAM Roles Anywhere	com.amazonaws. *region*. Rollen überall
Amazon Inspector	com.amazonaws. *region*.inspektor 2
	com.amazonaws. *region*.inspector-Scan
AWS IoT Core	com.amazonaws. *region*.iot.daten
	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.becher
	com.amazonaws. *region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws. *region*.ioflotwise
AWS IoT Greengrass	com.amazonaws. *region*. grünes Gras
AWS IoT RoboRunner	com.amazonaws. *region*.iotroborunner
AWS IoT SiteWise	com.amazonaws. *region*.iotsitewise.api
	com.amazonaws. *region*.iotsitewise.data

AWS-Service	Service-Name
AWS IoT TwinMaker	com.amazonaws. *region*.iottwinmaker.api
	com.amazonaws. *region*.iottwinmaker.data
Amazon Kendra	com.amazonaws. *region*.kendra
	aws.api. *region*.kendra-Rangliste
AWS Key Management Service	com.amazonaws. *region*. km
	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
	com.amazonaws. *region*. kinesis-streams-fips
AWS Lake Formation	com.amazonaws. *region*. Informationen zum See
AWS Lambda	com.amazonaws. *region*. Lambda
AWS Launch Wizard	com.amazonaws. *region*.launchwizard
Amazon Lex	com.amazonaws. *region*.models-v2-lex
	com.amazonaws. *region*.runtime-v2-lex
AWS License Manager	com.amazonaws. *region*.lizenzmanager
	com.amazonaws. *region*. license-manager-fips
	com.amazonaws. *region*. license-manager-linux-subscriptions
	com.amazonaws. *region*. license-manager-linux-subscriptions-Fips

AWS-Service	Service-Name
	com.amazonaws. *region*. license-manager-user-subscriptions
Amazon Lookout für Equipment	com.amazonaws. *region*. Ausrüstung aussuchen
Amazon Lookout for Metrics	com.amazonaws. *region*. Lookout-Metriken
Amazon Lookout for Vision	com.amazonaws. *region*. Lookout Vision
Amazon Macie	com.amazonaws. *region*.macie 2
AWS Mainframe Modernization	com.amazonaws. *region*.apptest
	com.amazonaws. *region*. m2
Amazon Managed Blockchain	com.amazonaws. *region*. verwaltete Blockchain-Abfrage
	com.amazonaws. *region*.managedblockchain.bitcoin.main.net
	com.amazonaws. *region*.managedblockchain.bitcoin.test.net
Amazon Managed Service for Prometheus	com.amazonaws. *region*.aps
	com.amazonaws. *region*.aps-Arbeitsbereiche
Amazon Managed Streaming für Apache Kafka	com.amazonaws. *region*.kafka
	com.amazonaws. *region*.kafka-fips
Amazon Managed Workflows für Apache Airflow	com.amazonaws. *region*.airflow.api
	com.amazonaws. *region*.airflow.api-fips
	com.amazonaws. *region*.airflow.env
	com.amazonaws. *region*.airflow.env-fips

AWS-Service	Service-Name
	com.amazonaws. *region*.airflow.ops
AWS Management Console	com.amazonaws. *region*.konsole
	com.amazonaws. *region*. einloggen
Amazon MemoryDB	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-Leerzeichen
Migration Hub Strategie-Empfehlungen	com.amazonaws. *region*.migrationhub-Strategie
Amazon MQ	com.amazonaws. *region*.mq
Amazon Neptune Analytics	com.amazonaws. *region*.Neptun-Graph
	com.amazonaws. *region*. neptune-graph-data
	com.amazonaws. *region*. neptune-graph-fips
AWS Network Firewall	com.amazonaws. *region*.network-firewall
	com.amazonaws. *region*. network-firewall-fips
OpenSearch Amazon-Dienst	Diese Endpunkte sind serviceverwaltet.
AWS Organizations	com.amazonaws. *region*. Organisationen
	com.amazonaws. *region*.organisationen-fips
AWS Outposts	com.amazonaws. *region*. Außenposten
AWS Panorama	com.amazonaws. *region*. Panorama

AWS-Service	Service-Name
AWS Kryptografie im Zahlungsverkehr	com.amazonaws. *region*.payment-cryptography.controlplane
	com.amazonaws. *region*.payment-cryptography.dataplane
AWS PCS	com.amazonaws. *region*. Stck
	com.amazonaws. *region*.pcs-fips
Amazon Personalize	com.amazonaws. *region*.personalisieren
	com.amazonaws. *region*.personalisieren Sie Ereignisse
	com.amazonaws. *region*.personalisieren-Laufzeit
Amazon Pinpoint	com.amazonaws. *region*. punktgenau
	com.amazonaws. *region*. pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws. *region*. Polly
AWS-Preisliste	com.amazonaws. *region*.pricing.api
AWS Privates 5G	com.amazonaws. *region*.private-netzwerke
AWS Private Certificate Authority	com.amazonaws. *region*.acm-pca
	com.amazonaws. *region*. pca-connector-ad
	com.amazonaws. *region*. pca-connector-scep
AWS Proton	com.amazonaws. *region*. Proton
Amazon Q Business	aws.api. *region*.q Geschäft
Amazon Q Developer	com.amazonaws. *region*. Codeflüsterer
	com.amazonaws. *region*q

AWS-Service	Service-Name
	com.amazonaws. *region*.apps
Amazon Q-Benutzerabonnements	com.amazonaws. *region*.service.user-Abonnements
Amazon QLDB	com.amazonaws. *region*.qldb.Sitzung
Amazon QuickSight	com.amazonaws. *region*.quicksight-Webseite
Amazon RDS	com.amazonaws. *region*.rds
RDSAmazon-Daten API	com.amazonaws. *region*.rds-Daten
RDSPerformance Insights von Amazon	com.amazonaws. *region*.pi
	com.amazonaws. *region*.pi-fips
AWS re:Post Privat	com.amazonaws. *region*.repostspace
Papierkorb	com.amazonaws. *region*.bin
Amazon-Redshift	com.amazonaws. *region*.redshift
	com.amazonaws. *region*.redshift-fips
	com.amazonaws. *region*.redshift - serverlos
	com.amazonaws. *region*. redshift-serverless-fips
Amazon Redshift Redshift-Daten API	com.amazonaws. *region*.redshift-Daten
	com.amazonaws. *region*. redshift-data-fips
Amazon Rekognition	com.amazonaws. *region*.rekognition
	com.amazonaws. *region*.rekognition-fips
	com.amazonaws. *region*.streaming-erkennung
	com.amazonaws. *region*. streaming-rekognition-fips

AWS-Service	Service-Name
AWS Resource Access Manager	com.amazonaws. *region*.ram
AWS Resource Groups	com.amazonaws. *region*.resource-groups
	com.amazonaws. *region*. resource-groups-fips
AWS RoboMaker	com.amazonaws. *region*. Robomaker
Amazon S3	com.amazonaws. *region*. 3
	com.amazonaws. *region*.s3-Tabellen
Mulitiregionale Amazon-S3-Zugriffspunkte	com.amazonaws.s3-global.accesspoint
Amazon S3 in Outposts	com.amazonaws. *region*.s3-Außenposten
Amazon SageMaker KI	Als Sagemaker. *region*. Experimente
	als Sagemaker. *region*. Notizbuch
	als Sagemaker. *region*.partner-App
	aws.sagemaker. *region*. Studio
	com.amazonaws. *region*. sagemaker-data-science-assistant
	com.amazonaws. *region*.sagemaker.api
	com.amazonaws. *region*.sagemaker.api-fips
	com.amazonaws. *region*.sagemaker.featurestore-runtime
	com.amazonaws. *region*.sagemaker.metrics
	com.amazonaws. *region*.sagemaker.runtime

AWS-Service	Service-Name
	com.amazonaws. *region*.sagemaker.runtime-fips
Savings Plans	com.amazonaws. *region*. Sparpläne
AWS Secrets Manager	com.amazonaws. *region*. Geheimnismanager
AWS Security Hub	com.amazonaws. *region*. Sicherheitshub
AWS Security Token Service	com.amazonaws. *region*.sts
AWS Serverless Application Repository	com.amazonaws. *region*. serverloses Repo
Servicekatalog	com.amazonaws. *region*.servicekatalog
	com.amazonaws. *region*.servicecatalog-app-Registrierung
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*.staaten
	com.amazonaws. *region*.sync-staaten
AWS Storage Gateway	com.amazonaws. *region*. Speichergateway
AWS Supply Chain	com.amazonaws. *region*.scn

AWS-Service	Service-Name
AWS Systems Manager	com.amazonaws. *region*.ec2-Nachrichten
	com.amazonaws. *region*.ssm
	com.amazonaws. *region*.ssm-Kontakte
	com.amazonaws. *region*.ssm-Vorfälle
	com.amazonaws. *region*.ssm-schnelle Einrichtung
	com.amazonaws. *region*.ssm-Nachrichten
AWS Telco Network Builder	com.amazonaws. *region*.tnb
Amazon Textract	com.amazonaws. *region*.textrahieren
	com.amazonaws. *region*.textract-fips
Amazon Timestream	com.amazonaws. *region*.timestream.ingest- *cell*
	com.amazonaws. *region*.timestream.query- *cell*
Amazon Timestream für InfluxDB	com.amazonaws. *region*.timestream-influxdb
	com.amazonaws. *region*. timestream-influxdb-fips
Amazon Transcribe	com.amazonaws. *region*.transkribieren
	com.amazonaws. *region*. transkribiert Streaming
Amazon Transcribe Medical	com.amazonaws. *region*.transkribieren
	com.amazonaws. *region*. transkribiert Streaming
AWS Transfer for SFTP	com.amazonaws. *region*. Übertragung
	com.amazonaws. *region*.transfer.server
Amazon Translate	com.amazonaws. *region*. übersetzen

AWS-Service	Service-Name
AWS Trusted Advisor	com.amazonaws. *region*. vertrauenswürdiger Berater
Amazon Verified Permissions	com.amazonaws. *region*. verifizierte Berechtigungen
VPCAmazon-Gitter	com.amazonaws. *region*.vpc-Gitter
AWS Well-Architected Tool	com.amazonaws. *region*. gut gestaltet
Amazon WorkMail	com.amazonaws. *region*.workmail
Amazon WorkSpaces	com.amazonaws. *region*. Arbeitsbereiche
Sicherer Browser von Amazon Workspaces	com.amazonaws. *region*.workspaces-web
	com.amazonaws. *region*. workspaces-web-fips
Amazon WorkSpaces Thin Client	com.amazonaws. *region*.thinclient.api
AWS X-Ray	com.amazonaws. *region*.xray

Verfügbare AWS-Service -Namen anzeigen

Sie können den describe-vpc-endpoint-servicesBefehl verwenden, um die Dienstnamen anzuzeigen, die VPC Endpunkte unterstützen.

Im folgenden Beispiel werden die Endpunkte angezeigt AWS-Services , die Schnittstellenendpunkte 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

Nachdem Sie den Dienstnamen gefunden haben, können Sie den describe-vpc-endpoint-servicesBefehl verwenden, um detaillierte Informationen zu jedem Endpunktdienst 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 Endpunktrichtlinien unterstützt, rufen Sie den describe-vpc-endpoint-servicesBefehl 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 diejenigen 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-ml",
    "com.amazonaws.us-east-1.cloudtrail",
    "com.amazonaws.us-east-1.codeguru-profiler",
    "com.amazonaws.us-east-1.codeguru-reviewer",
    "com.amazonaws.us-east-1.codepipeline",
    "com.amazonaws.us-east-1.codewhisperer",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.datazone",
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.email-smtp",
    "com.amazonaws.us-east-1.glue.dashboard",
    "com.amazonaws.us-east-1.grafana-workspace",
    "com.amazonaws.us-east-1.iot.credentials",
    "com.amazonaws.us-east-1.iot.data",
    "com.amazonaws.us-east-1.iotwireless.api",
    "com.amazonaws.us-east-1.lorawan.cups",
    "com.amazonaws.us-east-1.lorawan.lns",
    "com.amazonaws.us-east-1.macie2",
    "com.amazonaws.us-east-1.neptune-graph",
    "com.amazonaws.us-east-1.neptune-graph-fips",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.q",
    "com.amazonaws.us-east-1.redshift-data",
    "com.amazonaws.us-east-1.redshift-data-fips",
    "com.amazonaws.us-east-1.refactor-spaces",
    "com.amazonaws.us-east-1.sagemaker.runtime-fips",
    "com.amazonaws.us-east-1.storagegateway",
    "com.amazonaws.us-east-1.transfer",
    "com.amazonaws.us-east-1.transfer.server",
    "com.amazonaws.us-east-1.verifiedpermissions"
]
```

IPv6Support anzeigen

Sie können den folgenden describe-vpc-endpoint-servicesBefehl verwenden, um die anzuzeigen AWS-Services , auf die Sie IPv6 in der angegebenen Region 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.account",
    "com.amazonaws.us-east-1.applicationinsights",
    "com.amazonaws.us-east-1.apprunner",
    "com.amazonaws.us-east-1.aps",
    "com.amazonaws.us-east-1.aps-workspaces",
    "com.amazonaws.us-east-1.arsenal-discovery",
    "com.amazonaws.us-east-1.athena",
    "com.amazonaws.us-east-1.backup",
    "com.amazonaws.us-east-1.braket",
    "com.amazonaws.us-east-1.cloudcontrolapi",
    "com.amazonaws.us-east-1.cloudcontrolapi-fips",
    "com.amazonaws.us-east-1.cloudhsmv2",
    "com.amazonaws.us-east-1.compute-optimizer",
    "com.amazonaws.us-east-1.codeartifact.api",
    "com.amazonaws.us-east-1.codeartifact.repositories",
    "com.amazonaws.us-east-1.cost-optimization-hub",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.discovery",
    "com.amazonaws.us-east-1.drs",
    "com.amazonaws.us-east-1.ebs",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.elasticbeanstalk",
    "com.amazonaws.us-east-1.elasticbeanstalk-health",
    "com.amazonaws.us-east-1.execute-api",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.grafana",
    "com.amazonaws.us-east-1.groundstation",
    "com.amazonaws.us-east-1.internetmonitor".
    "com.amazonaws.us-east-1.internetmonitor-fips".
```

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

Zugriff und AWS-Service Verwendung eines VPC Schnittstellen-Endpunkts

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

Für jedes Subnetz, das Sie in Ihrem angebenVPC, erstellen wir eine Endpunkt-Netzwerkschnittstelle im Subnetz und weisen ihr eine private IP-Adresse aus dem Subnetzadressbereich 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 in Ihrem zugreifen. AWS-Service VPC
- Um Private zu verwendenDNS, müssen Sie DNS Hostnamen und DNS Auflösung für Ihre VPC aktivieren. Weitere Informationen finden Sie unter DNSAttribute anzeigen und aktualisieren im VPCAmazon-Benutzerhandbuch.
- Um sie IPv6 für einen Schnittstellen-Endpunkt zu aktivieren, AWS-Service muss der Access Over unterstützenIPv6. Weitere Informationen finden Sie unter the section called “IP-Adresstypen”.
- Erstellen Sie eine Sicherheitsgruppe für die Netzwerkschnittstelle des Endpunkts, die den erwarteten Datenverkehr von den Ressourcen in Ihrem ermöglichtVPC. Um beispielsweise sicherzustellen, dass sie HTTPS Anfragen an die senden AWS CLI kann AWS-Service, muss die Sicherheitsgruppe eingehenden HTTPS Datenverkehr zulassen.
- Wenn sich Ihre Ressourcen in einem Subnetz mit einem Netzwerk befindenACL, stellen Sie sicher, dass das Netzwerk den Verkehr zwischen den Ressourcen in Ihren VPC und den Netzwerkschnittstellen des Endpunkts ACL zulässt.
- Es gibt Kontingente für Ihre AWS PrivateLink Ressourcen. Weitere Informationen finden Sie unter AWS PrivateLink Kontingente.

VPC-Endpunkt erstellen

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

Um einen Schnittstellenendpunkt für einen zu erstellen AWS-Service

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Wählen Sie für Typ 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 die VPC aus VPC, von der aus Sie auf die zugreifen möchten AWS-Service.
7. Wenn Sie in Schritt 5 den Servicenamen für Amazon S3 ausgewählt haben und privaten DNS Support konfigurieren möchten, wählen Sie Zusätzliche Einstellungen, DNSName aktivieren aus. Wenn Sie diese Auswahl treffen, wird automatisch auch die Option DNSNur privat aktivieren für eingehenden Endpunkt ausgewählt. Sie können Private DNS mit einem Resolver-Endpunkt für eingehende Anrufe nur für Schnittstellenendpunkte für Amazon S3 konfigurieren. Wenn Sie keinen Gateway-Endpunkt für Amazon S3 haben und Private DNS nur für eingehenden Endpunkt aktivieren auswählen, erhalten Sie eine Fehlermeldung, wenn Sie den letzten Schritt in diesem Verfahren versuchen.

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

   Standardmäßig wählen wir IP-Adressen aus den Subnetz-IP-Adressbereichen aus und weisen sie den Endpunkt-Netzwerkschnittstellen zu. Um die IP-Adressen selbst auszuwählen, wählen Sie IP-Adressen festlegen aus. Beachten Sie, dass die ersten vier IP-Adressen und die letzte IP-Adresse in einem CIDR Subnetzblock 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 den Endpunkt-Netzwerkschnittstellen IPv4 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 Adressbereiche haben und der Dienst IPv4 Anfragen akzeptiert.
- IPv6— Weist den Endpunkt-Netzwerkschnittstellen IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv6 nur Subnetze sind und der Dienst Anfragen akzeptiertIPv6.
- Dualstack — Weisen Sie den IPv4 Endpunkt-Netzwerkschnittstellen sowohl als auch IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze sowohl als auch IPv6 Adressbereiche haben IPv4 und der Dienst sowohl Anfragen als auch IPv4 Anfragen akzeptiert. IPv6

10. Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppen aus, die den Security groups (Endpunkt-Netzwerkschnittstellen) zugeordnet werden sollen. Standardmäßig ordnen wir die Standardsicherheitsgruppe dem VPC zu.
11. Wählen Sie unter Richtlinie Vollzugriff aus, um alle Operationen aller Prinzipale auf allen Ressourcen über den Schnittstellenendpunkt zuzulassen. Um den Zugriff einzuschränken, wählen Sie Benutzerdefiniert aus und geben Sie eine Richtlinie ein. Diese Option ist nur verfügbar, wenn der Dienst 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

In Subnetzen, die mit Ihnen gemeinsam genutzt werden, können Sie keine VPC Endpoints erstellen, beschreiben, ändern oder löschen. Sie können die VPC Endpunkte jedoch in Subnetzen verwenden, die mit Ihnen gemeinsam genutzt werden.

ICMP

Schnittstellenendpunkte antworten nicht auf Anfragen. ping Sie können stattdessen die nmap Befehle nc oder verwenden.

Konfigurieren eines Schnittstellenendpunkts

Nachdem Sie einen VPC Schnittstellenendpunkt erstellt haben, können Sie dessen Konfiguration aktualisieren.

Aufgaben

- Hinzufügen oder Entfernen von Subnetzen
- Weisen Sie Sicherheitsgruppen zu
- Bearbeiten Sie die VPC Endpunktrichtlinie
- Aktivieren Sie private 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 VPC Amazon-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 IP-Adressen festlegen und geben Sie eine IPv4 Adresse aus dem Subnetz-Adressbereich ein. Wenn der Endpunktdienst dies unterstütztIPv6, 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 Endpunkt. VPC

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 Ihrem zur Endpunkt-Netzwerkschnittstelle zugelassen wirdVPC.

Ändern der Sicherheitsgruppen mithilfe der Konsole

1. Öffnen Sie die VPC Amazon-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 Sie die 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 VPC Amazon-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 Save (Speichern) aus.

So ändern Sie die Endpunktrichtlinie mithilfe der Befehlszeile

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

Aktivieren Sie private DNS Namen

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

Um private DNS Namen zu verwenden, müssen Sie sowohl die DNSHostnamen als auch die DNS Auflösung für Ihren aktivieren. VPC Nachdem Sie private DNS Namen aktiviert haben, kann es einige Minuten dauern, bis die privaten IP-Adressen verfügbar sind. Die DNS Datensätze, die wir erstellen, wenn Sie private DNS Namen aktivieren, sind privat. Daher ist der private DNS Name nicht öffentlich auflösbar.

Um die Option für private DNS Namen mithilfe der Konsole zu ändern

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Schnittstellenendpunkt.
4. Wählen Sie „Aktionen“, „DNSPrivatnamen 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 bei Auswahl von Enable for this Endpoint im vorherigen Schritt auch Enable Private DNS only for Inbound Endpoint aus. Wenn Sie die private DNS Standardfunktion bevorzugen, deaktivieren Sie die Option DNSNur privat für eingehenden Endpunkt aktivieren. Wenn Sie neben einem Schnittstellenendpunkt für Amazon S3 keinen Gateway-Endpunkt für Amazon S3 haben und Sie Private 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 “Privat DNS”.
7. Wählen Sie Save Changes (Änderungen speichern).

Um die Option für private DNS Namen über die Befehlszeile zu ändern

- 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 VPC Amazon-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 Save (Speichern) aus.

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

- Erstellen Sie eine SNS Benachrichtigung
- Eine Zugriffsrichtlinie hinzufügen
- Eine Schlüsselrichtlinie hinzufügen

Erstellen Sie eine SNS Benachrichtigung

Gehen Sie wie folgt vor, um ein SNS Amazon-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 VPC Amazon-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 unter Benachrichtigung ARN das 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-Benachrichtigung ()AWS CLI
- New-EC2VpcEndpointConnectionNotification(Tools für Windows PowerShell)

Eine Zugriffsrichtlinie hinzufügen

Fügen Sie dem SNS Amazon-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 SNS Amazon-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 AWS PrivateLink darauf vertrauen, dass AWS KMS API Operationen aufgerufen werden. 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 mit einem VPC Endpunkt fertig sind, 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 VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Schnittstellenendpunkt.
4. Wählen Sie Aktionen, VPCEndpunkte löschen aus.
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

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

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

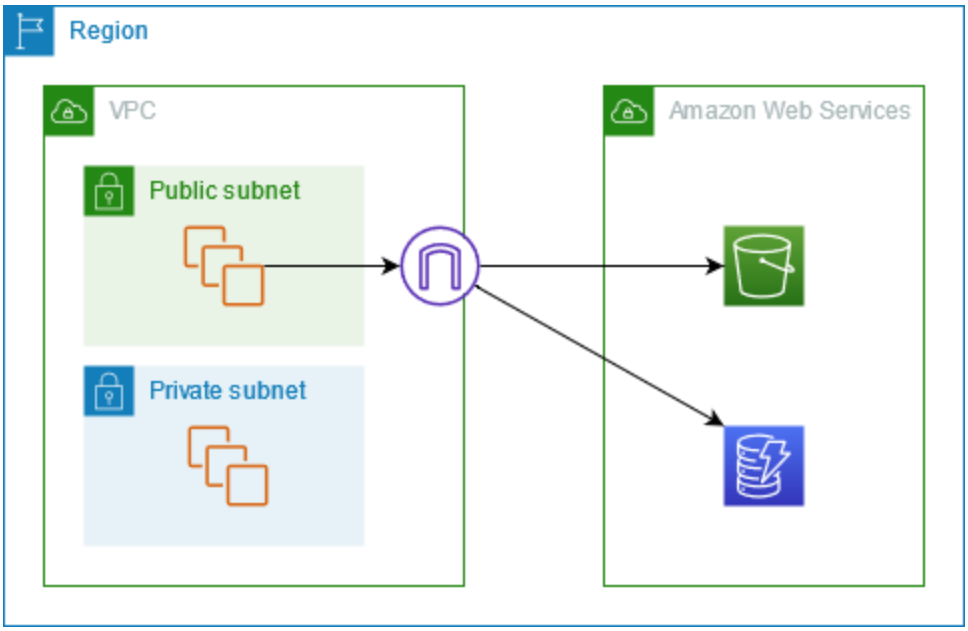
- Gateway-Endpunkte für Amazon DynamoDB

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

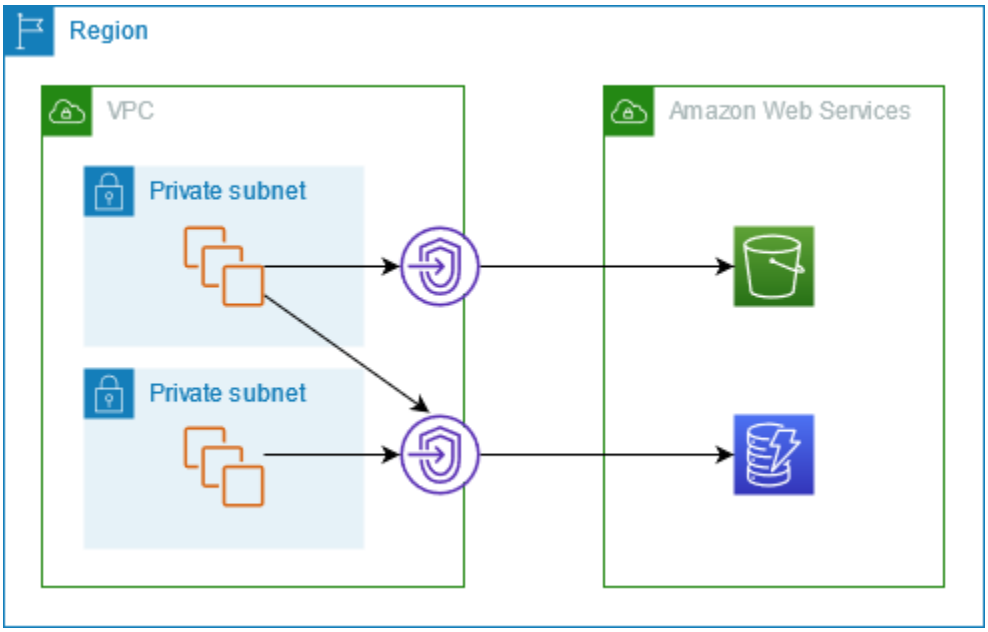
Das folgende Diagramm zeigt, wie Instances über ihre Endpunkte des öffentlichen Services auf Amazon S3 und DynamoDB zugreifen. Der Datenverkehr von einer Instance in einem öffentlichen Subnetz zu Amazon S3 oder DynamoDB wird an das Internet-Gateway für den VPC und dann an den Service weitergeleitet. 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 Traffic an Amazon S3 oder DynamoDB senden können, fügen Sie dem öffentlichen Subnetz ein NAT Gerät hinzu und leiten den Verkehr im privaten Subnetz an das Gerät weiter. NAT 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. Der Datenverkehr von Ihnen VPC zu Amazon S3 oder DynamoDB wird zum Gateway-Endpunkt weitergeleitet. 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 unter AWS-verwaltete Präfixlisten im VPCAmazon-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

Das Netzwerk ACLs für die Subnetze dieser Instances muss auch den Verkehr zum und vom Dienst zulassen. Es folgt ein Beispiel für eine Outbound-Regel. Sie können in ACL Netzwerkregeln nicht auf Präfixlisten verweisen, aber Sie können die IP-Adressbereiche 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 von Ihren VPC VPC Gateway-Endpunkten aus auf Amazon S3 zugreifen. Nachdem Sie den Gateway-Endpunkt erstellt haben, können Sie ihn als Ziel in Ihrer Routentabelle für den Datenverkehr hinzufügen, der von Ihnen 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 Ihrem aus auf Amazon S3 zugreifenVPC, ohne ein Internet-Gateway oder ein NAT Gerät für Sie zu benötigenVPC, und ohne zusätzliche Kosten. Gateway-Endpunkte erlauben jedoch keinen Zugriff über lokale Netzwerke, über Peering-Netzwerke 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 Arten von VPC Endpunkten für Amazon S3 im Amazon S3 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 DNS Amazon-Server verwenden, müssen Sie sowohl DNSHostnamen als auch DNS Auflösung für Ihre VPC aktivieren. Wenn Sie Ihren eigenen DNS Server verwenden, stellen Sie sicher, dass Anfragen an Amazon S3 korrekt an die IP-Adressen weitergeleitet werden, die von verwaltet werden AWS.
- 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.
- Das Netzwerk ACL für das Subnetz Ihrer Instances, die über einen Gateway-Endpunkt auf Amazon S3 zugreifen, muss den Datenverkehr von und zu Amazon S3 zulassen. Sie können in ACL Netzwerkregeln nicht auf Präfixlisten verweisen, aber Sie können den IP-Adressbereich für Amazon S3 aus der Präfixliste für Amazon S3 abrufen.
- Prüfen Sie, ob Sie einen verwenden AWS-Service , der Zugriff auf einen S3-Bucket benötigt. Beispielsweise benötigt ein Dienst möglicherweise Zugriff auf Buckets, die Protokolldateien enthalten, oder Sie müssen möglicherweise Treiber oder Agenten für 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 `aws:SourceIp` Bedingung nicht in einer Identitätsrichtlinie oder einer Bucket-Richtlinie für Anfragen an Amazon S3 verwenden, die einen VPC Endpunkt durchlaufen. Verwenden Sie stattdessen die Bedingung `aws:VpcSourceIp`. Alternativ können Sie Routing-Tabellen verwenden, um zu steuern, welche EC2 Instances über den VPC Endpunkt auf Amazon S3 zugreifen können.
- Gateway-Endpunkte unterstützen nur IPv4 Datenverkehr.
- Die IPv4 Quelladressen von Instances in Ihren betroffenen Subnetzen, die von Amazon S3 empfangen wurden, ändern sich von öffentlichen IPv4 Adressen zu privaten IPv4 Adressen in IhrenVPC. Ein Endpunkt wechselt die Netzwerkrouten und trennt offene TCP Verbindungen. Die vorherigen Verbindungen, für die öffentliche IPv4 Adressen verwendet wurden, werden nicht wieder aufgenommen. 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 von einem VPC aus erweitert werden. Ressourcen auf der anderen Seite einer Verbindung, einer VPN VPC Peering-Verbindung, eines Transit-Gateways

oder einer AWS Direct Connect Verbindung in Ihrem 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. Es gibt auch ein Limit von 255 Gateway-Endpunkten pro. VPC

Privat DNS

Sie können Private konfigurierenDNS, um die Kosten zu optimieren, wenn Sie sowohl einen Gateway-Endpunkt als auch einen Schnittstellen-Endpunkt für Amazon S3 erstellen.

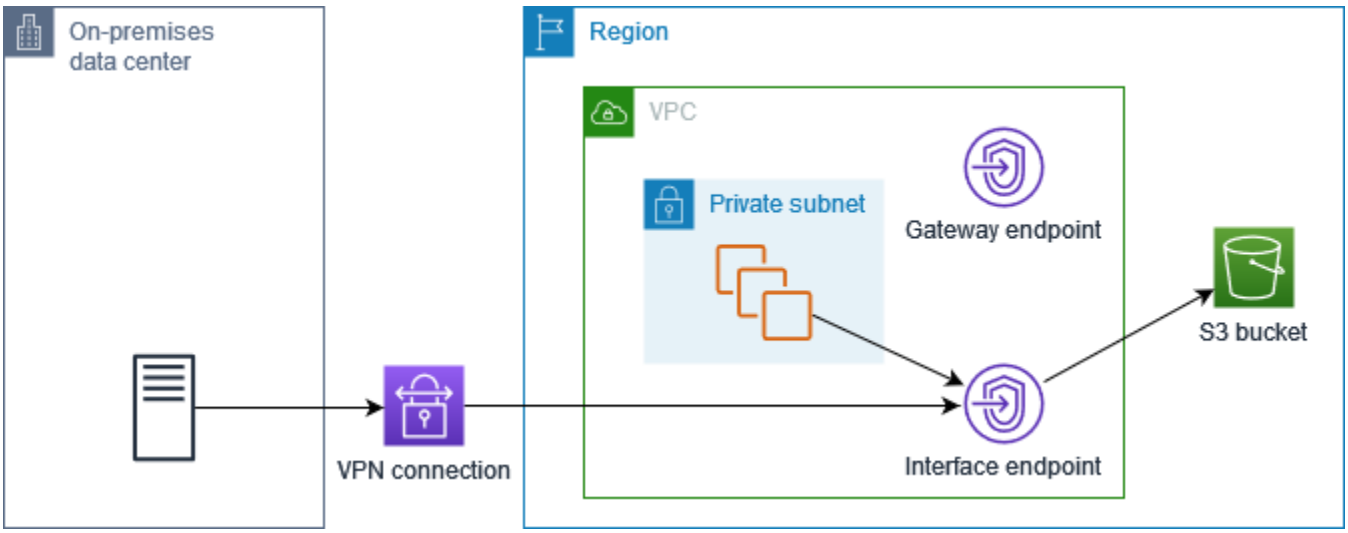
Route 53 Resolver

Amazon stellt Ihnen einen DNS Server namens Route 53 Resolver zur VerfügungVPC. Der Route 53 Resolver löst automatisch lokale VPC Domainnamen und Datensätze in privaten Hosting-Zonen auf. Sie können den Route 53 Resolver jedoch nicht von außerhalb Ihres verwenden. VPC Route 53 bietet Resolver-Endpunkte und Resolver-Regeln, sodass Sie den Route 53 Resolver von außerhalb Ihres verwenden können. VPC Ein eingehender Resolver-Endpunkt leitet DNS Anfragen vom lokalen Netzwerk an den Route 53 Resolver weiter. Ein ausgehender Resolver-Endpunkt leitet DNS Anfragen vom Route 53 Resolver an das lokale Netzwerk weiter.

Wenn Sie Ihren Schnittstellenendpunkt für Amazon S3 so konfigurieren, dass Private DNS nur für den eingehenden Resolver-Endpunkt verwendet wird, erstellen wir einen Resolver-Endpunkt für eingehende Anrufe. Der Inbound-Resolver-Endpunkt löst DNS Anfragen an Amazon S3 von lokalen Standorten an die privaten IP-Adressen des Schnittstellenendpunkts auf. Wir fügen auch ALIAS Datensätze für den Route 53 Resolver zur öffentlich gehosteten Zone für Amazon S3 hinzu, sodass DNS Anfragen von Ihnen VPC an die öffentlichen IP-Adressen von Amazon S3 weitergeleitet werden, die den Datenverkehr an den Gateway-Endpunkt weiterleiten.

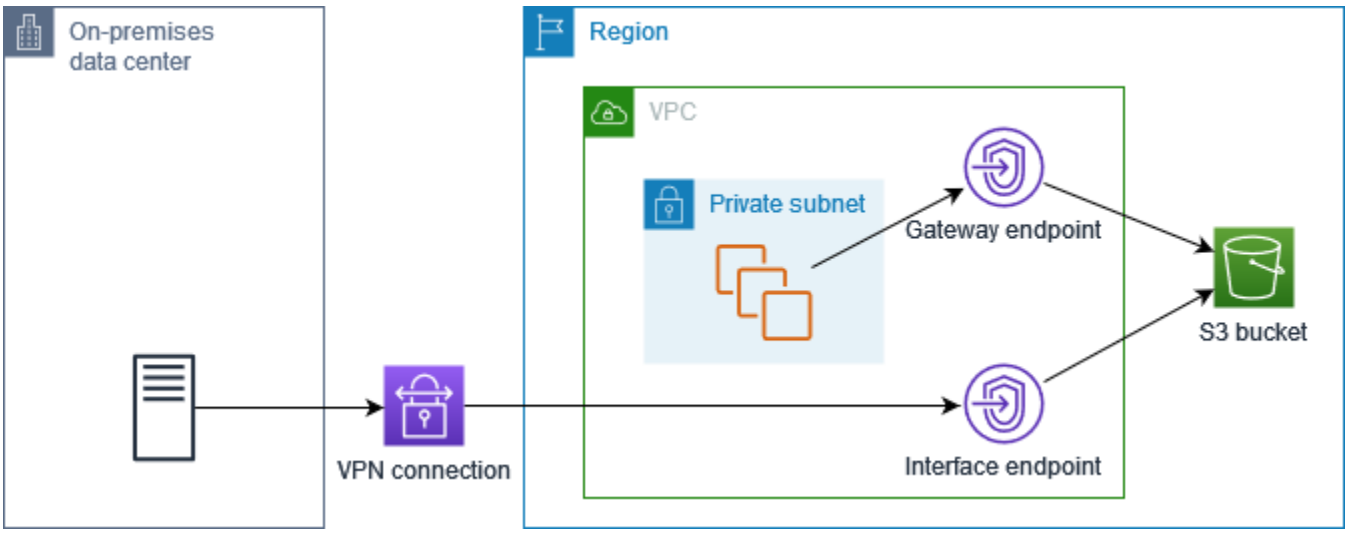
Privat DNS

Wenn Sie privat DNS für Ihren Schnittstellenendpunkt für Amazon S3 konfigurieren, aber nicht DNS nur privat für den eingehenden Resolver-Endpunkt konfigurieren, VPC verwenden Anfragen sowohl von Ihrem lokalen Netzwerk als auch von Ihnen den Schnittstellenendpunkt, um auf Amazon S3 zuzugreifen. Daher zahlen Sie für die Nutzung des Schnittstellenendpunkts für den Datenverkehr vomVPC, anstatt den Gateway-Endpunkt ohne zusätzliche Kosten zu verwenden.



DNSNur privat für den eingehenden Resolver-Endpunkt

Wenn Sie privat DNS nur für den eingehenden Resolver-Endpunkt konfigurieren, verwenden Anfragen aus Ihrem lokalen Netzwerk den Schnittstellenendpunkt, um auf Amazon S3 zuzugreifen, und Anfragen von Ihnen 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.



Privat konfigurieren DNS

Sie können privat 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 “VPC-Endpunkt erstellen” (während der Erstellung konfigurieren) oder the section called “Aktivieren Sie private 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 VPC Amazon-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*.s3.
6. Wählen Sie für den aus VPC, VPC in dem 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 Richtlinie die Option Vollzugriff aus, um alle Operationen aller Prinzipale auf allen Ressourcen über den VPC Endpunkt zuzulassen. Wählen Sie andernfalls Benutzerdefiniert aus, um eine VPC Endpunktrichtlinie anzuhängen, die die Berechtigungen steuert, die Prinzipale haben, um Aktionen an Ressourcen über den VPC Endpunkt auszuführen.
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 EndpunktenVPCs, 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

Mithilfe des Bedingungsschlüssels aws: sourceVpce können Sie eine Bucket-Richtlinie erstellen, die den Zugriff auf einen bestimmten Endpunkt einschränkt. 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 Sie den Zugriff auf einen bestimmten VPC

Mithilfe des sourceVpc Bedingungsschlüssels aws: können Sie eine Bucket-Richtlinie erstellen, die den Zugriff auf bestimmte VPCs Bereiche beschränkt. Dies ist nützlich, wenn Sie mehrere Endpunkte auf demselben konfiguriert haben. VPC Die folgende Richtlinie verweigert den Zugriff auf den angegebenen Bucket mithilfe der angegebenen Aktionen, es sei denn, die Anfrage stammt aus dem angegebenen Bucket. 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 VpcSourceIp Bedingungsschlüssels aws: 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 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 VPC Amazon-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 Sie die VPC Endpunktrichtlinie

Sie können die Endpunktrichtlinie für einen Gateway-Endpunkt bearbeiten, der den Zugriff auf Amazon S3 von VPC bis zum 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 VPC Amazon-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 Ihrem System habenVPC, 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 Sie den Zugriff auf eine bestimmte Rolle IAM

Sie können eine Richtlinie erstellen, die den Zugriff auf eine bestimmte IAM Rolle einschränkt. 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.

Sie können einen Gateway-Endpunkt nicht löschen, wenn Private aktiviert DNS ist.

So löschen Sie ein Gateway-Endpunkt mithilfe der Konsole

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Erstellen des Gateway-Endpunkts.
4. Wählen Sie „Aktionen“, „VPCEndpunkte 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 von Ihren VPC verwendeten VPC Gateway-Endpunkten aus auf Amazon DynamoDB zugreifen. Nachdem Sie den Gateway-Endpunkt erstellt haben, können Sie ihn in Ihrer Routentabelle als Ziel für den Datenverkehr hinzufügen, der von Ihnen 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 Ihrem aus auf DynamoDB zugreifenVPC, ohne ein Internet-Gateway oder ein NAT Gerät für Sie zu benötigenVPC, und ohne zusätzliche Kosten. Gateway-Endpunkte ermöglichen jedoch keinen Zugriff über lokale Netzwerke, über Peering-Netzwerke 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 DNS Amazon-Server verwenden, müssen Sie sowohl DNSHostnamen als auch DNS Auflösung für Ihre VPC aktivieren. Wenn Sie Ihren eigenen DNS Server verwenden, stellen Sie sicher, dass Anfragen an DynamoDB korrekt an die IP-Adressen weitergeleitet werden, die von verwaltet werden. AWS
- 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.

- Das 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 ACL Netzwerkregeln nicht auf Präfixlisten verweisen, aber Sie können den IP-Adressbereich für DynamoDB aus der Präfixliste für DynamoDB abrufen.
- Wenn Sie AWS CloudTrail DynamoDB-Operationen protokollieren, enthalten die Protokolldateien die privaten IP-Adressen der EC2 Instanzen im Service Consumer VPC und die ID des Gateway-Endpunkts für alle Anfragen, die über den Endpunkt ausgeführt werden.
- Gateway-Endpunkte unterstützen nur Datenverkehr. IPv4
- Die IPv4 Quelladressen von Instances in Ihren betroffenen Subnetzen ändern sich von öffentlichen IPv4 Adressen zu privaten IPv4 Adressen von Ihren. VPC Ein Endpunkt wechselt die Netzwerkrouten und trennt offene TCP Verbindungen. Die vorherigen Verbindungen, für die öffentliche IPv4 Adressen verwendet wurden, werden nicht wieder aufgenommen. 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 von einem VPC aus erweitert werden. Ressourcen auf der anderen Seite einer VPN Verbindung, VPC Peering-Verbindung, eines Transit-Gateways oder einer AWS Direct Connect Verbindung in Ihrem 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. Es gibt auch ein Limit von 255 Gateway-Endpunkten pro. VPC

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 VPC Amazon-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 den aus VPC, VPC in dem 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 Richtlinie die Option Vollzugriff aus, um alle Operationen aller Prinzipale auf allen Ressourcen über den VPC Endpunkt zuzulassen. Wählen Sie andernfalls Benutzerdefiniert aus, um eine VPC Endpunktrichtlinie anzuhängen, die die Berechtigungen steuert, die Prinzipale haben, um Aktionen an Ressourcen über den VPC Endpunkt auszuführen.
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)

Steuern Sie den Zugriff mithilfe von IAM Richtlinien

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

Example Beispiel: Beschränken des Zugriffs auf einen bestimmten Endpunkt

Mithilfe des Bedingungsschlüssels aws: können Sie eine Richtlinie erstellen, die den Zugriff auf einen bestimmten VPC Endpunkt einschränkt. sourceVpce 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",
         "Principal": "*",
```

```
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:region:account-id:table/*",
         "Condition": {
            "StringNotEquals" : {
               "aws:sourceVpce": "vpce-11aa22bb"
            }
         }
      }
   ]
}
```

Example Beispiel: Zugriff von einer bestimmten Rolle aus zulassen IAM

Sie können eine Richtlinie erstellen, die den Zugriff über eine bestimmte IAM Rolle ermöglicht. 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 VPC Amazon-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 Sie die VPC Endpunktrichtlinie

Sie können die Endpunktrichtlinie für einen Gateway-Endpunkt bearbeiten, die den Zugriff auf DynamoDB von VPC bis zum 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 VPC Amazon-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 VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Erstellen des Gateway-Endpunkts.
4. Wählen Sie „Aktionen“, „VPCEndpunkte 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 Ihren eigenen laufen würdenVPC.

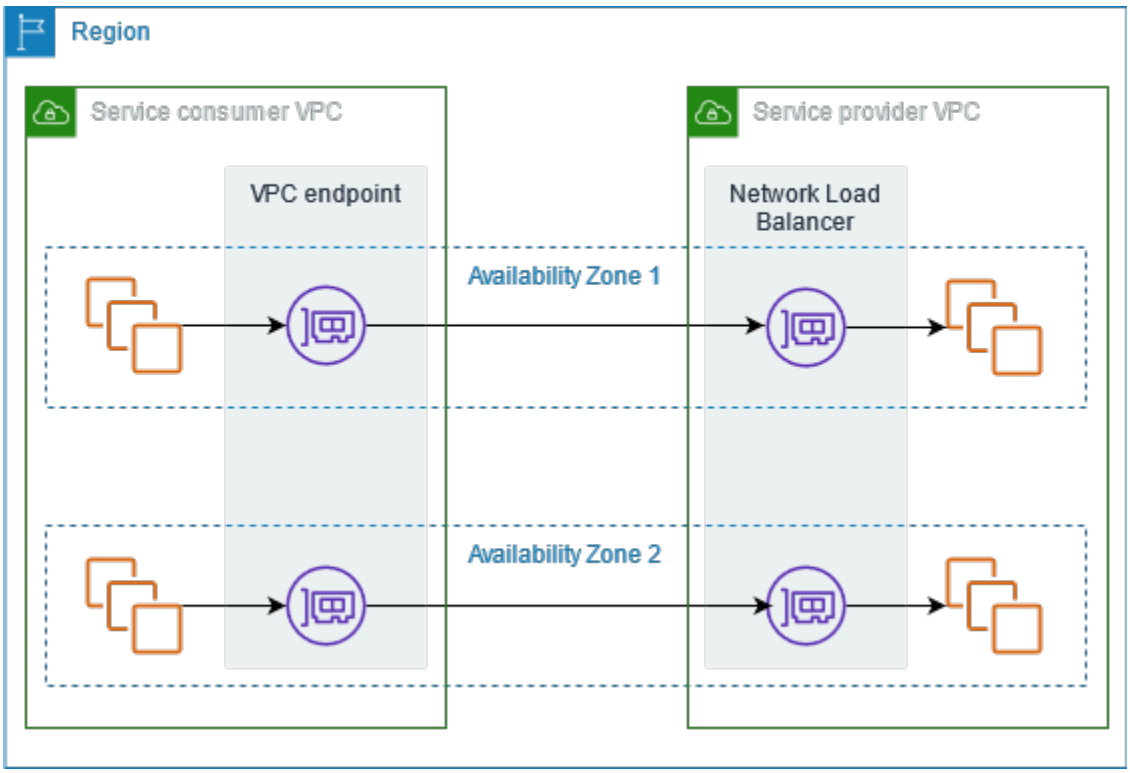
Inhalt

Übersicht

Sie können SaaS-Produkte, die von bereitgestellt werden, entdecken, kaufen und AWS PrivateLink bereitstellen AWS Marketplace. Weitere Informationen finden Sie unter Sicher und privat auf SaaS-Anwendungen zugreifen AWS 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 zu SaaS-Produkten herzustellen. Der Service-Anbieter erstellt einen Endpunkt-Service und gewährt seinen Kunden Zugriff auf den Endpunkt-Service. Als Servicekonsument erstellen Sie einen VPC Schnittstellenendpunkt, der Verbindungen zwischen einem oder mehreren Subnetzen in Ihrem VPC und dem Endpunktdienst herstellt.



Erstellen eines Schnittstellenendpunkts

Gehen Sie wie folgt vor, um einen VPC Schnittstellenendpunkt zu erstellen, der eine Verbindung zum SaaS-Produkt herstellt.

Anforderung

Den Service abonnieren.

So erstellen Sie einen Schnittstellenendpunkt zu einem Partnerservice

1. Öffnen Sie die VPC Amazon-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 für Typ die Option AWS Marketplace Dienste aus.
   b. Wählen Sie den Dienst aus.
5. Wenn Sie einen Dienst mit der Bezeichnung AWS Service Ready abonniert haben, gehen Sie wie folgt vor:

   a. Wählen Sie als Typ die Option PrivateLink Ready Partner Services aus.
   b. Geben Sie den Namen des Dienstes ein und wählen Sie dann Dienst verifizieren aus.
6. Wählen Sie für die Option VPC aus VPC, von der aus Sie auf das Produkt zugreifen möchten.
7. Wählen Sie unter Subnetze die Subnetze aus, in denen Netzwerkschnittstellen für Endpunkte erstellt werden sollen.
8. Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppen aus, die den Security groups (Endpunkt-Netzwerkschnittstellen) zugeordnet werden sollen. Die Sicherheitsgruppenregeln müssen den Verkehr zwischen den Ressourcen in den Netzwerkschnittstellen VPC und den Endpunkt-Netzwerkschnittstellen 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”.

Zugriff auf virtuelle Appliances 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 Endpunktdienst erstellen. Sonstige AWS -Prinzipale greifen auf den Endpunkt-Service zu, indem sie einen Gateway-Load-Balancer-Endpunkt.

Preisgestaltung

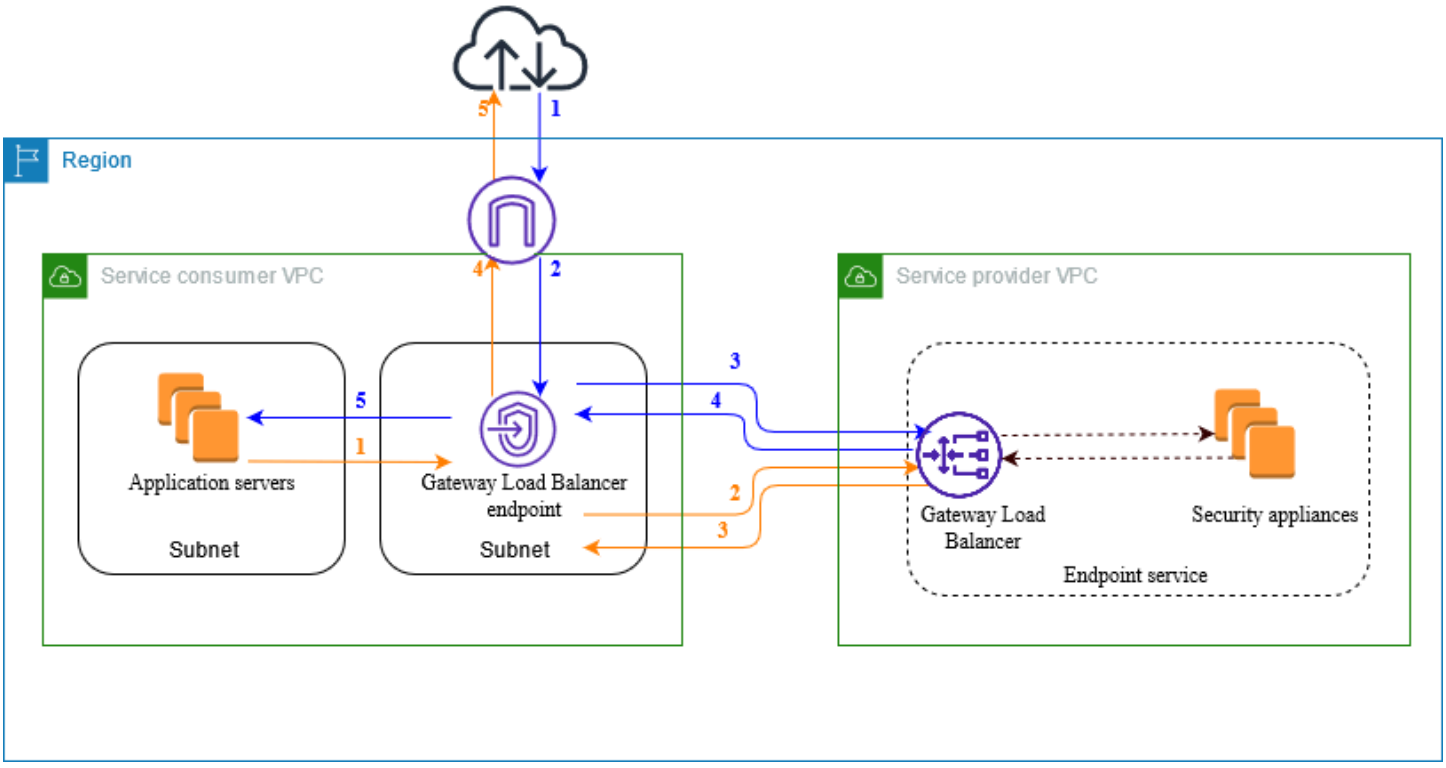
Ihnen wird jede Stunde in Rechnung gestellt, in der Ihr Gateway Load Balancer-Endpunkt in jeder Availability Zone bereitgestellt wird. Ihnen wird auch pro GB verarbeiteter Daten in Rechnung gestellt. Weitere Informationen finden Sie unter AWS PrivateLink -Preisgestaltung.

Inhalt

Weitere Informationen finden Sie unter Gateway Load Balancer.

Übersicht

Das folgende Diagramm zeigt, wie Anwendungsserver auf Sicherheits-Appliances zugreifen AWS PrivateLink. Die Anwendungsserver laufen in einem Subnetz des Service ConsumerVPC. Sie erstellen einen Gateway Load Balancer-Endpunkt in einem anderen Subnetz desselben. VPC Der gesamte Datenverkehr, der VPC über das Internet-Gateway an den Service Consumer gelangt, wird zunächst zur Überprüfung an den Gateway Load Balancer-Endpunkt und dann an das Zielsubnetz weitergeleitet. 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 VPC über das Internet-Gateway zum Servicenutzer.
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

Dienstanbieter können ihre Dienstendpunkte den Servicenutzern überIPv4, oder beides IPv6IPv4, zur Verfügung stellenIPv6, auch wenn ihre Sicherheitsanwendungen nur IPv4 Support bieten. Wenn Sie den Dual-Stack-Support aktivieren, können bestehende Kunden weiterhin auf Ihren Service zugreifenIPv4, und neue Kunden können sich dafür entscheiden, Ihren Service IPv6 zu nutzen.

Wenn ein Gateway Load Balancer-Endpunkt dies unterstütztIPv4, haben die Netzwerkschnittstellen des Endpunkts IPv4 Adressen. Wenn ein Gateway Load Balancer-Endpunkt dies unterstütztIPv6, haben die Netzwerkschnittstellen des Endpunkts IPv6 Adressen. Die IPv6 Adresse für eine Endpunkt-Netzwerkschnittstelle ist vom Internet aus nicht erreichbar. Wenn Sie eine Endpunkt-Netzwerkschnittstelle mit einer IPv6 Adresse beschreiben, beachten Sie, dass diese aktiviert `denyAllIgwTraffic` ist.

Voraussetzungen IPv6 für die Aktivierung eines Endpunktdienstes

- Den Subnetzen VPC und für den Endpunktdienst müssen IPv6 CIDR Blöcke zugeordnet sein.
- Der Gateway-Load-Balancer für den Endpunktservice muss den IP-Adresstyp Dualstack verwenden. Die Sicherheits-Appliances müssen den IPv6 Datenverkehr nicht unterstützen.

Anforderungen zur Aktivierung IPv6 für einen Gateway Load Balancer Balancer-Endpunkt

- Der Endpunktdienst 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 IPv4 Adressbereiche haben.
  - IPv6— Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv6 nur Subnetze sind.

  - Dualstack — Weisen Sie Ihren IPv4 Endpunkt-Netzwerkschnittstellen sowohl IPv6 Adressen als auch Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 sowohl IPv6 als auch Adressbereiche haben.
- Die Routing-Tabellen für die Subnetze im Service Consumer VPC müssen den IPv6 Verkehr weiterleiten, und das Netzwerk ACLs für diese Subnetze muss Verkehr zulassen. IPv6

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 Dual-Stack-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
Application subnet IPv4 CIDR	*vpc-endpoint-id*
Application subnet 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

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. Sie können AZ verwendenIDs, um die Availability Zones für Ihren Service konsistent zu identifizieren. Weitere Informationen finden Sie unter AZ IDs im EC2Amazon-Benutzerhandbuch.
- Es gibt Kontingente für Ihre AWS PrivateLink Ressourcen. Weitere Informationen finden Sie unter AWS PrivateLink Kontingente.

Voraussetzungen

- Erstellen Sie einen Dienstanbieter VPC mit mindestens zwei Subnetzen in der Availability Zone, in der der Service verfügbar sein sollte. Ein Subnetz ist für die Security-Appliance-Instances und das andere für den Gateway Load Balancer vorgesehen.
- Erstellen Sie einen Gateway Load Balancer in Ihrem Service ProviderVPC. Wenn Sie die IPv6 Unterstützung für Ihren Endpoint Service aktivieren möchten, müssen Sie die Dual-Stack-Unterstützung auf Ihrem Gateway Load Balancer aktivieren. Weitere Informationen finden Sie unter Erste Schritte mit Gateway Load Balancern.
- Starten Sie Sicherheits-Appliances im Service Provider 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 VPC Amazon-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 Endpunktservice für die Annahme von IPv4 Anfragen.
   - Wählen IPv6— Ermöglichen Sie dem Endpunktdienst die Annahme von IPv6 Anfragen.
   - Wählen Sie IPv4und IPv6— Aktivieren Sie den Endpunktdienst so, dass er IPv4 sowohl als auch IPv6 Anfragen akzeptiert.
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 Create (Erstellen) aus.

So erstellen Sie einen Endpunktservice unter Verwendung der Befehlszeile

- create-vpc-endpoint-service-Konfiguration ()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 Ihrem angebenVPC, 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 im Service Consumer nur eine Availability Zone auswählen. VPC 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. Sie können AZ verwendenIDs, um die Availability Zones für Ihren Service konsistent zu identifizieren. Weitere Informationen finden Sie unter AZ IDs im EC2Amazon-Benutzerhandbuch.
- Bevor Sie den Endpunkt-Service verwenden können, muss der Service-Anbieter die Verbindungsanforderungen akzeptieren. Der Service kann VPC über den VPC Endpunkt keine Anfragen an Ressourcen in Ihrem System initiieren. Der Endpunkt gibt nur Antworten auf Datenverkehr zurück, der durch Ressourcen in Ihrem ausgelöst wurdeVPC.
- 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-Erhaltung des Network Load Balancer-Clients wird nicht unterstützt, wenn der Datenverkehr über einen Gateway Load Balancer-Endpunkt geleitet wird, auch wenn sich das Ziel im selben Verzeichnis befindet VPC wie der Network Load Balancer.
- Wenn sich die Anwendungsserver und der Gateway Load Balancer-Endpunkt im selben Subnetz befinden, werden die NACL Regeln für den Datenverkehr von den Anwendungsservern zum Gateway Load Balancer-Endpunkt ausgewertet.
- Wenn Sie einen Gateway Load Balancer mit einem Internet-Gateway nur für ausgehenden Datenverkehr verwenden, wird der IPv6 Datenverkehr unterbrochen. Verwenden Sie stattdessen ein Internet-Gateway und Firewallregeln für eingehenden Datenverkehr.
- Es gibt Kontingente für Ihre AWS PrivateLink Ressourcen. Weitere Informationen finden Sie unter AWS PrivateLink Kontingente.

Voraussetzungen

- Erstellen Sie einen Service-Consumer 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 Endpunktdienst unterstützt werden, beschreiben Sie den Endpunktdienst mithilfe der Konsole oder des describe-vpc-endpoint-servicesBefehls.
- Wenn sich Ihre Ressourcen in einem Subnetz mit einem Netzwerk befinden, stellen Sie sicherACL, dass das Netzwerk den Datenverkehr zwischen den Netzwerkschnittstellen der Endpunkte und den Ressourcen in der ACL 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 VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Wählen Sie als Typ die Option Endpunktdienste, die NLBs und verwenden GWLBs.
5. Geben Sie für Service Name (Servicename) den Namen des Service ein und wählen Sie Verify service (Service überprüfen) aus.
6. Wählen Sie für die Option VPC aus VPC, von der aus Sie auf den Endpunktdienst zugreifen möchten.
7. Wählen Sie für Subnetze ein Subnetz aus, in dem Sie eine Endpunkt-Netzwerkschnittstelle erstellen möchten.
8. Wählen Sie für IP address type (IP-Adressentyp) eine der folgenden Optionen aus:
   - IPv4— Weisen Sie der Endpunkt-Netzwerkschnittstelle IPv4 Adressen zu. Diese Option wird nur unterstützt, wenn das ausgewählte Subnetz über einen IPv4 Adressbereich verfügt.
   - IPv6— Weist der Endpunkt-Netzwerkschnittstelle IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn das ausgewählte Subnetz ein IPv6 reines Subnetz ist.

- Dualstack — Weisen Sie der Netzwerkschnittstelle des IPv4 Endpunkts beide IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn das ausgewählte Subnetz IPv4 sowohl IPv6 als auch Adressbereiche hat.

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 den Service Consumer zu konfigurierenVPC. 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 VPC Amazon-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 dies unterstützenIPv4, wählen Sie Route hinzufügen. Geben Sie als Ziel den IPv4 CIDR Block des Subnetzes für die Anwendungsserver ein. Wählen Sie für Target den VPC Endpunkt aus.

   c. Wenn Sie dies unterstützenIPv6, wählen Sie Route hinzufügen. Geben Sie als Ziel den IPv6 CIDR Block des Subnetzes für die Anwendungsserver ein. Wählen Sie für Target 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 dies unterstützenIPv4, wählen Sie Route hinzufügen. Geben Sie für Destination **`0.0.0.0/0`** ein. Wählen Sie für Target den VPC Endpunkt aus.

   c. Wenn Sie dies unterstützenIPv6, wählen Sie Route hinzufügen. Geben Sie für Destination **`::/0`** ein. Wählen Sie für Target 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 dies unterstützenIPv4, wählen Sie Route hinzufügen. Geben Sie für Destination **`0.0.0.0/0`** ein. Wählen Sie für Target (Ziel) das Internet-Gateway aus.

   c. Wenn Sie dies unterstützenIPv6, wählen Sie Route hinzufügen. Geben Sie für Destination **`::/0`** ein. Wählen Sie für Target (Ziel) das Internet-Gateway aus.

   d. Wählen Sie Änderungen speichern.

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 VPC Amazon-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 Save (Speichern) aus.

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 VPC Amazon-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)

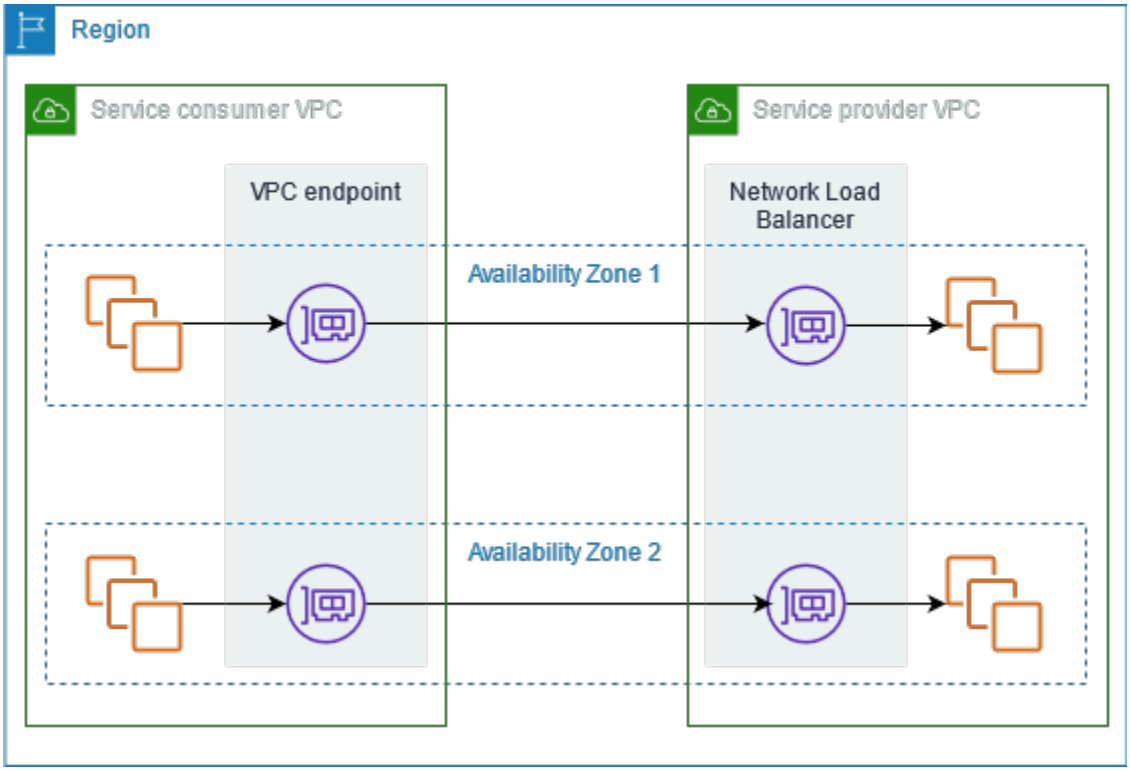
Teilen Sie Ihre Dienste über AWS PrivateLink

Sie können Ihren eigenen Dienst AWS PrivateLink , den so genannten 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 Dienstanbieter erstellen Sie einen Network Load Balancer in Ihrem VPC 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 Servicenutzer erstellt der Kunde einen VPC Schnittstellenendpunkt, der Verbindungen zwischen den Subnetzen, die er aus seinem Dienst auswählt, VPC und Ihrem Endpunktdienst 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.

DNSHostnamen

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
```

Im Folgenden finden Sie ein Beispiel für einen DNS Hostnamen für einen VPC Endpunktdienst in der Region us-east-2:

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

Wenn ein Dienstnutzer einen VPC Schnittstellenendpunkt erstellt, erstellen wir regionale und zonale DNS Namen, die der Dienstnutzer für die Kommunikation mit dem Endpunktdienst verwenden kann. Regionale Namen haben die folgende Syntax:

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

Zonale Namen haben die folgende Syntax:

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

Privat DNS

Ein Dienstanbieter kann seinem Endpunktdienst auch einen privaten DNS Namen zuweisen, sodass Dienstnutzer weiterhin mit seinem bestehenden DNS Namen auf den Dienst zugreifen können. Wenn ein Dienstanbieter seinem Endpunktdienst einen privaten DNS Namen zuordnet, können Dienstnutzer private DNS Namen für ihre Schnittstellenendpunkte aktivieren. Wenn ein Dienstanbieter private Dienste nicht aktiviertDNS, müssen Dienstnutzer möglicherweise ihre Anwendungen aktualisieren, sodass sie den öffentlichen DNS Namen des VPC Endpunktdienstes verwenden. Weitere Informationen finden Sie unter DNSNamen verwalten.

Regionsübergreifender Zugriff

Ein Dienstanbieter kann einen Dienst in einer Region hosten und ihn in einer Reihe unterstützter Regionen verfügbar machen. Ein Servicenutzer wählt bei der Erstellung eines Endpunkts eine Dienstregion aus.

Berechtigungen

- Standardmäßig sind IAM Entitäten nicht berechtigt, einen Endpunktdienst in mehreren Regionen verfügbar zu machen oder regionsübergreifend auf einen Endpunktdienst zuzugreifen. Um die für den regionsübergreifenden Zugriff erforderlichen Berechtigungen zu gewähren, kann ein IAM Administrator IAM Richtlinien erstellen, die diese Aktion nur mit `vpce:AllowMultiRegion` Berechtigungen zulassen.
- Verwenden Sie den Bedingungsschlüssel, um die Regionen zu steuern, die eine IAM Entität bei der Erstellung eines Endpunktdienstes als unterstützte Region angeben kann. `ec2:VpceSupportedRegion`
- Verwenden Sie den `ec2:VpceServiceRegion` Bedingungsschlüssel, um die Regionen zu steuern, die eine IAM Entität bei der Erstellung eines VPC Endpunkts als Dienstregion angeben kann.

Überlegungen

- Ein Dienstanbieter muss sich für eine Opt-in-Region entscheiden, bevor er sie als unterstützte Region für einen Endpunktdienst hinzufügen kann.
- Ihr Endpunktdienst muss von seiner Hostregion aus zugänglich sein. Sie können die Hostregion nicht aus der Gruppe der unterstützten Regionen entfernen. Aus Redundanzgründen können Sie Ihren Endpunktdienst in mehreren Regionen bereitstellen und den regionsübergreifenden Zugriff für jeden Endpunktdienst aktivieren.
- Ein Servicenutzer muss sich für eine Opt-in-Region entscheiden, bevor er sie als Service-Region für einen Endpunkt auswählen kann. Wann immer möglich, empfehlen wir, dass Servicenutzer über regionsinterne Konnektivität statt über regionsübergreifende Konnektivität auf einen Dienst zugreifen. Die Konnektivität innerhalb der Region sorgt für eine geringere Latenz und geringere Kosten.
- Wenn ein Dienstanbieter eine Region aus der Gruppe der unterstützten Regionen entfernt, können Servicekunden diese Region nicht als Dienstregion auswählen, wenn sie neue Endpunkte erstellen. Beachten Sie, dass dies den Zugriff auf den Endpunktdienst von bestehenden Endpunkten aus, die diese Region als Dienstregion verwenden, nicht beeinträchtigt.
- Für eine hohe Verfügbarkeit sollten sowohl Anbieter als auch Verbraucher mindestens zwei Availability Zones verwenden. Beachten Sie, dass für den regionsübergreifenden Zugriff nicht erforderlich ist, dass Anbieter und Verbraucher dieselben Availability Zones verwenden.
- AWS PrivateLink Verwaltet mit regionsübergreifendem Zugriff den Failover zwischen Availability Zones. Es verwaltet kein regionsübergreifendes Failover.
- Der regionsübergreifende Zugriff wird für AWS Marketplace Dienste mit einem benutzerfreundlichen DNS Namen nicht unterstützt.
- Der regionsübergreifende Zugriff wird für Network Load Balancer nicht unterstützt, bei denen ein benutzerdefinierter Wert für das Timeout im TCP Leerlauf konfiguriert ist.
- Regionsübergreifender Zugriff wird bei Fragmentierung nicht unterstützt. UDP

IP-Adresstypen

Dienstanbieter können ihre Dienstendpunkte Servicenutzern überIPv4, oder beides IPv6IPv4, zur Verfügung stellenIPv6, auch wenn ihre Backend-Server nur Support bieten. IPv4 Wenn Sie die Dual-Stack-Unterstützung aktivieren, können bestehende Kunden weiterhin auf Ihren Service zugreifenIPv4, und neue Kunden können sich dafür entscheiden, Ihren Service IPv6 zu nutzen.

Wenn ein VPC Schnittstellenendpunkt dies unterstütztIPv4, haben IPv4 die Endpunkt-Netzwerkschnittstellen Adressen. Wenn ein VPC Schnittstellenendpunkt diese unterstütztIPv6, haben die Endpunkt-Netzwerkschnittstellen IPv6 Adressen. Die IPv6 Adresse für eine Endpunkt-Netzwerkschnittstelle ist vom Internet aus nicht erreichbar. Wenn Sie eine Endpunkt-Netzwerkschnittstelle mit einer IPv6 Adresse beschreiben, beachten Sie, dass diese aktiviert `denyAllIgwTraffic` ist.

Voraussetzungen IPv6 für die Aktivierung eines Endpunktdienstes

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

Voraussetzungen für die Aktivierung IPv6 für einen Schnittstellenendpunkt

- Der Endpunktdienst 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 IPv4 Adressbereiche haben.
  - IPv6— Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv6 nur Subnetze sind.
  - Dualstack — Weisen Sie Ihren IPv4 Endpunkt-Netzwerkschnittstellen sowohl IPv6 Adressen als auch Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 sowohl IPv6 als auch Adressbereiche haben.

DNSden IP-Adresstyp für einen Schnittstellenendpunkt aufzeichnen

Der DNS Datensatz-IP-Adresstyp, den ein Schnittstellenendpunkt unterstützt, bestimmt die DNS Datensätze, die wir erstellen. Der DNS Datensatz-IP-Adresstyp eines Schnittstellenendpunkts muss mit dem IP-Adresstyp des Schnittstellenendpunkts kompatibel sein, wie hier beschrieben:

- IPv4— Erstellen Sie A-Einträge für die privaten, regionalen und zonalen DNS Namen. Der IP-Adresstyp muss IPv4oder Dualstack sein.

- IPv6— Erstellen Sie AAAA Datensätze für die privaten, regionalen und DNS zonalen Namen. Der IP-Adresstyp muss IPv6oder Dualstack sein.
- Dualstack — Erstellen Sie A und AAAA Datensätze für die privaten, regionalen und zonalen Namen. DNS 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. Verbraucher können von anderen Regionen aus auf Ihren Dienst zugreifen, wenn Sie den regionsübergreifenden Zugriff aktivieren oder wenn sie VPC Peering oder ein Transit-Gateway verwenden.
- 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. Sie können AZ verwendenIDs, um die Availability Zones für Ihren Service konsistent zu identifizieren. Weitere Informationen finden Sie unter AZ IDs im EC2Amazon-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 Proxy-Protokoll auf dem Load Balancer aktivieren, können Sie die Adressen der Service-Verbraucher und der Schnittstellen-Endpunkte IDs aus dem Proxy-Protokoll-Header abrufen. Weitere Informationen finden Sie unter Proxy-Protokoll im Benutzerhandbuch für Network Load Balancers.
- Ein Network Load Balancer kann einem einzelnen Endpunktdienst zugeordnet werden, ein Endpunktdienst kann jedoch mehreren Network Load Balancern zugeordnet werden.
- 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 VPC für Ihren Endpunkt einen Dienst mit mindestens einem Subnetz in jeder Availability Zone, in der der Dienst verfügbar sein soll.
- Damit Servicenutzer IPv6 VPC Schnittstellenendpunkte für Ihren Endpunktdienst erstellen können, müssen den Subnetzen VPC und den Subnetzen Blöcke zugeordnet sein. IPv6 CIDR
- Erstellen Sie einen Network Load Balancer in IhremVPC. 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 Endpunktdienst IPv6 Anfragen annehmen kann, müssen seine Network Load Balancer den Dualstack-IP-Adresstyp verwenden. Die Ziele müssen keinen Datenverkehr unterstützen. IPv6 Weitere Informationen finden Sie unter IP-Adresstyp im Benutzerhandbuch für Network Load Balancer.

  Wenn Sie Quell-IP-Adressen aus dem Header der Version 2 des Proxyprotokolls 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 Servicenutzer 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 VPC Amazon-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. Informationen zu den Availability Zones, die für den von Ihnen ausgewählten Load Balancer aktiviert sind, finden Sie unter Details der ausgewählten Load Balancer, Inbegriffene Availability Zones. Ihr Endpunktdienst wird in diesen Availability Zones verfügbar sein.
6. (Optional) Um Ihren Endpunktdienst in anderen Regionen als der Region, in der er gehostet wird, verfügbar zu machen, wählen Sie die Regionen unter Serviceregionen aus. Weitere Informationen finden Sie unter the section called “Regionsübergreifender Zugriff”.

7. 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.
8. Wählen Sie unter DNS Privaten Namen aktivieren die Option Dem Dienst einen privaten DNS Namen zuordnen aus, um einen privaten DNS Namen zuzuweisen, mit dem Dienstnutzer auf Ihren Dienst zugreifen können, und geben Sie dann den privaten DNS Namen ein. Andernfalls können Dienstnutzer den endpunktspezifischen DNS Namen verwenden, der von bereitgestellt wird. AWS Bevor Servicekunden den privaten DNS Namen verwenden können, muss der Dienstanbieter überprüfen, ob sie Eigentümer der Domain sind. Weitere Informationen finden Sie unter DNSNamen verwalten.
9. Führen Sie für Supported IP address types (Unterstützte IP-Adresstyp) einen der folgenden Schritte aus:

    - Wählen IPv4— Aktivieren Sie den Endpunktdienst für die Annahme von IPv4 Anfragen.
    - Wählen IPv6— Ermöglichen Sie dem Endpunktdienst die Annahme von IPv6 Anfragen.
    - Wählen Sie IPv4und IPv6— Aktivieren Sie den Endpunktdienst so, dass er IPv4 sowohl als auch IPv6 Anfragen akzeptiert.
10. (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.
11. Wählen Sie Create (Erstellen) aus.

So erstellen Sie einen Endpunktservice unter Verwendung der Befehlszeile

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

Bereitstellen des Endpunkt-Service für Service-Verbraucher

AWS Prinzipale können sich privat mit Ihrem Endpunktdienst verbinden, indem sie einen VPC Schnittstellenendpunkt 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 unter the section called “Herstellen einer Verbindung mit einem Endpunkt-Service als Service-Verbraucher”.
- 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 VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Wählen Sie als Typ die Option Endpunktdienste aus, die NLBs und verwenden GWLBs.
5. Geben Sie unter Dienstname den Namen des Dienstes ein (z. B.`com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`), und wählen Sie dann Dienst verifizieren aus.
6. (Optional) Um eine Verbindung zu einem Endpunktdienst herzustellen, der in einer anderen Region als der Endpunktregion verfügbar ist, wählen Sie Service-Region, Regionsübergreifenden Endpunkt aktivieren und dann die Region aus. Weitere Informationen finden Sie unter the section called “Regionsübergreifender Zugriff”.
7. Wählen Sie für die Option VPC aus VPC, von der aus Sie auf den Endpunktdienst zugreifen möchten.
8. Wählen Sie unter Subnetze die Subnetze aus, in denen Endpunkt-Netzwerkschnittstellen erstellt werden sollen.
9. Wählen Sie für IP address type (IP-Adressentyp) eine der folgenden Optionen aus:

    - IPv4— Weisen Sie den Endpunkt-Netzwerkschnittstellen IPv4 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 Adressbereiche haben und der Endpunktdienst IPv4 Anfragen akzeptiert.

- IPv6— Weist den Endpunkt-Netzwerkschnittstellen IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv6 nur Subnetze sind und der Endpunktdienst Anfragen akzeptiertIPv6.
- Dualstack — Weisen Sie den IPv4 Endpunkt-Netzwerkschnittstellen sowohl als auch IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze sowohl als auch IPv6 Adressbereiche haben IPv4 und der Endpunktdienst sowohl Anfragen als auch IPv4 akzeptiert. IPv6

10. Wählen Sie für den DNSDatensatz-IP-Typ eine der folgenden Optionen aus:

    - IPv4— Erstellen Sie A-Einträge für die privaten, regionalen und zonalen DNS Namen. Der IP-Adresstyp muss IPv4oder Dualstack sein.
    - IPv6— Erstellen Sie AAAA Datensätze für die privaten, regionalen und DNS zonalen Namen. Der IP-Adresstyp muss IPv6oder Dualstack sein.
    - Dualstack — Erstellen Sie A und AAAA Datensätze für die privaten, regionalen und zonalen Namen. DNS Der IP-Adresstyp muss Dualstack sein.
    - Service defined — Erstellen Sie A-Datensätze für die privaten, regionalen und zonalen DNS Namen und AAAA Datensätze für die regionalen und zonalen Namen. DNS Der IP-Adresstyp muss Dualstack sein.

11. Für Sicherheitsgruppe wählen Sie die Sicherheitsgruppen aus, die den Endpunktnetzwerkschnittstellen zugeordnet werden sollen.
12. 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
- Ordnen Sie einen privaten Namen DNS zu
- Ändern Sie die unterstützten Regionen
- 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 Schnittstellenendpunkt 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 Beispiele ARNs für unterstützte AWS Prinzipale.

ARNsfür Prinzipale AWS

AWS-Konto (beinhaltet alle Prinzipale im Konto)

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

Rolle

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

Benutzer

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

Alles in allem 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 VPC Amazon-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 die hinzuzufügenden Prinzipale den Namen 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-Berechtigungen ()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.

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.

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”.

So ändern Sie die Akzeptanzeinstellung mithilfe der Konsole

1. Öffnen Sie die VPC Amazon-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-Konfiguration ()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 VPC Amazon-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-connectionsoder 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 Servicekunden ihren VPC Schnittstellen-Endpunkten ein Subnetz aus dieser Availability Zone hinzufügen.

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

1. Öffnen Sie die VPC Amazon-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-Konfiguration ()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.

Ordnen Sie einen privaten Namen DNS zu

Sie können Ihrem Endpunktdienst einen privaten DNS Namen zuordnen. Nachdem Sie einen privaten DNS Namen zugeordnet haben, müssen Sie den Eintrag für die Domain auf Ihrem DNS Server aktualisieren. Bevor Servicekunden den privaten DNS Namen verwenden können, muss der Dienstanbieter überprüfen, ob sie Eigentümer der Domain sind. Weitere Informationen finden Sie unter DNSNamen verwalten.

Um den privaten DNS Namen eines Endpunktdienstes mithilfe der Konsole zu ändern

1. Öffnen Sie die VPC Amazon-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 „Aktionen“, „DNSPrivatnamen ändern“.
5. Wählen Sie Dem Dienst einen privaten DNS Namen zuordnen 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.

7. Der private DNS Name kann von den Servicekunden verwendet werden, wenn der Bestätigungsstatus verifiziert ist. Wenn sich der Überprüfungsstatus ändert, werden neue Verbindungsanforderungen abgelehnt, bestehende Verbindungen sind jedoch nicht betroffen.

Um den privaten DNS Namen eines Endpunktdienstes über die Befehlszeile zu ändern

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

So initiieren Sie den Domain-Überprüfungsprozess mithilfe der Konsole

1. Öffnen Sie die VPC Amazon-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 „Aktionen“ und „Domainbesitz verifizieren“ für den privaten DNS Namen aus.
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 Sie die unterstützten Regionen

Sie können die Gruppe der unterstützten Regionen für Ihren Endpunktdienst ändern. Bevor Sie eine Opt-in-Region hinzufügen können, müssen Sie sich anmelden. Sie können die Region, in der Ihr Endpunktdienst gehostet wird, nicht entfernen.

Nachdem Sie eine Region entfernt haben, können Servicekunden keine neuen Endpunkte mehr erstellen, die diese Region als Dienstregion angeben. Das Entfernen einer Region hat keine Auswirkungen auf bestehende Endpunkte, die sie als Dienstregion angeben. Wenn Sie eine Region entfernen, empfehlen wir Ihnen, alle bestehenden Endpunktverbindungen aus dieser Region abzulehnen.

Um die unterstützten Regionen für Ihren Endpunktdienst zu ändern

1. Öffnen Sie die VPC Amazon-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 „Aktionen“, „Unterstützte Regionen ändern“.
5. Wählen Sie nach Bedarf Regionen aus oder deaktivieren Sie sie.
6. Wählen Sie Änderungen speichern.

Ändern der unterstützten IP-Adresstypen

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

Überlegungen

Damit Ihr Endpunktdienst IPv6 Anfragen annehmen kann, müssen seine Network Load Balancer den Dualstack-IP-Adresstyp verwenden. Die Ziele müssen keinen Datenverkehr unterstützen. IPv6 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 VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den VPC Endpunkt-Service 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 IPv4— Ermöglichen Sie dem Endpunktdienst die Annahme von IPv4 Anfragen.
   - Wählen IPv6— Ermöglichen Sie dem Endpunktdienst die Annahme von IPv6 Anfragen.
   - Wählen Sie IPv4und IPv6— Aktivieren Sie den Endpunktdienst so, dass er IPv4 sowohl als auch IPv6 Anfragen akzeptiert.
6. Wählen Sie Änderungen speichern.

So ändern Sie die unterstützten IP-Adresstypen mithilfe der Befehlszeile

- modify-vpc-endpoint-service-Konfiguration ()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 VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den VPC Endpunkt-Service 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 Save (Speichern) aus.

So verwalten Sie Tags für Ihre Endpunktverbindungen mithilfe der Konsole

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunktservices aus.
3. Wählen Sie den VPC Endpunktservice und dann die Registerkarte Endpunktverbindungen aus.
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 Save (Speichern) aus.

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

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunktservices aus.
3. Wählen Sie den VPC Endpunktservice und dann die Registerkarte Allow Principals 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 Save (Speichern) aus.

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)

DNSNamen für VPC Endpunktdienste verwalten

Dienstanbieter können private DNS Namen für ihre Endpunktdienste konfigurieren. Angenommen, ein Dienstanbieter stellt seinen Dienst über einen öffentlichen Endpunkt und als Endpunktdienst zur Verfügung. Wenn der Dienstanbieter den DNS Namen des öffentlichen Endpunkts als privaten DNS Namen des Endpunktdienstes verwendet, können Dienstnutzer mit derselben Client-Anwendung ohne Änderung auf den öffentlichen Endpunkt oder den Endpunktdienst zugreifen. Wenn eine Anfrage vom Servicekonsumenten kommtVPC, lösen die privaten DNS Server den DNS Namen in die IP-Adressen der Endpunkt-Netzwerkschnittstellen auf. Andernfalls lösen die öffentlichen DNS Server den DNS Namen in den öffentlichen Endpunkt auf.

Bevor Sie einen privaten DNS Namen für Ihren Endpunktdienst konfigurieren können, müssen Sie nachweisen, dass Sie Eigentümer der Domain sind, indem Sie eine Überprüfung des Domainbesitzes durchführen.

Überlegungen

- Ein Endpunktdienst kann nur einen privaten DNS Namen haben.

- Wenn der Verbraucher einen Schnittstellenendpunkt erstellt, um eine Verbindung zu Ihrem Service herzustellen, erstellen wir eine private Hosting-Zone und ordnen sie dem Service-Consumer zuVPC. Wir erstellen einen CNAME Datensatz in der privaten Hosting-Zone, der den privaten DNS Namen des Endpunktdienstes dem regionalen DNS Namen des VPC Endpunkts zuordnet. Wenn ein Verbraucher eine Anfrage an den öffentlichen DNS Namen des Dienstes sendet, lösen die privaten DNS Server die Anfrage an die IP-Adressen der Endpunkt-Netzwerkschnittstellen auf.
- Um eine Domain zu verifizieren, 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 jetzt b.example.com als privaten DNS Namen hinzu. Sie müssen example.com oder b.example.com überprüfen, bevor Service-Verbraucher den Namen verwenden können.
- Private DNS Namen werden für Gateway Load Balancer-Endpunkte nicht unterstützt.

Domain-Verifizierungsname

Ihre Domain ist mit einer Reihe von Domain Name Service (DNS) -Einträgen verknüpft, die Sie über Ihren DNS Anbieter verwalten. Ein TXT Datensatz ist eine Art von DNS Datensatz, der zusätzliche Informationen über Ihre Domain enthält. 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.

Die Überprüfung des Domainbesitzes ist abgeschlossen, wenn wir das Vorhandensein des TXT Eintrags in den DNS Einstellungen Ihrer Domain feststellen.

Nachdem Sie einen Datensatz hinzugefügt haben, können Sie den Status des Domainverifizierungsprozesses mithilfe der VPC Amazon-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 „Aktionen“, „Domain-Inhaberschaft verifizieren“ für den privaten DNS Namen aus.

Der private DNS Name kann von den Servicekunden verwendet werden, sobald der Bestätigungsstatus bestätigt wurde. 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 den Wert, den Sie in der TXT Aufzeichnung 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 Datensatz 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:l6p0 ERxlTt45jevFwOCp

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 „_6e86v84tqgqubxbwii1m“ weglassen und einfach „example.com“ im Datensatz verwenden. TXT

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 dem Server Ihrer Domain einen Eintrag hinzu TXT DNS

Das Verfahren zum Hinzufügen von TXT Datensätzen zum DNS Server Ihrer Domain hängt davon ab, wer Ihren DNS Dienst anbietet. Ihr DNS Anbieter könnte Amazon Route 53 oder ein anderer Domainnamen-Registrar sein.

Amazon Route 53

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

- Wählen Sie als Datensatztyp die Option TXT.
- Geben Sie für TTL(Sekunden) ein**`1800`**.
- 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, auf der Sie die DNS Einträge für Ihre Domain aktualisieren können. Fügen Sie einen

TXT Datensatz mit dem von uns angegebenen Namen und Wert hinzu. Es kann bis zu 48 Stunden dauern, bis DNS Datensatzaktualisierungen wirksam werden, aber sie werden oft viel früher wirksam.

Genauere Anweisungen finden Sie in der Dokumentation Ihres DNS Anbieters. Die folgende Tabelle enthält Links zur Dokumentation verschiedener gängiger 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	Fügen Sie einen Datensatz TXT hinzu
Dreamhost	Hinzufügen von benutzerdefinierten DNS Datensätzen
Cloudflare	DNSDatensätze verwalten
HostGator	DNSDatensätze verwalten mit HostGator/eNom
Namecheap	Wie füge ich TXT/SPF/DKIM/DMARC Einträge für meine Domain hinzu?
Names.co.uk	Ändern Sie die DNS Einstellungen Ihrer Domain
Wix	Hinzufügen oder Aktualisieren von TXT Einträgen in Ihrem Wix-Konto

Prüfen Sie, ob der TXT Datensatz veröffentlicht wurde

Mithilfe der folgenden Schritte können Sie überprüfen, ob Ihr TXT Datensatz zur Überprüfung des Besitzes einer privaten DNS Name-Domain korrekt auf Ihrem DNS Server veröffentlicht wurde. 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 Domaininformationen auf andere DNS Server übertragen werden.

Um zu überprüfen, ob Ihr TXT Eintrag auf Ihrem DNS Server veröffentlicht wurde

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. Stellen Sie mithilfe des folgenden Befehls sicher, dass der TXT Datensatz korrekt veröffentlicht wurde. Dabei *name_server* handelt es sich um einen der Nameserver, die Sie im vorherigen Schritt gefunden haben.

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

3. Stellen Sie in der Ausgabe des vorherigen Schritts sicher, dass die folgende Zeichenfolge `text =` 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.

- Prüfen Sie, ob Ihr DNS Anbieter Unterstriche in TXT Datensatznamen zulässt. Wenn Ihr DNS Anbieter keine Unterstriche zulässt, können Sie den Domainbestätigungsnamen (z. B. „_6e86v84tqgqubxbwii1m“) aus dem Datensatz weglassen. TXT
- Prüfen Sie, ob Ihr Anbieter TXT den Domainnamen an das Ende des Datensatzes angehängt DNS hat. Einige DNS Anbieter hängen den Namen Ihrer Domain automatisch an den Attributnamen des TXT Eintrags an. Um diese Vervielfältigung des Domainnamens zu vermeiden, fügen Sie bei der Erstellung des Eintrags einen Punkt am Ende des Domainnamens hinzu. TXT Dadurch wird Ihrem DNS Anbieter mitgeteilt, dass es nicht erforderlich ist, den Domainnamen an den Datensatz anzuhängen. TXT
- Prüfen Sie, ob Ihr DNS Anbieter den DNS Datensatzwert so geändert hat, dass er nur noch Kleinbuchstaben verwendet. 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 Datensatzwerte so geändert hat, dass nur noch 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 zulässt, dass Sie mehr als einen TXT Datensatz mit demselben Attributnamen haben, überprüfen Sie, ob Ihr DNS Anbieter es Ihnen ermöglicht, demselben TXT Datensatz mehrere Attributwerte zuzuweisen. Wenn Ihr beispielsweise von Amazon Route 53 verwaltet DNS wird, können Sie das folgende Verfahren verwenden.

  1. Wählen Sie in der Route 53-Konsole den TXT Datensatz aus, den Sie bei der Bestätigung 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 es Ihnen nicht erlaubt, demselben TXT Datensatz mehrere Werte zuzuweisen, können Sie die Domain einmal mit dem Wert im Attributnamen des TXT Datensatzes und ein anderes Mal mit dem aus dem Attributnamen entfernten Wert 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

- Erstellen Sie eine SNS Benachrichtigung
- Eine Zugriffsrichtlinie hinzufügen
- Eine Schlüsselrichtlinie hinzufügen

Erstellen Sie eine SNS Benachrichtigung

Gehen Sie wie folgt vor, um ein SNS Amazon-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 VPC Amazon-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 unter Benachrichtigung ARN das 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-Benachrichtigung ()AWS CLI
- New-EC2VpcEndpointConnectionNotification(Tools für Windows PowerShell)

Eine Zugriffsrichtlinie hinzufügen

Fügen Sie dem SNS Thema eine Zugriffsrichtlinie hinzu, die es AWS PrivateLink ermöglicht, Benachrichtigungen in Ihrem Namen zu veröffentlichen, z. B. die folgenden. Weitere Informationen finden Sie unter Wie bearbeite ich die Zugriffsrichtlinie meines SNS Amazon-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 AWS PrivateLink darauf vertrauen, dass AWS KMS API Operationen aufgerufen werden. 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 VPC Amazon-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-Konfigurationen ()AWS CLI
- Remove-EC2EndpointServiceConfiguration(Tools für Windows PowerShell)

Greifen Sie auf VPC Ressourcen zu über AWS PrivateLink

Sie können privat auf eine VPC Ressource in einer anderen zugreifen, VPC indem Sie einen VPC Ressourcenendpunkt (Ressourcenendpunkt) verwenden. Mit einem Ressourcenendpunkt können Sie privat und sicher auf VPC Ressourcen wie eine Datenbank, einen Knotencluster, eine Instanz, einen Anwendungsendpunkt, ein Domainnamenziel oder eine IP-Adresse zugreifen, die sich in einem privaten Subnetz in einer anderen VPC oder in einer lokalen Umgebung befinden kann. Ohne Ressourcenendpunkte müssen Sie entweder ein Internet-Gateway zu Ihrem hinzufügen VPC oder über einen AWS PrivateLink Schnittstellenendpunkt und einen Network Load Balancer auf die Ressource zugreifen. Für Ressourcenendpunkte ist kein Load Balancer erforderlich, sodass Sie direkt auf die Ressource zugreifen können. VPC Eine VPC Ressource wird durch eine Ressourcenkonfiguration repräsentiert. Eine Ressourcenkonfiguration ist an ein Ressourcen-Gateway gebunden.

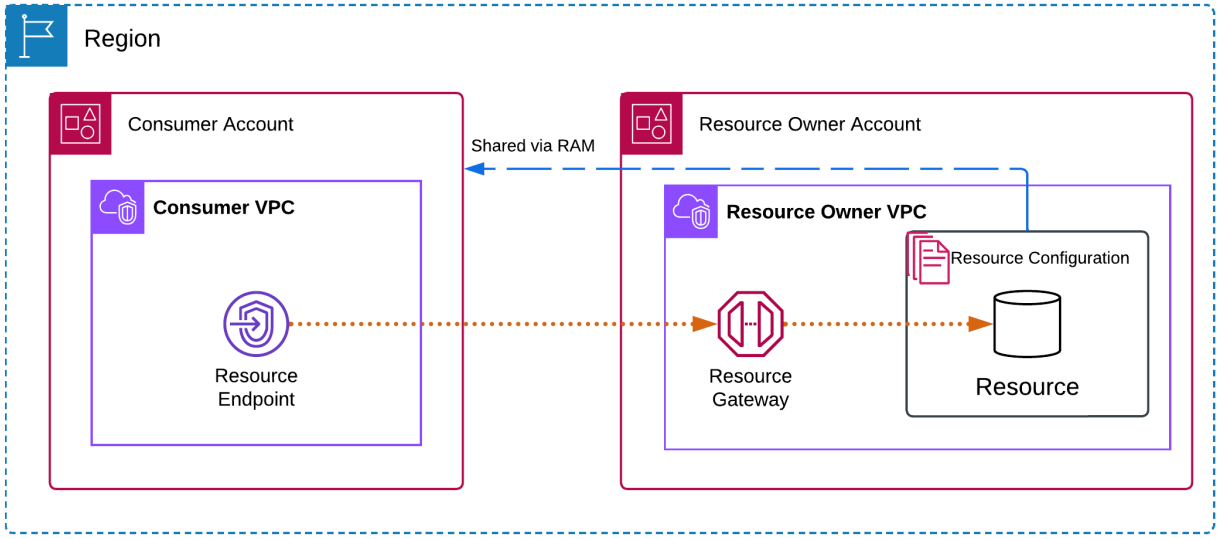
Preisgestaltung

Wenn Sie über Ressourcenendpunkte auf Ressourcen zugreifen, wird Ihnen jede Stunde in Rechnung gestellt, in der Ihr VPC Ressourcenendpunkt bereitgestellt wird. Außerdem wird Ihnen pro GB verarbeiteter Daten abgerechnet, wenn Sie auf Ressourcen zugreifen. Weitere Informationen finden Sie unter AWS PrivateLink Preise. Wenn Sie den Zugriff auf Ihre Ressourcen mithilfe von Ressourcenkonfigurationen und Ressourcen-Gateways aktivieren, wird Ihnen pro GB Daten abgerechnet, die von Ihren Ressourcen-Gateways verarbeitet werden. Weitere Informationen finden Sie unter Amazon VPC Lattice Preise.

Inhalt

Übersicht

Sie können auf Ressourcen in Ihrem Konto oder auf Ressourcen zugreifen, die von einem anderen Konto aus mit Ihnen geteilt wurden. Um auf eine Ressource zuzugreifen, erstellen Sie einen VPC Ressourcenendpunkt, der mithilfe von Netzwerkschnittstellen Verbindungen zwischen den Subnetzen in Ihrer VPC und der Ressource herstellt. Der für die Ressource bestimmte Datenverkehr wird über die privaten IP-Adressen der Netzwerkschnittstellen des Ressourcenendpunkts aufgelöst und dann über DNS die Verbindung zwischen dem VPC Endpunkt und der Ressource über das Ressourcengateway an die Ressource gesendet.



Überlegungen

- TCPVerkehr wird unterstützt. UDPVerkehr wird nicht unterstützt.
- Netzwerkverbindungen müssen von dem initiiert werdenVPC, der den Ressourcenendpunkt enthält, und nicht von demVPC, der die Ressource hat. Die Ressourcen VPC können keine Netzwerkverbindungen zum Endpunkt initiierenVPC.
- Die einzigen unterstützten ARN Ressourcen sind RDS Amazon-Ressourcen.

DNSHostnamen

Mit AWS PrivateLink senden Sie über private Endpunkte Traffic an Ressourcen. Wenn Sie einen VPC Ressourcenendpunkt erstellen, erstellen wir regionale DNS Namen (so genannter DNS Standardname), die Sie verwenden können, um mit der Ressource von Ihrem Standort VPC und von

Ihrem Standort aus zu kommunizieren. Der DNS Standardname für Ihren VPC Ressourcenendpunkt hat die folgende Syntax:

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

Wenn Sie einen VPC Ressourcenendpunkt für ausgewählte Ressourcenkonfigurationen erstellen, die verwendenARNs, können Sie private Ressourcen aktivierenDNS. Mit Private können Sie weiterhin Anfragen an die Ressource stellenDNS, indem Sie den DNS Namen verwenden, den der AWS Dienst für die Ressource bereitgestellt hat, und gleichzeitig die private Konnektivität über den VPC Ressourcenendpunkt nutzen. Weitere Informationen finden Sie unter the section called “DNSAuflösung”.

Der folgende describe-vpc-endpoint-associationsBefehl zeigt die DNS Einträge für einen Ressourcenendpunkt an.

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

Im Folgenden finden Sie eine Beispielausgabe für einen Ressourcenendpunkt für eine RDS Amazon-Datenbank mit aktivierten privaten DNS Namen. Der erste Eintrag ist der DNS Standardname. Der zweite Eintrag stammt aus der versteckten privaten Hosting-Zone, die Anfragen an den öffentlichen Endpunkt an die privaten IP-Adressen der Endpunkt-Netzwerkschnittstellen auflöst.

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

DNSAuflösung

Die DNS Datensätze, die wir für Ihren VPC Ressourcenendpunkt erstellen, sind öffentlich. Daher sind diese DNS Namen öffentlich auflösbar. DNSAnfragen von außerhalb geben jedoch VPC immer noch

die privaten IP-Adressen der Netzwerkschnittstellen des Ressourcenendpunkts zurück. Sie können diese DNS Namen verwenden, um lokal auf die Ressource zuzugreifen, sofern Sie Zugriff auf VPC das haben, in dem sich der Ressourcenendpunkt befindet, über VPN oder Direct Connect.

Privat DNS

Wenn Sie Private DNS für Ihren VPC Ressourcenendpunkt aktivieren und bei Ihrem VPC sowohl DNSHostnamen als auch DNS Auflösung aktiviert sind, erstellen wir versteckte, AWS verwaltete private Hosting-Zonen für Ressourcenkonfigurationen mit einem benutzerdefinierten DNS Namen. Die gehostete Zone enthält einen Datensatz für den DNS Standardnamen der Ressource, der ihn in die privaten IP-Adressen der Netzwerkschnittstellen des Ressourcenendpunkts in Ihrem auflöst. VPC

Amazon stellt für Sie einen DNS Server bereitVPC, den sogenannten Route 53 Resolver. Der Route 53 Resolver löst automatisch lokale VPC Domainnamen auf und zeichnet in privaten Hosting-Zonen auf. Sie können den Route 53 Resolver jedoch nicht von außerhalb Ihres verwenden. VPC Wenn Sie von Ihrem lokalen Netzwerk aus auf Ihren VPC Endpunkt zugreifen möchten, können Sie die DNS Standardnamen verwenden oder Sie können Route 53 Resolver-Endpunkte und Resolver-Regeln verwenden. Weitere Informationen finden Sie unter Integration mit und. AWS Transit GatewayAWS PrivateLinkAmazon Route 53 Resolver

Subnetze und Availability Zones

Sie können Ihren VPC Endpunkt 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 Anzahl der in jedem Subnetz zugewiesenen IP-Adressen hängt von der Anzahl der Ressourcenkonfigurationen ab. In einer Produktionsumgebung empfehlen wir für hohe Verfügbarkeit und Ausfallsicherheit, mindestens zwei Availability Zones für jeden VPC Endpunkt zu konfigurieren.

IP-Adresstypen

Ressourcenendpunkte können Dual-Stack-Adressen oder IPv4 IPv6 Dual-Stack-Adressen unterstützen. Endpunkte, die dies unterstützen, IPv6 können Abfragen mit Datensätzen beantwortenDNS. AAAA Der IP-Adresstyp eines Ressourcenendpunkts muss mit den Subnetzen für den Ressourcenendpunkt kompatibel sein, wie hier beschrieben:

- IPv4— Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv4 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 Adressbereiche haben.
- IPv6— Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv6 nur Subnetze sind.
- Dualstack — Weisen Sie Ihren IPv4 Endpunkt-Netzwerkschnittstellen sowohl IPv6 Adressen als auch Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 sowohl IPv6 als auch Adressbereiche haben.

Wenn ein VPC Ressourcenendpunkt dies unterstütztIPv4, haben die Netzwerkschnittstellen des Endpunkts IPv4 Adressen. Wenn ein VPC Ressourcenendpunkt dies unterstütztIPv6, haben die Netzwerkschnittstellen des Endpunkts IPv6 Adressen. Die IPv6 Adresse für eine Endpunkt-Netzwerkschnittstelle ist vom Internet aus nicht erreichbar. Wenn Sie eine Endpunkt-Netzwerkschnittstelle mit einer IPv6 Adresse beschreiben, beachten Sie, dass diese aktiviert `denyAllIgwTraffic` ist.

Greifen Sie über einen VPC Ressourcenendpunkt auf eine Ressource zu

Sie können über einen VPC Ressourcenendpunkt auf eine Ressource wie einen Domainnamen, eine IP-Adresse oder eine RDS Amazon-Datenbank zugreifen. Ein Ressourcenendpunkt bietet privaten Zugriff auf eine Ressource. Wenn Sie den Ressourcenendpunkt erstellen, geben Sie eine Ressourcenkonfiguration vom Typ Single, Group oder anARN. Ein Ressourcenendpunkt kann nur einer Ressourcenkonfiguration zugeordnet werden. Die Ressourcenkonfiguration kann eine einzelne Ressource oder eine Gruppe von Ressourcen darstellen.

Voraussetzungen

Um einen Ressourcenendpunkt zu erstellen, müssen Sie die folgenden Voraussetzungen erfüllen.

- Sie müssen über eine Ressourcenkonfiguration verfügen, die entweder von Ihnen erstellt oder von einem anderen Konto aus für Sie freigegeben wurde AWS RAM.
- Wenn eine Ressourcenkonfiguration von einem anderen Konto für Sie freigegeben wurde, müssen Sie die Ressourcenfreigabe, die die Ressourcenkonfiguration enthält, überprüfen und akzeptieren. Weitere Informationen finden Sie unter Annehmen und Ablehnen von Ressourcenfreigabeeinladungen im AWS RAM -Benutzerhandbuch.

Erstellen Sie einen VPC Ressourcenendpunkt

Gehen Sie wie folgt vor, um einen VPC Ressourcenendpunkt zu erstellen.

Um einen VPC Ressourcenendpunkt zu erstellen

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Sie können einen Namen angeben, um das Auffinden und Verwalten des Endpunkts zu erleichtern.
5. Wählen Sie für Typ die Option Ressourcen aus.
6. Wählen Sie unter Ressourcenkonfigurationen die Ressourcenkonfiguration aus, die für Sie freigegeben wurde.
7. Wählen Sie unter Netzwerkeinstellungen die VPC aus, von der aus Sie auf die Ressource zugreifen möchten.
8. Wenn Sie privaten DNS Support konfigurieren möchten, wählen Sie Zusätzliche Einstellungen, DNSNamen aktivieren aus. Um diese Funktion nutzen zu können, stellen Sie sicher, dass die Attribute DNSHostnamen aktivieren und DNS Support aktivieren für Sie VPC aktiviert sind.
9. Wählen Sie Endpunkt erstellen aus.

Um einen Ressourcenendpunkt über die Befehlszeile zu erstellen

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

Ressourcenendpunkte verwalten

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

Aufgaben

- Löschen eines Endpunkts
- Einen Endpunkt aktualisieren

Löschen eines Endpunkts

Wenn Sie mit einem VPC Endpunkt fertig sind, können Sie ihn löschen.

Um einen Endpunkt mit der Konsole zu löschen

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

Um einen Endpunkt über die Befehlszeile zu löschen

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

Einen Endpunkt aktualisieren

Sie können einen VPC Endpunkt aktualisieren.

Um einen Endpunkt mit der Konsole zu aktualisieren

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Endpunkt.
4. Wählen Sie Aktionen und die entsprechende Option.
5. Folgen Sie den Schritten auf der Konsole, um das Update einzureichen.

Um einen Endpunkt über die Befehlszeile zu aktualisieren

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

Ressourcenkonfiguration für VPC Ressourcen

Eine Ressourcenkonfiguration stellt eine Ressource oder eine Gruppe von Ressourcen dar, die Sie Kunden in anderen VPCs Konten zugänglich machen möchten. Durch die Definition einer Ressourcenkonfiguration können Sie private, sichere, unidirektionale Netzwerkkonnektivität VPC von Clients in anderen VPCs und Konten zu Ihren Ressourcen ermöglichen. Eine Ressourcenkonfiguration ist an ein Ressourcen-Gateway gebunden, über das sie Datenverkehr empfängt.

Inhalt

Arten von Ressourcenkonfigurationen

Es gibt verschiedene Typen von Ressourcenkonfigurationen. Die verschiedenen Typen helfen dabei, verschiedene Arten von Ressourcen darzustellen. Die Typen sind:

- Konfiguration einer einzelnen Ressource: Eine IP-Adresse oder ein Domainname. Sie kann unabhängig gemeinsam genutzt werden.
- Gruppenressourcenkonfiguration: Eine Sammlung von Konfigurationen untergeordneter Ressourcen, die einen Cluster von Knoten darstellen. Sie kann unabhängig gemeinsam genutzt werden.

- Konfiguration untergeordneter Ressourcen: Ein Mitglied einer Gruppenressourcenkonfiguration. Es steht für eine IP-Adresse oder einen Domainnamen. Es kann nicht unabhängig geteilt werden; es kann nur als Teil einer Gruppe geteilt werden. Es kann problemlos zu einer Gruppe hinzugefügt und daraus entfernt werden. Wenn es hinzugefügt wird, ist es automatisch für diejenigen zugänglich, die auf die Gruppe zugreifen können.
- ARNRessourcenkonfiguration: Stellt einen unterstützten Ressourcentyp dar, der von einem Dienst bereitgestellt wird. AWS Konfigurationen untergeordneter Ressourcen werden automatisch von verwaltet. AWS

Ressourcen-Gateway

Eine Ressourcenkonfiguration ist an ein Ressourcen-Gateway gebunden. Ein Ressourcen-Gateway besteht aus einer Gruppe von GatewaysENIs, die als Zugangspunkt zu dem dienen, VPC in dem sich die Ressource befindet. Mehrere Ressourcenkonfigurationen können an dasselbe Ressourcen-Gateway gebunden werden. Wenn Clients in anderen Konten VPCs oder Konten auf eine Ressource in Ihrem zugreifenVPC, sieht die Ressource den Datenverkehr, der lokal vom Ressourcen-Gateway kommtVPC.

Definition der Ressource

Identifizieren Sie die Ressource in der Ressourcenkonfiguration auf eine der folgenden Arten:

- Durch einen Amazon-Ressourcennamen (ARN): Unterstützte Ressourcentypen, die von AWS Services bereitgestellt werden, können anhand ihrer identifiziert werden. ARN Zum Beispiel eine RDS Amazon-Datenbank.
- Nach einem Domainnamen-Ziel: Jeder Domainname, der öffentlich auflösbar ist.
- Durch eine IP-Adresse: Für IPv4 und IPv6 werden nur IPs in unterstützt. VPC

Protokoll

Wenn Sie eine Ressourcenkonfiguration erstellen, können Sie die Protokolle definieren, die die Ressource unterstützt. Derzeit wird nur das TCP Protokoll unterstützt.

Portbereiche

Wenn Sie eine Ressourcenkonfiguration erstellen, können Sie die Ports definieren, an denen Anfragen akzeptiert werden. Der Client-Zugriff auf andere Ports ist nicht erlaubt.

Auf -Ressourcen zugreifen

Verbraucher können über einen VPC Endpunkt oder VPC über ein Servicenetzwerk direkt auf Ressourcenkonfigurationen zugreifen. Als Verbraucher können Sie den Zugriff von Ihrer VPC auf eine Ressourcenkonfiguration ermöglichen, die sich in Ihrem Konto befindet oder die von einem anderen Konto aus mit Ihnen geteilt wurde AWS RAM.

- Direkter Zugriff auf eine Ressourcenkonfiguration

  Sie können einen AWS PrivateLink VPC Endpunkt vom Typ Ressource (Ressourcenendpunkt) in Ihrem erstellenVPC, um privat von Ihrem aus auf eine Ressourcenkonfiguration zuzugreifenVPC. Weitere Informationen zum Erstellen eines Ressourcenendpunkts finden Sie unter Zugreifen auf VPC Ressourcen im AWS PrivateLink Benutzerhandbuch.
- Zugreifen auf eine Ressourcenkonfiguration über ein Servicenetzwerk

  Sie können eine Ressourcenkonfiguration einem Servicenetzwerk zuordnen und Ihre mit VPC dem Servicenetzwerk verbinden. Sie können Ihre Verbindung mit VPC dem Servicenetzwerk entweder über eine Zuordnung oder über einen AWS PrivateLink VPC Servicenetzwerk-Endpunkt herstellen.

  Weitere Informationen zu Dienstnetzwerkzuordnungen finden Sie unter Verwalten der Zuordnungen für ein VPC Lattice-Dienstnetzwerk.

  Weitere Informationen zu VPC Dienstnetzwerkendpunkten finden Sie im AWS PrivateLink Benutzerhandbuch unter Zugreifen auf Dienstnetzwerke.

Zuordnung zum Servicenetzwerktyp

Wenn Sie eine Ressourcenkonfiguration gemeinsam mit einem Verbraucherkonto verwenden, z. B. Account-B, kann Account-B entweder direkt über AWS RAM einen VPC Ressourcenendpunkt oder über ein Servicenetzwerk auf die Ressourcenkonfiguration zugreifen.

Um über ein Servicenetzwerk auf eine Ressourcenkonfiguration zuzugreifen, müsste Account-B die Ressourcenkonfiguration einem Servicenetzwerk zuordnen. Servicenetzwerke können von mehreren Konten gemeinsam genutzt werden. Somit kann Account-B sein Servicenetzwerk (dem die Ressourcenkonfiguration zugeordnet ist) mit Account-C teilen, sodass auf Ihre Ressource von Account-C aus zugegriffen werden kann.

Um eine solche transitive gemeinsame Nutzung zu verhindern, können Sie angeben, dass Ihre Ressourcenkonfiguration nicht zu Servicenetzwerken hinzugefügt werden kann, die von

Konten gemeinsam genutzt werden können. Wenn Sie dies angeben, kann Account-B Ihre Ressourcenkonfiguration nicht zu Servicenetzwerken hinzufügen, die gemeinsam genutzt werden oder in future mit einem anderen Konto geteilt werden können.

Arten von Servicenetzwerken

Wenn Sie eine Ressourcenkonfiguration mit einem anderen Konto teilen, z. B. mit Account-B, kann Account-B auf eine von drei Arten auf die Ressource zugreifen: AWS RAM

- Verwenden eines VPC Endpunkts vom Typ Ressource (Ressourcenendpunkt). VPC
- Verwendung eines VPC Endpunkts vom Typ Servicenetzwerk (VPCServicenetzwerk-Endpunkt).
- Verwenden einer VPC Dienstnetzwerkverbindung.

Für die VPC Zuordnung von VPC Servicenetzwerkendpunkt und Servicenetzwerk müsste die Ressourcenkonfiguration in einem Servicenetzwerk in Account-B gespeichert werden. Servicenetzwerke können von mehreren Konten gemeinsam genutzt werden. Somit kann Account-B sein Servicenetzwerk (das die Ressourcenkonfiguration enthält) mit Account-C teilen, sodass auf Ihre Ressource von Account-C aus zugegriffen werden kann. Um eine solche transitive gemeinsame Nutzung zu verhindern, können Sie verhindern, dass Ihre Ressourcenkonfiguration zu Servicenetzwerken hinzugefügt wird, die von Konten gemeinsam genutzt werden können. Wenn Sie dies verbieten, kann Account-B Ihre Ressourcenkonfiguration nicht zu einem Servicenetzwerk hinzufügen, das gemeinsam genutzt wird oder mit einem anderen Konto geteilt werden kann.

Gemeinsame Nutzung von Ressourcenkonfigurationen über AWS RAM

Ressourcenkonfigurationen sind integriert in AWS Resource Access Manager. Sie können Ihre Ressourcenkonfiguration über mit einem anderen Konto teilen AWS RAM. Wenn Sie eine Ressourcenkonfiguration mit einem AWS Konto teilen, können Kunden in diesem Konto privat auf die Ressource zugreifen. Sie können eine Ressourcenkonfiguration mithilfe eines Resource Share-In gemeinsam nutzen AWS RAM.

Verwenden Sie die AWS RAM Konsole, um die Ressourcenfreigaben anzuzeigen, zu denen Sie hinzugefügt wurden, die gemeinsam genutzten Ressourcen, auf die Sie zugreifen können, und die AWS Konten, die Ressourcen mit Ihnen gemeinsam genutzt haben. Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch unter Mit Ihnen geteilte Ressourcen.

Um von einer anderen Ressource VPC in demselben Konto wie die Ressourcenkonfiguration aus auf eine Ressource zuzugreifen, müssen Sie die Ressourcenkonfiguration nicht gemeinsam nutzen AWS RAM.

Überwachen

Sie können Überwachungsprotokolle in Ihrer Ressourcenkonfiguration aktivieren. Sie können ein Ziel auswählen, an das die Protokolle gesendet werden sollen.

Erstellen Sie eine Ressourcenkonfiguration in VPC Lattice

Verwenden Sie die Konsole, um eine Ressourcenkonfiguration zu erstellen.

Um eine Ressourcenkonfiguration mit der Konsole zu erstellen

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter PrivateLink und Lattice die Option Ressourcenkonfigurationen aus.
3. Wählen Sie Ressourcenkonfiguration erstellen aus.
4. Geben Sie einen Namen ein, der innerhalb Ihres AWS Kontos einzigartig ist. Sie können diesen Namen nicht ändern, nachdem die Ressourcenkonfiguration erstellt wurde.
5. Wählen Sie als Konfigurationstyp Ressource für eine einzelne oder untergeordnete Ressource oder Ressourcengruppe für eine Gruppe von untergeordneten Ressourcen aus.
6. Wählen Sie ein Ressourcen-Gateway aus, das Sie zuvor erstellt haben, oder erstellen Sie jetzt ein neues.
7. Wählen Sie den Bezeichner für die Ressource aus, die diese Ressourcenkonfiguration darstellen soll.
8. Wählen Sie die Portbereiche aus, über die Sie die Ressource gemeinsam nutzen möchten.
9. Geben Sie unter Zuordnungseinstellungen an, ob diese Ressourcenkonfiguration mit gemeinsam nutzbaren Dienstnetzwerken verknüpft werden kann.
10. Wählen Sie unter Konfiguration gemeinsam genutzter Ressourcen die Ressourcenfreigaben aus, anhand derer die Prinzipale identifiziert werden, die auf diese Ressource zugreifen können.
11. (Optional) Aktivieren Sie unter Überwachung die Option Ressourcenzugriffsprotokolle und das Zustellungsziel, wenn Sie Anfragen und Antworten an und von der Ressourcenkonfiguration überwachen möchten.

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 Ressourcenkonfiguration erstellen aus.

Um eine Ressourcenkonfiguration mit dem zu erstellen AWS CLI

Verwenden Sie den create-resource-configuration-Befehl.

Zuordnungen für eine VPC Lattice-Ressourcenkonfiguration verwalten

Benutzerkonten, mit denen Sie eine Ressourcenkonfiguration gemeinsam nutzen, und Clients in Ihrem Konto können entweder direkt über einen VPC Ressourcenendpunkt oder über einen Servicenetzwerk-Endpunkt auf die Ressourcenkonfiguration zugreifen. Daher wird Ihre Ressourcenkonfiguration über Endpunktzuordnungen und Dienstnetzwerkzuordnungen verfügen.

Verwalten Sie Dienstnetzwerkzuordnungen

Erstellen oder löschen Sie eine Dienstnetzwerkverbindung.

Um eine Dienstnetzwerkverbindung mit der Konsole zu verwalten

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter PrivateLink und Lattice die Option Ressourcenkonfigurationen aus.
3. Wählen Sie den Namen der Ressourcenkonfiguration aus, um die zugehörige Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Dienstnetzwerkzuordnungen aus.
5. Wählen Sie Verknüpfungen erstellen aus.
6. Wählen Sie unter VPCLattice Service Networks ein Servicenetzwerk aus. Um ein Servicenetzwerk zu erstellen, wählen Sie Create a VPC Lattice Network.
7. (Optional) Um ein Tag hinzuzufügen, erweitern Sie Dienstzuordnungs-Tags, wählen Sie Neues Tag hinzufügen aus und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
8. Wählen Sie Änderungen speichern.
9. Um eine Zuordnung zu löschen, aktivieren Sie das Kontrollkästchen für die Verknüpfung und wählen Sie dann Aktionen, Löschen aus. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

Um eine Dienstnetzwerkverbindung mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-service-network-resource-association.

Um eine Dienstnetzwerkverbindung mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-service-network-resource-association.

VPCEndpunktzuordnungen verwalten

Verwalten Sie eine VPC Endpunktzuweisung.

Um eine VPC Endpunktzuweisung mithilfe der Konsole zu verwalten

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter PrivateLink und Lattice die Option Ressourcenkonfigurationen aus.
3. Wählen Sie den Namen der Ressourcenkonfiguration aus, um die zugehörige Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Endpunktzuordnungen.
5. Wählen Sie die Zuordnungs-ID aus, um die zugehörige Detailseite zu öffnen. Von hier aus können Sie die Zuordnung ändern oder löschen.
6. Um eine neue Endpunktzuordnung zu erstellen, gehen Sie im linken Navigationsbereich zu PrivateLink und Lattice und wählen Sie Endpoints aus.
7. Wählen Sie Endpunkte erstellen aus.
8. Wählen Sie die Ressourcenkonfiguration aus, mit der Sie eine Verbindung herstellen VPC möchten.
9. Wählen Sie VPC die Subnetze und Sicherheitsgruppen aus.
10. (Optional) Um Ihren VPC Endpunkt zu taggen, wählen Sie Neues Tag hinzufügen aus und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
11. Wählen Sie Endpunkt erstellen aus.

Um eine VPC Endpunktzuordnung mit dem zu erstellen AWS CLI

Verwenden Sie den create-vpc-endpoint-Befehl.

Um eine VPC Endpunktassoziation zu löschen, verwenden Sie AWS CLI

Verwenden Sie den delete-vpc-endpoint-Befehl.

Ressourcen-Gateway in VPC Lattice

Ein Ressourcen-Gateway ist ein Zugangspunkt in den VPC Ort, an dem sich eine Ressource befindet. Es erstreckt sich über mehrere Availability Zones. Damit Ihre Ressource von allen Availability Zones aus zugänglich ist, sollten Sie Ihre Ressourcen-Gateways so einrichten, dass sie sich über so viele Availability Zones wie möglich erstrecken.

Ein Ressourcen-Gateway VPC muss vorhanden sein, wenn Sie planen, die Ressourcen innerhalb des Netzwerks von anderen VPCs Konten aus VPC zugänglich zu machen. Jede Ressource, die Sie gemeinsam nutzen, ist an ein Ressourcen-Gateway gebunden. Wenn Clients in anderen Konten VPCs oder Konten auf eine Ressource in Ihrem zugreifenVPC, sieht die Ressource den Datenverkehr, der lokal vom Ressourcen-Gateway kommtVPC. Die Quell-IP des Datenverkehrs ist die IP des Ressourcen-Gateways. Sie können einem Ressourcengateway mehrere IP-Adressen zuweisen, um mehr Netzwerkverbindungen mit der Ressource zu ermöglichen. Mehrere Ressourcen in einem VPC können an dasselbe Ressourcen-Gateway gebunden werden.

Ein Ressourcen-Gateway bietet keine Lastenausgleichsfunktionen.

Inhalt

Sicherheitsgruppen

Sie können Sicherheitsgruppen an ein Ressourcengateway anhängen. Sicherheitsgruppenregeln für Ressourcengateways steuern den ausgehenden Verkehr vom Ressourcengateway zu Ressourcen.

Empfohlene Regeln für ausgehenden Datenverkehr, der von einem Ressourcen-Gateway zu einer Datenbankressource fließt

Damit der Datenverkehr von einem Ressourcen-Gateway zu einer Ressource fließen kann, müssen Sie Regeln für ausgehenden Datenverkehr für die akzeptierten Listener-Protokolle und Portbereiche der Ressource erstellen.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich	Kommentar
CIDR range for resource	TCP	3306	Ermöglicht den Datenverkehr vom Ressourcen-Gateway zu Datenbanken.

IP-Adresstypen

Ein Ressourcen-Gateway kann über IPv6 oder über Dual-Stack-Adressen verfügenIPv4. Der IP-Adresstyp eines Ressourcengateways muss mit den Subnetzen des Ressourcengateways und dem IP-Adresstyp der Ressource kompatibel sein, wie hier beschrieben:

- IPv4— Weisen Sie Ihren Gateway-Netzwerkschnittstellen IPv4 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 Adressbereiche haben und die Ressource auch eine IPv4 Adresse hat.
- IPv6— Weisen Sie Ihren Gateway-Netzwerkschnittstellen IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv6 nur Subnetze sind und die Ressource auch eine IPv6 Adresse hat.
- Dualstack — Weisen Sie Ihren IPv4 Gateway-Netzwerkschnittstellen sowohl als auch IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze sowohl als auch IPv6 Adressbereiche haben IPv4 und die Ressource entweder eine IPv4 Oder-Adresse hat. IPv6

Der IP-Adresstyp des Ressourcen-Gateways ist unabhängig vom IP-Adresstyp des Clients oder des VPC Endpunkts, über den auf die Ressource zugegriffen wird.

Erstellen Sie ein Ressourcen-Gateway in VPC Lattice

Verwenden Sie die Konsole, um ein Ressourcen-Gateway zu erstellen.

Um ein Ressourcen-Gateway mit der Konsole zu erstellen

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter PrivateLink und Lattice die Option Resource Gateways aus.
3. Wählen Sie Create Resource Gateway aus.

4. Geben Sie einen Namen ein, der innerhalb Ihres AWS Kontos einzigartig ist.
5. Wählen Sie den IP-Typ für das Ressourcen-Gateway.
6. Wählen Sie die ausVPC, in der sich die Ressource befindet.
7. Wählen Sie bis zu fünf Sicherheitsgruppen aus, um den eingehenden Verkehr vom Servicenetzwerk zum Servicenetzwerk VPC zu kontrollieren.
8. (Optional) Sie fügen ein Tag hinzu, indem Sie neuen Tag hinzufügen auswählen und den Schlüssel und den Wert für den Tag eingeben.
9. Wählen Sie Create Resource Gateway aus.

Um ein Ressourcen-Gateway mit dem zu erstellen AWS CLI

Verwenden Sie den create-resource-gateway-Befehl.

Löschen Sie ein Ressourcen-Gateway in VPC Lattice

Verwenden Sie die Konsole, um ein Ressourcen-Gateway zu löschen.

Um ein Ressourcen-Gateway mit der Konsole zu löschen

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter PrivateLink und Lattice die Option Resource Gateways aus.
3. Aktivieren Sie das Kontrollkästchen für das Resource Gateway, das Sie löschen möchten, und wählen Sie Aktionen, Löschen aus. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

Um ein Resource Gateway mit dem zu löschen AWS CLI

Verwenden Sie den delete-resource-gateway-Befehl.

Zugriff auf Servicenetzwerke über AWS PrivateLink

Sie können über einen VPC Servicenetzwerk-Endpunkt (Servicenetzwerk-Endpunkt) eine private Verbindung zu einem Servicenetzwerk VPC herstellen. Über einen Servicenetzwerk-Endpunkt können Sie privat und sicher auf die Ressourcen und Dienste zugreifen, die dem Servicenetzwerk zugeordnet sind. Auf diese Weise können Sie über einen einzigen VPC Endpunkt privat auf mehrere Ressourcen und Dienste zugreifen.

Ein Servicenetzwerk ist eine logische Sammlung von Ressourcenkonfigurationen und VPC Lattice-Diensten. Mithilfe eines Servicenetzwerk-Endpunkts können Sie ein Servicenetzwerk mit Ihrem VPC verbinden und auf diese Ressourcen und Dienste privat von Ihnen VPC oder vor Ort aus zugreifen. Über einen Servicenetzwerk-Endpunkt können Sie eine Verbindung zu einem Servicenetzwerk herstellen. Um von Ihrem aus eine Verbindung zu mehreren Servicenetzwerken herzustellenVPC, können Sie mehrere Dienstnetzwerk-Endpunkte erstellen, von denen jeder auf ein anderes Servicenetzwerk verweist.

Servicenetzwerke sind in AWS Resource Access Manager ()AWS RAM integriert. Sie können Ihr Servicenetzwerk über mit einem anderen Konto teilen AWS RAM. Wenn Sie ein Servicenetzwerk mit einem anderen AWS Konto teilen, kann dieses Konto einen Servicenetzwerk-Endpunkt erstellen, über den Sie eine Verbindung zum Servicenetzwerk herstellen können. Sie können ein Servicenetzwerk mithilfe eines Resource Share-In AWS RAM gemeinsam nutzen.

Verwenden Sie die AWS RAM Konsole, um die Ressourcenfreigaben, zu denen Sie hinzugefügt wurden, die gemeinsamen Dienstnetzwerke, auf die Sie zugreifen können, und die AWS Konten, die die Ressourcen mit Ihnen gemeinsam genutzt haben, anzuzeigen. Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch unter Mit Ihnen geteilte Ressourcen.

Preisgestaltung

Die Ressourcenkonfigurationen, die mit Ihrem Servicenetzwerk verknüpft sind, werden Ihnen stündlich in Rechnung gestellt. Ihnen wird auch pro GB verarbeiteter Daten in Rechnung gestellt, wenn Sie über den Endpunkt des Servicenetzwerks VPC auf Ressourcen zugreifen. Der Endpunkt des Servicenetzwerks VPC selbst wird Ihnen nicht stündlich in Rechnung gestellt. Weitere Informationen finden Sie unter Amazon VPC Lattice Preise.

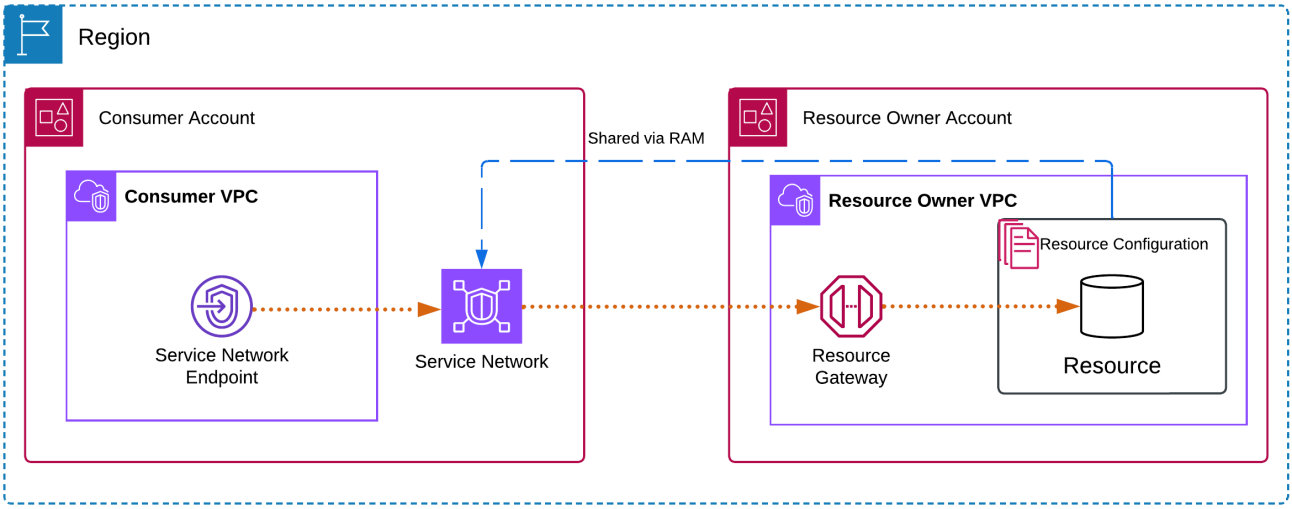
Inhalt

- DNSHostnamen
- DNSLösung
- Privat DNS
- Subnetze und Availability Zones
- IP-Adresstypen
- Greifen Sie über einen Servicenetzwerk-Endpunkt auf ein Servicenetzwerk zu
- Dienstnetzwerk-Endpunkte verwalten

Übersicht

Sie können entweder Ihr eigenes Servicenetzwerk erstellen, oder ein Servicenetzwerk kann von einem anderen Konto aus mit Ihnen geteilt werden. In beiden Fällen können Sie einen Servicenetzwerk-Endpunkt erstellen, um von Ihrem VPC aus eine Verbindung zu diesem herzustellen. Weitere Informationen zum Erstellen eines Servicenetzwerks und zum Zuordnen von Ressourcenkonfigurationen finden Sie im Amazon VPC Lattice-Benutzerhandbuch.

Das folgende Diagramm zeigt, wie ein Servicenetzwerk-Endpunkt in Ihrem Netzwerk auf ein Servicenetzwerk VPC zugreift.



Netzwerkverbindungen können nur von dem Endpunkt aus initiiert werdenVPC, der den Servicenetzwerk-Endpunkt hat, zu den Ressourcen und Diensten im Servicenetzwerk. VPCMit den Ressourcen und Diensten können keine Netzwerkverbindungen zum Endpunkt VPC initiiert werden.

DNSHostnamen

Mit AWS PrivateLink senden Sie über private Endpunkte Datenverkehr an Servicenetzwerke. Wenn Sie einen VPC Servicenetzwerk-Endpunkt erstellen, erstellen wir regionale DNS Namen (DNSStandardname genannt) für jede Ressource und jeden Dienst, die Sie verwenden können, um mit der Ressource und dem Dienst von Ihrem Standort aus und von Ihrem Standort VPC aus zu kommunizieren.

Der DNS Standardname für eine Ressource im Servicenetzwerk hat die folgende Syntax:

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

Der DNS Standardname für einen Lattice-Dienst im Dienstnetzwerk hat die folgende Syntax:

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

Wenn Ihr Servicenetzwerk über Ressourcenkonfigurationen verfügt, die verwendenARNs, können Sie Private aktivieren. DNS Mit Private können Sie weiterhin Anfragen an die Ressource stellenDNS, indem Sie den DNS Namen verwenden, den der Dienst für die Ressource bereitgestellt hat, und gleichzeitig die private Konnektivität über den AWS VPC Dienstnetzwerk-Endpunkt nutzen. Weitere Informationen finden Sie unter the section called “DNSAuflösung”.

DNSLösung

Wenn Sie einen Servicenetzwerkendpunkt erstellen, erstellen wir DNS Namen für jede Ressourcenkonfiguration und jeden Lattice-Dienst, der dem Dienstnetzwerk zugeordnet ist. Diese DNS Aufzeichnungen sind öffentlich. Daher sind diese DNS Namen öffentlich auflösbar. DNSAnfragen von außerhalb geben jedoch VPC immer noch die privaten IP-Adressen der Netzwerkschnittstellen des Servicenetzwerkendpunkts zurück. Sie können diese DNS Namen verwenden, um lokal auf die Ressourcen und Dienste zuzugreifen, sofern Sie Zugriff auf den Endpunkt habenVPC, in dem sich der Servicenetzwerk-Endpunkt befindet, über VPN oder Direct Connect.

Privat DNS

Wenn Sie Private DNS für Ihren VPC Service-Netzwerk-Endpunkt aktivieren und bei Ihrem VPC sowohl DNSHostnamen als auch DNS Auflösung aktiviert sind, erstellen wir versteckte, AWS verwaltete private Hosting-Zonen für die Ressourcenkonfigurationen mit benutzerdefinierten Namen.

DNS Die gehostete Zone enthält einen Datensatz für den DNS Standardnamen der Ressource, der ihn in die privaten IP-Adressen der Netzwerkschnittstellen des Servicenetzwerk-Endpunkts in Ihrem auflöst. VPC

Amazon stellt für Sie einen DNS Server bereitVPC, den sogenannten Route 53 Resolver. Der Route 53 Resolver löst automatisch lokale VPC Domainnamen auf und zeichnet in privaten Hosting-Zonen auf. Sie können den Route 53 Resolver jedoch nicht von außerhalb Ihres verwenden. VPC Wenn Sie von Ihrem lokalen Netzwerk aus auf Ihren VPC Endpunkt zugreifen möchten, können Sie die DNS Standardnamen verwenden oder Sie können Route 53 Resolver-Endpunkte und Resolver-Regeln verwenden. Weitere Informationen finden Sie unter Integration mit und. AWS Transit GatewayAWS PrivateLinkAmazon Route 53 Resolver

Subnetze und Availability Zones

Sie können Ihren VPC Endpunkt 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. In einer Produktionsumgebung empfehlen wir für hohe Verfügbarkeit und Ausfallsicherheit, mindestens zwei Availability Zones für jeden VPC Endpunkt zu konfigurieren.

IP-Adresstypen

Service-Netzwerk-Endpunkte können Dual-Stack-Adressen oder IPv4 IPv6 Dual-Stack-Adressen unterstützen. Endpunkte, die dies unterstützen, IPv6 können Anfragen mit Datensätzen beantwortenDNS. AAAA Der IP-Adresstyp eines Dienstnetzwerkendpunkts muss mit den Subnetzen für den Ressourcenendpunkt kompatibel sein, wie hier beschrieben:

- IPv4— Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv4 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 Adressbereiche haben.
- IPv6— Weisen Sie Ihren Endpunkt-Netzwerkschnittstellen IPv6 Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv6 nur Subnetze sind.
- Dualstack — Weisen Sie Ihren IPv4 Endpunkt-Netzwerkschnittstellen sowohl IPv6 Adressen als auch Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 sowohl IPv6 als auch Adressbereiche haben.

Wenn ein VPC Servicenetzwerkendpunkt dies unterstütztIPv4, haben IPv4 die Netzwerkschnittstellen des Endpunkts Adressen. Wenn ein VPC Servicenetzwerk-Endpunkt dies unterstütztIPv6,

haben IPv6 die Endpunkt-Netzwerkschnittstellen Adressen. Die IPv6 Adresse für eine Endpunkt-Netzwerkschnittstelle ist vom Internet aus nicht erreichbar. Wenn Sie eine Endpunkt-Netzwerkschnittstelle mit einer IPv6 Adresse beschreiben, beachten Sie, dass diese aktiviert `denyAllIgwTraffic` ist.

Greifen Sie über einen Servicenetzwerk-Endpunkt auf ein Servicenetzwerk zu

Sie können über einen Servicenetzwerk-Endpunkt auf ein Servicenetzwerk zugreifen. Ein Servicenetzwerk-Endpunkt bietet privaten Zugriff auf Ressourcenkonfigurationen und Dienste im Servicenetzwerk.

Voraussetzungen

Um einen Servicenetzwerk-Endpunkt zu erstellen, müssen Sie die folgenden Voraussetzungen erfüllen.

- Sie müssen über ein Servicenetzwerk verfügen, das entweder von Ihnen erstellt oder von einem anderen Konto aus für Sie freigegeben wurde. AWS RAM
- Wenn ein Servicenetzwerk von einem anderen Konto aus mit Ihnen gemeinsam genutzt wird, müssen Sie die Ressourcenfreigabe, die das Servicenetzwerk enthält, überprüfen und akzeptieren. Weitere Informationen finden Sie unter Annehmen und Ablehnen von Ressourcenfreigabeeinladungen im AWS RAM -Benutzerhandbuch.

Erstellen Sie einen Servicenetzwerk-Endpunkt

Erstellen Sie einen Servicenetzwerk-Endpunkt für den Zugriff auf das Servicenetzwerk, das mit Ihnen geteilt wurde.

Um einen Servicenetzwerk-Endpunkt zu erstellen

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen.
4. Sie können einen Namen angeben, um das Auffinden und Verwalten des Endpunkts zu erleichtern.

5. Wählen Sie als Typ die Option Servicenetzwerke aus.
6. Wählen Sie für Servicenetzwerke das Dienstnetzwerk aus, das mit Ihnen geteilt wurde.
7. Wählen Sie unter Netzwerkeinstellungen Ihr Netzwerk aus, VPC von dem aus Sie auf das Servicenetzwerk zugreifen möchten.
8. Wenn Sie privaten DNS Support konfigurieren möchten, wählen Sie Zusätzliche Einstellungen, DNSNamen aktivieren aus. Um diese Funktion nutzen zu können, stellen Sie sicher, dass die Attribute DNSHostnamen aktivieren und DNS Support aktivieren für Sie VPC aktiviert sind.
9. Wählen Sie Endpunkt erstellen aus.

So erstellen Sie einen Service-Network-Endpunkt über die Befehlszeile

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

Dienstnetzwerk-Endpunkte verwalten

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

Aufgaben

- Löschen eines Endpunkts
- Aktualisieren Sie einen Dienstnetzwerk-Endpunkt

Löschen eines Endpunkts

Wenn Sie mit einem VPC Endpunkt fertig sind, können Sie ihn löschen.

Um einen Endpunkt mit der Konsole zu löschen

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Service-Netzwerk-Endpunkt aus.
4. Wählen Sie Aktionen, VPCEndpunkte löschen aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein.

6. Wählen Sie Löschen.

Um einen Endpunkt über die Befehlszeile zu löschen

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

Aktualisieren Sie einen Dienstnetzwerk-Endpunkt

Sie können einen VPC Endpunkt aktualisieren.

Um einen Endpunkt mit der Konsole zu aktualisieren

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Endpunkt.
4. Wählen Sie Aktionen und die entsprechende Option.
5. Folgen Sie den Schritten auf der Konsole, um das Update einzureichen.

Um einen Endpunkt über die Befehlszeile zu aktualisieren

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

Identitäts- und Zugriffsmanagement für AWS PrivateLink

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

Inhalt

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie arbeiten 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 Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern 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 anschließend bei Ihrem IAM-Administrator entsprechende Änderungen für die Berechtigungen Ihrer Service-Benutzer anfordern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM zu verstehen.

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff darauf zu verwalten AWS PrivateLink.

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 übernehmen. 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 (IAMIdentity Center-) Nutzer, 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 der 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 IAMBenutzerhandbuch unter AWS Signature Version 4 für API Anfragen.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. 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 AWS Multi-Faktor-Authentifizierung IAM 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. Verwenden Sie diese nur, 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 im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

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 IAMBenutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Ein 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 eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung 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 im Benutzerhandbuch unter Anwendungsfälle für IAM IAM Benutzer.

IAM-Rollen

Eine IAMRolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM Rolle in der zu übernehmen AWS Management Console, können Sie von einem Benutzer zu einer IAM Rolle (Konsole) wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Methoden zur Übernahme einer Rolle im IAMBenutzerhandbuch.

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 im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter (Federation). Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, 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 verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff: Sie können eine IAM-Rolle verwenden, um jemandem (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 zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen. AWS-Services Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Wenn Sie einige Dienste verwenden, führen Sie möglicherweise eine Aktion aus, die dann eine weitere Aktion in einem anderen Dienst auslöst. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgeschaltete Dienste zu stellen. FASAnfragen 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 beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.
  - Dienstbezogene Rolle — Eine dienstverknüpfte 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 serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API Anfragen stellen AWS CLI . Das ist empfehlenswerter, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2 Instance eine AWS Rolle zuzuweisen und sie all 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 im IAMBenutzerhandbuch unter Verwenden einer IAM

Rolle, um Berechtigungen für Anwendungen zu erteilen, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese mit AWS Identitäten oder Ressourcen verknüpfen. 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. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

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 aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie im Benutzerhandbuch unter Definieren benutzerdefinierter IAM Berechtigungen mit vom Kunden verwalteten Richtlinien. IAM

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 oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Wählen Sie zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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 nicht IAM in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Amazon S3 und AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bietenACLs. Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

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 eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM

Entität (IAMBenutzer oder Rolle) gewähren 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 zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.

- Dienststeuerungsrichtlinien (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 Geräte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — RCPs sind JSON Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Sie RCP schränken die Berechtigungen für Ressourcen in Mitgliedskonten ein und können sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu OrganizationsRCPs, einschließlich einer Liste AWS-Services dieser Support-LeistungenRCPs, finden Sie unter Resource Control Policies (RCPs) 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 Benutzerhandbuch zu IAM.

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 IAMBenutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS PrivateLink funktioniert mit IAM

Informieren Sie sich vor der Verwendung IAM zur Verwaltung des Zugriffs auf AWS PrivateLink, welche IAM Funktionen zur Verwendung verfügbar sind 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
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

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

Identitätsbasierte Richtlinien für AWS PrivateLink

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie im Benutzerhandbuch unter Definieren benutzerdefinierter IAM Berechtigungen mit vom Kunden verwalteten Richtlinien. IAM

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. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie in der Referenz zu IAM JSON Richtlinienelementen im IAMBenutzerhandbuch.

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 anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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 IAMim IAMBenutzerhandbuch unter Kontoübergreifender Ressourcenzugriff.

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 bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Action` Element 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, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API 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.

Aktionen im ec2-Namespace

Einige Aktionen für AWS PrivateLink sind Teil des Amazon EC2API. Diese Richtlinienaktionen verwenden das `ec2` Präfix. Weitere Informationen finden Sie unter AWS PrivateLink Aktionen in der EC2APIAmazon-Referenz.

Aktionen im VPCE-Namespace

AWS PrivateLink stellt auch die Aktion nur für `AllowMultiRegion` Berechtigungen bereit. Diese Richtlinienaktion verwendet das Präfix. `vpce`

Politische Ressourcen für AWS PrivateLink

Unterstützt Richtlinienressourcen: Ja

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

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. 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": "*"
```

Schlüssel zur Richtlinienbedingung für AWS PrivateLink

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: 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 `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 im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

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

Die folgenden Bedingungsschlüssel sind spezifisch für AWS PrivateLink:

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

Weitere Informationen finden Sie unter Condition Keys for Amazon EC2.

ACLsin AWS PrivateLink

UnterstütztACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

ABACmit AWS PrivateLink

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. In werden AWS 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 vonABAC. Anschließend entwerfen

Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich 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 dazu finden Sie ABAC unter Definieren von Berechtigungen mit ABAC Autorisierung im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

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 darüber, AWS-Services wie Sie mit temporären Anmeldeinformationen arbeiten können AWS-Services , finden Sie IAM im IAMBenutzerhandbuch unter Diese Informationen.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Kennwort 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 Rollenwechsel finden Sie im Benutzerhandbuch unter Von einem Benutzer zu einer IAM Rolle (Konsole) wechseln. IAM

Mit dem AWS CLI oder können Sie manuell temporäre Anmeldeinformationen erstellen AWS API. 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 unter IAM.

Serviceübergreifende Prinzipalberechtigungen für AWS PrivateLink

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Wenn Sie einige Dienste verwenden, führen Sie möglicherweise eine Aktion aus, die dann eine weitere Aktion in einem anderen Dienst auslöst. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgeschaltete Dienste zu stellen. FASAnfragen 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 beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS PrivateLink

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.

Mit Diensten verknüpfte Rollen für AWS PrivateLink

Unterstützt serviceverknüpfte Rollen: Ja

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 serviceverknüpfte 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 von AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen AWS API. Um Benutzern die Berechtigung zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein

IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie mithilfe dieser Beispieldokumente zu JSON Richtlinien finden Sie im IAMBenutzerhandbuch unter IAM Richtlinien erstellen (Konsole).

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

Beispiele

- Steuern Sie die Verwendung von VPC Endpunkten
- Steuern Sie die Erstellung von VPC Endpunkten auf der Grundlage des Dienstbesitzers
- Steuern Sie die privaten DNS Namen, die für VPC Endpunktdienste angegeben werden können
- Steuern Sie die Dienstnamen, die für VPC Endpunktdienste angegeben werden können

Steuern Sie die Verwendung 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":"*"
        }
    ]
}
```

Hinweise zur Steuerung des Zugriffs auf Dienste mithilfe von VPC Endpunkten finden Sie unter. the section called “Endpunktrichtlinien”

Steuern Sie die Erstellung von VPC Endpunkten auf der Grundlage des Dienstbesitzers

Sie können den `ec2:VpceServiceOwner` Bedingungsschlüssel verwenden, um zu steuern, welcher VPC Endpunkt basierend darauf erstellt werden kann, wem der Dienst gehört (`amazon`,`aws-marketplace`, oder die Konto-ID). Das folgende Beispiel erteilt die Erlaubnis, VPC Endpoints mit dem angegebenen Dienstbesitzer zu erstellen. 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 Sie die privaten DNS Namen, die für VPC Endpunktdienste angegeben werden können

Sie können den `ec2:VpceServicePrivateDnsName` Bedingungsschlüssel verwenden, um zu steuern, welcher VPC Endpunktdienst auf der Grundlage des privaten DNS Namens, der dem VPC Endpunktdienst zugeordnet ist, geändert oder erstellt werden kann. Das folgende Beispiel erteilt die Erlaubnis, einen VPC Endpunktdienst mit dem angegebenen privaten DNS Namen zu erstellen. 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 Sie die Dienstnamen, die für VPC Endpunktdienste angegeben werden können

Sie können den `ec2:VpceServiceName` Bedingungsschlüssel verwenden, um zu steuern, welcher VPC Endpunkt auf der Grundlage des VPC Endpunktdienstnamens erstellt werden kann. Das folgende Beispiel erteilt die Erlaubnis, einen VPC Endpunkt mit dem angegebenen Dienstnamen zu erstellen. 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 Sie den Zugriff auf VPC Endgeräte 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 eine verwenden können. AWS-Service

Eine Endpunktrichtlinie setzt keine identitätsbasierten Richtlinien oder ressourcenbasierten Richtlinien außer Kraft oder ersetzt sie. Wenn Sie beispielsweise einen Schnittstellenendpunkt verwenden, um eine Verbindung zu Amazon S3 herzustellen, können Sie auch Amazon S3 S3-Bucket-

Richtlinien verwenden, um den Zugriff auf Buckets von bestimmten Endpunkten oder bestimmten zu kontrollieren. VPCs

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 hinzufügen. 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 Endpunktdienst als einen erstellen AWS-Service, gewähren wir vollen Zugriff auf den Endpunkt.
- Sie können keine Platzhalterzeichen (* oder?) verwenden oder numerische Bedingungsoperatoren mit globalen Kontextschlüsseln, die auf vom System generierte Bezeichner verweisen (z. B. oder). `aws:PrincipalAccount` `aws:SourceVpc`
- Wenn Sie einen Bedingungsoperator für Zeichenfolgen verwenden, müssen Sie vor oder nach jedem Platzhalterzeichen mindestens sechs aufeinanderfolgende Zeichen verwenden.
- Wenn Sie ARN in einer Ressource oder Bedingung ein Element angeben, ARN kann der Kontoteil von eine Konto-ID oder ein Platzhalterzeichen enthalten, jedoch nicht beides.

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 finden Sie AWS-Services 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 den Benutzern und Rollen für das Konto gewährt, nicht allen Benutzern und Rollen.

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

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

- Endpunkte für Amazon S3
- Endpunkte für DynamoDB

Aktualisieren Sie eine 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 VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den VPC Endpunkt aus.
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 Save (Speichern) aus.

Ändern einer Endpunktrichtlinie mithilfe der Befehlszeile

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

AWS verwaltete Richtlinien für AWS PrivateLink

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS PrivateLink Aktualisierungen AWS verwalteter Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien AWS PrivateLink seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst. Abonnieren Sie den RSS Feed auf der Seite AWS PrivateLink Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AWS PrivateLink hat begonnen, Änderungen zu verfolgen	AWS PrivateLink hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	1. März 2021

CloudWatch Metriken für AWS PrivateLink

AWS PrivateLink veröffentlicht Datenpunkte CloudWatch für Ihre Schnittstellenendpunkte, Gateway Load Balancer-Endpunkte und Endpunktdienste auf Amazon. CloudWatch ermöglicht es Ihnen, Statistiken über diese Datenpunkte in Form eines geordneten Satzes von Zeitreihendaten, den so genannten Metriken, 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 beispielsweise einen CloudWatch Alarm erstellen, um eine bestimmte Metrik zu überwachen und eine Aktion einzuleiten (z. B. das Senden einer Benachrichtigung an eine E-Mail-Adresse), wenn die Metrik außerhalb des 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 AWS PrivateLink sendet Metriken ohne zusätzliche Kosten CloudWatch in Intervallen von einer Minute an.

Weitere Informationen finden Sie im CloudWatch Amazon-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. Dazu gehören Verbindungen in den ESTABLISHED Bundesstaaten SYN _ SENT und.

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 Endpunktdienst 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.

Die CloudWatch Metriken anzeigen

Sie können diese CloudWatch Metriken über die VPC Amazon-Konsole, die CloudWatch Konsole oder AWS CLI wie folgt anzeigen.

So zeigen Sie Metriken mit der VPC Amazon-Konsole an

1. Öffnen Sie die VPC Amazon-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.

Um Metriken mit der CloudWatch Konsole anzuzeigen

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

Um Metriken mit dem anzuzeigen 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 bietet integrierte Contributor Insights-Regeln für Ihre Endpunktdienste, mit denen Sie herausfinden können, welche Endgeräte die meisten Beiträge zu den einzelnen unterstützten Metriken leisten. Weitere Informationen finden Sie unter Contributor Insights im CloudWatch Amazon-Benutzerhandbuch.

AWS PrivateLink bietet die folgenden 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 an.

Bevor Sie eine integrierte Regel verwenden können, müssen Sie sie aktivieren. Nachdem Sie eine Regel aktiviert haben, beginnt sie mit dem Sammeln von Teilnehmerdaten. Informationen zu den Gebühren für Contributor Insights finden Sie unter CloudWatch Amazon-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 für die AWS PrivateLink Verwendung von AWS Management Console oder zu aktivieren. AWS CLI

Um die Contributor Insights-Regeln für die AWS PrivateLink Verwendung der Konsole zu aktivieren

1. Öffnen Sie die VPC Amazon-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.

Um die Contributor Insights-Regeln für die AWS PrivateLink Verwendung von zu aktivieren AWS CLI

1. Verwenden Sie den list-managed-insight-rulesBefehl wie folgt, um die verfügbaren Regeln aufzulisten. 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 put-managed-insight-rulesBefehl wie folgt, um die Regel zu aktivieren. Sie müssen den Vorlagennamen und den Namen 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 jederzeit 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.

Um die Contributor Insights-Regeln für die AWS PrivateLink Verwendung der Konsole zu deaktivieren

1. Öffnen Sie die VPC Amazon-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.

Um die Contributor Insights-Regeln für die AWS PrivateLink Verwendung von zu deaktivieren AWS CLI

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

Contributor-Insights-Regeln löschen

Gehen Sie wie folgt vor, um die integrierten Regeln für die AWS PrivateLink Verwendung von AWS Management Console oder zu löschen AWS CLI. Nachdem Sie eine Regel gelöscht haben, werden keine Leistungsträgerdaten mehr erfasst, und wir löschen die vorhandenen Leistungsträgerdaten.

Um Contributor Insights-Regeln für die AWS PrivateLink Verwendung der Konsole zu löschen

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).

Um Contributor Insights-Regeln für die AWS PrivateLink Verwendung von zu löschen AWS CLI

Verwenden Sie den delete-insight-rulesBefehl, um eine Regel zu löschen.

AWS PrivateLink Kontingente

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Dienst. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden. Wenn Sie eine Erhöhung des pro Ressource geltenden Kontingents beantragen, erhöhen wir das Kontingent für alle Ressourcen in der Region.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Drosselung anfordern

Die API Aktionen für AWS PrivateLink sind Teil des Amazon EC2API. Amazon EC2 drosselt seine API Anfragen auf der AWS-Konto Ebene. Weitere Informationen finden Sie unter Request Throttling im Amazon EC2 Developer Guide. Darüber hinaus werden API Anfragen auch auf Organisationsebene gedrosselt, um die Leistung von zu verbessern. AWS PrivateLink Wenn Sie die App verwenden AWS Organizations und einen `RequestLimitExceeded` Fehlercode erhalten, während Sie sich noch innerhalb der API Limits auf Kontoebene befinden, finden Sie weitere Informationen unter So identifizieren Sie AWS Konten, die eine große Anzahl von Anrufen tätigen. API Wenn Sie Hilfe benötigen, wenden Sie sich an Ihr Account-Team oder eröffnen Sie über den VPCService und die Kategorie VPCEndpunkte eine Anfrage beim technischen Support. Stellen Sie sicher, dass Sie ein Bild des `RequestLimitExceeded` Fehlercodes anhängen.

VPCEndpunktkontingente

Ihr AWS Konto hat die folgenden Kontingente für VPC Endgeräte.

Name	Standard	Anpassbar	Kommentare
Interface- und Gateway Load Balancer Balancer-Endpunkte pro VPC	50	Ja	Dies ist ein kombiniertes Kontingent für Schnittstellenendpunkte und Gateway-Load-Balancer-Endpunkte
VPCGateway-Endpunkte pro Region	20	Ja	Sie können bis zu 255 Gateway-Endpunkte pro erstellen VPC

Name	Standard	Anpassbar	Kommentare
Zeichen pro VPC Endpunktrichtlinie	20.480	Nein	Die maximale Größe einer VPC Endpunktrichtlinie, einschließlich Leerraum

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

- Standardmäßig unterstützt jeder VPC Endpunkt eine Bandbreite von bis zu 10 Gbit/s pro Availability Zone und skaliert automatisch auf bis zu 100 Gbit/s. Die maximale Bandbreite für einen VPC Endpunkt bei der Verteilung der Last auf alle Availability Zones entspricht der Anzahl der Availability Zones multipliziert mit 100 Gbit/s. Wenn Ihre Anwendung einen höheren Durchsatz benötigt, wenden Sie sich an den AWS -Support.
- Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe des größten zulässigen Pakets in Byte, das über einen VPC Endpunkt übertragen werden kann. Je größer derMTU, desto mehr Daten können in einem einzigen Paket übertragen werden. Ein VPC Endpunkt unterstützt einen Wert MTU von 8500 Byte. Pakete mit einer Größe von mehr als 8500 Byte, die am VPC Endpunkt ankommen, werden verworfen.
- Path MTU Discovery (PMTUD) wird nicht unterstützt. VPCEndpunkte generieren die folgende ICMP Meldung nicht: `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (Typ 3, Code 4).
- VPCEndpunkte erzwingen die Begrenzung der maximalen Segmentgröße (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
Greifen Sie auf Ressourcen und Servicenetzwerke zu	AWS PrivateLink unterstützt den Zugriff auf Ressourcen und Servicenetzwerke über VPC Kontogrenzen hinweg.	01. Dezember 2024
Regionsübergreifender Zugriff	Ein Dienstanbieter kann einen Dienst in einer Region hosten und ihn in einer Reihe von AWS Regionen verfügbar machen. Ein Servicenutzer wählt bei der Erstellung eines Endpunkts eine Service-R egion aus.	26. November 2024
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 Gateway Load Balancer-Endpunktdienste und Gateway Load Balancer-Endpunkte so konfigurieren, dass sie beide IPv6 Adressen oder IPv4 nur Adressen unterstützen. IPv6	12. Dezember 2022
Contributor Insights	Sie können die integrierten Contributor Insights-Regeln verwenden, um bestimmte	18. August 2022

	Endpunkte zu identifizieren, die am meisten zu den Metriken beitragen. CloudWatch AWS PrivateLink	
IPv6--Support	Dienstanbieter können ihren Endpunktdienst so einrichten, dass er IPv6 Anfragen akzeptiert, auch wenn ihre Back-End-Dienste nur Support bieten. IPv4 Wenn ein Endpunktdienst IPv6 Anfragen akzeptiert, können Dienstnutzer die IPv6 Unterstützung für ihre Schnittstellenendpunkte aktivieren, sodass sie über diesen Zugriff auf den Endpunktdienst zugreifen können. IPv6	11. Mai 2022
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 in Ihrem einen Gateway Load Balancer-Endpunkt erstellenVPC, um den Datenverkehr an einen VPC Endpunktdienst weiterzuleiten, den Sie mit einem Gateway Load Balancer konfiguriert haben.	10. November 2020

VPCEndpunkt-Richtlinien	Sie können eine IAM Richtlinie an einen VPC Schnittstellenendpunkt für einen AWS Dienst anhängen, um den Zugriff auf den Dienst zu kontrollieren.	23. März 2020
Bedingungsschlüssel für VPC Endpunkte und Endpunktdienste	Sie können EC2 Bedingungsschlüssel verwenden, um den Zugriff auf Endgeräte und VPC Endpunktdienste zu steuern.	6. März 2020
Kennzeichnen Sie VPC Endpunkte und Endpunktdienste bei der Erstellung	Sie können Tags hinzufügen, wenn Sie VPC Endpunkte und Endpunktdienste erstellen.	5. Februar 2020
Private Namen DNS	Sie können von Ihrem VPC privaten DNS Namen aus AWS PrivateLink auf basierte Dienste zugreifen.	6. Januar 2020
VPCEndpunktdienste	Sie können Ihre eigenen Endpunktdienste erstellen und es anderen Benutzern AWS-Konten und Benutzern ermöglichen, über einen VPC Schnittstellenendpunkt eine Verbindung zu Ihrem Dienst herzustellen. Sie können Ihre Endpunktservices für ein Abonnement im AWS Marketplace anbieten.	28. November 2017

VPCSchnittstellen-Endpunkte für AWS-Services	Sie können einen Schnittstellenendpunkt erstellen, mit dem Sie eine Verbindung zu AWS-Services dieser Integration herstellen können, AWS PrivateLink ohne ein Internet-Gateway oder ein NAT Internetgerät zu verwenden.	8. November 2017
VPCEndpunkte für DynamoDB	Sie können einen VPC Gateway-Endpunkt erstellen, um von Ihrem aus auf Amazon DynamoDB zuzugreifen, VPC ohne ein Internet-Gateway oder NAT ein Gerät zu verwenden.	16. August 2017
VPCEndpunkte für Amazon S3	Sie können einen VPC Gateway-Endpunkt erstellen, um von Ihrem aus auf Amazon S3 zuzugreifen, VPC 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.