AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

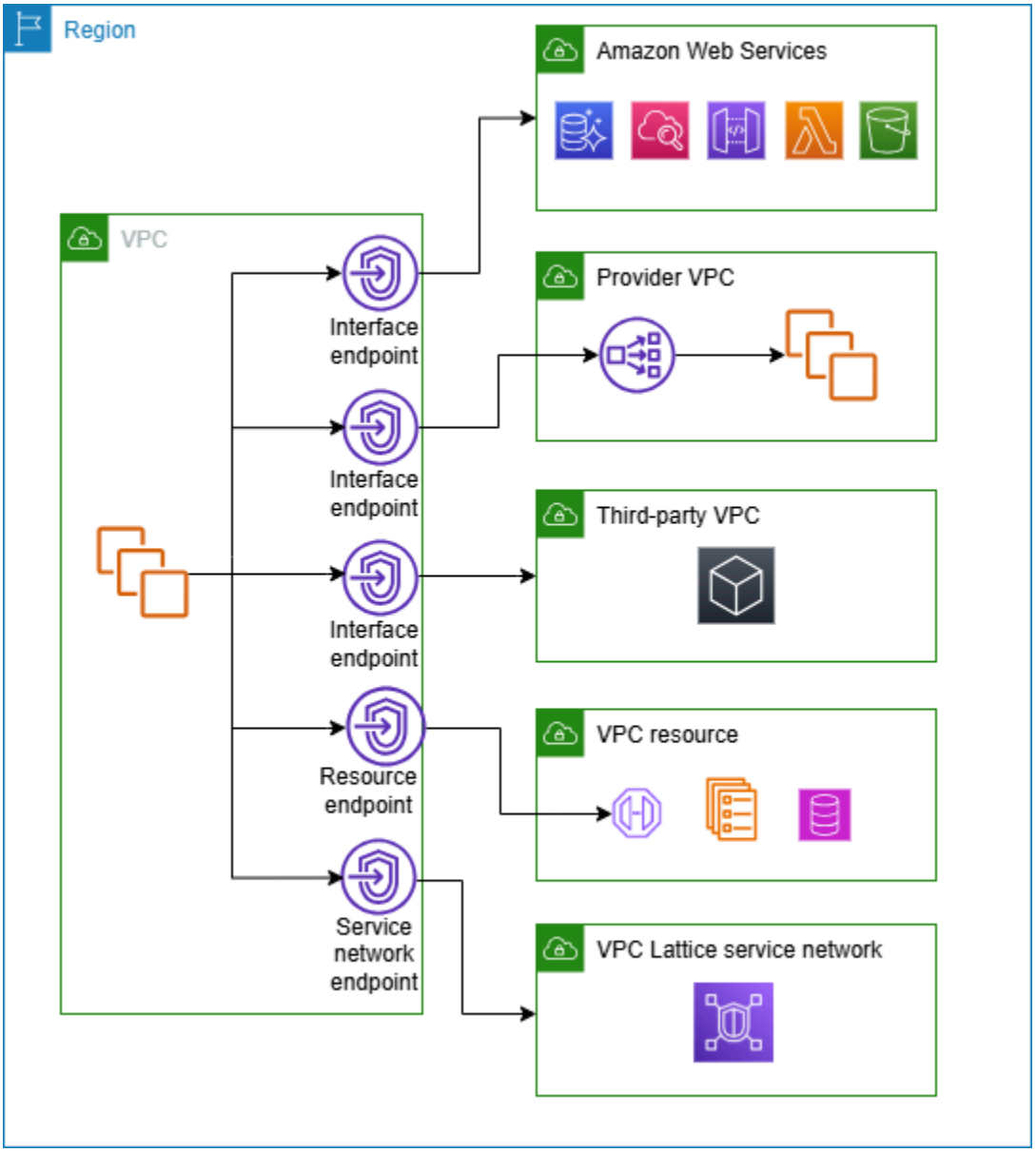
Was ist AWS PrivateLink?

AWS PrivateLink ist eine hochverfügbare, skalierbare Technologie, mit der Sie Ihre VPC privat mit Diensten und Ressourcen verbinden können, als ob sie sich in Ihrer VPC befinden würden. Sie müssen kein Internet-Gateway, kein NAT-Gerät, keine öffentliche IP-Adresse, Verbindung oder 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, Websites, Dienste und Ressourcen, die von Ihrer VPC aus erreichbar sind.

Anwendungsfälle

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

In der folgenden Abbildung hat die VPC auf der linken Seite mehrere Amazon EC2 EC2-Instances in einem privaten Subnetz und fünf VPC-Endpunkte — drei Schnittstellen-VPC-Endpunkte, einen Ressourcen-VPC-Endpunkt und einen VPC-Endpunkt für das Servicenetzwerk. Der erste VPC-Endpunkt der Schnittstelle stellt eine Verbindung zu einem AWS Dienst her. Der VPC-Endpunkt der zweiten Schnittstelle stellt eine Verbindung zu einem Dienst her, der von einem anderen AWS Konto gehostet wird (einem VPC-Endpunktdienst). Der dritte VPC-Schnittstellen-Endpunkt stellt eine Verbindung zu einem AWS Marketplace-Partnerdienst her. Der VPC-Endpunkt der Ressource stellt eine Verbindung zu einer Datenbank her. Der VPC-Endpunkt des Servicenetzwerks stellt eine Verbindung zu einem Servicenetzwerk her.



Weitere Informationen

- Konzepte
- Zugriff auf AWS-Services
- Zugriff auf SaaS-Produkte
- Zugriff auf virtuelle Appliances
- Teilen Sie Ihre Services

Arbeiten mit VPC-Endpunkten

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

- AWS-Managementkonsole— Stellt eine Weboberfläche bereit, über die Sie auf Ihre Ressourcen zugreifen können. AWS PrivateLink Öffnen Sie die Amazon VPC-Konsole und wählen Sie Endpoints oder Endpoint Services.
- AWS Command Line Interface (AWS CLI) — Stellt Befehle für eine Vielzahl von Befehlen bereit AWS-Services, darunter. AWS PrivateLink Weitere Informationen zu Befehlen für AWS PrivateLink finden Sie unter ec2 in der AWS CLI Befehlsreferenz.
- 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: VPCEndpoint ConnectionNotification
  - AWS: :EC2:: Dienst VPCEndpoint
  - AWS: :EC2: VPCEndpoint ServicePermissions
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS SDKs— Geben Sie sprachspezifisch an. APIs SDKs Sie 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 – Bietet API-Aktionen auf niedriger Ebene, die Sie mithilfe von HTTPS-Anforderungen aufrufen. Die Verwendung der Abfrage-API ist die direkteste Möglichkeit für den Zugriff auf Amazon VPC. Allerdings müssen dann viele technische Abläufe, wie beispielsweise das Erzeugen des Hashwerts zum Signieren der Anforderung und zur Fehlerbehandlung, in der Anwendung durchgeführt werden. Weitere Informationen finden Sie unter AWS PrivateLink -Aktionen in der Amazon-EC2-API-Referenz.

Preisgestaltung

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

AWS PrivateLink Konzepte

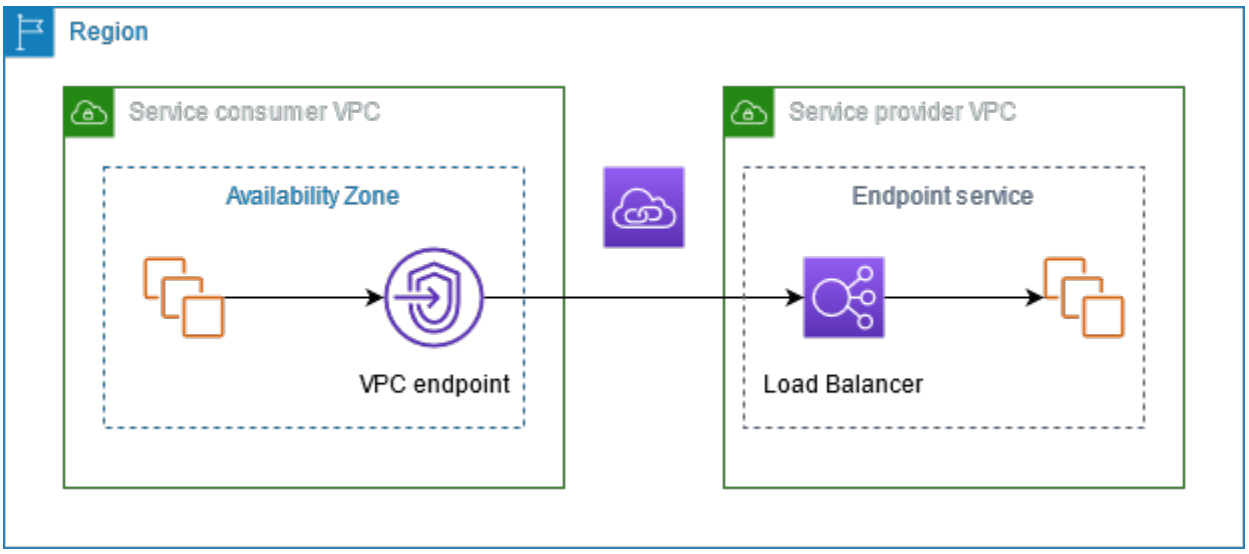
Sie können mithilfe von Amazon VPC eine Virtual Private Cloud (VPC) definieren. Dabei handelt es sich um ein logisch isoliertes virtuelles Netzwerk. Sie können den Clients in Ihrer VPC erlauben, sich mit Zielen außerhalb dieser VPC zu verbinden. Fügen Sie beispielsweise ein Internet-Gateway zur VPC hinzu,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

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

Inhalt

Architekturdiagramm

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



Anbieter

Verstehen Sie die Konzepte, die sich auf einen Anbieter beziehen.

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-Instances oder mithilfe von lokalen Servern hosten.

Ressourcenanbieter

Der Besitzer einer Ressource, beispielsweise einer Datenbank oder einer Amazon EC2 EC2-Instance, 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
- Konfiguration der Ressourcen
- 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 Service-Verbraucher muss beim Erstellen eines VPC-Endpunkts den Namen des Services angeben. Dienstnutzer können die Dienstnamen für AWS-Services abfragen. Service-Anbieter müssen die Namen ihrer Services mit den Service-Verbrauchern teilen.

Service-Zustände

Die folgenden Zustände sind für einen Endpunkt-Service möglich:

- Ausstehend — Der Endpunktdienst wird gerade erstellt.
- Verfügbar — Der Endpunktdienst ist verfügbar.
- Fehlgeschlagen — Der Endpunktdienst konnte nicht erstellt werden.
- Löschen — Der Dienstanbieter hat den Endpunktdienst gelöscht und der Löschvorgang ist im Gange.
- Gelöscht — Der Endpunktdienst wurde gelöscht.

Konfiguration der Ressourcen

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 darstellt. Eine Ressource kann eine IP-Adresse, ein Domainnamenziel oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank sein.

Bei der gemeinsamen Nutzung mit anderen Konten muss der Ressourcenanbieter die Ressource über eine AWS Resource Access Manager(AWS RAM) -Ressourcenfreigabe gemeinsam nutzen,

damit bestimmte AWS Prinzipale des anderen Kontos über einen Ressourcen-VPC-Endpunkt eine Verbindung mit der Ressource herstellen können.

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

Ressourcen-Gateway

Ein Ressourcen-Gateway ist ein Zugangspunkt in eine VPC, von dem aus eine Ressource gemeinsam genutzt wird. Der Anbieter erstellt ein Ressourcen-Gateway, um Ressourcen aus der 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 VPC-Endpunkt, um seine VPC mit einem Endpunktdienst oder einer Endpunktressource zu verbinden. Ein Verbraucher muss bei der Erstellung eines VPC-Endpunkts den Endpunktdienst, die Ressource oder das Dienstnetzwerk angeben. Es gibt mehrere Arten von VPC-Endpunkten. Sie müssen den VPC-Endpunkttyp erstellen, den Sie benötigen.

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

- `Resource`- Erstellen Sie einen Ressourcenendpunkt, um auf eine Ressource zuzugreifen, die mit Ihnen gemeinsam genutzt wurde und sich in einer anderen VPC befindet. Mit einem Ressourcenendpunkt können Sie privat und sicher auf Ressourcen wie eine Datenbank, eine Amazon EC2 EC2-Instance, 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-Endpunkt, `Gateway`, der einen Gateway-Endpunkt erstellt, um Datenverkehr an Amazon S3 oder DynamoDB zu senden. Gateway-Endpunkte verwenden im AWS PrivateLink Gegensatz zu den anderen Arten von VPC-Endpunkten nicht. Weitere Informationen finden Sie unter the section called “Gateway-Endpunkte”.

Endpunkt-Netzwerkschnittstellen

Eine Endpunkt-Netzwerkschnittstelle ist eine vom Anforderer verwaltete Netzwerkschnittstelle, die als Einstiegspunkt für Datenverkehr dient, der an einen Endpunktdienst, eine Ressource oder ein Dienstnetzwerk gerichtet ist. Für jedes Subnetz, das Sie beim Erstellen eines VPC-Endpunkts angeben, erstellen wir eine Endpunkt-Netzwerkschnittstelle im Subnetz.

Wenn ein VPC-Endpunkt dies unterstützt IPv4, haben seine Endpunkt-Netzwerkschnittstellen IPv4 Adressen. Wenn ein VPC-Endpunkt dies unterstützt IPv6, 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 VPC-Endpunktrichtlinie ist eine IAM-Ressourcenrichtlinie, die Sie Ihrem VPC-Endpunkt anfügen können. Sie bestimmt, welche Prinzipale den VPC-Endpunkt verwenden können, um auf den Endpunkt-Service zuzugreifen. Die standardmäßige VPC-Endpunktrichtlinie erlaubt alle Aktionen aller Prinzipale auf allen Ressourcen über den VPC-Endpunkt.

Endpunktzustände

Wenn Sie einen VPC-Schnittstellen-Endpunkt erstellen, erhält der Endpunktdienst eine Verbindungsanforderung. Der Service-Anbieter kann die Anfrage annehmen oder ablehnen. Wenn der Dienstanbieter die Anfrage akzeptiert, kann der Servicekonsument den VPC-Endpunkt verwenden, nachdem er in den Status Verfügbar übergegangen ist.

Die folgenden Zustände sind für einen VPC-Endpunkt möglich:

- PendingAcceptance - Die Verbindungsanforderung steht noch aus. Dies ist der Ausgangszustand, wenn Anfragen manuell akzeptiert werden.
- Ausstehend — Der Dienstanbieter hat die Verbindungsanfrage akzeptiert. Dies ist der Ausgangszustand, wenn Anfragen automatisch akzeptiert werden. Der VPC-Endpunkt kehrt in diesen Zustand zurück, wenn der Service-Verbraucher den VPC-Endpunkt ändert.
- Verfügbar — Der VPC-Endpunkt kann verwendet werden.
- Abgelehnt — Der Dienstanbieter hat die Verbindungsanforderung abgelehnt. Der Service-Anbieter kann eine Verbindung auch ablehnen, nachdem sie zur Verwendung verfügbar ist.
- Abgelaufen — Die Verbindungsanforderung ist abgelaufen.
- Fehlgeschlagen — Der VPC-Endpunkt konnte nicht verfügbar gemacht werden.
- Löschen — Der Service Consumer hat den VPC-Endpunkt gelöscht und der Löschvorgang ist im Gange.
- Gelöscht — Der VPC-Endpunkt wurde gelöscht.

Die AWS PrivateLink API gibt die möglichen Zustände mithilfe von Camel Case zurück.

AWS PrivateLink Verbindungen

Der Datenverkehr von Ihrer VPC wird über eine Verbindung zwischen dem VPC-Endpunkt und dem Endpunktdienst oder der 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.

Mit Schnittstellen-VPC-Endpunkten können Verbraucher mithilfe von Endpunktrichtlinien steuern, welche IAM-Prinzipale einen VPC-Endpunkt für den Zugriff auf einen Endpunktdienst oder eine Endpunktressource verwenden können.

Private, gehostete Zonen

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

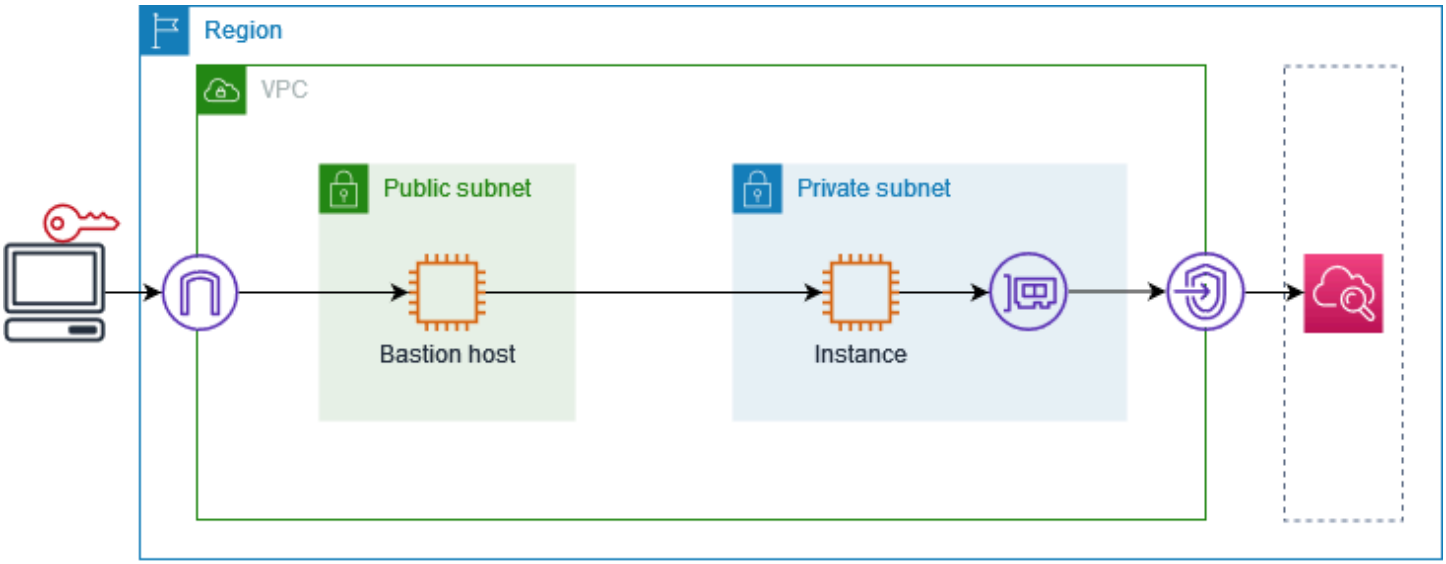
Sie können Amazon Route 53 so konfigurieren, dass der Domain-Datenverkehr an einen VPC-Endpunkt weitergeleitet wird. Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs an einen VPC-Endpunkt mit Ihrem Domain-Namen.

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

Fangen Sie an mit AWS PrivateLink

Dieses Tutorial zeigt, wie Sie 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 Instance, für die bestimmt CloudWatch ist, zur Endpunkt-Netzwerkschnittstelle aufgelöst und dann an die CloudWatch Verwendung des VPC-Endpunkts gesendet.



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

Aufgaben

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

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

Schritt 1: Erstellen einer VPC mit Subnetzen

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

So erstellen Sie die VPC

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

Schritt 2: Starten der Instances

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

Voraussetzungen

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

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

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. Wählen Sie unter VPC Ihre VPC aus.
    b. Wählen Sie unter Subnet (Subnetz) das öffentliche Subnetz aus.
    c. Wählen Sie unter Auto-assign public IP (Öffentlche IP automatisch zuweisen) die Option Enable (Aktivieren) aus.
    d. Wählen Sie unter Firewall die Option Select existing security group (Vorhandene Sicherheitsgruppe auswählen) aus und wählen Sie dann die Sicherheitsgruppe für den Bastion-Host aus.
7. Wählen Sie Launch Instance (Instance starten) aus.

So starten Sie die Instance

1. Öffnen Sie die 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. Wählen Sie unter VPC Ihre VPC aus.

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

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

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

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

Schritt 3: CloudWatch Zugriff testen

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

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

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

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

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

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

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

Voraussetzung

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

So erstellen Sie einen VPC-Endpunkt für CloudWatch

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

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

Schritt 5: Testen des VPC-Endpunkts

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

So testen Sie den VPC-Endpunkt

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

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

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

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

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

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

Schritt 6: Bereinigen

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

So beenden Sie die Instances

1. Öffnen Sie die 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.

Löschen des VPC-Endpunkts

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

Zugriff AWS-Services über AWS PrivateLink

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

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

Preisgestaltung

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

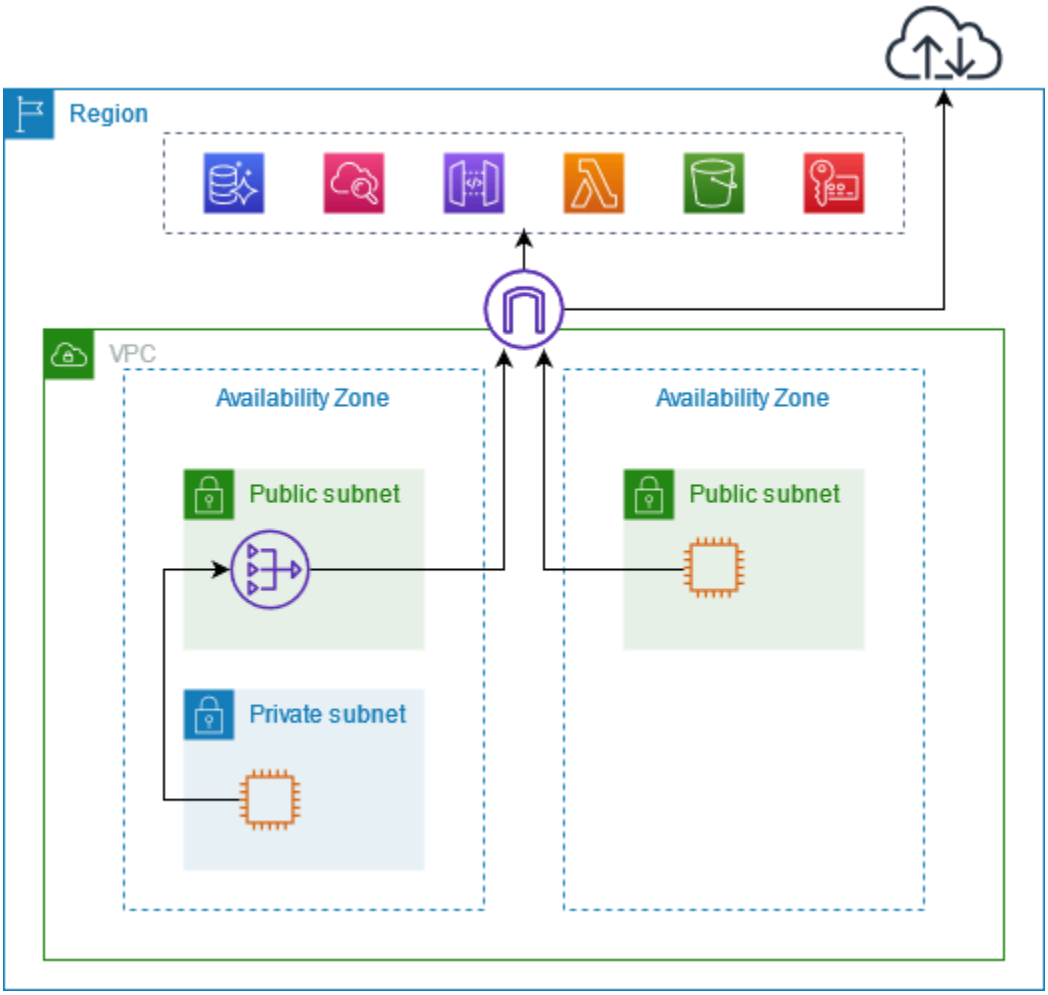
Inhalt

-Übersicht

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

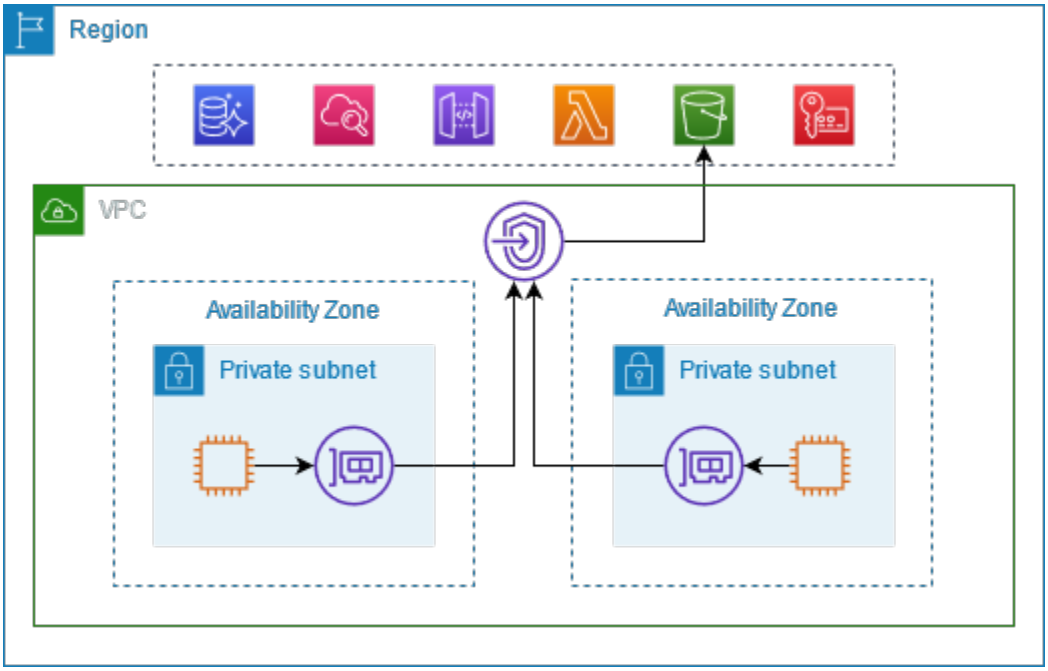
Zugang über Endpunkte für öffentliche Services

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



Connect über AWS PrivateLink

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



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

DNS-Hostnamen

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

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

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

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

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

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

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

Die zonalen DNS-Namen haben die folgende Syntax:

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

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

Der folgende 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"
        }
    ]
]
```

DNS-Auflösung

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

Privates DNS

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

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

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

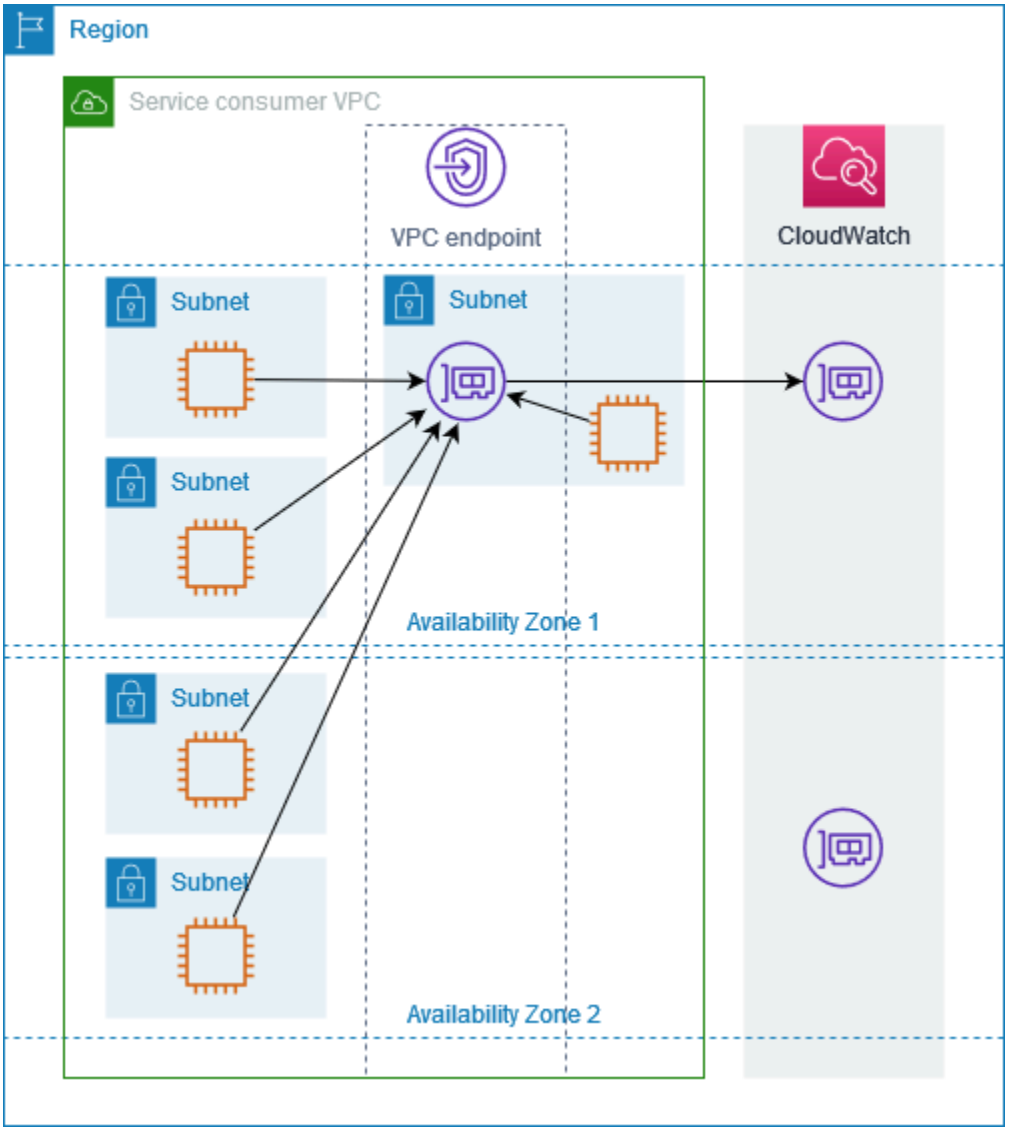
Subnetze und Availability Zones

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

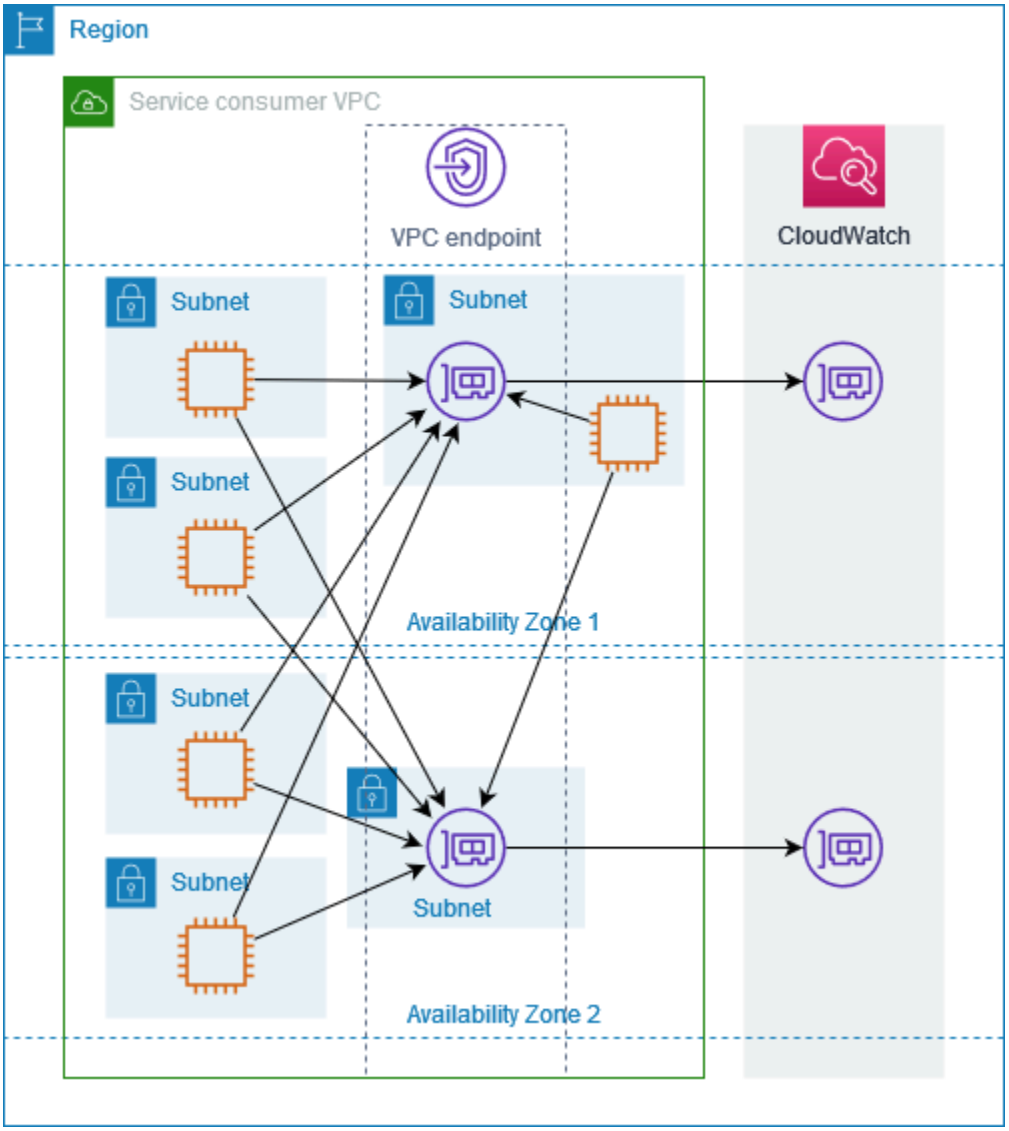
In einer Produktionsumgebung empfehlen wir für hohe Verfügbarkeit und Ausfallsicherheit Folgendes:

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

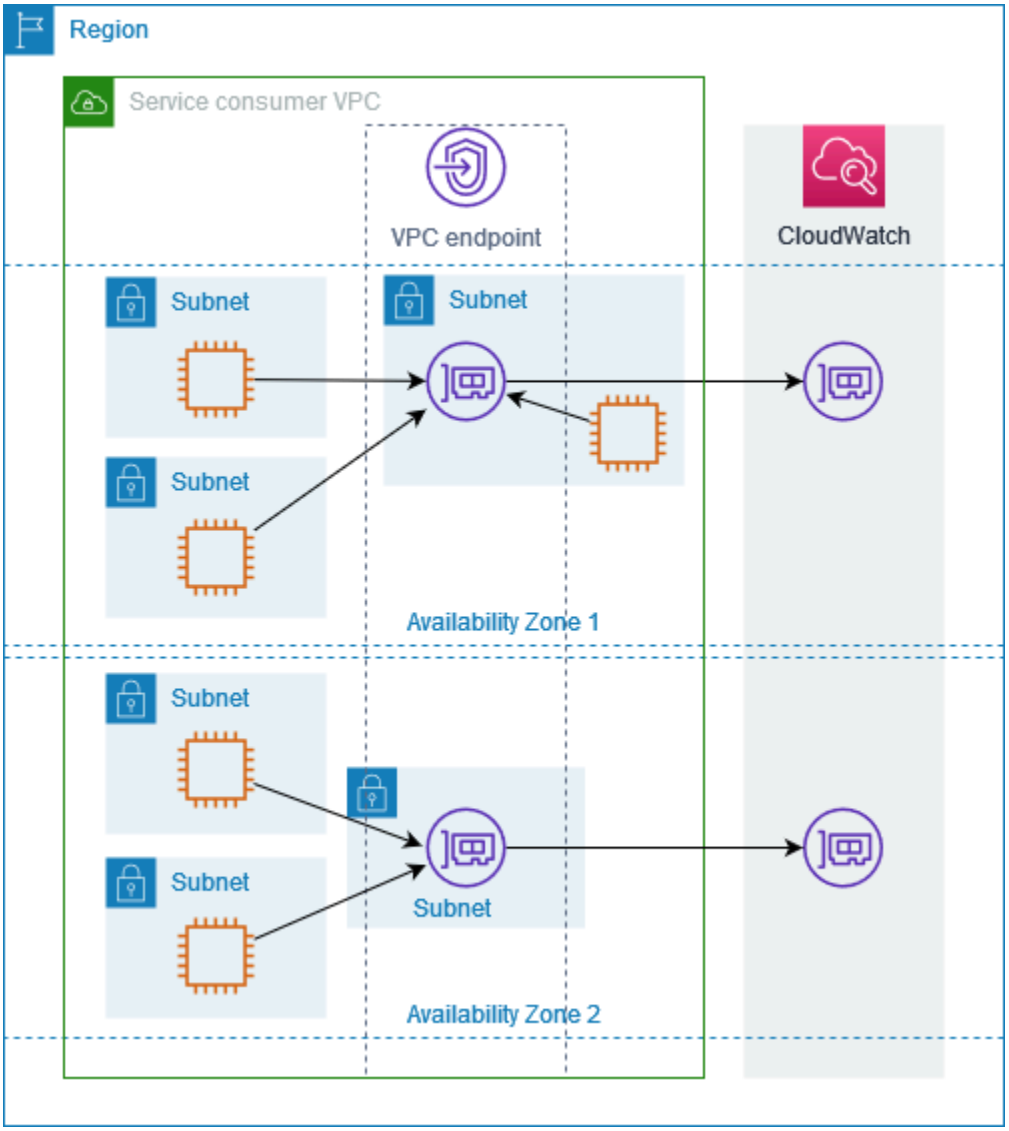
Das folgende Diagramm zeigt einen VPC-Endpunkt für Amazon CloudWatch mit einer Endpunkt-Netzwerkschnittstelle in einer einzigen Availability Zone. Wenn eine Ressource in einem Subnetz in der VPC CloudWatch über ihren öffentlichen Endpunkt auf Amazon zugreift, lösen wir den Datenverkehr an die IP-Adresse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



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



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



IP-Adresstypen

AWS-Services kann IPv6 über ihre privaten Endpunkte Support bieten, auch wenn sie keinen Support IPv6 über ihre öffentlichen Endpunkte anbieten. Endgeräte, die dies unterstützen, IPv6 können auf DNS-Anfragen mit AAAA-Einträgen antworten.

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 “IPv6 Support 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 eine Schnittstelle, die der VPC-Endpunkt unterstützt IPv4, haben die Endpunkt-Netzwerkschnittstellen IPv4 Adressen. Wenn eine Schnittstelle, die der VPC-Endpunkt unterstützt IPv6, 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.

IP-Typ des DNS-Eintrags

Abhängig von Ihrem IP-Adresstyp kann der AWS Service beim Aufrufen eines VPC-Endpunkts A-Datensätze, AAAA-Datensätze oder sowohl A- als auch AAAA-Datensätze zurückgeben. Sie können anpassen, welche Eintragstypen Ihr AWS Dienst zurückgibt, indem Sie den IP-Typ des DNS-Eintrags ändern. Die folgende Tabelle zeigt die unterstützten DNS-Eintrags-IP-Typen und die zurückgegebenen Eintragstypen:

IP-Typ des DNS-Eintrags	Zurückgegebene Datensatztypen
IPv4	A
IPv6	AAAA
Dualstack	A und AAAA

Standardmäßig entspricht der DNS-Eintragstyp dem IP-Adresstyp. Sie können einen anderen IP-Eintragstyp wählen, müssen jedoch einen kompatiblen IP-Adresstyp für den Endpunktdienst verwenden. Die folgende Tabelle zeigt den unterstützten DNS-Eintrags-IP-Typ für jeden IP-Adresstyp für Schnittstellenendpunkte:

IP-Adresstyp	Unterstützte IP-Typen für DNS-Einträge
IPv4	IPv4
IPv6	IPv6
Dualstack	Dualstack*,,, dienstdefiniert IPv4 IPv6

* Stellt den Standard-IP-Typ für DNS-Einträge dar.

Ein vom Dienst definierter DNS-Eintrags-IP-Typ gibt DNS-Einträge zurück, die auf dem von Ihnen aufgerufenen Dienstendpunkt basieren. Wenn Sie einen vom Dienst definierten DNS-Eintrags-IP-Typ verwenden, stellen Sie sicher, dass Ihr Dienst variable Aufrufe von Dienstendpunkten verarbeiten kann. Um die von Ihrem Schnittstellenendpunkt unterstützten DNS-Einträge zu sehen, sehen Sie sich die DNS-Namen für Ihren VPC-Endpunkt in oder an. AWS-ManagementkonsoleDescribeVpcEndpoints

Das Verhalten des DNS-Eintrags-IP-Typs ist bei Gateway-Endpunkten anders. Weitere Informationen finden Sie unter IP-Typ des DNS-Eintrags für Gateway-Endpunkte.

AWS-Services die sich integrieren in AWS PrivateLink

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

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

AWS-Service	Service-Name
AWS -Kontenverwaltung	com.amazonaws. *region*.konto
Amazon API Gateway	com.amazonaws. *region*.execute-api
	com.amazonaws. *region*.api-Gateway

AWS-Service	Service-Name
AWS AppConfig	com.amazonaws. *region*.appconfig
	com.amazonaws. *region*.appconfig-fips
	com.amazonaws. *region*.appconfig-Daten
	com.amazonaws. *region*.appconfigdata-fips
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
WorkSpaces Amazon-Anwendungen	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
	com.amazonaws. *region*.rds-fips

AWS-Service	Service-Name
Amazon Aurora DSQL	com.amazonaws. *region*.dsql
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
Amazon Bedrock	com.amazonaws. *region*. Grundgestein
	com.amazonaws. *region*. Bedrock-Agent
	com.amazonaws. *region*. bedrock-agent-runtime
	com.amazonaws. *region*. bedrock-data-automation
	com.amazonaws. *region*. bedrock-data-automation-fips
	com.amazonaws. *region*. bedrock-data-automation-runtime
	com.amazonaws. *region*. bedrock-data-automation-runtime-Fips
	com.amazonaws. *region*.bedrock-Laufzeit
AWS Fakturierung und Kostenmanagement	com.amazonaws. *region*.fakturierung
	com.amazonaws. *region*.kostenloser Tarif
	com.amazonaws. *region*.steuer
AWS Billing Conductor	com.amazonaws. *region*. Abrechnungsleiter
Amazon Braket	com.amazonaws. *region*. Klammer

AWS-Service	Service-Name
AWS Certificate Manager	com.amazonaws. *region*.acm
	com.amazonaws. *region*.acm-fips
AWS Clean Rooms	com.amazonaws. *region*. saubere Räume
	com.amazonaws. *region*.cleanrooms-fips
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
	com.amazonaws. *region*.cloudformation-fips
Amazon CloudFront	com.amazonaws.cloudfront
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 CloudTrail	com.amazonaws. *region*. Wolkenpfad
AWS Cloud-WAN	com.amazonaws. *region*. Netzwerkmanager
Amazon CloudWatch	com.amazonaws. *region*.Anwendungssignale
	com.amazonaws. *region*. Einblicke in die Anwendung

AWS-Service	Service-Name
	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
	com.amazonaws. *region*.oam
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
	com.amazonaws. *region*.codebuild-fips
AWS CodeCommit	com.amazonaws. *region*.codecommit
	com.amazonaws. *region*.codecommit-fips
	com.amazonaws. *region*.git-codecommit

AWS-Service	Service-Name
	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
	com.amazonaws. *region*.codedeploy-fips
Amazon CodeGuru Profiler	com.amazonaws. *region*.codeguru-profiler
CodeGuru Amazon-Rezensent	com.amazonaws. *region*.codeguru-gutachter
AWS CodePipeline	com.amazonaws. *region*.codepipeline
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
	com.amazonaws. *region*.config-fips
Amazon Connect	com.amazonaws. *region*.app-Integrationen
	com.amazonaws. *region*.fälle
	com.amazonaws. *region*.connect-kampagnen
	com.amazonaws. *region*.profil
	com.amazonaws. *region*. Stimmen-ID
	com.amazonaws. *region*. Weisheit

AWS-Service	Service-Name
AWS Connector Service	com.amazonaws. *region*.aws-Anschluss
AWS Control Catalog	com.amazonaws. *region*.control catalog
AWS Cost Explorer	com.amazonaws. *region*.ce
AWS Cost Optimization Hub	com.amazonaws. *region*. cost-optimization-hub
AWS Control Tower	com.amazonaws. *region*. Kontrollturm
	com.amazonaws. *region*.controltower-fips
AWS Data Exchange	com.amazonaws. *region*. Datenaustausch
AWS Data Exports	aws.api. *region*. bcm-data-exports
	com.amazonaws. *region*. bcm-pricing-calculator
Amazon Data Firehose	com.amazonaws. *region*.kinesis-Feuerwehrhose
Amazon Data Lifecycle Manager	com.amazonaws. *region*.dlm
	com.amazonaws. *region*.dlm-fips
AWS Database Migration Service	com.amazonaws. *region*.dms
	com.amazonaws. *region*.dms-fips
AWS DataSync	com.amazonaws. *region*.datasync
Amazon DataZone	com.amazonaws. *region*. Datazone
	com.amazonaws. *region*.datazone-fips
AWS Deadline Cloud	com.amazonaws. *region*.termin.management
	com.amazonaws. *region*.Deadline.Terminplanung
Amazon Detective	com.amazonaws. *region*. Detektiv

AWS-Service	Service-Name
	com.amazonaws. *region*.detektiv-fips
DevOpsAmazon-Guru	com.amazonaws. *region*.devops-guru
AWS Direct Connect	com.amazonaws. *region*. Direktverbindung
	com.amazonaws. *region*.directconnect-fips
AWS Directory Service	com.amazonaws. *region*.ds
	com.amazonaws. *region*.ds-Daten
	com.amazonaws. *region*. ds-data-fips
Amazon DocumentDB	com.amazonaws. *region*.rds
Amazon-DynamoDB	com.amazonaws. *region*.dynamodb
	com.amazonaws. *region*.dynamodb-fips
	com.amazonaws. *region*.dynamodb-Streams
Amazon EBS direkt APIs	com.amazonaws. *region*.ebs
	com.amazonaws. *region*.ebs-fips
Amazon EC2	com.amazonaws. *region*.ec2
	com.amazonaws. *region*.ec2-fips
Amazon EC2 Auto Scaling	com.amazonaws. *region*.automatische Skalierung
	com.amazonaws. *region*.autoscaling-fips
EC2 Image Builder	com.amazonaws. *region*.imagebuilder
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr

AWS-Service	Service-Name
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
	com.amazonaws. *region*.eks-fips
	com.amazonaws. *region*.eks-Proxy
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 Elastic VMware Service	com.amazonaws. *region*.evs
	com.amazonaws. *region*.evs-fips
Amazon ElastiCache	com.amazonaws. *region*. elastischer Cache
	com.amazonaws. *region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws. *region*.mediaconnect
AWS Elemental MediaConvert	com.amazonaws. *region*.mediaconvert
	com.amazonaws. *region*.mediaconvert-fips

AWS-Service	Service-Name
Amazon EMR	com.amazonaws. *region*.elasticmapreduce
	com.amazonaws. *region*.elasticmapreduce-fips
Amazon EMR in EKS	com.amazonaws. *region*.emr-Behälter
Amazon EMR Serverless	com.amazonaws. *region*.emr-serverlos
	com.amazonaws. *region*. emr-serverless-services. Livius
	com.amazonaws. *region*.emr-serverless.dashboard
Amazon EMR WAL	com.amazonaws. *region*.emrwal.prod
AWS Nachrichten für Endbenutzer in sozialen Netzwerken	com.amazonaws. *region*.soziale Nachrichtenübermittlung
	com.amazonaws. *region*. social-messaging-fips
AWS Entity Resolution	com.amazonaws. *region*. Entitätsauflösung
	com.amazonaws. *region*.entityresolution-fips
Amazon EventBridge	com.amazonaws. *region*.veranstaltungen
	com.amazonaws. *region*.events-fips
	com.amazonaws. *region*. Rohre
	com.amazonaws. *region*.pipes-Daten
	com.amazonaws. *region*.pipes-fips
	com.amazonaws. *region*.schemas
Amazon EventBridge Scheduler	com.amazonaws. *region*. Scheduler
AWS Fault Injection Service	com.amazonaws. *region*.fis

AWS-Service	Service-Name
	com.amazonaws. *region*.fis-fips
Amazon FinSpace	com.amazonaws. *region*.finspace
	com.amazonaws. *region*.finspace-api
AWS Firewall Manager	com.amazonaws. *region*.fms
	com.amazonaws. *region*.fms-fips
Amazon Forecast	com.amazonaws. *region*. Prognose
	com.amazonaws. *region*. Prognoseabfrage
	com.amazonaws. *region*.Forecast-Fips
	com.amazonaws. *region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws. *region*. Betrugsdetektor
Amazon FSx	com.amazonaws. *region*.fsx
	com.amazonaws. *region*.fsx-fips
GameLift Amazon-Server	com.amazonaws. *region*. Spielelift
GameLift Amazon-Streams	com.amazonaws. *region*.gameliftstreams
AWS Globale Netzwerke für Transit Gateways	com.amazonaws. *region*. Netzwerkmanager
AWS Glue	com.amazonaws. *region*. kleben
	com.amazonaws. *region*.glue.dashboard
AWS Glue DataBrew	com.amazonaws. *region*. Databrew
	com.amazonaws. *region*.databrew-Fips
Amazon Managed Grafana	com.amazonaws. *region*. Grafana

AWS-Service	Service-Name
	com.amazonaws. *region*.grafana-workspace
AWS Ground Station	com.amazonaws. *region*. Bodenstation
	com.amazonaws. *region*.groundstation-fips
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*. analytics-omics-fips
	com.amazonaws. *region*. control-storage-omics
	com.amazonaws. *region*. control-storage-omics-fips
	com.amazonaws. *region*.storage-comics
	com.amazonaws. *region*.tags-Comics
	com.amazonaws. *region*. tags-omics-fips
	com.amazonaws. *region*.workflows-Comics
	com.amazonaws. *region*. workflows-omics-fips

AWS-Service	Service-Name
AWS Identity and Access Management (ICH BIN)	com.amazonaws.iam
IAM Access Analyzer	com.amazonaws. *region*.access-analyzer
	com.amazonaws. *region*. access-analyzer-fips
IAM Identity Center	com.amazonaws. *region*. Identitätsspeicher
IAM Roles Anywhere	com.amazonaws. *region*. Rollen überall
	com.amazonaws. *region*.rolesanywhere-fips
Amazon Inspector	com.amazonaws. *region*. Inspektor 2
	com.amazonaws. *region*.inspector2-fips
	com.amazonaws. *region*.inspector-Scan
	com.amazonaws. *region*. inspector-scan-fips
Amazon Interactive Video Service	com.amazonaws. *region*.ivs.beitragen
AWS IoT Core	com.amazonaws. *region*.iot.api
	com.amazonaws. *region*.iot-fips.api
	com.amazonaws. *region*.iot.daten
	com.amazonaws. *region*.iot.credentials
AWS IoT Device Management sicheres Tunneling	com.amazonaws. *region*.iot.tunneling.api
	com.amazonaws. *region*.iot-fips.tunneling.api
	com.amazonaws. *region*.iot.tunneling.data
	com.amazonaws. *region*.iot-fips.tunneling.data
AWS IoT Core Device Advisor	com.amazonaws. *region*.deviceadvisor.iot

AWS-Service	Service-Name
Verwaltete Integrationen für AWS IoT Device Management	com.amazonaws. *region*.iotmanagedintegrations.api
	com.amazonaws. *region*.iot-verwaltete Integrationen — fips.api
AWS IoT Core für 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 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-Service	Service-Name
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
	com.amazonaws. *region*. license-manager-user-subscriptions
	com.amazonaws. *region*. license-manager-user-subscriptions-Fips
Amazon Lightsail	com.amazonaws. *region*. Leichtsegel
Amazon Location Service	com.amazonaws. *region*.geo.maps
	com.amazonaws. *region*.geo.places
	com.amazonaws. *region*.geo.routes
	com.amazonaws. *region*.geo.geofencing
	com.amazonaws. *region*.geo.tracking
	com.amazonaws. *region*.geo.metadata

AWS-Service	Service-Name
Amazon Lookout für Equipment	com.amazonaws. *region*. Ausrüstung aussuchen
Amazon Lookout for Vision	com.amazonaws. *region*. Lookout Vision
Amazon Macie	com.amazonaws. *region*.macie 2
	com.amazonaws. *region*.macie2-fips
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
AWS Marketplace Metering Service	com.amazonaws. *region*.metering-marktplatz
Amazon Managed Service for Prometheus	com.amazonaws. *region*.aps
	com.amazonaws. *region*.aps-Arbeitsbereiche
Amazon Managed Streaming for Apache Kafka (MSK)	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
	com.amazonaws. *region*.airflow.ops

AWS-Service	Service-Name
Amazon Route 53	com.amazonaws.route53
Amazon Route 53 Global Resolver	aws.api.us-east-2.route53globaler Resolver
	aws.api.us-east-2.route53globalresolver-fips
AWS-Managementkonsole	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
	com.amazonaws. *region*.mq-fips
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.
OpenSearch Einnahme durch Amazon	com.amazonaws. *region*.osis

AWS-Service	Service-Name
AWS Organizations	com.amazonaws. *region*. Organisationen
	com.amazonaws. *region*.organisationen-fips
AWS Outposts	com.amazonaws. *region*. Außenposten
AWS Panorama	com.amazonaws. *region*. Panorama
AWS Kryptografie im Zahlungsverkehr	com.amazonaws. *region*.payment-cryptography.controlplane
	com.amazonaws. *region*.payment-cryptography.dataplane
AWS 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
	com.amazonaws. *region*.polly-fips
AWS-Preisliste	com.amazonaws. *region*.pricing.api
AWS Private Certificate Authority	com.amazonaws. *region*.acm-pca
	com.amazonaws. *region*. acm-pca-fips
	com.amazonaws. *region*. pca-connector-ad

AWS-Service	Service-Name
	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
	com.amazonaws. *region*.apps
Amazon Q-Benutzerabonnements	com.amazonaws. *region*.service.user-Abonnements
Schnell	com.amazonaws. *region*.quicksight-Webseite
Amazon RDS	com.amazonaws. *region*.rds
	com.amazonaws. *region*.rds-fips
Amazon RDS Daten-API	com.amazonaws. *region*.rds-Daten
Erkenntnisse zur Amazon-RDS-Leistung	com.amazonaws. *region*.pi
	com.amazonaws. *region*.pi-fips
AWS re:Post Privat	com.amazonaws. *region*.repostspace
Papierkorb	com.amazonaws. *region*.bin
	com.amazonaws. *region*.rbin-fips
Amazon Redshift	com.amazonaws. *region*.redshift
	com.amazonaws. *region*.redshift-fips
	com.amazonaws. *region*.redshift - serverlos
	com.amazonaws. *region*. redshift-serverless-fips

AWS-Service	Service-Name
Amazon 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 Resource Access Manager	com.amazonaws. *region*.ram
	com.amazonaws. *region*.ram-fips
AWS Resource Explorer	com.amazonaws. *region*.resource-explorer-2
	com.amazonaws. *region*.resource-explorer-2-fips
AWS -Ressourcengruppen	com.amazonaws. *region*.resource-groups
	com.amazonaws. *region*. resource-groups-fips
AWS Resource Groups Tagging API	com.amazonaws. *region*.taggen
Amazon S3	com.amazonaws. *region*. 3
	com.amazonaws. *region*.s3-Tabellen
Mulitiregionale Amazon-S3-Zugriffs punkte	com.amazonaws.s3-global.accesspoint
Amazon S3 on Outposts	com.amazonaws. *region*.s3-Außenposten
Amazon SageMaker KI	Als Sagemaker. *region*. Experimente
	als Sagemaker. *region*. Notizbuch
	als Sagemaker. *region*.partner-App

AWS-Service	Service-Name
	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. featurestore-runtime-fips
	com.amazonaws. *region*.sagemaker.metrics
	com.amazonaws. *region*.sagemaker.runtime
	com.amazonaws. *region*.sagemaker.runtime-fips
Savings Plans	com.amazonaws.sparpläne
AWS Secrets Manager	com.amazonaws. *region*. Geheimnismanager
AWS Security Hub CSPM	com.amazonaws. *region*. Sicherheitshub
	com.amazonaws. *region*.securityhub-fips
Amazon Security Lake	com.amazonaws. *region*. Sicherheitssee
	com.amazonaws. *region*.securitylake-fips
AWS -Security-Token-Service	com.amazonaws. *region*.sts
	com.amazonaws. *region*.sts-fips
AWS Serverless Application Repository	com.amazonaws. *region*. serverloses Repo

AWS-Service	Service-Name
Servicekatalog	com.amazonaws. *region*.servicekatalog
	com.amazonaws. *region*.servicecatalog-app-Registrierung
Service Quotas	com.amazonaws. *region*. Servicequoten
Amazon SES	com.amazonaws. *region*.email-smtp
	com.amazonaws. *region*.mail-manager
	com.amazonaws. *region*. mail-manager-fips
	com.amazonaws. *region*. mail-manager-smtp.auth.fips
	com.amazonaws. *region*. mail-manager-smtp.fips öffnen
AWS SimSpace Weaver	com.amazonaws. *region*.simspaceweaver
AWS Snowball Edge Device Management	com.amazonaws. *region*. snow-device-management
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
	com.amazonaws. *region*.sqs-fips
Amazon SWF	com.amazonaws. *region*.swf
	com.amazonaws. *region*.swf-fips
AWS Step Functions	com.amazonaws. *region*.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-incidents-fips
	com.amazonaws. *region*.ssm-schnelle Einrichtung
	com.amazonaws. *region*.ssm-Nachrichten
AWS Systems Manager für SAP	com.amazonaws. *region*.ssm-Sap
	com.amazonaws. *region*. ssm-sap-fips
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
	com.amazonaws. *region*. transkribiert Streaming-Fips
Amazon Transcribe Medical	com.amazonaws. *region*.transkribieren

AWS-Service	Service-Name
	com.amazonaws. *region*. transkribiert Streaming
AWS Transfer for SFTP	com.amazonaws. *region*. Übertragung
	com.amazonaws. *region*.transfer.server
AWS Transform	com.amazonaws. *region*.transformieren
AWS Transform benutzerdefiniert	com.amazonaws. *region*.transform-benutzerdefiniert
Amazon Translate	com.amazonaws. *region*. übersetzen
AWS Trusted Advisor	com.amazonaws. *region*. vertrauenswürdiger Berater
AWS-Benutzerbenachrichtigungen	com.amazonaws. *region*. Benachrichtigungen
	com.amazonaws. *region*. Benachrichtigungen-Kontakte
Amazon Verified Permissions	com.amazonaws. *region*. verifizierte Berechtigungen
	com.amazonaws. *region*. verifizierte Berechtigungen — FIPS
Amazon VPC Lattice	com.amazonaws. *region*.vpc-Gitter
AWS WAFV2	com.amazonaws. *region*.wafv2
	com.amazonaws. *region*.wafv2-fips
AWS Well-Architected Tool	com.amazonaws. *region*. gut gestaltet
Amazon WorkMail	com.amazonaws. *region*.workmail
	com.amazonaws. *region*.workmail-Nachrichtenfluss
Amazon WorkSpaces	com.amazonaws. *region*. Arbeitsbereiche
WorkSpaces Sicherer Browser von Amazon	com.amazonaws. *region*.workspaces-web
	com.amazonaws. *region*. workspaces-web-fips

AWS-Service	Service-Name
WorkSpaces Streamen	com.amazonaws. *region*. Highlander
Amazon WorkSpaces Thin Client	com.amazonaws. *region*.thinclient.api
AWS X-Ray	com.amazonaws. *region*.xray
Amazon Managed Service für Apache Flink	com.amazonaws. *region*.kinesisanalytics
	com.amazonaws. *region*.kinesisanalytics-fips

Verfügbare Namen anzeigen AWS-Service

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
```

Es folgt eine Beispielausgabe. Die vollständige Ausgabe wird nicht angezeigt.

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

Anzeigen von Informationen über einen Service

Sobald Sie den Dienstnamen 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"
```

```
                },
                {
                    "PrivateDnsName": "monitoring.us-east-1.api.aws"
                },
                {
                    "PrivateDnsName": "monitoring-fips.us-east-1.amazonaws.com"
                },
                {
                    "PrivateDnsName": "monitoring-fips.us-east-1.api.aws"
                }            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": [],
            "PrivateDnsNameVerificationState": "verified",
            "SupportedIpAddressTypes": [
                "ipv6",
                "ipv4"
            ]
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.monitoring"
    ]
}
```

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. Die vollständige Ausgabe wird nicht angezeigt.

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

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. Die vollständige Ausgabe wird nicht angezeigt.

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

IPv6 Support anzeigen

Informationen zum IPv6 Support für AWS Dienste finden Sie unter AWS Dienste, die unterstützen IPv6. Sie können auch 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
```

Es folgt eine Beispielausgabe. Die vollständige Ausgabe wird nicht angezeigt.

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

Regionsübergreifend aktiviert AWS-Services

Die folgenden AWS-Services lassen sich regionsübergreifend integrieren. AWS PrivateLink Sie können einen Schnittstellenendpunkt erstellen, um privat eine Verbindung zu diesen Diensten in einer anderen AWS Region herzustellen, als ob sie in Ihrer eigenen VPC ausgeführt würden.

Wählen Sie den Link in der AWS-ServiceSpalte, um die Servicedokumentation aufzurufen. Die Spalte Dienstname enthält den Dienstnamen, den Sie bei der Erstellung des Schnittstellenendpunkts angeben.

AWS-Service	Service-Name
Amazon S3	com.amazonaws. *region*. 3
AWS Identity and Access Management (ICH BIN)	com.amazonaws.iam
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
AWS Key Management Service	com.amazonaws. *region*. km
	com.amazonaws. *region*.kms-fips
Amazon ECS	com.amazonaws. *region*.ecs
AWS Lambda	com.amazonaws. *region*. Lambda
Amazon Data Firehose	com.amazonaws. *region*.kinesis-Feuerwehrhose
Amazon Managed Service für Apache Flink	com.amazonaws. *region*.kinesisanalytics
	com.amazonaws. *region*.kinesisanalytics-fips
Amazon Route 53	com.amazonaws.route53

Verfügbare Namen anzeigen AWS-Service

Sie können den describe-vpc-endpoint-servicesBefehl verwenden, um regionsübergreifende Dienste anzuzeigen.

Das folgende Beispiel zeigt AWS-Services , wie ein Benutzer in der `us-east-1` Region über Schnittstellenendpunkte auf die angegebene (`us-west-2`) Dienstregion zugreifen kann. 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 \
  --service-region us-west-2 \
  --query ServiceNames
```

Es folgt eine Beispielausgabe. Die vollständige Ausgabe wird nicht angezeigt.

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

> **Note**
>
> Sie müssen regionales DNS verwenden. Zonales DNS wird beim Zugriff AWS-Services in einer anderen Region nicht unterstützt. Weitere Informationen finden Sie unter DNS-Attribute anzeigen und aktualisieren im Amazon VPC-Benutzerhandbuch.

Berechtigungen und Überlegungen

- Standardmäßig sind IAM-Entitäten nicht berechtigt, auf eine AWS-Service in einer anderen Region zuzugreifen. Um die für den regionsübergreifenden Zugriff erforderlichen Berechtigungen zu gewähren, kann ein IAM-Administrator IAM-Richtlinien erstellen, die diese Aktion nur mit Zugriffsrechten zulassen. `vpce:AllowMultiRegion`

- Stellen Sie sicher, dass Ihre Service Control Policy (SCP) keine Aktion verweigert, die nur auf Berechtigungen beschränkt ist. `vpce:AllowMultiRegion` Um die Funktion für AWS PrivateLink regionsübergreifende Konnektivität nutzen zu können, müssen sowohl Ihre Identitätsrichtlinie als auch Ihr SCP diese Aktion zulassen.
- Verwenden Sie den `ec2:VpceServiceRegion` Bedingungsschlüssel, um die Regionen zu steuern, die eine IAM-Entität beim Erstellen eines VPC-Endpunkts als Dienstregion angeben kann.
- 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.
- Sie können den neuen `aws:SourceVpcArn` globalen Bedingungsschlüssel von IAM verwenden, um zu sichern, aus welchen Regionen AWS-Konten und auf VPCs Ihre Ressourcen zugegriffen werden kann. Dieser Schlüssel hilft bei der Implementierung der Datenresidenz und der regionsbasierten Zugriffskontrolle.
- Für eine hohe Verfügbarkeit sollten Sie einen regionsübergreifenden Schnittstellenendpunkt in mindestens zwei Availability Zones einrichten. In diesem Fall müssen Anbieter und Verbraucher nicht dieselben Availability Zones verwenden.
- AWS PrivateLink Verwaltet mit regionsübergreifendem Zugriff den Failover zwischen Availability Zones sowohl in Service- als auch in Kundenregionen. Es verwaltet kein regionsübergreifendes Failover.
- Der regionsübergreifende Zugriff wird für die folgenden Availability Zones nicht unterstützt: `use1-az3usw1-az2`,`apne1-az3`,`apne2-az2`, und`apne2-az4`.
- Sie können AWS Fault Injection Service es verwenden, um regionale Ereignisse zu simulieren und Ausfallszenarien für regionsinterne und regionsübergreifende Schnittstellenendpunkte zu modellieren. Weitere Informationen finden Sie in der Dokumentation.AWS FIS

Erstellen Sie einen Schnittstellenendpunkt zu einer AWS-Service in einer anderen Region

Informationen zum Erstellen eines Schnittstellenendpunkts mithilfe der Konsole finden Sie im Abschnitt VPC-Endpunkt erstellen.

In der CLI können Sie den create-vpc-endpointBefehl verwenden, um einen VPC-Endpunkt für eine AWS-Service in einer anderen Region zu erstellen. Das folgende Beispiel erstellt einen Schnittstellenendpunkt zu Amazon S3 in `us-west-2` einem VPC-Eingang. `us-east-1`

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

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

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

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

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

Inhalt

Voraussetzungen

- Stellen Sie die Ressourcen bereit, die auf die zugreifen, AWS-Service in Ihrer VPC.

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

Erstellen eines VPC-Endpunkts

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

Um einen Schnittstellenendpunkt für eine zu erstellen AWS-Service

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen aus.
4. Wählen Sie für Typ die Option AWS -Services aus.
5. (Optional) Wenn Sie einen Endpunkt zu einem Endpunkt AWS-Service in einer anderen Region erstellen, aktivieren Sie das Kontrollkästchen Regionsübergreifenden Endpunkt aktivieren und wählen Sie dann die Serviceregion aus der Dropdownliste aus.
6. Wählen Sie für Service name (Servicename) den Service aus. Weitere Informationen finden Sie unter the section called “Services, die integrieren”.
7. Wählen Sie für VPC die VPC aus, von der aus Sie auf AWS-Service zugreifen.
8. Wenn Sie in Schritt 5 den Servicenamen für Amazon S3 ausgewählt haben und die Unterstützung für privates DNS konfigurieren möchten, wählen Sie Zusätzliche Einstellungen, DNS-Namen aktivieren aus. Wenn Sie diese Auswahl treffen, wird automatisch auch die Option

Private DNS nur für eingehenden Endpunkt aktivieren ausgewählt. Sie können privates DNS mit einem eingehenden Resolver-Endpunkt nur für Schnittstellenendpunkte für Amazon S3 konfigurieren. Wenn Sie keinen Gateway-Endpunkt für Amazon S3 haben und die Option Private DNS nur für eingehende Endpunkte aktivieren wählen, erhalten Sie eine Fehlermeldung, wenn Sie den letzten Schritt in diesem Verfahren ausführen.

Wenn Sie in Schritt 5 den Servicenamen für einen anderen Dienst als Amazon S3 ausgewählt haben, ist Zusätzliche Einstellungen, DNS-Namen aktivieren bereits ausgewählt. Wir empfehlen Ihnen, die Standardeinstellungen beizubehalten. Dadurch wird sichergestellt, dass Anfragen, die die Endpunkte des öffentlichen Dienstes verwenden, z. B. Anfragen, die über ein AWS SDK gestellt wurden, an Ihren VPC-Endpunkt weitergeleitet werden.

9. 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-Block für den internen Gebrauch reserviert sind, sodass Sie sie nicht für Ihre Endpunkt-Netzwerkschnittstellen angeben können.

10. 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 akzeptiert IPv6 .
    - 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

11. Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppen aus, die den Security groups (Endpunkt-Netzwerkschnittstellen) zugeordnet werden sollen. Standardmäßig ordnen wir die Standard-Sicherheitsgruppe für die VPC zu.

12. Wählen Sie unter Richtlinie die Option 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 Service VPC-Endpunktrichtlinien unterstützt. Weitere Informationen finden Sie unter Endpunktrichtlinien.
13. (Optional) Sie fügen ein Tag hinzu, indem Sie Neuen Tag hinzufügen auswählen und den Schlüssel und den Wert für den Tag eingeben.
14. Wählen Sie Endpunkt erstellen.

So erstellen Sie einen Schnittstellenendpunkt mithilfe der Befehlszeile

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

Gemeinsam genutzte Subnetze

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

ICMP

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

Konfigurieren eines Schnittstellenendpunkts

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

Aufgaben

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

- Verwalten von Tags

Hinzufügen oder Entfernen von Subnetzen

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

So ändern Sie die Subnetze mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Schnittstellenendpunkt.
4. Wählen Sie Actions (Aktionen), Manage Subnets (Subnetze verwalten).
5. Aktivieren oder deaktivieren Sie Availability Zones nach Bedarf. Wählen Sie für jede Availability Zone ein Subnetz aus. Standardmäßig wählen wir IP-Adressen aus den Subnetz-IP-Adressbereichen aus und weisen sie den Endpunkt-Netzwerkschnittstellen zu. Um die IP-Adressen für eine Endpunkt-Netzwerkschnittstelle auszuwählen, wählen Sie IP-Adressen festlegen und geben Sie eine IPv4 Adresse aus dem Subnetzadressbereich ein. Wenn der Endpunktdienst dies unterstützt IPv6, können Sie auch eine IPv6 Adresse aus dem Subnetz-Adressbereich eingeben.

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

So ändern Sie die Subnetze über die Befehlszeile

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

Weisen Sie Sicherheitsgruppen zu

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

Ändern der Sicherheitsgruppen mithilfe der Konsole

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

Ändern der Sicherheitsgruppen mithilfe der Befehlszeile

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

Bearbeiten der VPC-Endpunktrichtlinie

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

So ändern Sie die Endpunktrichtlinie mithilfe der Konsole

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

6. Wählen Sie Speichern.

So ändern Sie die Endpunktrichtlinie mithilfe der Befehlszeile

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

Aktivieren von privaten DNS-Namen

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

Um privates DNS zu verwenden, müssen Sie sowohl DNS-Hostnamen als auch die DNS-Auflösung für Ihre VPC aktivieren. Nachdem Sie private DNS-Namen aktiviert haben, kann es einige Minuten dauern, bis die privaten IP-Adressen verfügbar sind. Die DNS-Einträge, die wir erstellen, wenn Sie private DNS-Namen aktivieren, sind privat. Daher kann der private DNS-Name nicht öffentlich aufgelöst werden.

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

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

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

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

Verwalten von Tags

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

So verwalten Sie Tags mit der Konsole

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

So verwalten Sie Tags mit der Befehlszeile

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

Empfangen von Warnmeldungen für Schnittstellen-Endpunkt-Ereignisse

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

Aufgaben

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

Eine SNS-Benachrichtigung erstellen

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

So erstellen Sie mithilfe der Konsole eine Benachrichtigung für einen Schnittstellenendpunkt

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Schnittstellenendpunkt.
4. Wählen Sie aus der Registerkarte Notifications (Benachrichtigungen) die Option Create notification (Benachrichtigung erstellen) aus.
5. Wählen Sie für Notification ARN den Amazon-Ressourcennamen (ARN) für das SNS-Thema, 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 Amazon SNS SNS-Thema eine Zugriffsrichtlinie hinzu, die es ermöglicht, Benachrichtigungen in Ihrem Namen AWS PrivateLink zu veröffentlichen, z. B. die folgenden. Weitere Informationen finden Sie unter Wie bearbeite ich die Zugriffsrichtlinie meines Amazon-SNS-Themas? Verwenden Sie die globalen Konditionsschlüssel `aws:SourceArn` und `aws:SourceAccount` zum Schutz vor dem Problem des verwirrten Stellvertreters.

JSON

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

Eine Schlüsselrichtlinie hinzufügen

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

JSON

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

Löschen eines Schnittstellenendpunkts

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

So löschen Sie einen Schnittstellen-Endpunkt unter Verwendung der Konsole

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

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

So löschen Sie einen Schnittstellen-Endpunkt unter Verwendung der Befehlszeile

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

Gateway-Endpunkte

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

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

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

Preisgestaltung

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

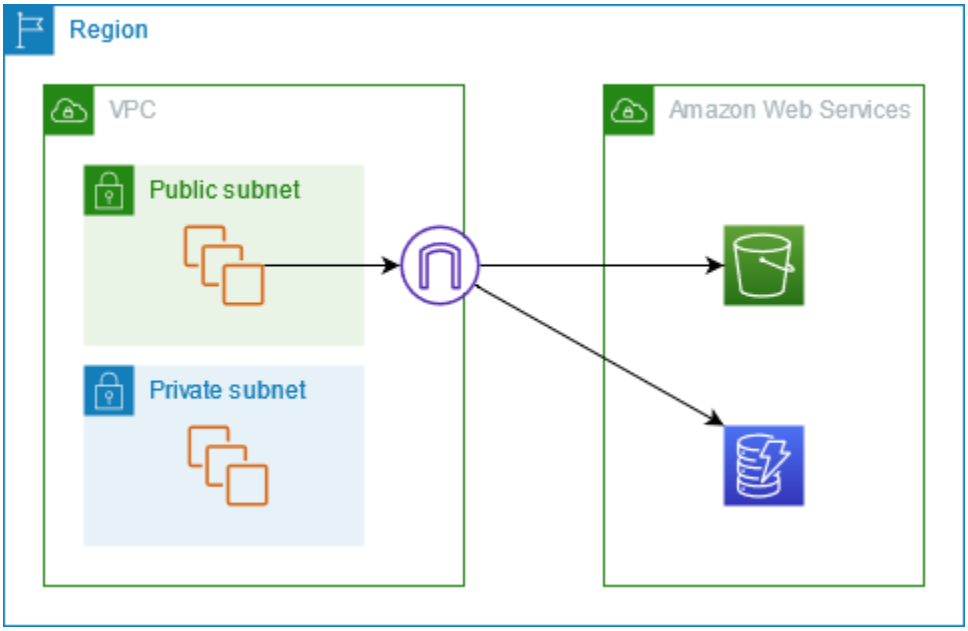
Inhalt

-Übersicht

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

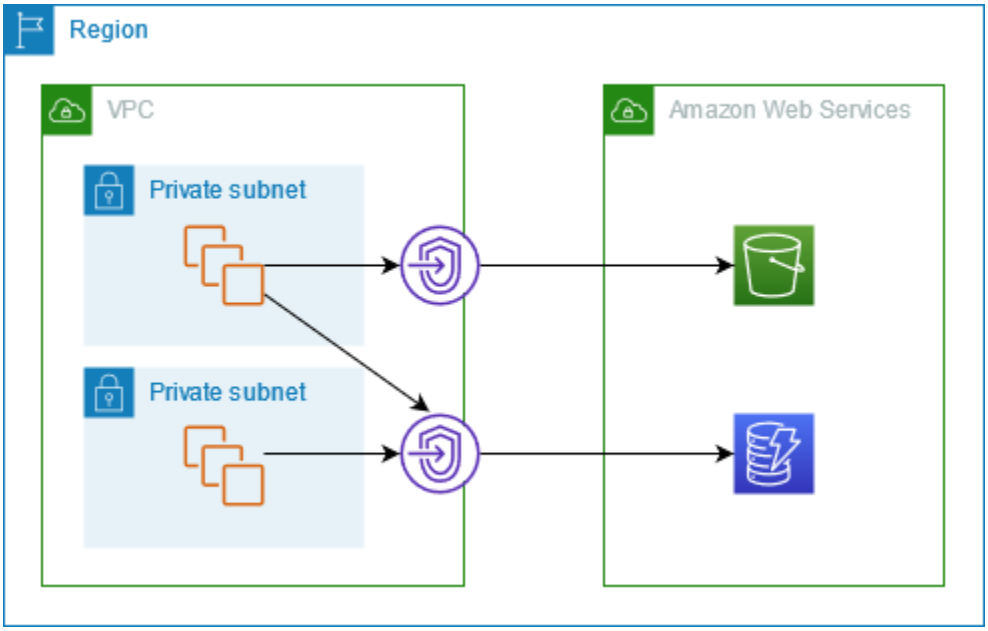
Zugriff über ein Internet-Gateway

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



Zugriff über einen Gateway-Endpunkt

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



Routing

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

Bestimmungsort	Target
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.

Ziel	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 Netzwerk-ACL-Regeln nicht auf Präfixlisten verweisen, aber Sie können die IP-Adresse für den Dienst aus der Präfixliste abrufen.

Ziel	Protocol (Protokoll)	Port-Bereich
service_cidr_block_1	TCP	443

Ziel	Protocol (Protokoll)	Port-Bereich
service_cidr_block_2	TCP	443
service_cidr_block_3	TCP	443

IP address type (IP-Adresstyp)

Der IP-Adresstyp bestimmt, welche Präfixliste Ihrer Routing-Tabelle zugeordnet ist.

Anforderungen zur Aktivierung IPv6 für einen Gateway-Endpunkt

- Der IP-Adresstyp eines Gateway-Endpunkts muss mit den Subnetzen für den Gateway-Endpunkt kompatibel sein, wie hier beschrieben:
  - IPv4— Fügen Sie die IPv4 Präfixliste des Dienstes zu Ihrer Routentabelle hinzu.
  - IPv6— Fügen Sie die IPv6 Präfixliste des Dienstes zu Ihrer Routentabelle hinzu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv6 nur Subnetze sind.
  - Dualstack — Fügen Sie die IPv4 Präfixliste des Dienstes zu Ihrer Routing-Tabelle hinzu und fügen Sie die IPv6 Präfixliste des Dienstes zu Ihrer Routing-Tabelle hinzu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze IPv4 sowohl IPv6 als auch Adressbereiche haben.

IP-Typ des DNS-Eintrags

Standardmäßig gibt ein Gateway-Endpunkt DNS-Einträge zurück, die auf dem von Ihnen aufgerufenen Dienstendpunkt basieren. Wenn Sie Ihren Gateway-Endpunkt mithilfe des IPv4 Service-Endpunkts erstellen`s3.us-east-2.amazonaws.com`, z. B. gibt Amazon S3 A-Datensätze an Ihre Clients zurück, und alle Subnetze in Ihrer Routing-Tabelle verwenden diese IPv4.

Wenn Sie dagegen Ihren Gateway-Endpunkt mithilfe des Dual-Stack-Serviceendpunkts erstellen, gibt Amazon S3 sowohl A- als `s3.dualstack.us-east-2.amazonaws.com` auch AAAA-Datensätze an Ihre Clients zurück, und die Subnetze in Ihrer Routing-Tabelle verwenden und. IPv4 IPv6

> **Note**
>
> Bei Directory-Buckets oder S3 Express One Zone wären die Gateway-Endpunkte für die Datenebene jeweils und. `s3express-use2-az1.us-east-2.amazonaws.com` `s3express-use2-az1.dualstack.us-east-2.amazonaws.com`

Der IP-Typ des DNS-Eintrags wirkt sich darauf aus, wie der Datenverkehr an Ihre Clients weitergeleitet wird. Wenn Sie mithilfe des IPv4 Service-Endpunkts einen Gateway-Endpunkt erstellen und dann den Dual-Stack-Dienstendpunkt aufrufen, wird Datenverkehr, der AAAA-Datensätze verwendet, nicht über den Gateway-Endpunkt geleitet. Der Datenverkehr wird gelöscht oder über einen IPv6 -kompatiblen Pfad geleitet, falls einer vorhanden ist. Wenn Sie einen vom Dienst definierten IP-Typ für DNS-Einträge verwenden, stellen Sie sicher, dass Ihr Dienst variable Aufrufe von mehreren Dienstendpunkten verarbeiten kann.

Anstelle der standardmäßigen Einstellung für den DNS-Eintrags-IP-Typ von service-defined können Sie den IP-Typ des DNS-Eintrags anpassen, um auszuwählen, welche Datensätze für einen bestimmten Endpunkt zurückgegeben werden. Die folgende Tabelle zeigt die unterstützten DNS-Eintrags-IP-Typen und die zurückgegebenen Eintragstypen:

IP-Typ des DNS-Eintrags	Zurückgegebene Datensatztypen
IPv4	A
IPv6	AAAA
Dualstack	A und AAAA
dienstdefiniert	Die Datensätze hängen vom Service-Endpunkt ab

Um einen IP-Typ für DNS-Einträge auszuwählen, müssen Sie einen kompatiblen IP-Adresstyp für den Endpunktdienst verwenden. Die folgende Tabelle zeigt den unterstützten DNS-Eintrags-IP-Typ für jeden IP-Adresstyp für Gateway-Endpunkte:

IP-Adresstyp	Unterstützte IP-Typen für DNS-Einträge
IPv4	IPv4, dienstdefiniert*
IPv6	IPv6, servicedefiniert*
Dualstack	IPv4,, Dualstack, IPv6 servicedefiniert*

* Stellt den Standard-IP-Typ für DNS-Einträge dar.

> **Note**
>
> Um für Ihren Gateway-Endpunkt andere als die vom Dienst definierten IP-Typen für DNS-Einträge zu verwenden, müssen Sie in Ihren VPC-Einstellungen die entsprechenden `enableDnsHostnames` Attribute zulassen`enableDnsSupport`.

Sie können den IP-Typ des DNS-Eintrags für einen DynamoDB-Gateway-Endpunkt nicht ändern. DynamoDB unterstützt nur den dienstdefinierten IP-Typ des DNS-Eintrags.

Das Verhalten des DNS-Eintrags-IP-Typs ist für Schnittstellenendpunkte unterschiedlich. Weitere Informationen finden Sie unter IP-Typ des DNS-Eintrags für Schnittstellenendpunkte.

Gateway-Endpunkte für Amazon S3

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

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

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

Inhalt

Überlegungen

- Ein Gateway-Endpunkt ist nur in der Region verfügbar, in der Sie ihn erstellt haben. Stellen Sie sicher, dass Sie Ihren Gateway-Endpunkt in derselben Region wie Ihre S3-Buckets erstellen.
- Wenn Sie die Amazon-DNS-Server verwenden, müssen Sie sowohl DNS-Hostnamen als auch DNS-Auflösung für Ihre VPC aktivieren. Wenn Sie Ihren eigenen DNS-Server verwenden, stellen Sie sicher, dass Anforderungen an Amazon S3 korrekt in die von AWS verwalteten IP-Adressen erfüllt werden.
- Die ausgehenden Regeln für die Sicherheitsgruppe für Instances, die über den Gateway-Endpunkt auf Amazon S3 zugreifen, müssen Datenverkehr zu Amazon S3 zulassen. Sie können in den Regeln der Sicherheitsgruppe auf die ID der Präfixliste für Amazon S3 verweisen.
- Die Netzwerk-ACL für das Subnetz für Ihre Instances, die über einen Gateway-Endpunkt auf Amazon S3 zugreifen, müssen Datenverkehr zu und von Amazon S3 zulassen. Sie können in Netzwerk-ACL-Regeln nicht auf Präfixlisten verweisen, aber Sie können die IP-Adresse für Amazon S3 aus der Präfixliste für Amazon S3 abrufen.
- Prüfen Sie, ob Sie eine verwenden AWS-Service , die Zugriff auf einen S3-Bucket erfordert. Beispielsweise kann ein Dienst Zugriff auf Buckets benötigen, die Protokolldateien enthalten, oder Sie müssen Treiber oder Agenten auf Ihre EC2-Instances herunterladen. Wenn ja, stellen Sie sicher, dass Ihre Endpunktrichtlinie es der AWS-Service OR-Ressource erlaubt, mithilfe der `s3:GetObject` Aktion auf diese Buckets zuzugreifen.
- Sie können die Bedingung `aws:SourceIp` nicht in einer Identitätsrichtlinie oder einer Bucket-Richtlinie für Anforderungen an Amazon S3 verwenden, die einen VPC-Endpunkt durchlaufen. Verwenden Sie stattdessen die Bedingung `aws:VpcSourceIp`. Alternativ können Sie auch Routing-Tabellen verwenden, um zu steuern, welche EC2-Instanzen über den VPC-Endpunkt auf Amazon S3 zugreifen können.

- Die Quelle IPv4 oder IPv6 Adressen von Instances in Ihren betroffenen Subnetzen, die von Amazon S3 empfangen wurden, ändern sich von öffentlichen Adressen zu privaten Adressen in Ihrer VPC. Endpunkte wechseln zwischen Netzwerkrouten und trennen offene TCP-Verbindungen. Die vorherigen Verbindungen, für die öffentliche 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 auf einen Bereich außerhalb einer VPC erweitert werden. Ressourcen auf der anderen Seite einer VPN-Verbindung, VPC-Peering-Verbindung, eines Transit-Gateways oder einer Direct Connect Verbindung in Ihrer VPC können keinen Gateway-Endpunkt für die Kommunikation mit Amazon S3 verwenden.
- Ihr Konto hat ein Standardkontingent von 20 Gateway-Endpunkten pro Region, das anpassbar ist. Pro VPC sind auch höchstens 255 Gateway-Endpunkte zulässig.

Privates DNS

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

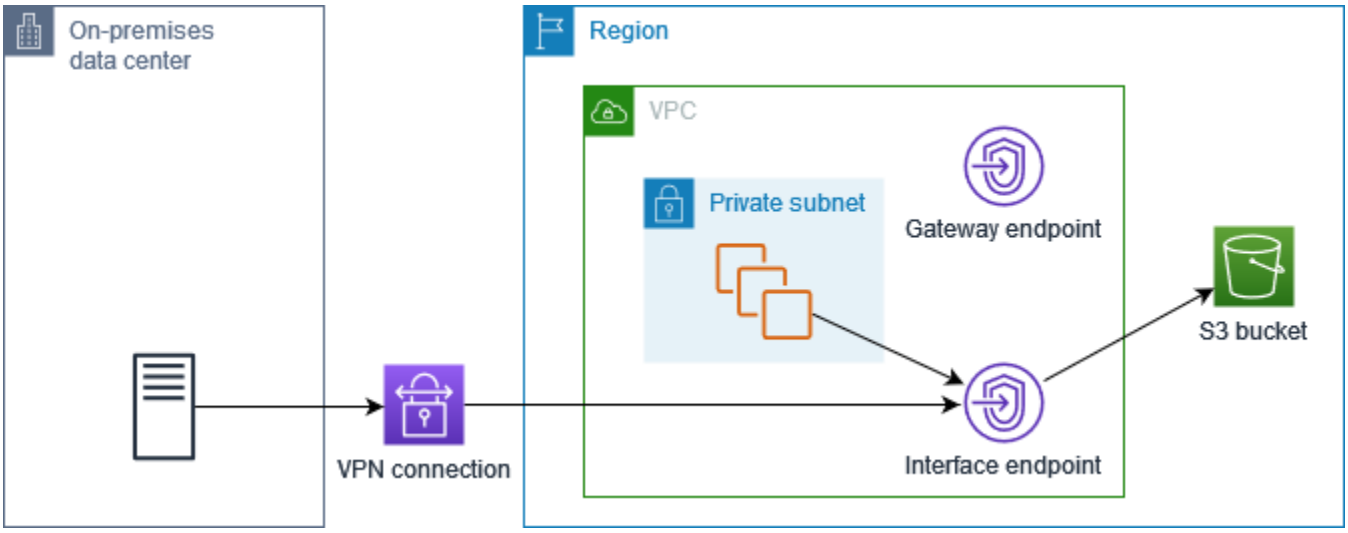
Route 53 Resolver

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

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

Privates DNS

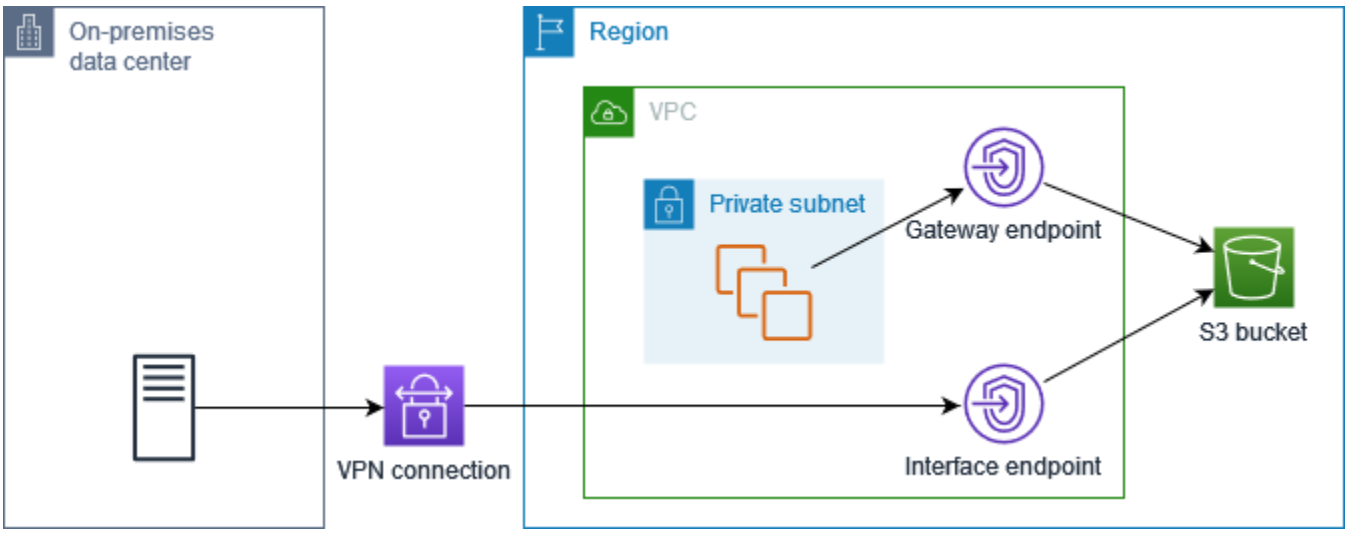
Wenn Sie privates DNS für Ihren Schnittstellenendpunkt für Amazon S3 konfigurieren, aber nicht nur privates DNS für den eingehenden Resolver-Endpunkt konfigurieren, verwenden Anfragen sowohl aus Ihrem On-Premises-Netzwerk als auch aus Ihrer VPC den Schnittstellenendpunkt, um auf Amazon S3 zuzugreifen.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



Privates DNS nur für den eingehenden Resolver-Endpunkt

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

Um dies zu konfigurieren, muss der DNS-Eintrags-IP-Typ des Gateway-Endpunkts mit dem Schnittstellenendpunkt übereinstimmen oder sein`service-defined`. AWS PrivateLink unterstützt keine andere Kombination. Weitere Informationen finden Sie unter the section called “IP-Typ des DNS-Eintrags”.



Privates DNS konfigurieren

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

Erstellen eines Gateway-Endpunkts

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

So erstellen Sie ein Gateway-Endpunkt mithilfe der Konsole

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

   Wenn Ihre Amazon S3 S3-Daten in Allzweck-Buckets gespeichert sind, wählen Sie com.amazonaws aus. *region*.s3.

   Wenn Ihre Amazon S3 S3-Daten in Verzeichnis-Buckets gespeichert sind, wählen Sie com.amazonaws aus. *region*.s3express.
6. Wählen Sie für VPC eine VPC, in der der Endpunkt erstellt werden soll.

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

   - IPv4— Weisen Sie den IPv4 Netzwerkschnittstellen der Endpunkte 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 akzeptiert IPv6 .
   - 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
8. 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.
9. Wählen Sie für Policy (Richtlinie) Full access (Vollzugriff), um alle Operationen aller Prinzipale auf allen Ressourcen über den VPC-Endpunkt zuzulassen. Wählen Sie andernfalls Custom (Benutzerdefiniert), um eine VPC-Endpunktrichtlinie anzufügen, die die Berechtigungen steuert, die Prinzipale zum Ausführen von Aktionen für Ressourcen über den VPC-Endpunkt haben.
10. (Optional) Sie fügen ein Tag hinzu, indem Sie neuen Tag hinzufügen auswählen und den Schlüssel und den Wert für den Tag eingeben.
11. Wählen Sie Endpunkt erstellen.

So erstellen Sie ein Gateway-Endpunkt mithilfe der Befehlszeile

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

Zugriffssteuerung mithilfe von Bucket-Richtlinien

Sie können Bucket-Richtlinien verwenden, um den Zugriff auf Buckets von bestimmten Endpunkten VPCs, IP-Adressbereichen und aus zu steuern. AWS-Konten In diesen Beispielen wird davon ausgegangen, dass es auch Richtlinienanweisungen gibt, die den für Ihre Anwendungsfälle erforderlichen Zugriff zulassen.

Example Beispiel: Beschränken des Zugriffs auf einen bestimmten Endpunkt

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

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPCE",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example Beispiel: Beschränken des Zugriffs auf eine bestimmte VPC

Mithilfe des Bedingungsschlüssels aws:SourceVpc können Sie eine Bucket-Richtlinie erstellen, die VPCs den Zugriff auf bestimmte Bereiche beschränkt. Dies ist hilfreich, wenn Sie mehrere Endpunkte innerhalb derselben VPC konfiguriert haben. Die folgende Richtlinie lehnt Zugriff auf den angegebenen Bucket mit den angegebenen Aktionen ab, es sei denn, die Anforderung stammt von einer angegebenen VPC. Beachten Sie, dass diese Richtlinie den Zugriff auf den angegebenen Bucket mit den angegebenen Aktionen über die AWS-Managementkonsole blockiert.

JSON

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

Example Beispiel: Beschränken des Zugriffs auf einen bestimmten IP-Adressbereich

Mithilfe des Bedingungsschlüssels aws: können Sie eine Richtlinie erstellen, die den Zugriff auf bestimmte IP-Adressbereiche einschränkt. VpcSourceIp 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-Managementkonsole blockiert.

JSON

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

```
                "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
    }
  ]
}
```

Example 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.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-bucket-in-specific-account",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:GetObject", "s3:PutObject", "s3:DeleteObject"],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

Zuordnen von Routing-Tabellen

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

Zuordnen von Routing-Tabellen mithilfe der Konsole

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

Zuordnen von Routing-Tabellen mithilfe der Befehlszeile

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

Bearbeiten der VPC-Endpunktrichtlinie

Sie können die Endpunktrichtlinie für einen Gateway-Endpunkt bearbeiten, der den Zugriff auf Amazon S3 von der VPC über den Endpunkt steuert. Nachdem Sie eine Endpunktrichtlinie aktualisiert haben, kann es einige Minuten dauern, bis die Änderungen wirksam werden. Die Standardrichtlinie lässt Vollzugriff zu. Weitere Informationen finden Sie unter Endpunktrichtlinien.

So ändern Sie die Endpunktrichtlinie mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Erstellen des Gateway-Endpunkts.
4. Wählen Sie Aktionen, Verwalten von Richtlinien.

5. Wählen Sie Full Access (Voller Zugriff), um vollen Zugriff auf den Service zu gewähren, oder wählen Sie Custom (Benutzerdefiniert), und fügen Sie eine benutzerdefinierte Richtlinie hinzu.
6. Wählen Sie Speichern.

Nachfolgend sind Beispielendpunktrichtlinien für den Zugriff auf Amazon S3 aufgeführt.

Example Beispiel: Beschränken des Zugriffs auf einen bestimmten Bucket

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

JSON

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

Example Beispiel: Beschränken des Zugriffs auf eine bestimmte IAM-Rolle

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

JSON

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

Example Beispiel: Beschränken des Zugriffs auf Benutzer in einem bestimmten Konto

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

JSON

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

```
  ]
}
```

Löschen eines Gateway-Endpunkts

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

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

So löschen Sie ein Gateway-Endpunkt mithilfe der Konsole

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

So löschen Sie ein Gateway-Endpunkt mithilfe der Befehlszeile

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

Gateway-Endpunkte für Amazon DynamoDB

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

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

DynamoDB unterstützt sowohl Gateway-Endpunkte als auch Schnittstellenendpunkte. Mit einem Gateway-Endpunkt können Sie von Ihrer VPC aus auf DynamoDB zugreifen, ohne dass ein Internet-Gateway oder ein NAT-Gerät für Ihre VPC erforderlich ist, und ohne zusätzliche Kosten. Gateway-Endpunkte ermöglichen jedoch keinen Zugriff von lokalen Netzwerken, von Peering-Netzwerken VPCs in anderen AWS Regionen oder über ein Transit-Gateway. Für diese Szenarien müssen Sie

einen Schnittstellenendpunkt verwenden, der gegen Aufpreis verfügbar ist. Weitere Informationen finden Sie unter Typen von VPC-Endpunkten für DynamoDB im Amazon DynamoDB Developer Guide.

Inhalt

Überlegungen

- Ein Gateway-Endpunkt ist nur in der Region verfügbar, in der Sie ihn erstellt haben. Stellen Sie sicher, dass Sie Ihren Gateway-Endpunkt in derselben Region wie Ihre DynamoDB-Tabellen erstellen.
- Wenn Sie die Amazon-DNS-Server verwenden, müssen Sie sowohl DNS-Hostnamen als auch DNS-Auflösung für Ihre VPC aktivieren. Wenn Sie Ihren eigenen DNS-Server verwenden, stellen Sie sicher, dass Anforderungen an DynamoDB korrekt in die von AWS verwalteten IP-Adressen erfüllt werden.
- Die ausgehenden Regeln für die Sicherheitsgruppe für Instances, die über den Gateway-Endpunkt auf DynamoDB zugreifen, müssen Datenverkehr zu DynamoDB zulassen. Sie können in den Regeln der Sicherheitsgruppe auf die ID der Präfixliste für DynamoDB verweisen.
- Die Netzwerk-ACL für das Subnetz für Ihre Instances, die über einen Gateway-Endpunkt auf DynamoDB zugreifen, muss Datenverkehr zu und von DynamoDB zulassen. Sie können in Netzwerk-ACL-Regeln nicht auf Präfixlisten verweisen, aber Sie können die IP-Adresse für DynamoDB aus der Präfixliste für DynamoDB abrufen.
- Wenn Sie AWS CloudTrail DynamoDB-Operationen protokollieren, enthalten die Protokolldateien die privaten IP-Adressen der EC2-Instances in der Service Consumer-VPC und die ID des Gateway-Endpunkts für alle Anfragen, die über den Endpunkt ausgeführt werden.
- Gateway-Endpunkte unterstützen nur Datenverkehr. IPv4
- Die IPv4 Quelladressen von Instances in Ihren betroffenen Subnetzen ändern sich von öffentlichen IPv4 Adressen zu privaten IPv4 Adressen aus Ihrer VPC. Endpunkte wechseln zwischen

Netzwerkrouten und trennen 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 auf einen Bereich außerhalb einer VPC erweitert werden. Ressourcen auf der anderen Seite einer VPN-Verbindung, VPC-Peering-Verbindung, eines Transit-Gateways oder einer Direct Connect Verbindung in Ihrer VPC können keinen Gateway-Endpunkt für die Kommunikation mit DynamoDB verwenden.
- Ihr Konto hat ein Standardkontingent von 20 Gateway-Endpunkten pro Region, das anpassbar ist. Pro VPC sind auch höchstens 255 Gateway-Endpunkte zulässig.

Erstellen eines Gateway-Endpunkts

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

So erstellen Sie ein Gateway-Endpunkt mithilfe der Konsole

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

10. Wählen Sie Endpunkt erstellen.

So erstellen Sie ein Gateway-Endpunkt mithilfe der Befehlszeile

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

Zugriffssteuerung mit IAM-Richtlinien

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

Example Beispiel: Beschränken des Zugriffs auf einen bestimmten Endpunkt

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

JSON

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

Example Beispiel: Erlauben des Zugriffs von einer bestimmten IAM-Rolle

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

JSON

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

Example 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.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-account",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
```

```
            "Resource": "*",
            "Condition": {
               "StringEquals": {
                  "aws:PrincipalAccount": "111122223333"
               }
            }
         }
      ]
}
```

Zuordnen von Routing-Tabellen

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

Zuordnen von Routing-Tabellen mithilfe der Konsole

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

Zuordnen von Routing-Tabellen mithilfe der Befehlszeile

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

Bearbeiten der VPC-Endpunktrichtlinie

Sie können die Endpunktrichtlinie für einen Gateway-Endpunkt bearbeiten, der den Zugriff auf DynamoDB von der VPC über den Endpunkt steuert. Nachdem Sie eine Endpunktrichtlinie

aktualisiert haben, kann es einige Minuten dauern, bis die Änderungen wirksam werden. Die Standardrichtlinie lässt Vollzugriff zu. Weitere Informationen finden Sie unter Endpunktrichtlinien.

So ändern Sie die Endpunktrichtlinie mithilfe der Konsole

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

So ändern Sie ein Gateway-Endpunkt mithilfe der Befehlszeile

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

Nachfolgend sind Beispielendpunktrichtlinien für den Zugriff auf DynamoDB aufgeführt.

Example Beispiel: Schreibgeschützten Zugriff zulassen

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

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

```
  ]
}
```

Example Beispiel: Beschränken des Zugriffs auf eine bestimmte Tabelle

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

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

Löschen eines Gateway-Endpunkts

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

So löschen Sie ein Gateway-Endpunkt mithilfe der Konsole

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

So löschen Sie ein Gateway-Endpunkt mithilfe der Befehlszeile

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

Zugriff auf SaaS-Produkte über AWS PrivateLink

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

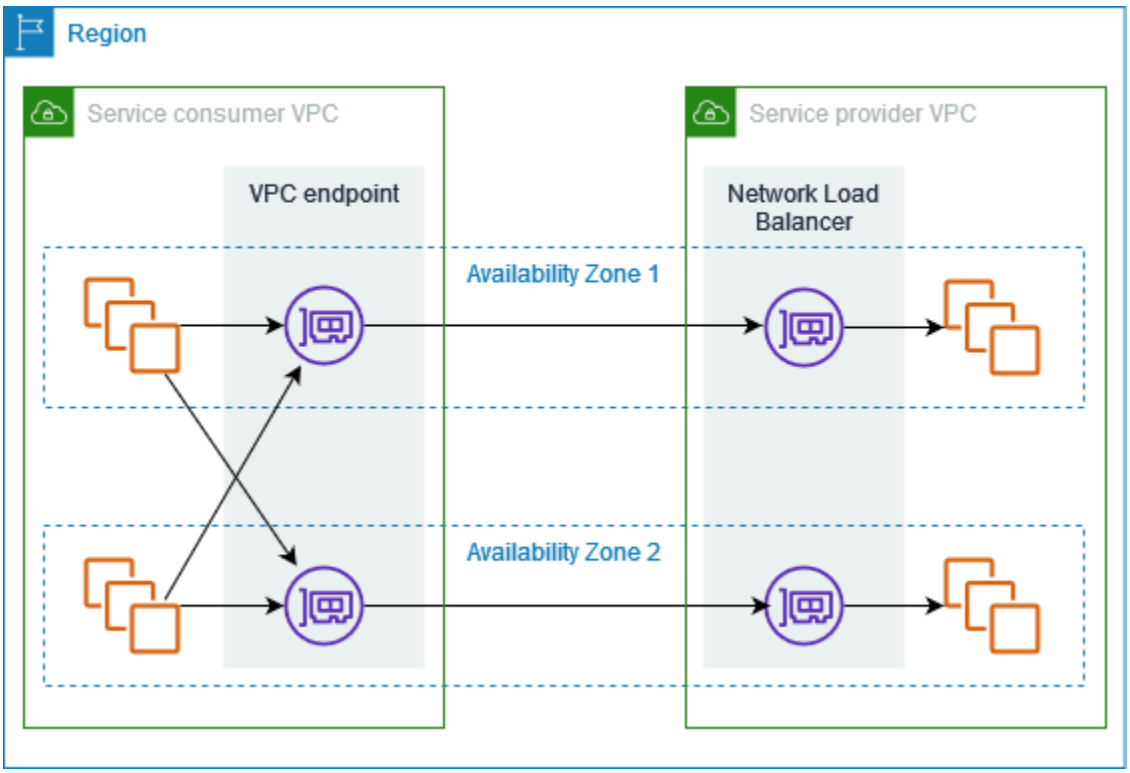
Inhalt

Übersicht

Sie können SaaS-Produkte, die von bereitgestellt werden, entdecken, kaufen und AWS PrivateLink bereitstellen AWS Marketplace. Weitere Informationen finden Sie unter 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 mit SaaS-Produkten herzustellen. Der Service-Anbieter erstellt einen Endpunkt-Service und gewährt seinen Kunden Zugriff auf den Endpunkt-Service. Als Service-Verbraucher erstellen Sie einen Schnittstellen-VPC-Endpunkt, der Verbindungen zwischen einem oder mehreren Subnetzen in Ihrer VPC und dem Endpunkt-Service herstellt.



Erstellen eines Schnittstellenendpunkts

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

Anforderung

Den Service abonnieren.

So erstellen Sie einen Schnittstellenendpunkt zu einem Partnerservice

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen aus.
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 VPC die VPC aus, von der aus Sie auf das Produkt zugreifen.
7. Wählen Sie unter Subnetze die Subnetze aus, in denen Endpunkt-Netzwerkschnittstellen erstellt werden sollen.
8. Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppen aus, die den Security groups (Endpunkt-Netzwerkschnittstellen) zugeordnet werden sollen. Die Sicherheitsgruppenregeln müssen Datenverkehr zwischen den Ressourcen in der VPC und den Endpunktnetzwerkschnittstellen zulassen.
9. (Optional) Sie fügen ein Tag hinzu, indem Sie neues Tag hinzufügen auswählen und den Schlüssel und den Wert für das 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-Endpunkt-Service erstellen. Sonstige AWS -Prinzipale greifen auf den Endpunkt-Service zu, indem sie einen Gateway-Load-Balancer-Endpunkt.

Preise

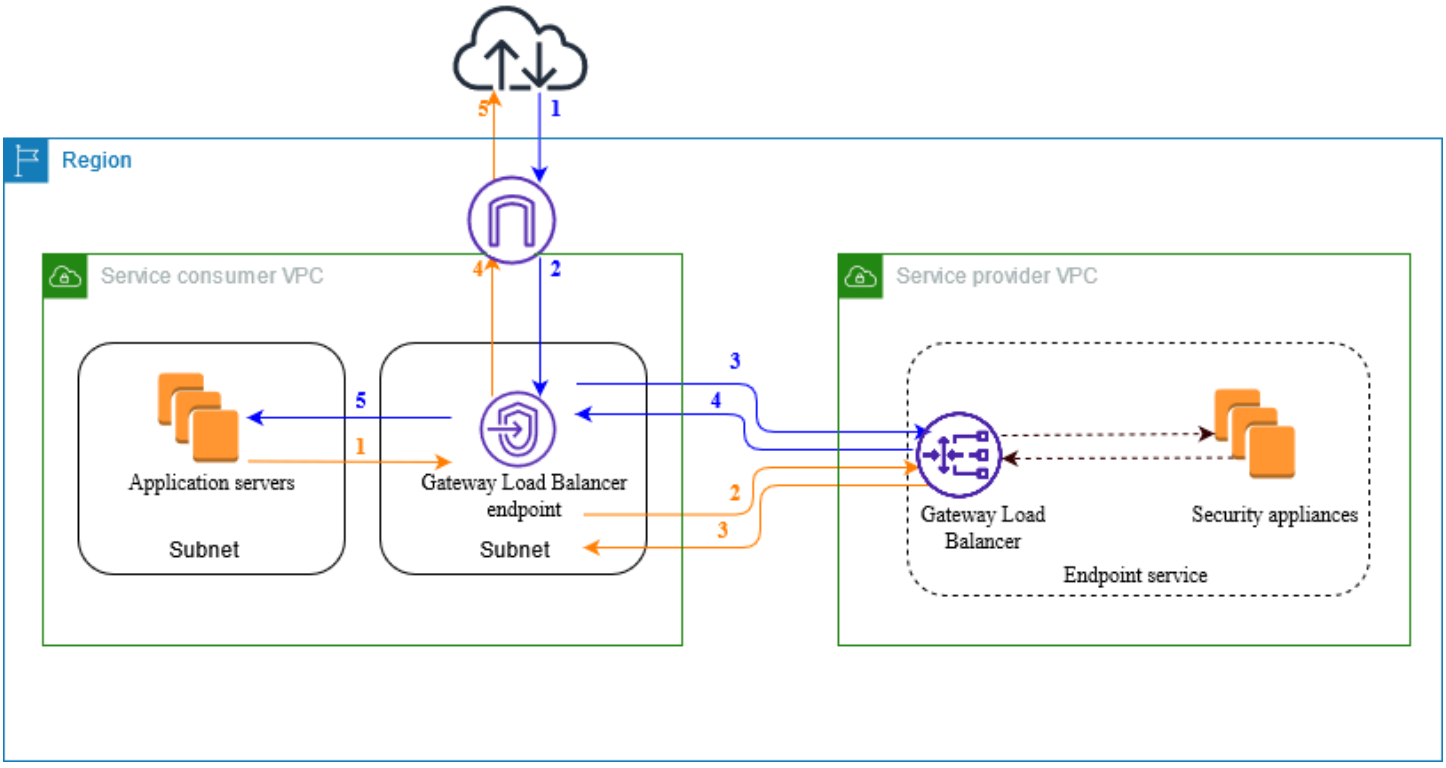
Ihnen wird jede Stunde in Rechnung gestellt, in der Ihr Gateway Load Balancer-Endpunkt in jeder Availability Zone bereitgestellt wird. Ihnen wird auch pro GB verarbeiteter Daten in Rechnung gestellt. Weitere Informationen finden Sie unter AWS PrivateLink – Preise.

Inhalt

Weitere Informationen finden Sie unter Gateway Load Balancer.

Übersicht

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



Datenverkehr vom Internet zu den Anwendungsservern (blaue Pfeile):

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

Datenverkehr von den Anwendungsservern ins Internet (orangefarbene Pfeile):

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

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

IP-Adresstypen

Service Provider können ihre Service-Endpunkte Servicenutzern über IPv4, oder beides IPv6 IPv4 , zur Verfügung stellen IPv6, selbst wenn ihre Sicherheits-Appliances nur IPv4 Support bieten. Wenn Sie den Dual-Stack-Support aktivieren, können bestehende Kunden weiterhin auf Ihren Service zugreifen IPv4 , und neue Kunden können sich dafür entscheiden, Ihren Service IPv6 zu nutzen.

Wenn ein Gateway Load Balancer-Endpunkt dies unterstützt IPv4, haben die Netzwerkschnittstellen des Endpunkts IPv4 Adressen. Wenn ein Gateway Load Balancer-Endpunkt dies unterstützt IPv6, 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

- Die VPC und die Subnetze für den Endpunktdienst müssen zugeordnete IPv6 CIDR-Blöcke haben.
- Der Gateway-Load-Balancer für den Endpunktservice muss den IP-Adresstyp Dualstack verwenden. Die Sicherheits-Appliances müssen den Datenverkehr nicht unterstützen. IPv6

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 Routentabellen für die Subnetze in der 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. Wenn Sie einen Gateway Load Balancer-Endpunkt als Ziel verwenden, können Sie keine Präfixliste als Ziel angeben. In diesen Tabellen sind IPv6 Routen für eine Dual-Stack-Konfiguration enthalten.

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

Bestimmungsort	Ziel
VPC IPv6 CIDR	Local
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 verwenden IDs , um die Availability Zones für Ihren Service konsistent zu identifizieren. Weitere Informationen finden Sie unter AZ IDs im EC2 Amazon-Benutzerhandbuch.
- Es gibt Kontingente für Ihre AWS PrivateLink Ressourcen. Weitere Informationen finden Sie unter AWS PrivateLink Kontingente.

Voraussetzungen

- Erstellen Sie eine Service-Verbraucher-VPC mit mindestens zwei Subnetzen in der Availability Zone, in der der Service zur Verfügung stehen soll. Ein Subnetz ist für die Security-Appliance-Instances und das andere für den Gateway Load Balancer vorgesehen.
- Erstellen Sie einen Gateway Load Balancer in Ihrer Service-Verbraucher-VPC. Wenn Sie 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 in der Service-Verbraucher-VPC und registrieren Sie sie bei einer Load-Balancer-Zielgruppe.

Erstellen Sie den Endpunktservice

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

So erstellen Sie einen Endpunktservice unter Verwendung der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie Create Endpoint Service (Endpunkt-Service erstellen) aus.
4. Wählen Sie für Load-Balancer-Typ Gateway aus.
5. Wählen Sie für Available load balancers (verfügbare Load Balancer) Ihren Gateway-Load-Balancer aus.
6. Wählen Sie für Require acceptance for endpoint (Akzeptanz für Endpunkt erforderlich) Acceptance required (Akzeptanz erforderlich), um zu verlangen, dass Verbindungsanforderungen an Ihren Endpunkt-Service manuell akzeptiert werden. Andernfalls werden sie automatisch akzeptiert.
7. Führen Sie für Unterstützte IP-Adresstyp einen der folgenden Schritte aus:
   - Wählen Sie IPv4— Aktivieren Sie den Endpunktdienst für die Annahme von Anfragen. IPv4
   - 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 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 Ihrer VPC angeben, erstellen wir eine Endpunkt-Netzwerkschnittstelle im Subnetz und weisen ihr eine private IP-Adresse aus dem Subnetz-Adressbereich zu. Eine Endpunkt-Netzwerkschnittstelle ist eine vom Anforderer verwaltete Netzwerkschnittstelle. Sie können sie in Ihrem anzeigen AWS-Konto, aber nicht selbst verwalten.

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

Inhalt

- Routing konfigurieren
- Verwalten von Tags
- Löschen eines Gateway-Load-Balancer-Endpunkts

Überlegungen

- Sie können nur eine Availability Zone in der Service-Verbraucher-VPC auswählen. Sie können dieses Subnetz später nicht mehr ändern. Um einen Gateway-Load-Balancer-Endpunkt in einem anderen Subnetz zu verwenden, müssen Sie einen neuen Gateway-Load-Balancer-Endpunkt erstellen.
- Sie können je Service einen Gateway-Load-Balancer-Endpunkt pro Availability Zone erstellen und müssen die Availability Zone auswählen, die vom Gateway Load Balancer unterstützt wird. Wenn sich der Service-Anbieter und der Service-Verbraucher in verschiedenen Konten befinden, kann ein Name der Availability Zone, z. B. `us-east-1a`, in jedem AWS-Konto einer anderen physischen Verfügbarkeitszone zugeordnet werden. Sie können AZ verwenden IDs , um die Availability Zones für Ihren Service konsistent zu identifizieren. Weitere Informationen finden Sie unter AZ IDs im EC2 Amazon-Benutzerhandbuch.
- Bevor Sie den Endpunkt-Service verwenden können, muss der Service-Anbieter die Verbindungsanforderungen akzeptieren. Der Service kann keine Anfragen an Ressourcen in Ihrer VPC über den VPC-Endpunkt veranlassen. Der Endpunkt gibt nur Antworten auf Datenverkehr zurück, der von Ressourcen in Ihrer VPC initiiert wurde.
- Jeder Gateway Load Balancer-Endpunkt kann eine Bandbreite von bis zu 10 GBit/s pro Availability Zone unterstützen und skaliert automatisch auf bis zu 100 Gbit/s.
- Wenn ein Endpunktservice mehreren Gateway Load Balancers zugeordnet ist, richtet ein Gateway-Load-Balancer-Endpunkt eine Verbindung mit nur einem Load Balancer pro Availability Zone ein.
- Um den Datenverkehr innerhalb derselben Availability Zone zu halten, empfehlen wir Ihnen, in jeder Availability Zone, an die Sie Datenverkehr senden, einen Gateway-Load-Balancer-Endpunkt zu erstellen.
- Die IP-Beibehaltung des Network-Load-Balancer-Clients wird nicht unterstützt, wenn der Datenverkehr über einen Gateway-Load-Balancer-Endpunkt weitergeleitet wird, selbst wenn sich das Ziel in derselben VPC wie der Network Load Balancer befindet.
- Wenn sich die Anwendungsserver und der Gateway Load Balancer-Endpunkt im selben Subnetz befinden, werden die NACL-Regeln für den Verkehr 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 eine Service-Verbraucher-VPC mit mindestens zwei Subnetzen in der Availability Zone, von der aus Sie auf den Service zugreifen. Ein Subnetz ist für die Anwendungsserver und das andere für den Gateway-Load-Balancer-Endpunkt.
- Um zu überprüfen, welche Availability Zones vom Endpoint Service unterstützt werden, beschreiben Sie den Endpoint Service mithilfe der Konsole oder des describe-vpc-endpoint-servicesBefehls.
- Wenn sich Ihre Ressourcen in einem Subnetz mit einer Netzwerk-ACL befinden, stellen Sie sicher, dass die Netzwerk-ACL Datenverkehr zwischen den Netzwerkschnittstellen des Endpunkts und den Ressourcen in der VPC zulässt.

Endpunkt erstellen

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

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

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen aus.
4. Wählen Sie als Typ die Option Endpunktdienste aus, 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 VPC die VPC aus, von der aus Sie auf den Endpoint Service zugreifen.
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 neues Tag hinzufügen auswählen und den Schlüssel und den Wert für das Tag eingeben.
10. Wählen Sie Endpunkt erstellen. Der ursprüngliche Status ist `pending acceptance`.

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

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

Routing konfigurieren

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

So konfigurieren Sie Routing mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Wählen Sie die Routing-Tabelle für den Internet-Gateway aus, und führen Sie die folgenden Schritte aus:

   a. Wählen Sie Aktionen und dann Routen bearbeiten.
   b. Wenn Sie dies unterstützen IPv4, wählen Sie Route hinzufügen. Geben Sie als Ziel den IPv4 CIDR-Block des Subnetzes für die Anwendungsserver ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.

c. Wenn Sie dies unterstützen IPv6, wählen Sie Route hinzufügen. Geben Sie als Ziel den IPv6 CIDR-Block des Subnetzes für die Anwendungsserver ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.

d. Wählen Sie Änderungen speichern.

4. Wählen Sie die Routing-Tabelle für das Subnetz mit den Anwendungsservern aus, und führen Sie folgende Schritte aus:

   a. Wählen Sie Aktionen und dann Routen bearbeiten.

   b. Wenn Sie dies unterstützen IPv4, wählen Sie Route hinzufügen. Geben Sie für Destination **`0.0.0.0/0`** ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.

   c. Wenn Sie dies unterstützen IPv6, wählen Sie Route hinzufügen. Geben Sie für Destination **`::/0`** ein. Wählen Sie für Target (Ziel) den VPC-Endpunkt aus.

   d. Wählen Sie Änderungen speichern.

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

   a. Wählen Sie Aktionen und dann Routen bearbeiten.

   b. Wenn Sie dies unterstützen IPv4, 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 unterstützen IPv6, wählen Sie Route hinzufügen. Geben Sie für Destination **`::/0`** ein. Wählen Sie für Target (Ziel) das Internet-Gateway aus.

   d. Wählen Sie Änderungen speichern aus.

So konfigurieren Sie das Routing mithilfe der Befehlszeile

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

Verwalten von Tags

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

So verwalten Sie Tags mit der Konsole

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

So verwalten Sie Tags mit der Befehlszeile

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

Löschen eines Gateway-Load-Balancer-Endpunkts

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

So löschen Sie einen Gateway-Load-Balancer-Endpunkt

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

So löschen Sie einen Gateway-Load-Balancer-Endpunkt

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

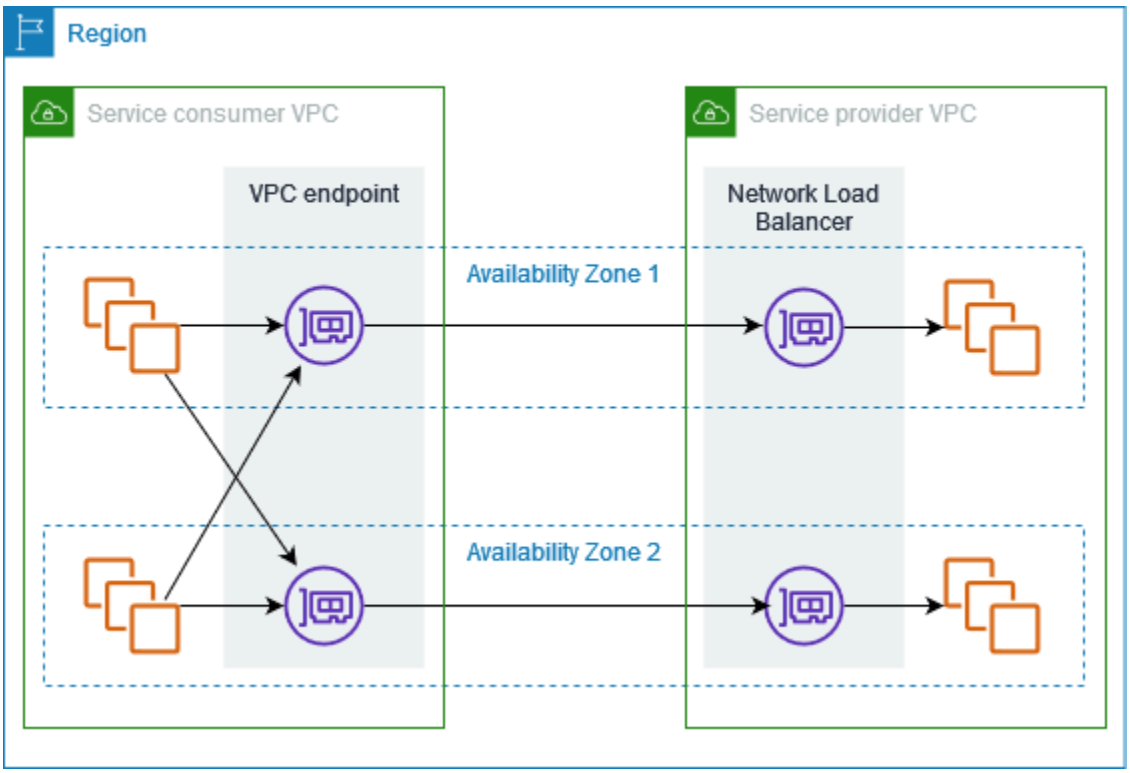
Teilen Sie Ihre Dienste über AWS PrivateLink

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

Inhalt

-Übersicht

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



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

DNS-Hostnamen

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

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

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

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

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

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

Zonale Namen haben die folgende Syntax:

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

Privates DNS

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

Subnetze und Availability Zones

Ihr Endpunktdienst ist in den Availability Zones verfügbar, die Sie für Ihren Network Load Balancer aktivieren. Für hohe Verfügbarkeit und Ausfallsicherheit empfehlen wir, dass Sie Ihren Load Balancer in mindestens zwei Availability Zones aktivieren, EC2-Instances in jeder aktivierten Zone bereitstellen und diese Instances bei Ihrer Load Balancer-Zielgruppe registrieren.

Sie können den zonenübergreifenden Load Balancing als Alternative zum Hosten Ihres Endpunktdienstes in mehreren Availability Zones aktivieren. Verbraucher verlieren jedoch den Zugriff auf den Endpunktdienst von beiden Zonen aus, wenn die Zone, in der der Endpunktdienst gehostet wird, ausfällt. Beachten Sie auch, dass beim Aktivieren des zonenübergreifenden Lastenausgleichs für einen Network Load Balancer EC2-Datenübertragungsgebühren anfallen.

Der Verbraucher kann VPC-Schnittstellen-Endpunkte in den Availability Zones erstellen, in denen Ihr Endpunktservice verfügbar ist. Wir erstellen in jedem Subnetz, das der Verbraucher für den VPC-Endpunkt konfiguriert, eine Endpunkt-Netzwerkschnittstelle. Wir weisen jeder Endpunkt-Netzwerkschnittstelle aus ihrem Subnetz IP-Adressen zu, basierend auf dem IP-Adresstyp des VPC-Endpunkts. Wenn eine Anfrage den regionalen Endpunkt für den VPC-Endpunktdienst verwendet, wählen wir eine fehlerfreie Endpunkt-Netzwerkschnittstelle aus und verwenden den Round-Robin-Algorithmus, um zwischen den Netzwerkschnittstellen in verschiedenen Availability Zones zu wechseln. Anschließend leiten wir den Datenverkehr an die IP-Adresse der ausgewählten Endpunkt-Netzwerkschnittstelle weiter.

Der Verbraucher kann die zonalen Endpunkte für den VPC-Endpunkt verwenden, wenn es für seinen Anwendungsfall besser ist, den Verkehr in derselben Availability Zone zu halten.

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 Berechtigungen zulassen. `vpce:AllowMultiRegion`
- 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 beim Erstellen 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 Endpunktservice 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 müssen Anbieter mindestens zwei Availability Zones verwenden. Für den regionsübergreifenden Zugriff ist es nicht erforderlich, dass Anbieter und Verbraucher dieselben Availability Zones verwenden.
- Der regionsübergreifende Zugriff wird für die folgenden Availability Zones nicht unterstützt:`use1-az3`,`usw1-az2`, `apne1-az3``apne2-az2`, und. `apne2-az4`
- AWS PrivateLink Verwaltet mit regionsübergreifendem Zugriff den Failover zwischen Availability Zones. Es verwaltet kein regionsübergreifendes Failover.
- Der regionsübergreifende Zugriff wird für Network Load Balancer nicht unterstützt, wenn für das TCP-Leerlauf-Timeout ein benutzerdefinierter Wert konfiguriert ist.
- Regionsübergreifender Zugriff wird bei UDP-Fragmentierung nicht unterstützt.
- Der regionsübergreifende Zugriff wird nur für Dienste unterstützt, die Sie gemeinsam nutzen. AWS PrivateLink

IP-Adresstypen

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

Wenn eine Schnittstelle, die der VPC-Endpunkt unterstützt IPv4, haben die Endpunkt-Netzwerkschnittstellen IPv4 Adressen. Wenn eine Schnittstelle, die der VPC-Endpunkt unterstützt IPv6, 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

- Die VPC und die Subnetze für den Endpunktdienst müssen zugeordnete IPv6 CIDR-Blöcke haben.
- Alle Network Load Balancer für den Endpunkt-Service müssen den Dualstack-IP-Adresstyp verwenden. Die Ziele müssen keinen Datenverkehr unterstützen. IPv6 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.

IP-Adresstyp des DNS-Eintrags für einen Schnittstellenendpunkt

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

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

Erstellen Sie einen Dienst, der unterstützt wird von AWS PrivateLink

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

Endpunkt-Services erfordern entweder einen Network Load Balancer oder einen Gateway Load Balancer. Der Load Balancer erhält Anfragen von Service-Verbrauchern und leitet sie an Ihren Service weiter. In diesem Fall erstellen Sie einen Endpunkt-Service mit einem Network Load Balancer. Weitere Informationen zum Erstellen eines Endpunktservice mit einem Gateway Load Balancer finden Sie unter Zugriff auf virtuelle Appliances.

Inhalt

Überlegungen

- Ein Endpunktservice ist in der Region verfügbar, in der Sie ihn erstellt haben. Verbraucher können von anderen Regionen aus auf Ihren Service 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 verwenden, IDs um die Availability Zones für Ihren Service konsistent zu identifizieren. Weitere Informationen finden Sie unter AZ IDs im Amazon EC2 EC2-Benutzerhandbuch.
- Wenn Service-Verbraucher Datenverkehr über einen Schnittstellenendpunkt an einen Service senden, sind die der Anwendung bereitgestellten Quell-IP-Adressen die privaten IP-Adressen der Load-Balancer-Knoten, nicht die IP-Adressen der Service-Verbraucher. Wenn Sie das 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 eine VPC für Ihren Endpunktservice mit mindestens einem Subnetz in jeder Availability Zone, in der der Service verfügbar sein soll.
- Damit Servicekonsumenten IPv6 VPC-Schnittstellen-Endpunkte für Ihren Endpunktdienst erstellen können, müssen der VPC und den Subnetzen zugeordnete CIDR-Blöcke vorhanden sein. IPv6
- Erstellen eines Network Load Balancers in Ihrer VPC. Wählen Sie pro Availability Zone ein Subnetz aus, in dem der Service für Service-Verbraucher verfügbar sein soll. Für niedrige Latenz und Fehlertoleranz empfehlen wir, dass Sie Ihren Service in mindestens zwei Availability Zones der Region zur Verfügung stellen.
- Wenn Ihr Network Load Balancer über eine Sicherheitsgruppe verfügt, muss er eingehenden Datenverkehr von den IP-Adressen der Clients zulassen. Alternativ können Sie die Auswertung der Regeln für eingehende Sicherheitsgruppen für den durchgehenden Datenverkehr deaktivieren. AWS PrivateLink Weitere Informationen finden Sie unter Sicherheitsgruppen im Benutzerhandbuch für Network Load Balancers.
- Damit Ihr 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 Service-Verbraucher zu unterstützen, die zonale DNS-Hostnamen für den Zugriff

auf den Service verwenden. Gebühren für regionale Datenübertragungen fallen an, wenn Sie den zonenübergreifenden Lastausgleich aktivieren. Weitere Informationen finden Sie unter Zonenübergreifendes Load Balancing im Benutzerhandbuch für Network Load Balancers.

Erstellen eines Endpunktservice

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

So erstellen Sie einen Endpunktservice unter Verwendung der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie Create Endpoint Service (Endpunkt-Service erstellen) aus.
4. Wählen Sie für Load balancer type (Load-Balancer-Typ) die Option Network (Netzwerk) aus.
5. Wählen Sie für Available load balancers (verfügbare Load Balancer) die Network Load Balancer aus, die dem Endpunktservice zugeordnet werden sollen. Informationen zu den Availability Zones, die für den 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 für Enable private DNS (Privates DNS aktivieren) Associate a private DNS name with the service (Zuordnen eines privaten DNS-Namens zum Service), um einen privaten DNS-Namen zuzuordnen, den Service-Verbraucher für den Zugriff auf Ihren Service verwenden können, und geben Sie dann den privaten DNS-Namen ein. Andernfalls können Servicenutzer den endpunktspezifischen DNS-Namen verwenden, der von bereitgestellt wird. AWS Bevor Service-Verbraucher den privaten DNS-Namen verwenden können, muss der Service-Anbieter überprüfen, ob er Eigentümer der Domain ist. Weitere Informationen finden Sie unter DNS-Namen verwalten.

9. Führen Sie für Supported IP address types (Unterstützte IP-Adresstyp) einen der folgenden Schritte aus:
   - Wählen Sie IPv4— Aktivieren Sie den Endpunktdienst für die Annahme IPv4 von 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 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 Principals können sich privat mit Ihrem Endpunktdienst verbinden, indem sie einen VPC-Schnittstellen-Endpunkt erstellen. Service-Anbieter müssen Folgendes tun, um ihre Services den Service-Verbrauchern zur Verfügung zu stellen.

- Fügen Sie Berechtigungen hinzu, die es jedem Service-Verbraucher ermöglichen, eine Verbindung mit Ihrem Endpunkt-Service herzustellen. Weitere Informationen finden Sie unter the section called “Verwalten von Berechtigungen”.
- Geben Sie dem Service-Verbraucher den Namen Ihres Service und der unterstützten Availability Zonen, damit er einen Schnittstellenendpunkt erstellen kann, um eine Verbindung mit dem Service herzustellen. Weitere Informationen finden Sie 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 Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen aus.
4. Wählen Sie als Typ die Option Endpunktdienste aus, die und verwenden NLBs . 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 VPC die VPC aus, von der aus Sie auf den Endpoint Service zugreifen.
8. Wählen Sie für 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 akzeptiert IPv6 .
   - 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 DNS record IP type (IP-Typ des DNS-Eintrags) 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-Einträge für die privaten, regionalen und zonalen DNS-Namen. Der IP-Adresstyp muss IPv6oder Dualstack sein.
- Dualstack – Erstellen Sie A- und AAAA-Datensätze für die privaten, regionalen und zonalen DNS-Namen. Der IP-Adresstyp muss Dualstack sein.
- Service defined (Service definiert) – Erstellen Sie A-Datensätze für die privaten, regionalen und zonalen DNS-Namen und AAAA-Einträge für die regionalen und zonalen DNS-Namen. Der IP-Adresstyp muss Dualstack sein.

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
- Zuordnen eines privaten DNS-Namens
- 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-Schnittstellen-Endpunkt zu erstellen, um eine Verbindung zu Ihrem Endpunktdienst herzustellen. Um Berechtigungen für einen AWS Prinzipal hinzuzufügen, benötigen Sie dessen Amazon-Ressourcennamen (ARN). Die folgende Liste enthält Beispiele ARNs für unterstützte AWS Principals.

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

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

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

So ändern Sie die Akzeptanzeinstellung mithilfe der Befehlszeile

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

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

- accept-vpc-endpoint-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 Ihre Load Balancer aktivieren, wird die Availability Zone unter der Registerkarte Load Balancers auf der Seite Endpoint Services angezeigt. Sie wird jedoch nicht für den Endpunktdienst aktiviert oder auf der Registerkarte Details Ihres Endpunktdienstes auf der aufgeführt. AWS-Managementkonsole Sie müssen den Endpunktdienst für die neue Availability Zone aktivieren.

Es kann einige Minuten dauern, bis die Availability Zone des Load Balancers für Ihren Endpunktdienst bereit ist. Wenn Sie eine Automatisierung verwenden, empfehlen wir Ihnen, Ihrem Automatisierungsprozess eine Wartezeit hinzuzufügen, bevor Sie den Endpunktdienst für die neue Availability Zone aktivieren.

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

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den Endpunktservice aus.
4. Wählen Sie Actions (Aktionen), Associate or disassociate load balancers (Load Balancer zuordnen oder trennen).
5. Ändern Sie die Konfiguration des Endpunktdienstes nach Bedarf. Beispiel:
   - 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.
6. Wählen Sie Save Changes (Änderungen speichern)

   Der Endpunktdienst wird für alle neuen Availability Zones aktiviert, die Sie Ihrem Load Balancer hinzugefügt haben. Die neue Availability Zone ist auf den Registerkarten Load Balancers und Details des Endpoint Service aufgeführt.

Nachdem Sie eine Availability Zone für den Endpoint Service aktiviert haben, können Service Consumer ein Subnetz aus dieser Availability Zone zu ihren Schnittstellen-VPC-Endpunkten hinzufügen.

Um die Load Balancer für Ihren Endpoint Service 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.

Zuordnen eines privaten DNS-Namens

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

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

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

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

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

So initiieren Sie den Domain-Überprüfungsprozess mithilfe der Konsole

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

So initiieren Sie den Domain-Überprüfungsprozess mithilfe der Befehlszeile

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

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

3. Wählen Sie den Endpunktservice aus.
4. Wählen Sie Aktionen, Unterstützte Regionen ändern aus.
5. Wählen Sie nach Bedarf Regionen aus oder deaktivieren Sie sie.
6. Wählen Sie Änderungen speichern aus.

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 Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den VPC-Endpunktservice aus.
4. Wählen Sie Actions (Aktionen), Modify supported IP address types (Unterstützte IP-Adresstypen ändern).
5. Führen Sie für Supported IP address types (Unterstützte IP-Adresstyp) einen der folgenden Schritte aus:
   - Wählen 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.
6. Wählen Sie Änderungen speichern aus.

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

So verwalten Sie Tags für Ihre Endpunktverbindungen mithilfe der Konsole

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

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

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

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

So fügen Sie Tags über die Befehlszeile hinzu und entfernen sie

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

DNS-Namen für VPC-Endpunktservices verwalten

Service-Anbieter können private DNS-Namen für ihre Endpunkt-Services konfigurieren. 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 von der Service Consumer-VPC kommt, 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 zum öffentlichen Endpunkt auf.

Bevor Sie einen privaten DNS-Namen für den Endpunkt-Service konfigurieren können, müssen Sie nachweisen, dass Sie Eigentümer der Domain sind, indem Sie eine Überprüfung des Domain-Besitzes durchführen.

Überlegungen

- Ein Endpunktservice kann nur einen privaten DNS-Namen haben.
- Wenn der Verbraucher einen Schnittstellenendpunkt erstellt, um eine Verbindung zu Ihrem Service herzustellen, erstellen wir eine private gehostete Zone und ordnen sie der Service-Consumer-VPC zu. Wir erstellen einen CNAME-Eintrag 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 überprüfen, benötigen Sie einen öffentlichen Hostnamen oder einen öffentlichen DNS-Anbieter.
- Sie können die Domain einer Sub-Domain überprüfen. Beispielsweise können Sie example.com anstelle von a.example.com überprüfen. Jedes DNS-Label kann bis zu 63 Zeichen lang sein und der gesamte Domainname darf eine Gesamtlänge von 255 Zeichen nicht überschreiten.

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

Domain-Verifizierungsname

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

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

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

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

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

Abrufen des Namens und des Werts

Wir geben Ihnen den Namen und Wert, den Sie im TXT-Datensatz verwenden. Beispielsweise sind die Informationen im AWS-Managementkonsole verfügbar. Wählen Sie den Endpunkt-Service aus und siehe Domain verification nameDomain-Verifizierungsname) und Domain verification value on the Details tab for the endpoint service (Domain-Verifizierungswert) auf der Details-Registerkarte für den Endpunkt-Service. Sie können auch den folgenden AWS CLI Befehl describe-vpc-endpoint-service-configurations verwenden, um Informationen über die Konfiguration des privaten DNS-Namens für den angegebenen Endpunktdienst abzurufen.

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

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

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

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

Name	Typ	Wert
_6e86v84tqgqubxbwii1m.example.com	TXT	vpce:l6p0 TT45jevfw ERxl OCp

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

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

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

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

Amazon Route 53

Erstellen Sie mithilfe einer einfachen Routing-Richtlinie einen Datensatz für Ihre öffentliche Hosting-Zone. Verwenden Sie die folgenden Werte:

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

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

Allgemeines Verfahren

Gehen Sie zur Website Ihres DNS-Anbieters und melden Sie sich bei Ihrem Konto an. Suchen Sie die Seite zum Aktualisieren der DNS-Einträge für Ihre Domain. Fügen Sie einen TXT-Eintrag

mit dem angegebenen Namen und Wert hinzu. Es kann bis zu 48 Stunden dauern, bis DNS-Eintragsaktualisierungen wirksam werden, aber sie werden oft viel früher wirksam.

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

DNS/Hosting-Anbieter	Link zur Dokumentation
GoDaddy	Einen TXT-Datensatz hinzufügen
Dreamhost	Hinzufügen von benutzerdefinierten DNS-Datensätzen
Cloudflare	DNS-Datensätze verwalten
HostGator	Verwalten Sie DNS-Einträge mit HostGator /eNOM
Namecheap	Wie füge ich TXT/SPF/DKIM/DMARC Einträge für meine Domain hinzu?
Names.co.uk	Ändern der DNS-Einstellungen für Domain
Wix	Hinzufügen oder Aktualisieren von TXT-Datensätzen in Ihrem Wix-Konto

Prüfen Sie, ob der TXT-Datensatz veröffentlicht ist

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

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

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

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

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

In der Ausgabe werden alle Nameserver für Ihre Domain aufgelistet. Im nächsten Schritt werden Sie einen dieser Server abfragen.

2. Stellen Sie mithilfe des folgenden Befehls sicher, dass der TXT-Eintrag 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. Überprüfen Sie in der Ausgabe des vorherigen Schritts, ob die Zeichenfolge, die auf `text =` folgt, mit dem TXT-Wert übereinstimmt.

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

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

Probleme mit der Domain-Verifizierung beheben

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

- Überprüfen Sie, ob Ihr DNS-Anbieter Unterstriche in TXT-Eintragsnamen zulässt. Wenn Ihr DNS-Anbieter keine Unterstriche zulässt, können Sie den Domain-Überprüfungsnamen (z. B. „_6e86v84tqgqubxbwii1m“) im TXT-Eintrag weglassen.
- Überprüfen Sie, ob Ihr DNS-Anbieter den Domain-Namen an das Ende des TXT-Eintrags angehängt hat. Einige DNS-Anbieter hängen den Namen Ihrer Domain automatisch an den Attributnamen des TXT-Datensatzes an. Um diese Duplizierung des Domain-Namens zu vermeiden, fügen Sie beim Erstellen des TXT-Eintrags einen Punkt am Ende des Domain-Namens hinzu. Dies gibt Ihrem DNS-Anbieter zu verstehen, dass es nicht erforderlich ist, den Domain-Namen an den TXT-Datensatz anzuhängen.
- Überprüfen Sie, ob Ihr DNS-Anbieter den DNS-Datensatzwert geändert hat, um nur Kleinbuchstaben zu verwenden. Wir verifizieren Ihre Domain nur, wenn es einen Bestätigungsdatensatz mit einem Attributwert gibt, der genau mit dem von uns angegebenen

Wert übereinstimmt. Wenn der DNS-Anbieter Ihre TXT-Eintragswerte so geändert hat, dass nur Kleinbuchstaben verwendet werden, wenden Sie sich an ihn, um Unterstützung zu erhalten.

- Möglicherweise müssen Sie Ihre Domain mehr als einmal überprüfen, da Sie mehrere Regionen oder mehrere AWS-Konten unterstützen. Wenn Ihr DNS-Anbieter nicht mehr als einen TXT-Datensatz mit demselben Attributnamen zulässt, überprüfen Sie, ob Ihr DNS-Anbieter Ihnen gestattet, demselben TXT-Datensatz mehrere Attributwerte mit demselben Attributnamen zuzuweisen. Wenn Ihr DNS von Amazon Route 53 verwaltet wird, können Sie das folgende Verfahren verwenden.

  1. Wählen Sie in der Route 53-Konsole den TXT-Datensatz aus, den Sie bei der Verifizierung Ihrer Domain in der ersten Region erstellt haben.
  2. Navigieren Sie im Feld Value (Wert) zum Ende des vorhandenen Attributwertes und drücken Sie dann die Eingabetaste.
  3. Fügen Sie den Attributwert für die zusätzliche Region hinzu und speichern Sie dann den Datensatz.

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

Empfangen von Warnmeldungen für Endpunkt-Serviceereignisse

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

Aufgaben

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

Eine SNS-Benachrichtigung erstellen

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

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

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie den Endpunktservice aus.
4. Wählen Sie aus der Registerkarte Notifications (Benachrichtigungen) die Option Create notification (Benachrichtigung erstellen) aus.
5. Wählen Sie für Notification ARN (Benachrichtigungs-ARN) den ARN für das SNS-Thema aus, das Sie erstellt haben.
6. Um ein Ereignis zu abonnieren, wählen Sie es aus Events (Ereignisse).
   - Connect (Verbinden) – Der Service-Verbraucher hat den Schnittstellenendpunkt erstellt. Dadurch wird eine Verbindungsanfrage an den Service-Anbieter gesendet.
   - Accept (Akzeptieren) – Der Service-Anbieter hat die Verbindungsanfrage akzeptiert.
   - Reject (Ablehnen) – Der Service-Anbieter hat die Verbindungsanfrage abgelehnt.
   - Delete (Löschen) – Der Service-Verbraucher hat den Schnittstellenendpunkt gelöscht.
7. Wählen Sie Benachrichtigung erstellen aus.

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

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

Eine Zugriffsrichtlinie hinzufügen

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

JSON

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

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

Eine Schlüsselrichtlinie hinzufügen

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

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
```

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

Löschen eines Endpunktservice

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

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

So löschen Sie einen Endpunktservice unter Verwendung der Konsole

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

So löschen Sie einen Endpunktservice unter Verwendung der Befehlszeile

- delete-vpc-endpoint-service-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 VPC zugreifen, indem Sie einen Ressourcen-VPC-Endpunkt (Ressourcenendpunkt) verwenden. Mit einem Ressourcenendpunkt können Sie privat und sicher auf VPC-Ressourcen wie eine Datenbank, eine EC2 Amazon-Instance, 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 Ihrer VPC entweder ein Internet-Gateway hinzufügen oder über einen AWS PrivateLink Schnittstellenendpunkt und einen Network Load Balancer auf die Ressource zugreifen. Ressourcenendpunkte benötigen keinen Load Balancer, sodass Sie direkt auf die VPC-Ressource zugreifen können. Eine VPC-Ressource wird durch eine Ressourcenkonfiguration dargestellt. Eine Ressourcenkonfiguration ist einem Ressourcen-Gateway zugeordnet.

Preisgestaltung

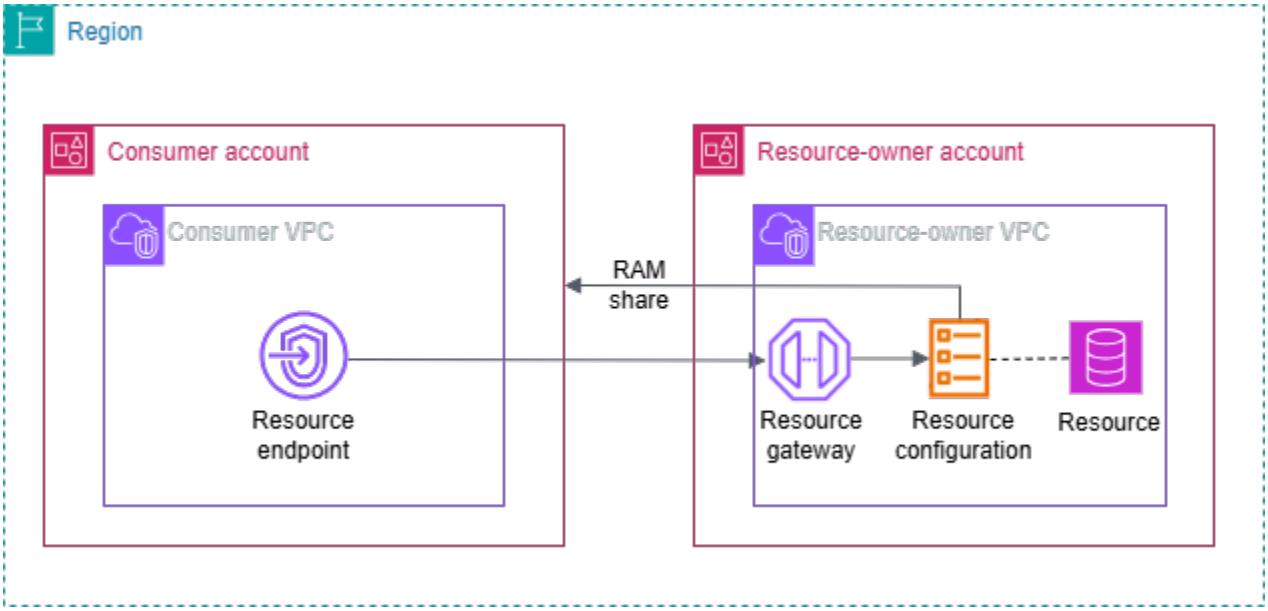
Wenn Sie mithilfe von Ressourcenendpunkten auf Ressourcen zugreifen, wird Ihnen jede Stunde in Rechnung gestellt, in der Ihr Ressourcen-VPC-Endpunkt bereitgestellt wird. Außerdem wird Ihnen pro GB verarbeiteter Daten abgerechnet, wenn Sie auf Ressourcen zugreifen. Weitere Informationen finden Sie unter 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 Ressourcen-VPC-Endpunkt, der mithilfe von Netzwerkschnittstellen Verbindungen zwischen den Subnetzen in Ihrer VPC und der Ressource herstellt. Der für die Ressource bestimmte Datenverkehr wird mithilfe von DNS an die privaten IP-Adressen der Netzwerkschnittstellen des Ressourcenendpunkts weitergeleitet. Anschließend wird der Verkehr über die Verbindung zwischen dem VPC-Endpunkt und der Ressource über das Ressourcen-Gateway an die Ressource gesendet.

Die folgende Abbildung zeigt einen Ressourcenendpunkt in einem Verbraucherkonto, der auf eine Ressource zugreift, die einem anderen Konto gehört und über AWS RAM:



Überlegungen

- TCP-Verkehr wird unterstützt. UDP-Verkehr wird nicht unterstützt.
- Netzwerkverbindungen müssen von der VPC initiiert werden, die den Ressourcenendpunkt enthält, und nicht von der VPC, die über die Ressource verfügt. Die VPC der Ressource kann keine Netzwerkverbindungen zur Endpunkt-VPC initiieren.
- Die einzigen unterstützten ARN-basierten Ressourcen sind Amazon RDS-Ressourcen.
- Mindestens eine Availability Zone des VPC-Endpunkts und des Resource Gateways muss sich überschneiden.

DNS-Hostnamen

Mit AWS PrivateLink senden Sie Traffic über private Endpunkte an Ressourcen. Wenn Sie einen Ressourcen-VPC-Endpunkt erstellen, erstellen wir regionale DNS-Namen (auch Standard-DNS-Name genannt), die Sie für die Kommunikation mit der Ressource von Ihrer VPC und vor Ort verwenden können. Wir empfehlen, dass Sie DNS statt Endpoint verwenden, IPs um eine Verbindung zu Ihren Ressourcen herzustellen. Der Standard-DNS-Name für Ihren Ressourcen-VPC-Endpunkt hat die folgende Syntax:

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

Wenn Sie einen Ressourcen-VPC-Endpunkt für ausgewählte Ressourcenkonfigurationen erstellen, die verwendet werden ARNs, können Sie privates DNS aktivieren. Mit privatem DNS können Sie weiterhin Anfragen an die Ressource stellen, indem Sie den vom AWS Dienst für die Ressource bereitgestellten DNS-Namen verwenden und gleichzeitig die private Konnektivität über den Ressourcen-VPC-Endpunkt nutzen. Weitere Informationen finden Sie unter the section called “DNS-Auflösung”.

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[*].*'
```

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

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

```
            "HostedZoneId": "ABCDEFGH123456789000"
        },
        {
            "DnsName": "database-5-test.cluster-ro-example.us-
east-1.rds.amazonaws.com",
            "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
        },
        "arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890abcdefg",
        "arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890xyz"
    ]
]
```

DNS-Auflösung

Die DNS-Einträge, die wir für Ihren Ressourcen-VPC-Endpunkt erstellen, sind öffentlich. Daher sind diese DNS-Namen öffentlich auflösbar. DNS-Anfragen von außerhalb der VPC geben jedoch 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 über VPN oder Direct Connect Zugriff auf die VPC haben, in der sich der Ressourcenendpunkt befindet.

Privates DNS

Wenn Sie privates DNS für Ihren Ressourcen-VPC-Endpunkt für ausgewählte Ressourcenkonfigurationen aktivieren, die diese verwenden ARNs, und in Ihrer VPC sowohl DNS-Hostnamen als auch DNS-Auflösung aktiviert sind, erstellen wir versteckte, AWS verwaltete privat gehostete Zonen für Ressourcenkonfigurationen mit einem benutzerdefinierten DNS-Namen. Die gehostete Zone enthält einen Datensatz für den Standard-DNS-Namen für die Ressource, der ihn in die privaten IP-Adressen der Netzwerkschnittstellen des Ressourcenendpunkts in Ihrer VPC auflöst.

Amazon stellt einen DNS-Server für Ihre VPC zu Verfügung, den Route 53 Resolver. Der Route 53 Resolver löst automatisch lokale VPC-Domainnamen und Datensätze in privaten gehosteten Zonen. Sie können den Route 53 Resolver jedoch nicht von außerhalb Ihrer VPC verwenden. Wenn Sie von Ihrem lokalen Netzwerk aus auf Ihren VPC-Endpunkt zugreifen möchten, können Sie den benutzerdefinierten DNS-Namen oder 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 Ihre VPC-Endpunkte mit einem Subnetz pro Availability Zone konfigurieren. Wir erstellen eine Endpunkt-Netzwerkschnittstelle für den VPC-Endpunkt in Ihrem Subnetz. Wir weisen jeder Endpunkt-Netzwerkschnittstelle aus ihrem Subnetz IP-Adressen zu, basierend auf dem IP-Adresstyp des VPC-Endpunkts. In einer Produktionsumgebung empfehlen wir für hohe Verfügbarkeit und Ausfallsicherheit, mindestens zwei Availability Zones für jeden VPC-Endpunkt zu konfigurieren.

IP-Adresstypen

Ressourcenendpunkte können IPv4 IPv6 Dual-Stack-Adressen unterstützen. Endpunkte, die dies unterstützen, IPv6 können auf DNS-Abfragen mit AAAA-Einträgen antworten. 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 Ressourcen-VPC-Endpunkt unterstützt IPv4, haben die Endpunkt-Netzwerkschnittstellen IPv4 Adressen. Wenn ein Ressourcen-VPC-Endpunkt unterstützt IPv6, 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.

Greifen Sie über einen Ressourcen-VPC-Endpunkt auf eine Ressource zu

Sie können über einen Ressourcenendpunkt auf eine VPC-Ressource wie einen Domainnamen, eine IP-Adresse oder eine Amazon RDS-Datenbank zugreifen. Ein Ressourcenendpunkt bietet privaten Zugriff auf eine Ressource. Wenn Sie den Ressourcenendpunkt erstellen, geben Sie eine

Ressourcenkonfiguration vom Typ Single, Group oder ARN an. 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 von Ihnen erstellte Ressourcenkonfiguration oder ein anderes Konto verfügen, das erstellt und mit Ihnen geteilt wurde AWS RAM.
- Wenn eine Ressourcenkonfiguration von einem anderen Konto aus 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. Nachdem Sie einen Ressourcenendpunkt erstellt haben, können Sie nur seine Sicherheitsgruppen oder Tags ändern.

So erstellen Sie einen VPC-Ressourcenendpunkt

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Endpunkt erstellen aus.
4. Sie können einen Namen angeben, um den Endpunkt leichter zu finden und zu verwalten.
5. Wählen Sie für Typ die Option Ressourcen aus.
6. Wählen Sie für Ressourcenkonfigurationen die Ressourcenkonfiguration aus.
7. Wählen Sie unter Netzwerkeinstellungen die VPC aus, von der aus Sie auf die Ressource zugreifen möchten.
8. Wenn Sie private DNS-Unterstützung für Ressourcenkonfigurationen konfigurieren möchten, wählen Sie Zusätzliche Einstellungen, DNS-Name aktivieren aus. Um diese Funktion verwenden zu können, stellen Sie sicher, dass die Attribute DNS-Hostnamen aktivieren und DNS-Unterstützung aktivieren für Ihre VPC aktiviert sind. Weitere Informationen finden Sie unter the section called “Benutzerdefinierte Domainnamen für Ressourcennutzer”.

9. Wählen Sie für Subnetze ein Subnetz aus, in dem die Endpunkt-Netzwerkschnittstelle erstellt werden soll.

   In einer Produktionsumgebung empfehlen wir für hohe Verfügbarkeit und Ausfallsicherheit, mindestens zwei Availability Zones für jeden VPC-Endpunkt zu konfigurieren.
10. Wählen Sie für Sicherheitsgruppen eine Sicherheitsgruppe aus.

    Wenn Sie keine Sicherheitsgruppen-ID angeben, ordnen wir der VPC die Standardsicherheitsgruppe zu.
11. 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 Sicherheitsgruppen oder Tags verwalten.

Aufgaben

- Löschen eines Endpunkts
- Einen Endpunkt aktualisieren

Löschen eines Endpunkts

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

Um einen Endpunkt mit der Konsole zu löschen

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

6. Wählen Sie Löschen aus.

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 Amazon-VPC-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 aus.
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 zu Ressourcen in Ihrer VPC von Clients in anderen Ländern VPCs und Konten zulassen. Eine Ressourcenkonfiguration ist einem Ressourcen-Gateway zugeordnet, über das sie Datenverkehr empfängt.

Inhalt

- Ressourcen-Gateway
- Benutzerdefinierte Domainnamen für Ressourcenanbieter
- Benutzerdefinierte Domainnamen für Ressourcennutzer
- Benutzerdefinierte Domänennamen für Besitzer von Servicenetzwerken
- Definition der Ressource
- Protocol (Protokoll)
- Portbereiche
- Auf -Ressourcen zugreifen
- Zuordnung zum Servicenetzwerktyp
- Arten von Servicenetzwerken
- Gemeinsame Nutzung von Ressourcenkonfigurationen über AWS RAM
- Überwachen
- Erstellen einer Ressourcenkonfiguration in VPC Lattice
- Verwalten von Zuordnungen für eine VPC-Lattice-Ressourcenkonfiguration

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.
- Konfiguration von Gruppenressourcen: Eine Sammlung von Konfigurationen untergeordneter Ressourcen. 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.
- ARN-Ressourcenkonfiguration: Stellt einen unterstützten Ressourcentyp dar, der von einem Dienst bereitgestellt wird. AWS Zum Beispiel eine Amazon RDS-Datenbank. Konfigurationen untergeordneter Ressourcen werden automatisch von verwaltet AWS.

Ressourcen-Gateway

Eine Ressourcenkonfiguration ist einem Ressourcen-Gateway zugeordnet. Ein Ressourcen-Gateway ist eine Gruppe von Gateways ENIs , die als Eingangspunkt in die VPC dienen, in der sich die Ressource befindet. Diesem Ressourcen-Gateway können mehrere Ressourcenkonfigurationen zugeordnet werden. Wenn Clients in anderen Konten VPCs oder Konten auf eine Ressource in Ihrer VPC zugreifen, sieht die Ressource Datenverkehr, der lokal vom Ressourcen-Gateway in dieser VPC kommt.

Benutzerdefinierte Domainnamen für Ressourcenanbieter

Ressourcenanbieter können einer Ressourcenkonfiguration einen benutzerdefinierten Domainnamen zuordnen, z. B. `example.com` den Ressourcenverbraucher für den Zugriff auf die Ressourcenkonfiguration verwenden können. Der benutzerdefinierte Domainname kann Eigentum des Ressourcenanbieters sein und von diesem verifiziert werden, oder es kann sich um einen Drittanbieter oder eine AWS Domain handeln. Ressourcenanbieter können Ressourcenkonfigurationen verwenden, um Cache-Cluster und Kafka-Cluster, TLS-basierte Anwendungen oder andere Ressourcen gemeinsam zu nutzen. AWS

Die folgenden Überlegungen gelten für Anbieter von Ressourcenkonfigurationen:

- Eine Ressourcenkonfiguration kann nur eine benutzerdefinierte Domäne haben.
- Der benutzerdefinierte Domainname einer Ressourcenkonfiguration kann nicht geändert werden.
- Der benutzerdefinierte Domänenname ist für alle Benutzer der Ressourcenkonfiguration sichtbar.
- Sie können Ihren benutzerdefinierten Domainnamen mithilfe des Domainnamen-Überprüfungsprozesses in VPC Lattice verifizieren. Weitere Informationen Weitere Informationen finden Sie unter. https://docs.aws.amazon.com/vpc-lattice/latest/ug/create-and-verify.html
- Für Ressourcenkonfigurationen vom Typ Gruppe und Kind müssen Sie zunächst eine Gruppendomäne in der Gruppenressourcenkonfiguration angeben. Danach können die Konfigurationen der untergeordneten Ressourcen benutzerdefinierte Domänen haben, die Unterdomänen der Gruppendomäne sind. Wenn die Gruppe keine Gruppendomäne hat, können Sie einen beliebigen benutzerdefinierten Domänennamen für das Kind verwenden, aber VPC Lattice stellt keine gehosteten Zonen für die untergeordneten Domänennamen in der VPC des Ressourcennutzers bereit.

Benutzerdefinierte Domainnamen für Ressourcennutzer

Wenn Ressourcenverbraucher Konnektivität zu einer Ressourcenkonfiguration mit einem benutzerdefinierten Domänennamen aktivieren, können sie VPC Lattice erlauben, eine private gehostete Route 53-Zone in ihrer VPC zu verwalten. Ressourcennutzer haben detaillierte Optionen für die Domänen, für die sie VPC Lattice erlauben möchten, private gehostete Zonen zu verwalten.

Ressourcenverbraucher können den `private-dns-enabled` Parameter festlegen, wenn sie die Konnektivität zu Ressourcenkonfigurationen über einen Ressourcenendpunkt, einen Servicenetzwerkendpunkt oder eine Servicenetzwerk-VPC-Zuordnung aktivieren. Zusammen mit dem `private-dns-enabled` Parameter können Verbraucher mithilfe von DNS-Optionen angeben, für welche Domänen VPC Lattice private gehostete Zonen verwalten soll. Verbraucher können zwischen den folgenden privaten DNS-Einstellungen wählen:

`ALL_DOMAINS`

VPC Lattice stellt private Hosting-Zonen für alle benutzerdefinierten Domainnamen bereit.

`VERIFIED_DOMAINS_ONLY`

VPC Lattice stellt nur dann eine private gehostete Zone bereit, wenn der benutzerdefinierte Domainname vom Anbieter verifiziert wurde.

`VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`

VPC Lattice stellt private Hosting-Zonen für alle verifizierten benutzerdefinierten Domainnamen und andere Domainnamen bereit, die der Ressourcennutzer angibt. Der Ressourcenverbraucher gibt die Domänennamen im Parameter an`private DNS specified domains`.

`SPECIFIED_DOMAINS_ONLY`

VPC Lattice stellt eine private gehostete Zone für vom Ressourcennutzer angegebene Domainnamen bereit. Der Ressourcenverbraucher gibt die Domänennamen im Parameter an`private DNS specified domains` .

Wenn Sie privates DNS aktivieren, erstellt VPC Lattice eine private gehostete Zone in Ihrer VPC für den benutzerdefinierten Domainnamen, der der Ressourcenkonfiguration zugeordnet ist. Standardmäßig ist die private DNS-Präferenz auf eingestellt. `VERIFIED_DOMAINS_ONLY` Das bedeutet, dass private Hosting-Zonen nur erstellt werden, wenn der benutzerdefinierte Domainname vom Ressourcenanbieter verifiziert wurde. Wenn Sie Ihre private DNS-

Präferenz auf `ALL_DOMAINS` oder `SPECIFIED_DOMAINS_ONLY` setzen, erstellt VPC Lattice unabhängig vom Bestätigungsstatus des benutzerdefinierten Domainnamens private gehostete Zonen. Wenn eine private gehostete Zone für eine bestimmte Domain erstellt wird, wird der gesamte Datenverkehr von Ihrer VPC zu dieser Domain über VPC Lattice geleitet. Wir empfehlen, die `SPECIFIED_DOMAINS_ONLY` Einstellungen`ALL_DOMAINS`, oder nur zu verwenden`VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`, wenn Sie möchten, dass der Datenverkehr zu diesen benutzerdefinierten Domainnamen über VPC Lattice geleitet wird.

Wir empfehlen, dass Ressourcennutzer ihre private DNS-Präferenz auf setzen. `VERIFIED_DOMAINS_ONLY` Auf diese Weise können Verbraucher ihren Sicherheitsbereich verschärfen, indem sie VPC Lattice nur erlauben, private gehostete Zonen für verifizierte Domänen im Konto des Ressourcennutzers bereitzustellen.

Um Domänen in den vom privaten DNS angegebenen Domänen auszuwählen, können Ressourcennutzer einen vollqualifizierten Domänennamen eingeben, z. B. `my.example.com` oder einen Platzhalter wie verwenden. `*.example.com`

Die folgenden Überlegungen gelten für Nutzer von Ressourcenkonfigurationen:

- Der private DNS-Enabled-Parameter kann nicht geändert werden.
- Privates DNS sollte in einer Dienstnetzwerkressourcenzuordnung aktiviert sein, damit private Hosts in einer VPC erstellt werden können. Bei einer Ressourcenkonfiguration überschreibt der private DNS-aktivierte Status der Dienstnetzwerkressourcenzuordnung den privaten DNS-aktivierten Status entweder des Dienstnetzwerkendpunkts oder der Dienstnetz-VPC-Zuordnung.

Benutzerdefinierte Domänennamen für Besitzer von Servicenetzwerken

Die private DNS-aktivierte Eigenschaft der Dienstnetzwerkressourcenzuordnung überschreibt die private DNS-aktivierte Eigenschaft des Dienstnetzwerkendpunkts und der Dienstnetz-VPC-Zuordnung.

Wenn ein Dienstnetzwerkbesitzer eine Dienstnetzwerkressourcenzuordnung erstellt und privates DNS nicht aktiviert, stellt VPC Lattice in keiner Ressourcenkonfiguration private gehostete Zonen für diese Ressourcenkonfiguration bereit, mit der VPCs das Dienstnetzwerk verbunden ist, obwohl privates DNS auf dem Dienstnetzwerkendpunkt oder den VPC-Zuordnungen des Dienstnetzwerks aktiviert ist.

Für Ressourcenkonfigurationen vom Typ ARN ist das private DNS-Flag wahr und unveränderlich.

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 ihres ARN identifiziert werden. Es werden nur Amazon RDS-Datenbanken unterstützt. Sie können keine Ressourcenkonfiguration für einen öffentlich zugänglichen Cluster erstellen.
- Nach einem Domainnamen-Ziel: Jeder Domainname, der öffentlich auflösbar ist. Wenn Ihr Domainname auf eine IP verweist, die sich außerhalb Ihrer VPC befindet, müssen Sie in Ihrer VPC über ein NAT-Gateway verfügen.
- Nach einer IP-Adresse: Geben Sie für eine private IP aus den folgenden Bereichen an: 10.0.0.0/8 IPv4, 100.64.0.0/10, 172.16.0.0/12, 192.168.0.0/16. Geben Sie für IPv6 eine IP von der VPC an. Öffentliche IPs werden nicht unterstützt.

Protocol (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 über ein Servicenetzwerk direkt von ihrer VPC aus auf Ressourcenkonfigurationen zugreifen. Als Verbraucher können Sie von Ihrer VPC aus den Zugriff auf eine Ressourcenkonfiguration aktivieren, 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 in Ihrer AWS PrivateLink VPC einen VPC-Endpunkt vom Typ Ressource (Ressourcenendpunkt) erstellen, um privat von Ihrer VPC aus auf eine Ressourcenkonfiguration zuzugreifen. Weitere Informationen zum Erstellen eines Ressourcenendpunkts finden Sie unter Zugreifen auf VPC-Ressourcen im AWS PrivateLink Benutzerhandbuch.

- Zugriff auf eine Ressourcenkonfiguration über ein Servicenetzwerk

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

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

  Weitere Informationen zu VPC-Endpunkten im Servicenetzwerk finden Sie im AWS PrivateLink Benutzerhandbuch unter Zugreifen auf Dienstnetzwerke.

Wenn privates DNS für Ihre VPC aktiviert ist, können Sie keinen Ressourcenendpunkt und keinen Servicenetzwerkendpunkt für dieselbe Ressourcenkonfiguration erstellen.

Zuordnung zum Servicenetzwerktyp

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

Um über ein Dienstnetzwerk auf eine Ressourcenkonfiguration zuzugreifen, müsste Account-B die Ressourcenkonfiguration einem Dienstnetzwerk 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

- Verwendung eines VPC-Endpunkts vom Typ Ressource (Ressourcen-VPC-Endpunkt).

- Verwendung eines VPC-Endpunkts vom Typ Dienstnetzwerk (Servicenetzwerk-VPC-Endpunkt).
- Verwenden einer VPC-Zuordnung für ein Servicenetzwerk.

  Wenn Sie eine Dienstnetzwerkverbindung verwenden, wird jeder Ressource eine IP pro Subnetz aus dem Block 129.224.0.0/17 zugewiesen, der Eigentümer ist und nicht routbar ist. AWS Dies ist eine Ergänzung zu der verwalteten Präfixliste, die VPC Lattice verwendet, um Datenverkehr über das VPC Lattice-Netzwerk an Dienste weiterzuleiten. Beide IPs werden in Ihrer VPC-Routentabelle aktualisiert.

Für die Zuordnung des VPC-Endpunkts des Servicenetzwerks und der VPC-Zuordnung des Servicenetzwerks müsste die Ressourcenkonfiguration in einem Servicenetzwerk in Account-B abgelegt werden. Servicenetzwerke können von mehreren Konten gemeinsam genutzt werden. Somit kann Account-B sein Servicenetzwerk (das die Ressourcenkonfiguration enthält) mit Account-C teilen, sodass Ihre Ressource von Account-C aus zugänglich ist. 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 VPC aus auf eine Ressource zuzugreifen, die sich in demselben Konto wie die Ressourcenkonfiguration befindet, 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 einer Ressourcenkonfiguration in VPC Lattice

Erstellen Sie eine Ressourcenkonfiguration.

AWS-Managementkonsole

Um eine Ressourcenkonfiguration mit der Konsole zu erstellen

1. Öffnen Sie die Amazon-VPC-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. (Optional) Gehen Sie wie folgt vor, um einen benutzerdefinierten Domainnamen einzugeben:
   - Wenn Sie eine Ressourcenkonfiguration vom Typ Single haben, können Sie einen benutzerdefinierten Domainnamen eingeben. Ressourcennutzer können diesen Domainnamen verwenden, um auf Ihre Ressourcenkonfigurationen zuzugreifen.
   - Wenn Sie über eine Ressourcenkonfiguration vom Typ Gruppe und Kind verfügen, müssen Sie zunächst eine Gruppendomäne in der Gruppenressourcenkonfiguration angeben. Als Nächstes können die Konfigurationen der untergeordneten Ressourcen benutzerdefinierte Domänen haben, die Unterdomänen der Gruppendomäne sind.
8. (Optional) Geben Sie die Bestätigungs-ID ein.

   Geben Sie eine Bestätigungs-ID an, wenn Sie möchten, dass Ihr Domainname verifiziert wird. Auf diese Weise wissen Ressourcennutzer, dass Sie der Eigentümer des Domainnamens sind.

9. Wählen Sie den Bezeichner für die Ressource aus, die diese Ressourcenkonfiguration darstellen soll.
10. Wählen Sie die Portbereiche aus, über die Sie die Ressource gemeinsam nutzen möchten.
11. Geben Sie unter Zuordnungseinstellungen an, ob diese Ressourcenkonfiguration mit gemeinsam nutzbaren Dienstnetzwerken verknüpft werden kann.
12. Wählen Sie unter Konfiguration gemeinsam genutzter Ressourcen die Ressourcenfreigaben aus, anhand derer die Prinzipale identifiziert werden, die auf diese Ressource zugreifen können.
13. (Optional) Aktivieren Sie unter Überwachung die Option Ressourcenzugriffsprotokolle und das Zustellungsziel, wenn Sie Anfragen und Antworten an und von der Ressourcenkonfiguration überwachen möchten.
14. (Optional) Sie fügen ein Tag hinzu, indem Sie neues Tag hinzufügen auswählen und den Schlüssel und den Wert für das Tag eingeben.
15. Wählen Sie Ressourcenkonfiguration erstellen aus.

AWS CLI

Der folgende create-resource-configurationBefehl erstellt eine einzelne Ressourcenkonfiguration und ordnet sie dem benutzerdefinierten Domänennamen zu`example.com`.

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

Der folgende create-resource-configurationBefehl erstellt eine Gruppenressourcenkonfiguration und ordnet sie dem benutzerdefinierten Domänennamen zu`example.com`.

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

Der folgende create-resource-configurationBefehl erstellt eine untergeordnete Ressourcenkonfiguration und ordnet sie dem benutzerdefinierten Domänennamen `zuchild.example.com`.

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

Verwalten von Zuordnungen für eine VPC-Lattice-Ressourcenkonfiguration

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

Verwalten Sie die Zuordnungen von Dienstnetzwerkressourcen

Erstellen oder löschen Sie eine Dienstnetzwerkzuordnung.

> **Note**
>
> Wenn Sie beim Erstellen der Verbindung zwischen dem Dienstnetzwerk und der Ressourcenkonfiguration die Meldung „Zugriff verweigert“ erhalten, überprüfen Sie Ihre AWS RAM Richtlinienversion und stellen Sie sicher, dass es sich um Version 2 handelt. Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch.

Um eine Service-Netzwerkverbindung mit der Konsole zu verwalten

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter PrivateLink und Lattice die Option Resource configurations 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 ein Servicenetzwerk aus den VPC Lattice-Dienstnetzwerken aus. Um ein Servicenetzwerk zu erstellen, wählen Sie Create a VPC Lattice network aus.
7. (Optional) Um ein Tag hinzuzufügen, erweitern Sie Service-Zuordnungs-Tags, wählen Sie Neues Tag hinzufügen aus und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
8. (Optional) Um private DNS-Namen für diese Dienstnetzwerkressourcenzuweisung zu aktivieren, wählen Sie „Privaten DNS-Namen aktivieren“. Weitere Informationen finden Sie unter the section called “Benutzerdefinierte Domänennamen für Besitzer von Servicenetzwerken”.
9. Wählen Sie Änderungen speichern aus.
10. Um eine Zuordnung zu löschen, aktivieren Sie das Kontrollkästchen für die Zuordnung 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.

VPC-Endpunktzuordnungen für Ressourcen verwalten

Verbraucherkonten mit Zugriff auf Ihre Ressourcenkonfiguration oder Clients in Ihrem Konto können über einen Ressourcen-VPC-Endpunkt auf die Ressourcenkonfiguration zugreifen. Wenn Ihre Ressourcenkonfiguration über einen benutzerdefinierten Domainnamen verfügt, können Sie Enable Private DNS verwenden, damit VPC Lattice private gehostete Zonen für Ihren Ressourcen- oder Servicenetzwerk-Endpunkt bereitstellen kann. Auf diese Weise können Kunden den Domainnamen direkt zusammenrollen, um auf die Ressourcenkonfiguration zuzugreifen. Weitere Informationen finden Sie unter the section called “Benutzerdefinierte Domainnamen für Ressourcennutzer”.

AWS-Managementkonsole

1. Um eine neue Endpunktzuordnung zu erstellen, gehen Sie im linken Navigationsbereich zu PrivateLink und Lattice und wählen Sie Endpoints aus.
2. Wählen Sie Endpunkte erstellen aus.

3. Wählen Sie die Ressourcenkonfiguration aus, die Sie mit Ihrer VPC verbinden möchten.
4. Wählen Sie die VPC, Subnetze und Sicherheitsgruppen aus.
5. (Optional) Um privates DNS zu aktivieren und DNS-Optionen zu konfigurieren, wählen Sie DNS-Name aktivieren aus.
6. (Optional) Um VPC VPC-Endpunkt zu taggen, wählen Sie Neues Tag hinzufügen aus und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
7. Wählen Sie Endpunkt erstellen aus.

AWS CLI

Der folgende create-vpc-endpointBefehl erstellt einen VPC-Endpunkt, der privates DNS verwendet. Die privaten DNS-Einstellungen sind auf eingestellt `VERIFIED_AND_SELECTED` und die ausgewählten Domänen sind `example.com` und`example.org`. VPC Lattice stellt nur private Hosting-Zonen für verifizierte Domains bereit oder oder`example.com`. `example.org`

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

So erstellen Sie eine VPC-Endpunktzuordnung mit dem AWS CLI

Verwenden Sie den Befehl create-vpc-endpoint.

Um eine VPC-Endpunktverknüpfung mit dem AWS CLI

Verwenden Sie den Befehl delete-vpc-endpoint.

Ressourcen-Gateway in VPC Lattice

Ein Ressourcen-Gateway ist ein Punkt für eingehenden Verkehr in die VPC, an dem sich eine Ressource befindet. Es erstreckt sich über mehrere Availability Zones.

Eine VPC muss über ein Ressourcen-Gateway verfügen, wenn Sie planen, Ressourcen innerhalb der VPC von anderen VPCs Konten aus zugänglich zu machen. Jede Ressource, die Sie gemeinsam nutzen, ist mit einem Ressourcen-Gateway verknüpft. Wenn Clients in anderen Konten VPCs oder Konten auf eine Ressource in Ihrer VPC zugreifen, sieht die Ressource Datenverkehr, der lokal vom Ressourcen-Gateway in dieser VPC kommt. Die Quell-IP des Datenverkehrs ist die IP-Adresse des Ressourcen-Gateways. Sie können einem Ressourcengateway mehrere IP-Adressen zuweisen, um mehr Netzwerkverbindungen mit der Ressource zu ermöglichen. Mehrere Ressourcen in einer VPC können demselben Ressourcen-Gateway zugeordnet werden.

Ein Ressourcen-Gateway bietet keine Lastenausgleichsfunktionen.

Inhalt

Überlegungen

Die folgenden Überlegungen gelten für Ressourcengateways:

- Damit auf Ihre Ressource von allen Availability Zones aus zugegriffen werden kann, sollten Sie Ihre Ressourcen-Gateways so einrichten, dass sie sich über möglichst viele Availability Zones erstrecken.
- Mindestens eine Availability Zone des VPC-Endpunkts und des Resource Gateways muss sich überschneiden.
- Eine VPC kann maximal 100 Ressourcen-Gateways haben. Weitere Informationen finden Sie unter Kontingente für VPC Lattice.
- Sie können kein Ressourcen-Gateway in einem gemeinsam genutzten Subnetz erstellen.

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.

Ziel	Protocol (Protokoll)	Port-Bereich	Comment
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 verfügen IPv4. 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.

IPv4 Adressen pro ENI

Wenn Ihr Resource Gateway über einen IPv4 oder einen Dual-Stack-IP-Adresstyp verfügt, können Sie die Anzahl der IPv4 Adressen konfigurieren, die jeder ENI Ihres Resource Gateways zugewiesen sind. Wenn Sie ein Resource Gateway erstellen, wählen Sie zwischen 1 und 62 IPv4 Adressen. Sobald Sie die Anzahl der IPv4 Adressen festgelegt haben, kann der Wert nicht mehr geändert werden.

Die IPv4 Adressen werden für die Netzwerkadressübersetzung verwendet und bestimmen die maximale Anzahl gleichzeitiger IPv4 Verbindungen zu einer Ressource. Standardmäßig werden allen Ressourcen-Gateways 16 IPv4 Adressen pro ENI zugewiesen. Dies ist eine geeignete Anzahl von IPs , um Verbindungen mit Ihren Backend-Ressourcen herzustellen.

Wenn Ihr Resource Gateway den IPv6 Adresstyp verwendet, empfängt das Resource Gateway automatisch einen /80 CIDR pro ENI. Dieser Wert kann nicht geändert werden.

Erstellen eines Ressourcen-Gateways 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 Amazon-VPC-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 Typ der IP-Adresse für das Ressourcen-Gateway.
6. Wählen Sie als IP-Adresstyp den IP-Adresstyp für das Ressourcen-Gateway aus.

   - Wenn Sie als IP-Adresstyp IPv4oder Dualstack ausgewählt haben, können Sie die Anzahl der IPv4 Adressen pro ENI für Ihr Ressourcen-Gateway eingeben.

     Die Standardeinstellung ist 16 IPv4 Adressen pro ENI. Dies ist eine geeignete Anzahl von IPs , um Verbindungen mit Ihren Backend-Ressourcen herzustellen.
7. Wählen Sie die VPC aus, in der sich die Ressource befindet.
8. Wählen Sie bis zu fünf Sicherheitsgruppen aus, um den eingehenden Verkehr von der VPC zum Servicenetzwerk zu kontrollieren.

9. (Optional) Sie fügen ein Tag hinzu, indem Sie neues Tag hinzufügen auswählen und den Schlüssel und den Wert für das Tag eingeben.
10. Wählen Sie Create Resource Gateway aus.

Um ein Ressourcen-Gateway mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-resource-gateway.

Löschen eines Ressourcen-Gateways 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 Amazon-VPC-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 Befehl delete-resource-gateway.

Zugriff auf Servicenetzwerke über AWS PrivateLink

Sie können von Ihrer VPC aus über einen VPC-Endpunkt des Servicenetzwerks (Servicenetzwerk-Endpunkt) eine private Verbindung zu einem Servicenetzwerk 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 privat über einen einzigen VPC-Endpunkt auf mehrere Ressourcen und Dienste zugreifen.

Ein Servicenetzwerk ist eine logische Sammlung von Ressourcenkonfigurationen und VPC-Lattice-Diensten. Mithilfe eines Servicenetzwerkendpunkts können Sie ein Servicenetzwerk mit Ihrer VPC verbinden und privat von Ihrer VPC oder lokal aus auf diese Ressourcen und Dienste zugreifen. Mit einem Servicenetzwerk-Endpunkt können Sie eine Verbindung zu einem Servicenetzwerk herstellen. Um von Ihrer VPC aus eine Verbindung zu mehreren Servicenetzwerken herzustellen, können Sie mehrere Dienstnetzwerk-Endpunkte erstellen, von denen jeder auf ein anderes Dienstnetzwerk verweist.

Servicenetzwerke sind in () integriert AWS Resource Access Manager .AWS RAM 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 VPC-Endpunkt des Servicenetzwerks auf Ressourcen zugreifen. Der VPC-Endpunkt des Servicenetzwerks selbst wird Ihnen nicht stündlich in Rechnung gestellt. Weitere Informationen finden Sie unter Amazon VPC Lattice Preise.

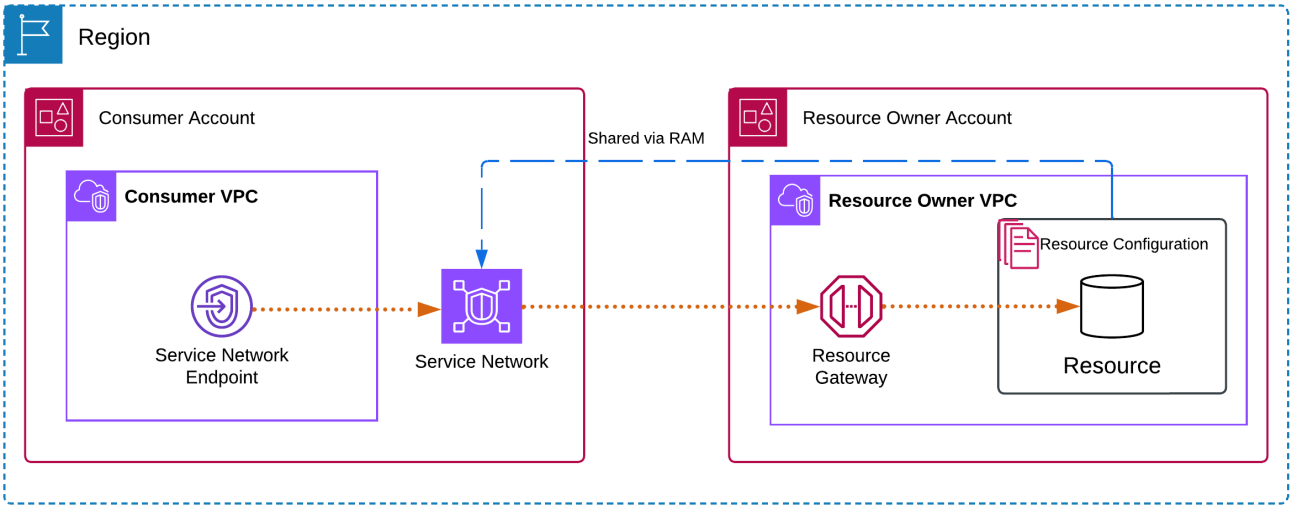
Inhalt

- DNS-Hostnamen
- DNS-Auflösung
- Privates 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 gemeinsam genutzt werden. In beiden Fällen können Sie einen Service-Netzwerk-Endpunkt erstellen, um von Ihrer 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 Ihrer VPC auf ein Servicenetzwerk zugreift.



Netzwerkverbindungen können nur von der VPC mit dem Dienstnetzwerkendpunkt zu den Ressourcen und Diensten im Dienstnetzwerk initiiert werden. Die VPC mit den Ressourcen und Diensten kann keine Netzwerkverbindungen zur Endpunkt-VPC initiieren.

DNS-Hostnamen

Mit AWS PrivateLink senden Sie über private Endpunkte Datenverkehr an Servicenetzwerke. Wenn Sie einen VPC-Endpunkt für ein Servicenetzwerk erstellen, erstellen wir regionale DNS-Namen (als Standard-DNS-Name bezeichnet) für jede Ressource und jeden Dienst, den Sie für die Kommunikation mit der Ressource und dem Dienst von Ihrer VPC und vor Ort aus verwenden können. Die mit dem Endpunkt verknüpften IP-Adressen können sich ändern. Wir empfehlen, dass Sie DNS anstelle von Endpoint verwenden IPs , um eine Verbindung zu Ihren Servicenetzwerken herzustellen.

Der Standard-DNS-Name für eine Ressource im Servicenetzwerk hat die folgende Syntax:

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

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

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

Wenn Sie den verwenden AWS-Managementkonsole, finden Sie den DNS-Namen auf der Registerkarte Verknüpfungen. Wenn Sie den verwenden AWS CLI, verwenden Sie den describe-vpc-endpoint-associationsBefehl.

Sie können privates DNS nur aktivieren, wenn Ihr Servicenetzwerk über eine ARN-Ressourcenkonfiguration für einen Amazon RDS-Datenbankservice verfügt. Mit privatem DNS können Sie weiterhin Anfragen an die Ressource stellen, indem Sie den vom Dienst für die Ressource bereitgestellten DNS-Namen verwenden und gleichzeitig die private Konnektivität über den VPC-Endpunkt des AWS Servicenetzwerks nutzen. Weitere Informationen finden Sie unter the section called “DNS-Auflösung”.

DNS-Auflösung

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

Privates DNS

Wenn Sie privates DNS für Ihren VPC-Endpunkt im Servicenetzwerk aktivieren und in Ihrer VPC sowohl DNS-Hostnamen als auch DNS-Auflösung aktiviert sind, erstellen wir versteckte, AWS verwaltete private gehostete Zonen für die Ressourcenkonfigurationen mit benutzerdefinierten DNS-Namen. Die gehostete Zone enthält einen Datensatz für den Standard-DNS-Namen für die Ressource, der ihn in die privaten IP-Adressen der Netzwerkschnittstellen des Servicenetzwerk-Endpunkts in Ihrer VPC auflöst.

Amazon stellt einen DNS-Server für Ihre VPC zu Verfügung, den Route 53 Resolver. Der Route 53 Resolver löst automatisch lokale VPC-Domainnamen und Datensätze in privaten gehosteten Zonen. Sie können den Route 53 Resolver jedoch nicht von außerhalb Ihrer VPC verwenden. Wenn Sie von Ihrem lokalen Netzwerk aus auf Ihren VPC-Endpunkt zugreifen möchten, können Sie die Standard-DNS-Namen oder 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 Ihre VPC-Endpunkte mit einem Subnetz pro Availability Zone konfigurieren. Wir erstellen eine elastic network interface für den VPC-Endpunkt in Ihrem Subnetz. Wir weisen jeder elastic network interface IP-Adressen aus ihrem Subnetz in Vielfachen von /28 zu, wenn der IP-Adresstyp des VPC-Endpunkts lautet. IPv4 Die Anzahl der in jedem Subnetz zugewiesenen IP-Adressen hängt von der Anzahl der Ressourcenkonfigurationen ab. Bei Bedarf fügen wir weitere Blöcke IPs in /28 hinzu. In einer Produktionsumgebung empfehlen wir für hohe Verfügbarkeit und Ausfallsicherheit, mindestens zwei Availability Zones für jeden VPC-Endpunkt zu konfigurieren und zusammenhängende IPs Availability Zones verfügbar zu haben.

IP-Adresstypen

Service-Netzwerk-Endpunkte können Dual-Stack-Adressen oder Dual-Stack-Adressen unterstützen IPv4. IPv6 Endpunkte, die dies unterstützen, IPv6 können auf DNS-Abfragen mit AAAA-Einträgen antworten. Der IP-Adresstyp eines Service-Netzwerk-Endpunkts 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-Endpunkt eines Servicenetzwerks dies unterstützt IPv4, haben IPv4 die Endpunkt-Netzwerkschnittstellen Adressen. Wenn ein VPC-Endpunkt eines Servicenetzwerks dies unterstützt IPv6, 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.
- Ein Servicenetzwerkendpunkt benötigt zunächst einen zusammenhängenden /28-Adressblock, der in einer IPv4 Availability Zone verfügbar ist. Wenn Sie dem Servicenetzwerk, das Ihrem Endpunkt zugeordnet ist, eine Ressourcenkonfiguration hinzufügen, benötigen Sie einen zusätzlichen /28-Block, der im selben Subnetz verfügbar ist, da jede Ressource eine eindeutige IP pro Availability Zone verbraucht.

Wenn Sie planen, einem Servicenetzwerk mehr als 16 Ressourcenkonfigurationen hinzuzufügen, werden zusätzliche /28-Blöcke auf dem Servicenetzwerk-Endpunkt verbraucht, um neue Ressourcen aufzunehmen. Wenn Sie die Verwendung von VPC CIDR vermeiden möchten, empfehlen wir IPs, eine VPC-Verbindung für ein Servicenetzwerk zu verwenden. Weitere Informationen finden Sie unter VPC-Endpunktzuordnungen verwalten im Amazon VPC Lattice-Benutzerhandbuch.

Erstellen Sie einen Servicenetzwerk-Endpunkt

Erstellen Sie einen Servicenetzwerk-Endpunkt für den Zugriff auf das Servicenetzwerk, das mit Ihnen geteilt wurde. Nachdem Sie einen Servicenetzwerk-Endpunkt erstellt haben, können Sie nur dessen Sicherheitsgruppen oder Tags ändern.

Um einen Servicenetzwerk-Endpunkt zu erstellen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter PrivateLink und Lattice die Option Endpoints aus.
3. Wählen Sie Endpunkt erstellen aus.
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 Servicenetzwerk aus.
7. Wählen Sie unter Netzwerkeinstellungen Ihre VPC aus, von der aus Sie auf das Servicenetzwerk zugreifen.
8. Wenn Sie die Unterstützung für privates DNS konfigurieren möchten, wählen Sie Zusätzliche Einstellungen, Privaten DNS-Namen aktivieren aus. Um diese Funktion verwenden zu können, stellen Sie sicher, dass die Attribute DNS-Hostnamen aktivieren und DNS-Unterstützung aktivieren für Ihre VPC aktiviert sind.
9. Wählen Sie für Subnetze ein Subnetz aus, in dem die Endpunkt-Netzwerkschnittstelle erstellt werden soll.

   In einer Produktionsumgebung empfehlen wir für hohe Verfügbarkeit und Ausfallsicherheit, mindestens zwei Availability Zones für jeden VPC-Endpunkt zu konfigurieren.
10. Wählen Sie für Sicherheitsgruppen eine Sicherheitsgruppe aus.

Wenn Sie keine Sicherheitsgruppen-ID angeben, ordnen wir der VPC die Standardsicherheitsgruppe zu.

11. Wählen Sie Endpunkt erstellen aus.

Um einen Service-Network-Endpunkt über die Befehlszeile zu erstellen

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

Dienstnetzwerk-Endpunkte verwalten

Nachdem Sie einen Servicenetzwerk-Endpunkt erstellt haben, können Sie dessen Sicherheitsgruppen oder Tags aktualisieren.

Aufgaben

- Löschen eines Endpunkts
- Aktualisieren Sie einen Dienstnetzwerk-Endpunkt

Löschen eines Endpunkts

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

Um einen Endpunkt mit der Konsole zu löschen

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

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 Amazon-VPC-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 aus.
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 Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS PrivateLink IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Inhalt

Zielgruppe

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

Dienstbenutzer — Wenn Sie den AWS PrivateLink Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS PrivateLink Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die 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. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen.

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

Authentifizierung mit Identitäten

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

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln oder indem Sie eine AWS Oder-API-Operation AWS CLI aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

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

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.

- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die sich daraus ergebenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

Wie AWS PrivateLink funktioniert mit IAM

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

IAM-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

IAM-Feature	AWS PrivateLink Unterstützung
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

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

Identitätsbasierte Richtlinien für AWS PrivateLink

Unterstützt Richtlinien auf Identitätsbasis: Ja

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

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS PrivateLink

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

Ressourcenbasierte Richtlinien finden Sie in AWS PrivateLink

Unterstützt ressourcenbasierte Richtlinien: Ja

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

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

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

Politische Aktionen für AWS PrivateLink

Unterstützt Richtlinienaktionen: Ja

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

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Aktionen im ec2-Namespace

Einige Aktionen für AWS PrivateLink sind Teil der Amazon EC2 EC2-API. Diese Richtlinienaktionen verwenden das `ec2` Präfix. Weitere Informationen finden Sie unter AWS PrivateLink -Aktionen in der Amazon-EC2-API-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 angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Richtlinien-Bedingungsschlüssel für AWS PrivateLink

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

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

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. 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. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Die folgenden Bedingungsschlüssel sind spezifisch für: AWS PrivateLink

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

Weitere Informationen finden Sie unter Bedingungsschlüssel für Amazon EC2.

ACLs in AWS PrivateLink

Unterstützt ACLs: Nein

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

ABAC mit AWS PrivateLink

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen, auch als Tags bezeichnet, definiert werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

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

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

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

Verwenden temporärer Anmeldeinformationen mit AWS PrivateLink

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Serviceübergreifende Prinzipalberechtigungen für AWS PrivateLink

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS PrivateLink

Unterstützt Servicerollen: Nein

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

Mit Diensten verknüpfte Rollen für AWS PrivateLink

Unterstützt serviceverknüpfte Rollen: 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 Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Beispiele für identitätsbasierte Richtlinien für AWS PrivateLink

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS PrivateLink -Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

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

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

Steuern der Nutzung von VPC-Endpunkten

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

JSON

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

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

Steuern der Erstellung von VPC-Endpunkten auf Grundlage des Servicebesitzers

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

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc/*",
                "arn:aws:ec2:us-east-1:111111111111:security-group/*",
                "arn:aws:ec2:us-east-1:111111111111:subnet/*",
                "arn:aws:ec2:us-east-1:111111111111:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceOwner": [
                        "amazon"
                    ]
                }
            }
        }
    ]
}
```

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

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

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint-service/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServicePrivateDnsName": [
                        "example.com"
                    ]
                }
            }
        }
    ]
}
```

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

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

JSON

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

```
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc/*",
                "arn:aws:ec2:us-east-1:111111111111:security-group/*",
                "arn:aws:ec2:us-east-1:111111111111:subnet/*",
                "arn:aws:ec2:us-east-1:111111111111:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.111111111111.s3"
                    ]
                }
            }
        }
    ]
}
```

Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien

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

Eine Endpunktrichtlinie setzt keine identitätsbasierten Richtlinien oder ressourcenbasierten Richtlinien außer Kraft oder ersetzt sie. 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 eine einzelne Endpunktrichtlinie an den Endpunkt anhängen. Sie können die Endpunktrichtlinie jederzeit aktualisieren. Wenn Sie keine Endpunktrichtlinie anfügen, fügen wir die Standard-Endpunktrichtlinie hinzu.
- Nicht alle AWS-Services unterstützen Endpunktrichtlinien. Wenn an AWS-Service keine Endpunktrichtlinien unterstützt, gewähren wir vollen Zugriff auf jeden Endpunkt für den Service. Weitere Informationen finden Sie unter the section called “Anzeigen der Unterstützung für Endpunkt-Richtlinien”.
- Wenn Sie einen VPC-Endpunkt für einen anderen Endpunktservice als einen AWS-Service erstellen, lassen wir vollen Zugriff auf den Endpunkt zu.
- 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 einen ARN in einem Ressourcen- oder Bedingungselement angeben, kann der Kontoteil des ARN eine Konto-ID oder ein Platzhalterzeichen enthalten, jedoch nicht beides.
- Nachdem Sie eine Endpunktrichtlinie aktualisiert haben, kann es einige Minuten dauern, bis die Änderungen wirksam werden.

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 einer VPC-Endpunktrichtlinie

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

Ändern einer Endpunktrichtlinie mithilfe der Konsole

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

Ändern einer Endpunktrichtlinie mithilfe der Befehlszeile

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

AWS verwaltete Richtlinien für AWS PrivateLink

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, 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 allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete 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 Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS PrivateLink Aktualisierungen der AWS verwalteten Richtlinien

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

Änderungen	Beschreibung	Date
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 oder für Endpunktdienst-Benutzer veröffentlicht, die den regionsübergreifenden Zugriff verwenden. Standardmäßig werden Metriken ohne zusätzliche Kosten CloudWatch in Intervallen von einer Minute an AWS PrivateLink gesendet.

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

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

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

Dimension	Description
`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.

Sehen Sie sich die CloudWatch Kennzahlen an

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

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

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

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 AWS/ PrivateLinkEndpoints Namespace aus.
4. Wählen Sie den AWS/ PrivateLinkServices Namespace aus.

Um Metriken anzuzeigen, verwenden Sie 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.

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-Managementkonsole oder zu aktivieren. AWS CLI

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

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Wählen Sie im Navigationsbereich Endpoint Services (Endpunktservices) aus.
3. Wählen Sie Ihren Endpunktservice aus.
4. Auf der Registerkarte Contributor Insights, wählen Sie Aktivieren aus.
5. (Optional) Standardmäßig sind alle Regeln aktiviert. Um nur bestimmte Regeln zu aktivieren, wählen Sie die Regeln aus, die nicht aktiviert werden sollen, und wählen Sie dann Aktionen, Regel deaktivieren aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie deaktivieren aus.

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

Um die Contributor Insights-Regeln für AWS PrivateLink die 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-Managementkonsole 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 der EC2 Amazon-API. 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 API-Limits auf Kontoebene verwenden AWS Organizations und einen `RequestLimitExceeded` Fehlercode erhalten, finden Sie weitere Informationen unter So identifizieren Sie AWS Konten, die eine große Anzahl von API-Aufrufen tätigen. Wenn Sie Hilfe benötigen, wenden Sie sich an Ihr Account-Team oder eröffnen Sie mithilfe des VPC-Dienstes und der Kategorie VPC-Endpunkte eine Anfrage an den technischen Support. Stellen Sie sicher, dass Sie ein Bild des Fehlercodes anhängen. `RequestLimitExceeded`

VPC-Endpunktkontingente

Ihr AWS Konto hat die folgenden Kontingente für VPC-Endpunkte.

Name	Standard	Anpassbar	Kommentare
Schnittstellen- und Gateway Load Balancer-Endpunkte pro VPC	50	Ja	Dies ist ein kombiniertes Kontingent für Schnittstellenendpunkte und Gateway-Load-Balancer-Endpunkte
Gateway VPC-Endpunkte pro Region	20	Ja	Sie können bis zu 255 Gateway-Endpunkte pro VPC erstellen
Ressourcen-VPC-Endpunkte pro VPC	200	Ja	

Name	Standard	Anpassbar	Kommentare
Servicenetzwerk-VPC-Endpunkte pro VPC	50	Ja	
Richtlinie für Zeichen pro VPC-Endpunkt	20.480	Nein	Die maximale Größe einer VPC-Endpunktrichtlinie, mit Leerzeichen

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

- Jeder VPC-Endpunkt kann standardmäßig eine Bandbreite von bis zu 10 GB/s pro Availability Zone unterstützen und skaliert automatisch auf bis zu 100 GB/s. Die maximale Bandbreite für einen VPC-Endpunkt bei der Verteilung der Last auf alle Availability Zones ist die Anzahl der Availability Zones multipliziert mit 100 GB/s. Wenn Ihre Anwendung einen höheren Durchsatz benötigt, wenden Sie sich an den AWS -Support.
- Die Maximum Transmission Unit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das einen VPC-Endpunkt durchläuft. Je größer die MTU, desto mehr Daten können in einem einzelnen Paket übergeben werden. Ein VPC-Endpunkt unterstützt eine MTU von 8.500 Byte. Pakete mit einer Größe von mehr als 8.500 Byte, die am VPC-Endpunkt ankommen, werden verworfen.
- Path MTU Discovery (PMTUD) wird nicht unterstützt. VPC-Endpunkte generieren nicht die folgende ICMP-Meldung: `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (Typ 3, Code 4).
- VPC-Endpunkte erzwingen das Klemmen der Maximum Segment Size (MSS) für alle Pakete. Weitere Informationen finden Sie unter RFC879.

Dokumenthistorie 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- und 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 Unterstützung	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	18. August 2022

	verwenden, um bestimmte Endgeräte zu identifizieren, die am meisten zu den Metriken beitragen. CloudWatch AWS PrivateLink	
IPv6 Unterstützung	Dienstanbieter können ihren Endpunktdienst so einrichten, dass sie IPv6 Anfragen annehmen, auch wenn ihre Backend-Dienste nur IPv4 Support bieten. 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 einen Gateway Load Balancer-Endpunkt in Ihrer VPC erstellen, um den Datenverkehr an einen VPC-Endpunktdienst zu leiten, den Sie mit einem Gateway Load Balancer konfiguriert haben.	10. November 2020

VPC-Endpunktrichtlinien	Sie können eine IAM-Richtlinie an einen Schnittstellen-VPC-Endpunkt für einen AWS -Service zur Steuerung des Zugriffs auf den Service anfügen.	23. März 2020
Bedingungsschlüssel für VPC-Endpunkte und Endpunktservices	Sie können EC2 Bedingungsschlüssel verwenden, um den Zugriff auf VPC-Endpunkte und Endpunktdienste zu steuern.	6. März 2020
Markierung von VPC-Endpunkt- und VPC-Endpunktservices bei der Erstellung	Sie können eine Markierung hinzufügen, wenn Sie VPC-Endpunkte und -Endpunktservices erstellen.	5. Februar 2020
Private DNS-Namen	Sie können von Ihrer VPC aus mithilfe von privaten DNS-Namen auf AWS PrivateLink basierte Dienste zugreifen.	6. Januar 2020
VPC-Endpunkt-Services	Sie können Ihre eigenen Endpunktservices erstellen und anderen AWS-Konten und Benutzern ermöglichen, über einen Schnittstellen-VPC-Endpunkt eine Verbindung zu Ihrem Service herzustellen. Sie können Ihre Endpunktservices für ein Abonnement im AWS Marketplace anbieten.	28. November 2017

Schnittstelle VPC-Endpunkte für AWS-Services	Sie können einen Schnittstellenendpunkt erstellen, mit dem Sie eine Verbindung zu AWS-Services diesem Integrationspunkt herstellen können, AWS PrivateLink ohne ein Internet-Gateway oder ein NAT-Gerät zu verwenden.	8. November 2017
VPC-Endpunkte für DynamoDB	Sie können einen Gateway-VPC-Endpunkt erstellen, um von Ihrer VPC aus auf Amazon DynamoDB zuzugreifen, ohne ein Internet-Gateway oder ein NAT-Gerät zu verwenden.	16. August 2017
VPC-Endpunkte für Amazon S3	Sie können einen Gateway-VPC-Endpunkt erstellen, um von Ihrer VPC aus auf Amazon S3 zuzugreifen, ohne ein Internet-Gateway oder ein NAT-Gerät zu verwenden.	11. Mai 2015

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