aws

Benutzerhandbuch

Amazon VPC Lattice

Amazon VPC Lattice: Benutzerhandbuch

Table of Contents

Was ist Amazon VPC Lattice?

Amazon VPC Lattice ist ein vollständig verwalteter Anwendungsnetzwerkservice, mit dem Sie die Services und Ressourcen für Ihre Anwendung verbinden, sichern und überwachen. Sie können VPC Lattice mit einer einzelnen Virtual Private Cloud (VPC) oder über mehrere Konten VPCs hinweg verwenden.

Moderne Anwendungen können aus mehreren kleinen und modularen Komponenten bestehen, die oft als Microservices bezeichnet werden, wie z. B. einer HTTP-API, Ressourcen wie Datenbanken und benutzerdefinierten Ressourcen, die aus DNS- und IP-Adressendpunkten bestehen.
Die Modernisierung hat zwar ihre Vorteile, kann aber auch zu Netzwerkkomplexitäten und Herausforderungen führen, wenn Sie diese Microservices und Ressourcen miteinander verbinden. Wenn die Entwickler beispielsweise auf verschiedene Teams verteilt sind, können sie Microservices und Ressourcen für mehrere Konten erstellen und bereitstellen oder. VPCs

In VPC Lattice bezeichnen wir einen Microservice als Service und stellen eine Ressource nur als Ressourcenkonfiguration dar. Dies sind die Begriffe, die Sie im VPC Lattice-Benutzerhandbuch finden.

Inhalt

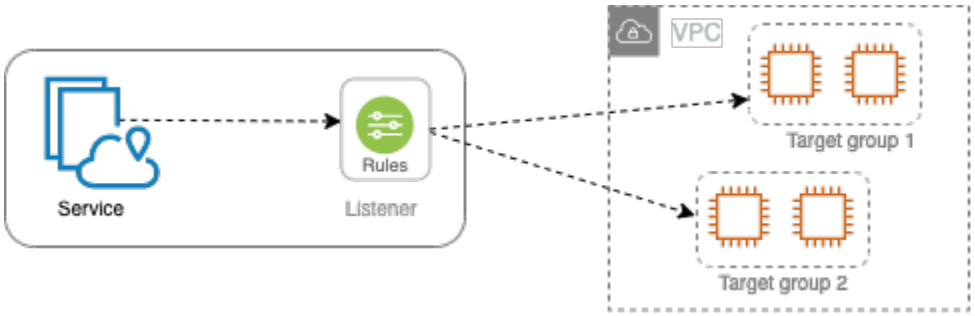
Zentrale Komponenten

Um Amazon VPC Lattice verwenden zu können, sollten Sie mit den wichtigsten Komponenten vertraut sein.

Service

> Eine unabhängig einsetzbare Softwareeinheit, die eine bestimmte Aufgabe oder Funktion erfüllt. Ein Dienst kann auf EC2 Instanzen oder ECS/EKS/Fargate Containern oder als Lambda-

Funktionen innerhalb eines Kontos oder einer Virtual Private Cloud (VPC) ausgeführt werden. Ein VPC Lattice-Dienst besteht aus den folgenden Komponenten: Zielgruppen, Listener und Regeln.



Zielgruppe

Eine Sammlung von Ressourcen, auch Ziele genannt, die Ihre Anwendung oder Ihren Dienst ausführen. Diese ähneln den Zielgruppen, die Elastic Load Balancing bietet, sind jedoch nicht austauschbar. Zu den unterstützten Zieltypen gehören EC2 Instances, IP-Adressen, Lambda-Funktionen, Application Load Balancers, Amazon ECS-Aufgaben und Kubernetes Pods.

Listener

Ein Prozess, der nach Verbindungsanfragen sucht und diese an Ziele in einer Zielgruppe weiterleitet. Sie konfigurieren einen Listener mit einem Protokoll und einer Portnummer.

Regel

Eine Standardkomponente eines Listeners, der Anfragen an die Ziele in einer VPC Lattice-Zielgruppe weiterleitet. Jede Rolle besteht aus einer Priorität, mindestens einer Aktion und mindestens einer Bedingung. Regeln bestimmen, wie der Listener Client-Anfragen weiterleitet.

Ressource

Eine Ressource ist eine Entität wie eine Amazon Relational Database Service (Amazon RDS) - Datenbank, eine EC2 Amazon-Instance, ein Anwendungsendpunkt, ein Domainnamenziel oder eine IP-Adresse. Sie können eine Ressource in Ihrer VPC gemeinsam nutzen, indem Sie eine Ressourcenfreigabe in AWS Resource Access Manager (AWS RAM) erstellen, ein Ressourcen-Gateway erstellen und eine Ressourcenkonfiguration definieren.

Ressourcen-Gateway

Ein Ressourcen-Gateway ist ein Zugangspunkt in die VPC, in dem sich Ressourcen befinden.

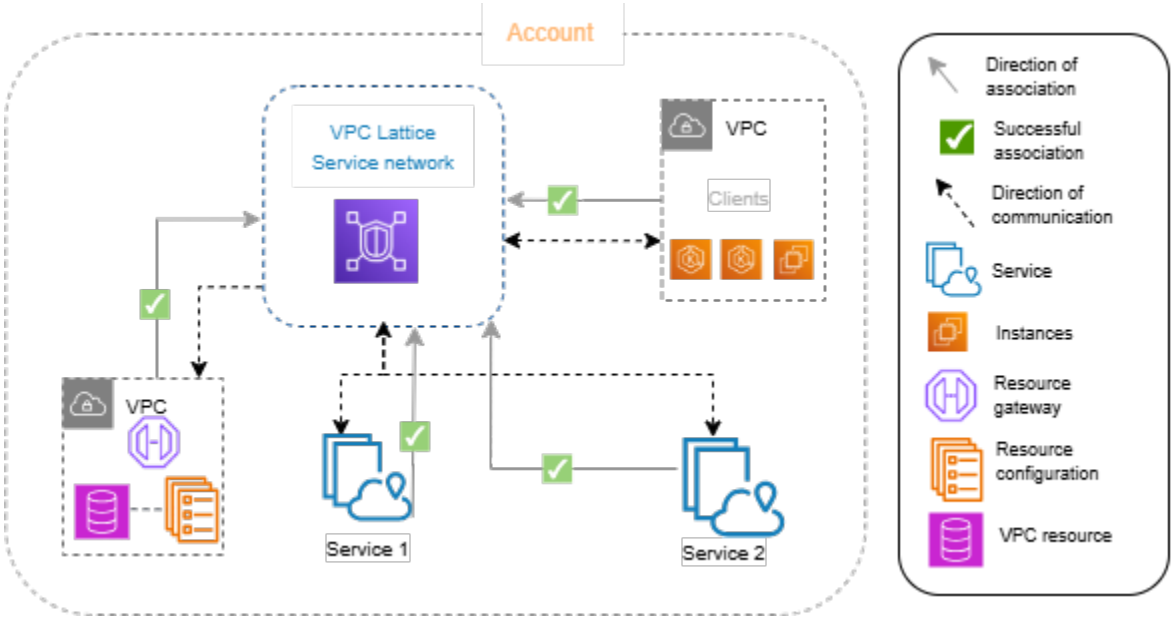
Ressourcenkonfiguration

Eine Ressourcenkonfiguration ist ein logisches Objekt, das entweder eine einzelne Ressource oder eine Gruppe von Ressourcen darstellt. Eine Ressource kann eine IP-Adresse, ein Domainnamenziel oder eine Amazon RDS-Datenbank sein.

Servicenetzwerk

Eine logische Grenze für eine Sammlung von Diensten und Ressourcenkonfigurationen. Ein Client kann sich in einer VPC befinden, die dem Servicenetzwerk zugeordnet ist. Clients und Dienste, die demselben Servicenetzwerk zugeordnet sind, können miteinander kommunizieren, sofern sie dazu autorisiert sind.

In der folgenden Abbildung können die Clients mit beiden Diensten kommunizieren, da die VPC und die Dienste demselben Dienstnetzwerk zugeordnet sind.



Dienstverzeichnis

Eine zentrale Registrierung aller VPC Lattice-Dienste, die Ihnen gehören oder über die Sie mit Ihrem Konto geteilt werden. AWS RAM

Richtlinien für die Authentifizierung

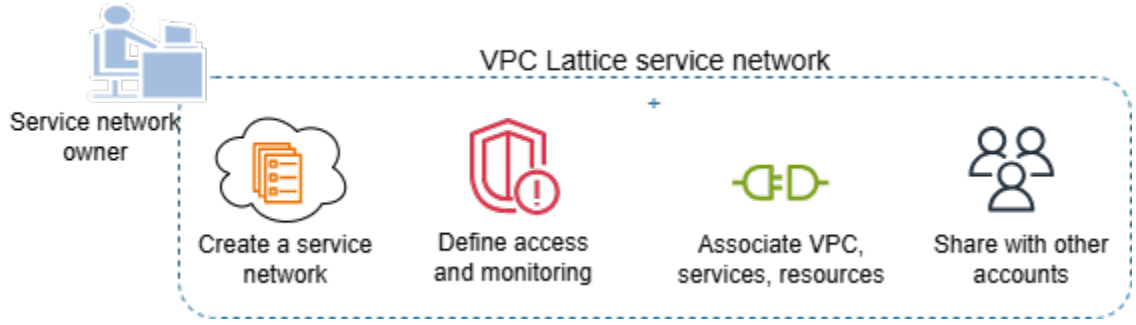
Detaillierte Autorisierungsrichtlinien, mit denen der Zugriff auf Dienste definiert werden kann. Sie können einzelnen Diensten oder dem Dienstnetzwerk separate Authentifizierungsrichtlinien zuordnen. Sie können beispielsweise eine Richtlinie dafür erstellen, wie ein Zahlungsdienst, der auf einer Auto Scaling-Gruppe von EC2 Instances ausgeführt wird, mit einem Rechnungsdienst interagieren soll, der in ausgeführt wird AWS Lambda.

Auth-Richtlinien werden in Ressourcenkonfigurationen nicht unterstützt. Die Authentifizierungsrichtlinien eines Dienstnetzwerks gelten nicht für Ressourcenkonfigurationen im Dienstnetzwerk.

Rollen und Zuständigkeiten

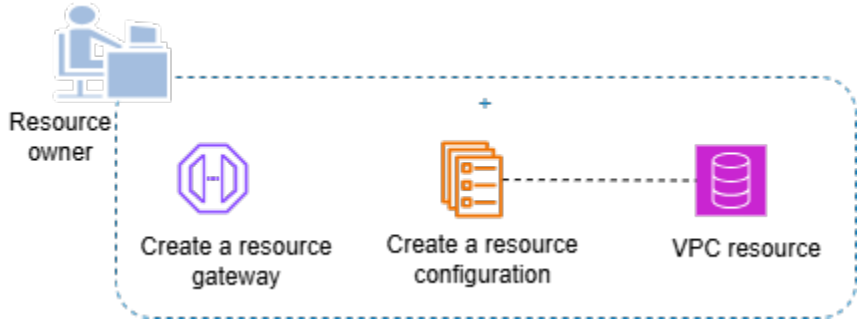
Eine Rolle bestimmt, wer für die Einrichtung und den Informationsfluss innerhalb von Amazon VPC Lattice verantwortlich ist. In der Regel gibt es zwei Rollen, den Eigentümer des Servicenetzwerks und den Eigentümer des Dienstes, und ihre Zuständigkeiten können sich überschneiden.

Eigentümer des Servicenetzwerks — Der Eigentümer des Servicenetzwerks ist normalerweise der Netzwerkadministrator oder der Cloud-Administrator in einer Organisation. Besitzer des Servicenetzwerks erstellen, teilen und stellen das Servicenetzwerk bereit. Sie verwalten auch, wer auf das Servicenetzwerk oder die Dienste innerhalb von VPC Lattice zugreifen kann. Der Eigentümer des Servicenetzwerks kann grobe Zugriffseinstellungen für die mit dem Servicenetzwerk verknüpften Dienste definieren. Diese Steuerelemente werden verwendet, um die Kommunikation zwischen Clients und Diensten mithilfe von Authentifizierungs- und Autorisierungsrichtlinien zu verwalten. Der Besitzer des Dienstnetzwerks kann eine Dienst- oder Ressourcenkonfiguration auch einem einzelnen oder mehreren Dienstnetzwerken zuordnen, wenn die Dienst- oder Ressourcenkonfiguration mit dem Konto des Dienstenetzwerkbesitzers gemeinsam genutzt wird.



Service Owner — Der Service Owner ist in der Regel ein Softwareentwickler in einer Organisation. Dienstbesitzer erstellen Dienste innerhalb von VPC Lattice, definieren Routing-Regeln und verknüpfen Dienste auch mit dem Dienstnetzwerk. Sie können auch detaillierte Zugriffseinstellungen definieren, mit denen der Zugriff nur auf authentifizierte und autorisierte Dienste und Clients beschränkt werden kann.

Ressourcenbesitzer — Der Ressourcenbesitzer ist normalerweise ein Softwareentwickler in einer Organisation und fungiert als Administrator für eine Ressource wie eine Datenbank. Der Ressourcenbesitzer erstellt eine Ressourcenkonfiguration für die Ressource, definiert Zugriffseinstellungen für die Ressourcenkonfiguration und ordnet die Ressourcenkonfiguration Servicenetzwerken zu.



Features

Im Folgenden sind die Kernfunktionen aufgeführt, die VPC Lattice bietet.

Serviceerkennung

Alle Clients und Dienste, die dem Servicenetzwerk VPCs zugeordnet sind, können mit anderen Diensten innerhalb desselben Servicenetzwerks kommunizieren. DNS leitet den client-to-service service-to-service Datenverkehr über den VPC-Lattice-Endpunkt weiter. Wenn ein Client eine Anfrage an einen Dienst senden möchte, verwendet er den DNS-Namen des Dienstes. Der Route 53 Resolver sendet den Datenverkehr an VPC Lattice, das dann den Zieldienst identifiziert.

Konnektivität

Client-to-service und die client-to-resource Konnektivität wird innerhalb der AWS Netzwerkinfrastruktur hergestellt. Wenn Sie eine VPC mit dem Servicenetzwerk verknüpfen, kann jeder Client innerhalb der VPC eine Verbindung zu Diensten und Ressourcen (über

Ressourcenkonfigurationen) im Dienstnetzwerk herstellen, sofern er über den erforderlichen Zugriff verfügt. VPC Lattice unterstützt die überlappende CIDR-Technologie.

Zugriff vor Ort

Sie können die Konnektivität zu einem Servicenetzwerk von einer VPC aus mithilfe eines VPC-Endpunkts (powered by AWS PrivateLink) aktivieren. Mit einem VPC-Endpunkt vom Typ Servicenetzwerk können Sie den Zugriff auf Dienste und Ressourcen im Servicenetzwerk von lokalen Netzwerken aus über Direct Connect und VPN ermöglichen. Datenverkehr, der VPC-Peering durchläuft oder auch über einen VPC-Endpunkt auf Ressourcen und Dienste zugreifen AWS Transit Gateway kann.

Beobachtbarkeit

VPC Lattice generiert Metriken und Protokolle für jede Anfrage und Antwort, die das Servicenetzwerk durchquert, um Sie bei der Überwachung und Fehlerbehebung von Anwendungen zu unterstützen. Standardmäßig werden Metriken auf dem Konto des Dienstbesitzers veröffentlicht. Dienstbesitzer und Ressourcenbesitzer haben die Möglichkeit, die Protokollierung zu aktivieren und Protokolle für alle Clients access/requests to their services and resources. Service network owners can also turn on logging on the service network, to log all access/requests zu den Diensten und Ressourcen von Clients zu erhalten VPCs , die mit dem Dienstnetzwerk verbunden sind.

VPC Lattice unterstützt Sie mit den folgenden Tools bei der Überwachung und Fehlerbehebung Ihrer Services: Amazon CloudWatch Protokollgruppen, Firehose-Lieferdatenströme und Amazon S3 S3-Buckets.

Sicherheit

VPC Lattice bietet ein Framework, mit dem Sie eine Verteidigungsstrategie auf mehreren Ebenen des Netzwerks implementieren können. Die erste Schicht ist die Kombination aus Dienst, Ressourcenkonfiguration, VPC-Zuordnung und VPC-Endpunkt vom Typ Dienstnetzwerk. Ohne eine VPC und eine Service Association oder einen VPC-Endpunkt vom Typ Service Network können Clients nicht auf Dienste zugreifen. Ebenso können Clients ohne eine VPC- und Ressourcenkonfiguration und eine Dienstzuordnung oder einen VPC-Endpunkt vom Typ Dienstnetzwerk nicht auf Ressourcen zugreifen.

Die zweite Schicht ermöglicht es Benutzern, Sicherheitsgruppen an die Verbindung zwischen der VPC und dem Servicenetzwerk anzuhängen. Die dritte und vierte Ebene sind Authentifizierungsrichtlinien, die individuell auf der Dienstnetzwerkebene und der Dienstebene angewendet werden können.

Zugreifen auf VPC Lattice

Sie können VPC Lattice über eine der folgenden Schnittstellen erstellen, darauf zugreifen und sie verwalten:

- AWS Management Console— Stellt eine Weboberfläche bereit, über die Sie auf VPC Lattice zugreifen können.
- AWS Command Line Interface (AWS CLI) — Stellt Befehle für eine Vielzahl von AWS Diensten bereit, einschließlich VPC Lattice. Das AWS CLI wird unter Windows, MacOS und Linux unterstützt. Weitere Informationen zur CLI finden Sie unter AWS Command Line Interface. Weitere Informationen zu finden Sie unter Amazon VPC Lattice API Reference. APIs
- VPC Lattice Controller für Kubernetes — Verwaltet VPC-Lattice-Ressourcen für einen Kubernetes-Cluster. Weitere Informationen zur Verwendung von VPC Lattice mit Kubernetes finden Sie im AWS Gateway API Controller User Guide.
- AWS CloudFormation— Hilft Ihnen bei der Modellierung und Einrichtung Ihrer Ressourcen. AWS Weitere Informationen finden Sie in der Referenz zum Amazon VPC Lattice-Ressourcentyp.

VPC-Lattice-Dienstendpunkte

Ein Endpunkt ist eine URL, die als Einstiegspunkt für einen AWS Webdienst dient. VPC Lattice unterstützt die folgenden Endpunkttypen:

- the section called “IPv4 Endpunkte”
- Dualstack-Endpunkte (unterstützen sowohl als auch) IPv4 IPv6

Wenn Sie eine Anfrage stellen, können Sie den zu verwendenden Endpunkt angeben. Wenn Sie keinen Endpunkt angeben, wird der IPv4 Endpunkt standardmäßig verwendet. Um einen anderen Endpunkttyp zu verwenden, müssen Sie ihn in Ihrer Anforderung angeben. Beispiele für diese Vorgehensweise finden Sie unter the section called “Angeben von Endpunkten”. Eine Tabelle der verfügbaren Endpunkte finden Sie unter Amazon VPC Lattice Endpoints.

IPv4 Endpunkte

IPv4 Endpunkte unterstützen nur IPv4 Datenverkehr. IPv4 Endpunkte sind für alle Regionen verfügbar.

Wenn Sie den allgemeinen Endpunkt, `vpc-lattice.amazonaws.com`, angeben, verwenden wir den Endpunkt für `us-east-1`. Um eine andere Region zu verwenden, geben Sie den zugehörigen Endpunkt an. Wenn Sie beispielsweise `vpc-lattice.us-east-2.amazonaws.com` als Endpunkt angeben, leiten wir Ihre Anfrage an den `us-east-2`-Endpunkt weiter.

IPv4 Endpunktnamen verwenden die folgende Benennungskonvention:

- `vpc-lattice.`*`region`*`.amazonaws.com`

Der IPv4 Endpunktname für die `eu-west-1` Region lautet beispielsweise`vpc-lattice.eu-west-1.amazonaws.com`.

Dualstack IPv4 - (und) Endpunkte IPv6

Dualstack-Endpunkte unterstützen sowohl den als auch den Datenverkehr. IPv4 IPv6 Dualstack-Endpunkte sind für alle Regionen verfügbar. Wenn Sie eine Anfrage an einen Dual-Stack-Endpunkt stellen, wird die Endpunkt-URL je nach dem von Ihrem Netzwerk und Client verwendeten Protokoll in eine IPv6 oder eine IPv4 Adresse aufgelöst.

Dual-Stack-Endpunktnamen verwenden die folgende Namenskonvention:

- `vpc-lattice.`*`region`*`.api.aws`

Beispielsweise ist der Dual-Stack-Endpunktname für die Region `eu-west-1` `vpc-lattice.eu-west-1.api.aws`.

Angeben von Endpunkten

Die folgenden Beispiele zeigen, wie Sie mithilfe von for einen Endpunkt für die `us-east-2` Region angeben. AWS CLI `vpc-lattice`

- IPv4

```
aws vpc-lattice get-service --service-identifier svc-0285b53b2eEXAMPLE --region us-east-2 --endpoint-url https://vpc-lattice.us-east-2.amazonaws.com
```

- Dualer Stack

```
aws vpc-lattice get-service --service-identifier svc-0285b53b2eEXAMPLE --region us-
east-2 --endpoint-url https://vpc-lattice.us-east-2.api.aws
```

Preisgestaltung

Mit VPC Lattice zahlen Sie für die Zeit, für die ein Service bereitgestellt wird, für die Datenmenge, die über jeden Service übertragen wird, und für die Anzahl der Anfragen. Als Ressourcenbesitzer zahlen Sie für die Daten, die zu und von jeder Ressource übertragen werden. Als Eigentümer eines Servicenetzwerks zahlen Sie stündlich für Ressourcenkonfigurationen, die mit Ihrem Servicenetzwerk verknüpft sind. Als Verbraucher, der eine VPC mit einem Servicenetzwerk verknüpft hat, zahlen Sie für Daten, die von Ihrer VPC zu und von Ressourcen im Servicenetzwerk übertragen werden. Weitere Informationen finden Sie unter Amazon VPC Lattice Pricing.

So funktioniert VPC Lattice

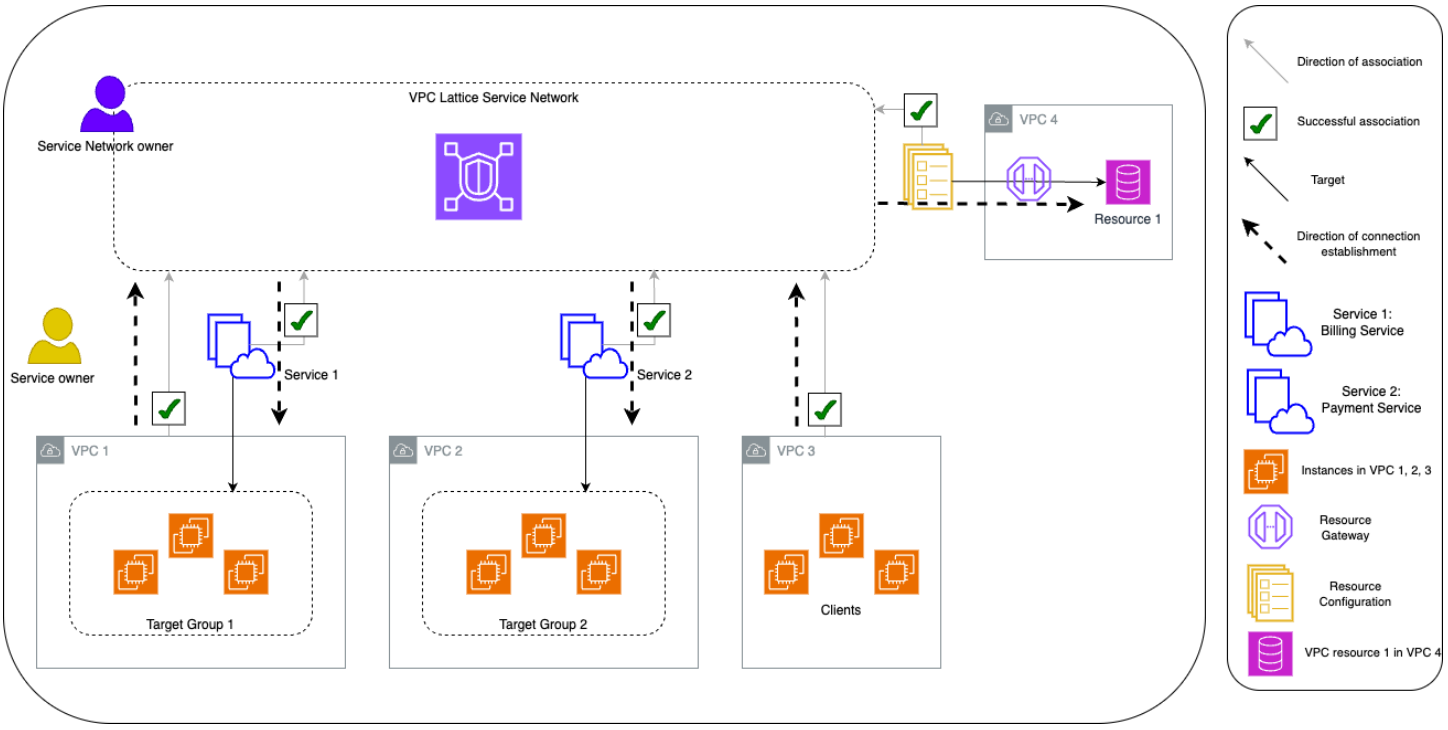
VPC Lattice wurde entwickelt, um Ihnen dabei zu helfen, alle darin enthaltenen Dienste und Ressourcen einfach und effektiv zu entdecken, zu sichern, zu verbinden und zu überwachen. Jede Komponente in VPC Lattice kommuniziert unidirektional oder bidirektional innerhalb des Servicenetzwerks, basierend auf ihrer Zuordnung zum Servicenetzwerk und ihren Zugriffseinstellungen. Die Zugriffseinstellungen bestehen aus Authentifizierungs- und Autorisierungsrichtlinien, die für diese Kommunikation erforderlich sind.

Die folgende Zusammenfassung beschreibt die Kommunikation zwischen Komponenten innerhalb von VPC Lattice:

- Es gibt zwei Möglichkeiten, eine VPC mit einem Servicenetzwerk zu verbinden: über eine VPC-Zuordnung und über einen VPC-Endpunkt vom Typ Servicenetzwerk.
- Dienste und Ressourcen, die dem Servicenetzwerk zugeordnet sind, können Anfragen von Clients empfangen, die ebenfalls mit dem Servicenetzwerk verbunden VPCs sind.
- Ein Client kann Anfragen an Dienste und Ressourcen senden, die einem Servicenetzwerk zugeordnet sind, nur wenn er sich in einer VPC befindet, die mit demselben Dienstnetzwerk verbunden ist. Client-Verkehr, der eine VPC-Peering-Verbindung, ein Transit-Gateway, Direct Connect oder VPN durchquert, kann Ressourcen und Dienste nur erreichen, wenn die VPC über einen VPC-Endpunkt mit dem Servicenetzwerk verbunden ist.
- Ziele von Diensten VPCs , die mit dem Servicenetzwerk verknüpft sind, sind ebenfalls Clients und können Anfragen an andere Dienste und Ressourcen senden, die dem Servicenetzwerk zugeordnet sind.
- Ziele von Diensten VPCs , die nicht mit dem Servicenetzwerk verknüpft sind, sind keine Clients und können keine Anfragen an andere Dienste und Ressourcen senden, die dem Servicenetzwerk zugeordnet sind.
- Clients VPCs , die über Ressourcen verfügen, bei denen die VPC jedoch nicht mit dem Servicenetzwerk verknüpft ist, sind keine Clients und können keine Anfragen an andere Dienste und Ressourcen senden, die dem Servicenetzwerk zugeordnet sind.

Das folgende Flussdiagramm verwendet ein Beispielszenario, um den Informationsfluss und die Richtung der Kommunikation zwischen den Komponenten innerhalb von VPC Lattice zu erklären. Einem Dienstnetzwerk sind zwei Dienste zugeordnet. Beide Dienste und alle VPCs wurden unter

demselben Konto wie das Servicenetzwerk erstellt. Beide Dienste sind so konfiguriert, dass sie Datenverkehr aus dem Servicenetzwerk zulassen.



Service 1 ist eine Abrechnungsanwendung, die auf einer Gruppe von Instanzen läuft, die bei Zielgruppe 1 in VPC 1 registriert sind. Service 2 ist eine Zahlungsanwendung, die auf einer Gruppe von Instances läuft, die bei Zielgruppe 2 in VPC 2 registriert sind. VPC 3 befindet sich im selben Konto und hat Kunden, aber keine Dienste. Ressource 1 ist eine Datenbank mit Kundendaten in VPC 4.

In der folgenden Liste wird der typische Aufgabenablauf für VPC Lattice der Reihe nach beschrieben.

1. Erstellen Sie ein Servicenetzwerk

   Der Besitzer des Servicenetzwerks erstellt das Servicenetzwerk.

2. Einen Service erstellen

   Die Dienstbesitzer erstellen ihre jeweiligen Dienste, Dienst 1 und Dienst 2. Bei der Erstellung fügt der Service Owner Listener hinzu und definiert Regeln für die Weiterleitung von Anfragen an die Zielgruppe für jeden Service.

3. Definieren Sie das Routing

Die Service Owner erstellen die Zielgruppe für jeden Service (Zielgruppe 1 und Zielgruppe 2). Sie tun dies, indem sie die Zielinstanzen angeben, auf denen die Dienste ausgeführt werden. Sie geben auch an, VPCs in welchen sich diese Ziele befinden.

Im obigen Diagramm stellen die durchgezogenen Pfeile Dienste dar, die den Datenverkehr an Zielgruppen weiterleiten, und die Ressourcenkonfigurationen, die zu Ressourcen weiterleiten.

4. Ordnen Sie Dienste dem Servicenetzwerk zu

   Der Besitzer des Servicenetzes oder der Dienstbesitzer ordnet die Dienste dem Servicenetzwerk zu. Die Zuordnungen werden als Pfeile mit Häkchen angezeigt, die vom Dienst aus auf das Servicenetzwerk zeigen. Wenn Sie einen Dienst einem Servicenetzwerk zuordnen, wird dieser Dienst für andere Dienste, die mit dem Servicenetzwerk verbunden sind, und für Clients, die mit dem Servicenetzwerk VPCs verbunden sind, auffindbar.

   Die gestrichelten Pfeile zwischen dem Servicenetzwerk und den Zielgruppen zeigen die Richtung des Verbindungsaufbaus an. Geben Sie den Datenverkehr zurück zu den Clients, die das Servicenetzwerk verwenden. Die Pfeile, die den wiederkehrenden Verkehr darstellen, sind in diesem Diagramm nicht enthalten.

5. Erstellen Sie ein Ressourcen-Gateway

   Der Ressourcenbesitzer erstellt ein Ressourcen-Gateway in VPC 4, um die Konnektivität von Clients zur Ressource 1 ermöglichen zu können.

6. Erstellen Sie eine Ressourcenkonfiguration

   Der Ressourcenbesitzer erstellt eine Ressourcenkonfiguration, die Ressource 1 darstellt, und gibt das Ressourcen-Gateway für Ressource 1 an.

7. Ordnen Sie Ressourcenkonfigurationen dem Dienstnetzwerk zu

   Der Besitzer des Dienstnetzwerks oder der Ressourcenbesitzer ordnet die Ressourcenkonfiguration dem Dienstnetzwerk zu. Die Zuordnung wird als Pfeil mit einem Häkchen angezeigt, das in der Ressourcenkonfiguration auf das Servicenetzwerk zeigt. Wenn Sie eine Ressourcenkonfiguration einem Dienstnetzwerk zuordnen, wird diese Ressourcenkonfiguration für andere Dienste, die dem Dienstnetzwerk zugeordnet sind, und für Clients in dem mit dem Servicenetzwerk VPCs verbundenen Clients auffindbar.

   Die gestrichelten Pfeile vom Servicenetzwerk zur Ressource stellen die Ressource dar, die Anfragen von Clients empfängt. Der Datenverkehr fließt über das Servicenetzwerk zurück zum

Client. Die Pfeile, die den zurückkehrenden Verkehr darstellen, sind in diesem Diagramm nicht enthalten.

8. Connect zum VPCs Servicenetzwerk her

   VPCs kann auf zwei Arten mit dem Servicenetzwerk verbunden werden: durch Zuordnen der VPC zum Servicenetzwerk oder durch Erstellen eines VPC-Endpunkts. Hier ordnet der Besitzer des Servicenetzes VPC1 und VPC3 dem Servicenetzwerk zu. Die Zuordnungen werden anhand von Pfeilen angezeigt, deren Häkchen auf das Servicenetzwerk zeigen. Mit diesen Zuordnungen können alle Ressourcen in der VPC als Clients fungieren und Anfragen an Dienste innerhalb des Servicenetzwerks stellen. Die gestrichelten Pfeile zwischen VPC 1 und dem Servicenetzwerk zeigen die Richtung des Verbindungsaufbaus. Das Servicenetzwerk initiiert nur Verbindungen zu Ressourcen, die für die Zielgruppen von Service 1 bestimmt sind. Jede Ressource in VPC 1 kann als Client fungieren und Verbindungen zu den Diensten und Ressourcen des Servicenetzwerks initiieren.

   VPC 2 hat weder einen Pfeil noch ein Häkchen, der eine Assoziation darstellt. Dies bedeutet, dass der Eigentümer des Servicenetzwerks oder der Dienstbesitzer VPC 2 nicht mit dem Dienstnetzwerk verknüpft hat. Dies liegt daran, dass Service 2 in diesem Beispiel nur Anfragen empfangen und Antworten mit derselben Anfrage senden muss. Mit anderen Worten, die Ziele für Dienst 2 sind keine Clients und müssen keine Anfragen an andere Dienste im Servicenetzwerk stellen.

   Ebenso hat VPC 4 weder einen Pfeil noch ein Häkchen, das eine Assoziation darstellt. Dies bedeutet, dass der Besitzer des Servicenetzwerks oder der Ressourcenbesitzer VPC 4 nicht mit dem Dienstnetzwerk verknüpft hat. Dies liegt daran, dass Ressource 1 nur Anfragen empfängt und Antworten mit derselben Anfrage sendet. Sie kann keine Anfragen an andere Dienste und Ressourcen im Dienstnetzwerk stellen.

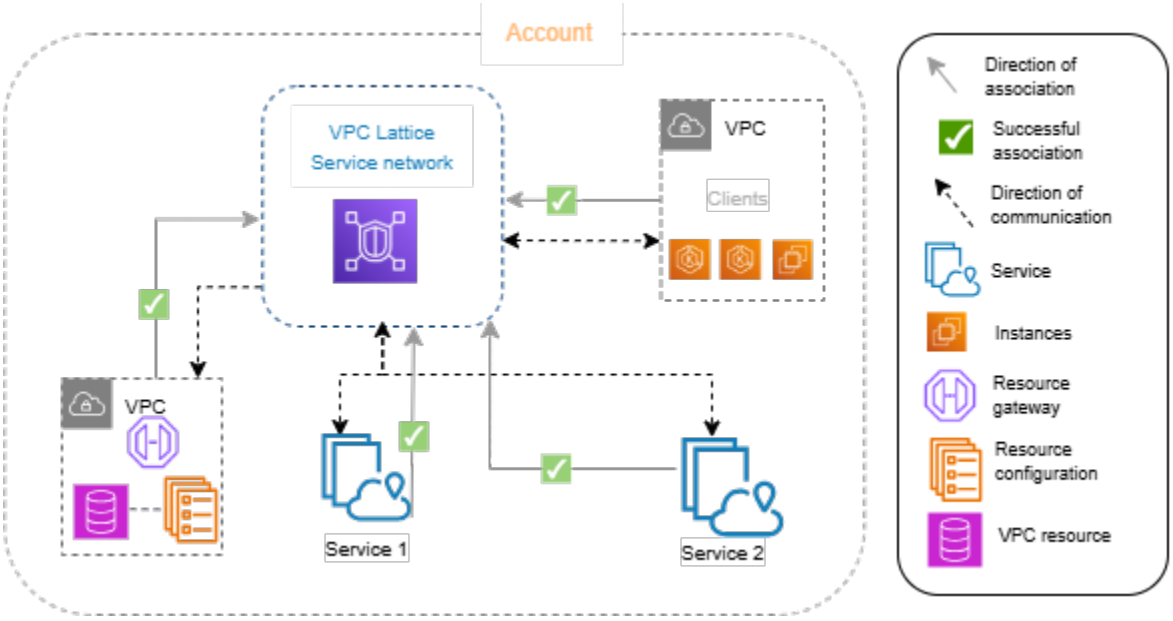
Zusammenfassend zeigte das nachfolgende Diagramm die folgenden Szenarien:

- VPCs mit reinen Eingangsverbindungen von VPC Lattice zu ihren Ressourcen. VPC 2 und VPC 4 repräsentieren diese Szenarien.
- Eine VPC mit reinen Ausgangsverbindungen von ihren Ressourcen zu VPC Lattice. VPC 3 repräsentiert dieses Szenario.
- Eine VPC mit eingehenden Verbindungen von VPC Lattice zu ihren Ressourcen und mit Ausgangsverbindungen von ihren Ressourcen zu VPC Lattice. VPC 1 steht für dieses Szenario.

Servicenetzwerke in VPC Lattice

Ein Servicenetzwerk ist eine logische Grenze für eine Sammlung von Diensten und Ressourcenkonfigurationen. Dienste und Ressourcenkonfigurationen, die mit dem Netzwerk verknüpft sind, können für Erkennung, Konnektivität, Zugänglichkeit und Beobachtbarkeit autorisiert werden. Um Anfragen an Dienste und Ressourcenkonfigurationen im Netzwerk stellen zu können, muss sich Ihr Service oder Client in einer VPC befinden, die entweder über eine Zuordnung oder über einen VPC-Endpunkt mit dem Dienstnetzwerk verbunden ist.

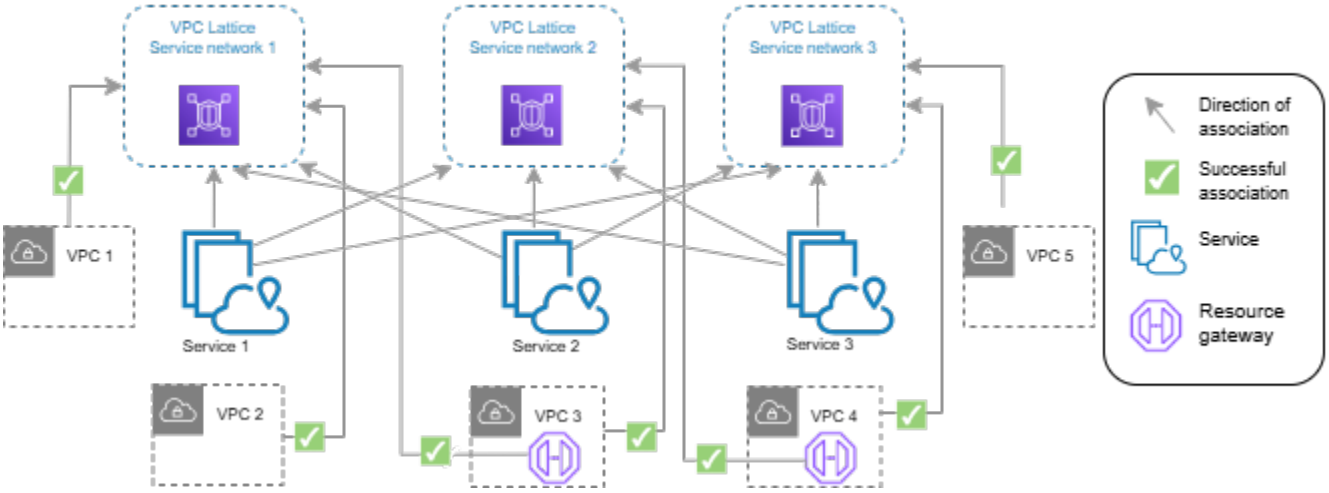
Das folgende Diagramm zeigt die wichtigsten Komponenten eines typischen Servicenetzwerks innerhalb von Amazon VPC Lattice. Häkchen auf den Pfeilen weisen darauf hin, dass die Dienste und die VPC dem Servicenetzwerk zugeordnet sind. Clients in der VPC, die dem Servicenetzwerk zugeordnet sind, können über das Dienstnetzwerk mit beiden Diensten kommunizieren.



Sie können eine oder mehrere Dienste und Ressourcenkonfigurationen mehreren Dienstnetzwerken zuordnen. Sie können auch mehrere VPCs mit einem Servicenetzwerk verbinden. Sie können eine VPC über eine Zuordnung nur mit einem Servicenetzwerk verbinden. Um eine VPC mit mehreren Servicenetzwerken zu verbinden, können Sie VPC-Endpunkte vom Typ Dienstnetzwerk verwenden. Weitere Informationen zu VPC-Endpunkten vom Typ Dienstnetzwerk finden Sie im AWS PrivateLink Benutzerhandbuch.

In der folgenden Abbildung stellen die Pfeile die Verknüpfungen zwischen Diensten und Dienstnetzwerken sowie die Verknüpfungen zwischen den Diensten VPCs und Dienstnetzwerken dar. Sie können sehen, dass mehrere Dienste mehreren Dienstnetzwerken zugeordnet VPCs

sind und dass jedem Dienstnetzwerk mehrere Dienste zugeordnet sind. Jede VPC hat genau eine Zuordnung zu einem Servicenetzwerk. VPC 3 und VPC 4 stellen jedoch eine Verbindung zu zwei Servicenetzwerken her. VPC 3 stellt über einen VPC-Endpunkt eine Verbindung zum Servicenetzwerk 1 her. In ähnlicher Weise stellt VPC 4 über einen VPC-Endpunkt eine Verbindung zum Servicenetzwerk 2 her.



Weitere Informationen finden Sie unter Kontingente für Amazon VPC Lattice.

Inhalt

- Erstellen Sie ein VPC-Lattice-Dienstnetzwerk
- Verwalten Sie die Zuordnungen für ein VPC Lattice-Dienstnetzwerk
- Zugriffseinstellungen für ein VPC Lattice-Dienstnetzwerk bearbeiten
- Bearbeiten Sie die Überwachungsdetails für ein VPC Lattice-Servicenetzwerk
- Tags für ein VPC Lattice-Servicenetzwerk verwalten
- Löschen Sie ein VPC-Lattice-Dienstnetzwerk

Erstellen Sie ein VPC-Lattice-Dienstnetzwerk

Verwenden Sie die Konsole, um ein Servicenetzwerk zu erstellen und es optional mit Diensten, Verknüpfungen, Zugriffseinstellungen und Zugriffsprotokollen zu konfigurieren.

So erstellen Sie mit der Konsole ein Servicenetzwerk

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

3. Wählen Sie Servicenetzwerk erstellen aus.
4. Geben Sie unter Identifikatoren einen Namen, eine optionale Beschreibung und optionale Tags ein. Der Name muss zwischen 3 und 63 Zeichen lang sein. Sie können Kleinbuchstaben, Zahlen und Bindestriche verwenden. Der Name muss mit einem Buchstaben oder einer Zahl beginnen und enden. Verwenden Sie keine aufeinanderfolgenden Bindestriche. Die Beschreibung kann bis zu 256 Zeichen lang sein. Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert an.
5. (Optional) Um einen Dienst zuzuordnen, wählen Sie den Dienst unter Dienstzuordnungen, Dienste aus. Die Liste umfasst Dienste, die sich in Ihrem Konto befinden, und alle Dienste, die von einem anderen Konto aus mit Ihnen geteilt werden. Wenn die Liste keine Services enthält, können Sie einen Service erstellen, indem Sie Create an VPC Lattice Service auswählen.

   Informationen zum Zuordnen eines Dienstes, nachdem Sie das Dienstnetzwerk erstellt haben, finden Sie alternativ unter. the section called “Dienstzuordnungen verwalten”
6. (Optional) Um eine Ressourcenkonfiguration zuzuordnen, wählen Sie unter Ressourcenkonfigurationszuordnungen, Ressourcenkonfiguration den Dienst für die Ressourcenkonfiguration aus. Die Liste enthält Ressourcenkonfigurationen, die sich in Ihrem Konto befinden, sowie alle Ressourcenkonfigurationen, die von einem anderen Konto aus mit Ihnen geteilt wurden. Wenn die Liste keine Ressourcenkonfigurationen enthält, können Sie eine Ressourcenkonfiguration erstellen, indem Sie Create an Amazon VPC Lattice resource configuration wählen.

   Informationen zum Zuordnen einer Ressourcenkonfiguration, nachdem Sie das Servicenetzwerk erstellt haben, finden Sie alternativ unter. the section called “Zuordnungen zur Ressourcenkonfiguration verwalten”
7. (Optional) Um eine VPC zuzuordnen, wählen Sie VPC-Zuordnung hinzufügen aus. Wählen Sie die VPC aus, die Sie der VPC zuordnen möchten, und wählen Sie bis zu fünf Sicherheitsgruppen unter Sicherheitsgruppen aus. Um eine Sicherheitsgruppe zu erstellen, wählen Sie Neue Sicherheitsgruppe erstellen aus.

   Alternativ können Sie diesen Schritt überspringen und eine VPC über einen VPC-Endpunkt (powered by AWS PrivateLink) mit VPC Servicenetzwerk verbinden. Weitere Informationen finden Sie im AWS PrivateLink Benutzerhandbuch unter Access Service Networks.
8. Beim Erstellen eines Dienstnetzwerks müssen Sie entscheiden, ob Sie das Dienstnetzwerk mit anderen Konten gemeinsam nutzen möchten oder nicht. Ihre Auswahl ist unveränderlich und kann nicht geändert werden, nachdem Sie das Servicenetzwerk erstellt haben. Wenn Sie

die gemeinsame Nutzung zulassen, kann das Servicenetzwerk über AWS Resource Access Manager für andere Konten freigegeben werden.

Um Ihr Servicenetzwerk mit anderen Konten zu teilen, wählen Sie die AWS RAM Ressourcenfreigaben unter Ressourcenfreigaben aus.

Um eine Ressourcenfreigabe zu erstellen, rufen Sie die AWS RAM Konsole auf und wählen Sie „Ressourcenfreigabe erstellen“.

9. Für den Netzwerkzugriff können Sie den Standardauthentifizierungstyp „Keine“ beibehalten, wenn Sie möchten, dass die Clients im zugehörigen Netzwerk VPCs auf die Dienste in diesem Dienstnetzwerk zugreifen. Um eine Authentifizierungsrichtlinie zur Steuerung des Zugriffs auf Ihre Dienste anzuwenden, wählen Sie AWS IAM und führen Sie für Auth-Richtlinie einen der folgenden Schritte aus:
   - Geben Sie eine Richtlinie in das Eingabefeld ein. Wählen Sie beispielsweise Richtlinien, die Sie kopieren und einfügen können, aus.
   - Wählen Sie Richtlinienvorlage anwenden und wählen Sie die Vorlage Authentifizierten und nicht authentifizierten Zugriff zulassen aus. Mit dieser Vorlage kann ein Kunde von einem anderen Konto aus auf den Service zugreifen, indem er entweder die Anfrage signiert (d. h. authentifiziert) oder anonym (d. h. nicht authentifiziert).
   - Wählen Sie Richtlinienvorlage anwenden und wählen Sie die Vorlage Nur authentifizierten Zugriff zulassen aus. Mit dieser Vorlage kann ein Kunde von einem anderen Konto aus nur dann auf den Service zugreifen, wenn er die Anfrage signiert (d. h. authentifiziert).
10. (Optional) Um Zugriffsprotokolle zu aktivieren, wählen Sie den Schalter Zugriffsprotokolle und geben Sie wie folgt ein Ziel für Ihre Zugriffsprotokolle an:
    - Wählen Sie CloudWatch Protokollgruppe und wählen Sie eine CloudWatch Protokollgruppe aus. Um eine Protokollgruppe zu erstellen, wählen Sie Protokollgruppe erstellen in CloudWatch.
    - Wählen Sie S3-Bucket aus und geben Sie den S3-Bucket-Pfad einschließlich eines beliebigen Präfixes ein. Um Ihre S3-Buckets zu durchsuchen, wählen Sie Browse S3.
    - Wählen Sie Kinesis Data Firehose Delivery Stream und wählen Sie einen Delivery Stream aus. Um einen Delivery Stream zu erstellen, wählen Sie Create a delivery stream in Kinesis.
11. (Optional) Um Ihr Servicenetzwerk mit anderen Konten gemeinsam zu nutzen, wählen Sie die AWS RAM Ressourcenfreigaben unter Ressourcenfreigaben aus. Um eine Ressourcenfreigabe zu erstellen, wählen Sie in der RAM-Konsole die Option Ressourcenfreigabe erstellen aus.

12. Überprüfen Sie Ihre Konfiguration im Abschnitt Zusammenfassung und wählen Sie dann Create service network aus.

Um ein Servicenetzwerk mit dem zu erstellen AWS CLI

Verwenden Sie den create-service-network-Befehl. Dieser Befehl erstellt nur das grundlegende Servicenetzwerk. Um ein voll funktionsfähiges Servicenetzwerk zu erstellen, müssen Sie auch die Befehle verwenden, mit denen Dienstzuordnungen, VPC-Zuordnungen und Zugriffseinstellungen erstellt werden.

Verwalten Sie die Zuordnungen für ein VPC Lattice-Dienstnetzwerk

Wenn Sie dem Dienstnetzwerk einen Dienst oder eine Ressourcenkonfiguration zuordnen, können Clients, die mit dem Dienstnetzwerk VPCs verbunden sind, Anfragen an den Dienst und die Ressourcenkonfiguration stellen. Wenn Sie eine VPC mit dem Servicenetzwerk verbinden, können alle Ziele innerhalb dieser VPC Clients sein und mit anderen Diensten und Ressourcenkonfigurationen im Servicenetzwerk kommunizieren.

Inhalt

Dienstzuordnungen verwalten

Sie können Dienste verknüpfen, die sich in Ihrem Konto befinden, oder Dienste, die von verschiedenen Konten aus mit Ihnen geteilt wurden. Dies ist ein optionaler Schritt beim Erstellen eines Servicenetzwerks. Ein Servicenetzwerk ist jedoch erst dann voll funktionsfähig, wenn Sie einen Dienst zuordnen. Dienstinhaber können ihre Dienste einem Servicenetzwerk zuordnen, wenn ihr Konto über den erforderlichen Zugriff verfügt. Weitere Informationen finden Sie unter Beispiele für identitätsbasierte Richtlinien für VPC Lattice.

Wenn Sie eine Dienstzuordnung löschen, kann der Dienst keine Verbindung mehr mit anderen Diensten im Dienstnetzwerk herstellen.

Um Dienstzuordnungen mithilfe der Konsole zu verwalten

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Service networks aus.
3. Wählen Sie den Namen des Servicenetzwerks aus, um dessen Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Dienstzuordnungen.
5. Gehen Sie wie folgt vor, um eine Assoziation zu erstellen:
   a. Wählen Sie Verknüpfungen erstellen aus.
   b. Wählen Sie unter Dienste einen Dienst aus. Um einen Service zu erstellen, wählen Sie Create an Amazon VPC Lattice Service.
   c. (Optional) Um ein Tag hinzuzufügen, erweitern Sie Service-Zuordnungs-Tags, wählen Sie Neues Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
   d. Wählen Sie Änderungen speichern aus.
6. Um eine Zuordnung zu löschen, aktivieren Sie das Kontrollkästchen für die Zuordnung und wählen Sie dann Aktionen, Dienstzuordnungen löschen aus. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

Um eine Dienstverknüpfung mit dem zu erstellen AWS CLI

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

Um eine Dienstzuordnung mit dem zu löschen AWS CLI

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

Zuordnungen zur Ressourcenkonfiguration verwalten

Eine Ressourcenkonfiguration ist ein logisches Objekt, das entweder eine einzelne Ressource oder eine Gruppe von Ressourcen darstellt. Sie können Ressourcenkonfigurationen, die sich in Ihrem Konto befinden, oder Ressourcenkonfigurationen, die von verschiedenen Konten für Sie gemeinsam genutzt wurden, zuordnen. Dies ist ein optionaler Schritt beim Erstellen eines Servicenetzwerks. Besitzer der Ressourcenkonfiguration können ihre Ressourcenkonfigurationen einem Servicenetzwerk zuordnen, sofern ihr Konto über den erforderlichen Zugriff verfügt. Weitere Informationen finden Sie unter Beispiele für identitätsbasierte Richtlinien für VPC Lattice.

Verwalten Sie Verknüpfungen zwischen Dienstnetzwerken und Ressourcenkonfigurationen

Sie können die Zuordnung zwischen dem Dienstnetzwerk und der Ressourcenkonfiguration erstellen oder löschen.

Um Zuordnungen zur Ressourcenkonfiguration mithilfe 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 Service Networks aus.
3. Wählen Sie den Namen des Servicenetzwerks aus, um die zugehörige Detailseite zu öffnen.
4. Wählen Sie die Registerkarte „Zuordnungen zur Ressourcenkonfiguration“.
5. Gehen Sie wie folgt vor, um eine Zuordnung zu erstellen:
   a. Wählen Sie Verknüpfungen erstellen aus.
   b. Wählen Sie unter Ressourcenkonfigurationen eine Ressourcenkonfiguration aus. Wählen Sie Create an Amazon VPC Lattice Resource configuration aus. .
   c. (Optional) Um ein Tag hinzuzufügen, erweitern Sie Dienstverknüpfungs-Tags, wählen Sie Neues Tag hinzufügen aus und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
   d. Wählen Sie Änderungen speichern aus.
6. Um eine Zuordnung zu löschen, aktivieren Sie das Kontrollkästchen für die Verknüpfung und wählen Sie dann Aktionen, Löschen aus. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

Um eine Zuordnung zur Ressourcenkonfiguration zu erstellen, verwenden Sie den AWS CLI

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

Um eine Zuordnung zur Ressourcenkonfiguration mit dem AWS CLI

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

VPC-Zuordnungen verwalten

Clients können Anfragen an Dienste und Ressourcen senden, die in Ressourcenkonfigurationen angegeben sind, die einem Dienstnetzwerk zugeordnet sind, wenn der Client mit dem Dienstnetzwerk VPCs verknüpft ist. Client-Verkehr, der eine VPC-Peering-Verbindung oder ein Transit-Gateway

durchquert, wird nur über ein Dienstnetzwerk zugelassen, das einen VPC-Endpunkt vom Typ Dienstnetzwerk verwendet.

Das Zuordnen einer VPC ist ein optionaler Schritt, wenn Sie ein Servicenetzwerk erstellen. Netzwerkbesitzer können eine Verbindung VPCs zu einem Servicenetzwerk herstellen, wenn ihr Konto über den erforderlichen Zugriff verfügt. Weitere Informationen finden Sie unter Beispiele für identitätsbasierte Richtlinien für VPC Lattice.

Wenn Sie eine VPC-Zuordnung löschen, VPCs können Clients in der keine Verbindung mehr zu Diensten im Dienstnetzwerk herstellen.

So verwalten Sie VPC-Zuordnungen mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Service networks aus.
3. Wählen Sie den Namen des Servicenetzwerks aus, um dessen Detailseite zu öffnen.
4. Wählen Sie die Registerkarte VPC-Zuordnungen aus.
5. Gehen Sie wie folgt vor, um eine VPC-Zuordnung zu erstellen:
    a. Wählen Sie Create VPC Associations aus.
    b. Wählen Sie VPC-Assoziation hinzufügen aus.
    c. Wählen Sie eine VPC aus VPC und bis zu fünf Sicherheitsgruppen aus Sicherheitsgruppen aus. Um eine Sicherheitsgruppe zu erstellen, wählen Sie Neue Sicherheitsgruppe erstellen.
    d. (Optional) Um ein Tag hinzuzufügen, erweitern Sie die VPC-Zuordnungs-Tags, wählen Sie Neues Tag hinzufügen aus und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
    e. Wählen Sie Änderungen speichern aus.
6. Um die Sicherheitsgruppen für eine Zuordnung zu bearbeiten, aktivieren Sie das Kontrollkästchen für die Zuordnung und wählen Sie dann Aktionen, Sicherheitsgruppen bearbeiten aus. Fügen Sie nach Bedarf Sicherheitsgruppen hinzu und entfernen Sie sie.
7. Um eine Zuordnung zu löschen, aktivieren Sie das Kontrollkästchen für die Zuordnung und wählen Sie dann Aktionen, VPC-Zuordnungen löschen aus. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

So erstellen Sie eine VPC-Assoziation mit dem AWS CLI

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

Um die Sicherheitsgruppen für eine VPC-Assoziation mit dem zu aktualisieren AWS CLI

Verwenden Sie den Befehl update-service-network-vpc-association.

So löschen Sie eine VPC-Assoziation mit dem AWS CLI

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

VPC-Endpunktzuordnungen verwalten

Clients können Anfragen an Dienste und Ressourcen, die in Ressourcenkonfigurationen angegeben sind, über einen VPC-Endpunkt (powered by AWS PrivateLink) in ihrer VPC senden. Ein VPC-Endpunkt vom Typ Service Network verbindet eine VPC mit einem Servicenetzwerk. Client-Verkehr, der von außerhalb der VPC über eine VPC-Peering-Verbindung, Transit Gateway, Direct Connect oder VPN kommt, kann den VPC-Endpunkt verwenden, um Dienste und Ressourcenkonfigurationen zu erreichen. Mit VPC-Endpunkten können Sie eine VPC mit mehreren Servicenetzwerken verbinden. Wenn Sie einen VPC-Endpunkt in einer VPC erstellen, werden IP-Adressen aus der VPC (und nicht IP-Adressen aus der Liste der verwalteten Präfixe) verwendet, um die Konnektivität zum Servicenetzwerk herzustellen.

So verwalten Sie VPC-Endpunktzuordnungen mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Service networks aus.
3. Wählen Sie den Namen des Servicenetzwerks aus, um dessen Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Endpunktzuordnungen, um die VPC-Endpunkte anzuzeigen, die mit Ihrem Servicenetzwerk verbunden sind.
5. Wählen Sie die Endpunkt-ID des VPC-Endpunkts aus, um dessen Detailseite zu öffnen. Ändern oder löschen Sie dann die VPC-Endpunktzuweisung.

So erstellen Sie mit der Konsole eine neue VPC-Endpunktzuordnung

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Endpoints aus.
3. Wählen Sie Create Endpoints aus.
4. Wählen Sie als Typ die Option Servicenetzwerke aus.
5. Wählen Sie das Servicenetzwerk aus, das Sie mit Ihrer VPC verbinden möchten.

6. Wählen Sie die VPC, Subnetze und Sicherheitsgruppen aus.
7. (Optional) Um ein Tag hinzuzufügen, erweitern Sie die VPC-Zuordnungs-Tags, wählen Sie Neues Tag hinzufügen aus und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
8. Wählen Sie Endpunkt erstellen aus.

Weitere Informationen zum VPC-Endpunkt und zum Herstellen einer Verbindung zu Dienstnetzwerken finden Sie im AWS PrivateLink Benutzerhandbuch unter Zugreifen auf Dienstnetzwerke.

Zugriffseinstellungen für ein VPC Lattice-Dienstnetzwerk bearbeiten

Mit den Zugriffseinstellungen können Sie den Clientzugriff auf ein Servicenetzwerk konfigurieren und verwalten. Zu den Zugriffseinstellungen gehören der Authentifizierungstyp und die Authentifizierungsrichtlinien. Mithilfe von Authentifizierungsrichtlinien können Sie den Datenverkehr, der zu Diensten innerhalb von VPC Lattice fließt, authentifizieren und autorisieren. Die Zugriffseinstellungen des Servicenetzwerks gelten nicht für die Ressourcenkonfigurationen, die dem Servicenetzwerk zugeordnet sind.

Sie können Authentifizierungsrichtlinien auf Dienstnetzwerkebene, Dienstebene oder auf beiden Ebenen anwenden. In der Regel werden Authentifizierungsrichtlinien von den Netzwerkbesitzern oder Cloud-Administratoren angewendet. Sie können eine maßgeschneiderte Autorisierung implementieren, die beispielsweise authentifizierte Anrufe innerhalb der Organisation oder anonyme GET-Anfragen, die einer bestimmten Bedingung entsprechen, ermöglicht. Auf der Serviceebene können Dienstinhaber feinkörnige Kontrollen anwenden, die restriktiver sein können. Weitere Informationen finden Sie unter Steuern Sie den Zugriff auf VPC Lattice-Dienste mithilfe von Authentifizierungsrichtlinien.

Um Zugriffsrichtlinien mithilfe der Konsole hinzuzufügen oder zu aktualisieren

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Service networks aus.
3. Wählen Sie den Namen des Servicenetzwerks aus, um dessen Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Zugriff, um die aktuellen Zugriffseinstellungen zu überprüfen.
5. Um die Zugriffseinstellungen zu aktualisieren, wählen Sie Zugriffseinstellungen bearbeiten.
6. Wenn Sie möchten, dass die Clients im zugehörigen Netzwerk VPCs auf die Dienste in diesem Servicenetzwerk zugreifen, wählen Sie None als Authentifizierungstyp aus.

7. Um eine Ressourcenrichtlinie auf das Servicenetzwerk anzuwenden, wählen Sie AWS IAM als Authentifizierungstyp und gehen Sie für Auth-Richtlinie wie folgt vor:
   - Geben Sie eine Richtlinie in das Eingabefeld ein. Wählen Sie beispielsweise Richtlinien, die Sie kopieren und einfügen können, aus.
   - Wählen Sie Richtlinienvorlage anwenden und wählen Sie die Vorlage Authentifizierten und nicht authentifizierten Zugriff zulassen aus. Mit dieser Vorlage kann ein Kunde von einem anderen Konto aus auf den Service zugreifen, indem er entweder die Anfrage signiert (d. h. authentifiziert) oder anonym (d. h. nicht authentifiziert).
   - Wählen Sie Richtlinienvorlage anwenden und wählen Sie die Vorlage Nur authentifizierten Zugriff zulassen aus. Mit dieser Vorlage kann ein Kunde von einem anderen Konto aus nur dann auf den Service zugreifen, wenn er die Anfrage signiert (d. h. authentifiziert).
8. Wählen Sie Änderungen speichern aus.

Um eine Zugriffsrichtlinie hinzuzufügen oder zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie den put-auth-policy-Befehl.

Bearbeiten Sie die Überwachungsdetails für ein VPC Lattice-Servicenetzwerk

VPC Lattice generiert Metriken und Protokolle für jede Anfrage und Antwort, sodass Anwendungen effizienter überwacht und Fehler behoben werden können.

Sie können Zugriffsprotokolle aktivieren und die Zielressource für Ihre Protokolle angeben. VPC Lattice kann Protokolle an die folgenden Ressourcen senden: CloudWatch Protokollgruppen, Firehose-Lieferstreams und S3-Buckets.

Um Zugriffsprotokolle zu aktivieren oder ein Protokollziel mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Service networks aus.
3. Wählen Sie den Namen des Servicenetzwerks aus, um dessen Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Überwachung. Überprüfen Sie die Zugriffsprotokolle, um festzustellen, ob Zugriffsprotokolle aktiviert sind.
5. Um Zugriffsprotokolle zu aktivieren oder zu deaktivieren, wählen Sie Zugriffsprotokolle bearbeiten und schalten Sie dann den Schalter Zugriffsprotokolle ein oder aus.

6. Wenn Sie Zugriffsprotokolle aktivieren, müssen Sie die Art des Lieferziels auswählen und dann das Ziel für die Zugriffsprotokolle erstellen oder auswählen. Sie können das Lieferziel auch jederzeit ändern. Zum Beispiel:
   - Wählen Sie CloudWatch Protokollgruppe und wählen Sie eine CloudWatch Protokollgruppe aus. Um eine Protokollgruppe zu erstellen, wählen Sie Protokollgruppe erstellen in CloudWatch.
   - Wählen Sie S3-Bucket aus und geben Sie den S3-Bucket-Pfad einschließlich eines beliebigen Präfixes ein. Um Ihre S3-Buckets zu durchsuchen, wählen Sie Browse S3.
   - Wählen Sie Kinesis Data Firehose Delivery Stream und wählen Sie einen Delivery Stream aus. Um einen Delivery Stream zu erstellen, wählen Sie Create a delivery stream in Kinesis.
7. Wählen Sie Änderungen speichern aus.

Um Zugriffsprotokolle zu aktivieren, verwenden Sie AWS CLI

Verwenden Sie den create-access-log-subscription-Befehl.

Um das Protokollziel mit dem zu aktualisieren AWS CLI

Verwenden Sie den update-access-log-subscription-Befehl.

Um Zugriffsprotokolle zu deaktivieren, verwenden Sie AWS CLI

Verwenden Sie den delete-access-log-subscription-Befehl.

Tags für ein VPC Lattice-Servicenetzwerk verwalten

Mithilfe von Tags können Sie Ihr Servicenetzwerk auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung.

Sie können jedem Servicenetzwerk mehrere Tags hinzufügen. Tag-Schlüssel müssen für jedes Servicenetzwerk eindeutig sein. Wenn Sie ein Tag mit einem Schlüssel hinzufügen, der bereits mit dem Servicenetzwerk verknüpft ist, wird der Wert dieses Tags aktualisiert. Sie können Zeichen wie Buchstaben, Leerzeichen, Zahlen (in UTF-8) und die folgenden Sonderzeichen verwenden: + - =. _ : / @. Verwenden Sie keine führenden oder nachgestellten Leerzeichen. Bei Tag-Werten muss die Groß- und Kleinschreibung beachtet werden.

Um Tags mit der Konsole hinzuzufügen oder zu löschen

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

2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Service networks aus.
3. Wählen Sie den Namen des Servicenetzwerks aus, um dessen Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Tags aus.
5. Um ein Tag hinzuzufügen, wählen Sie Tags hinzufügen und geben Sie den Tag-Schlüssel und den Tag-Wert ein. Zum Hinzufügen eines weiteren Tags wählen Sie Neues Tag hinzufügen erneut aus. Wenn Sie fertig mit dem Hinzufügen der Tags sind, klicken Sie auf Save changes (Änderungen speichern).
6. Um ein Tag zu löschen, aktivieren Sie das Kontrollkästchen für das Tag und wählen Sie Löschen. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

Um Tags hinzuzufügen oder zu löschen, verwenden Sie AWS CLI

Verwenden Sie die Befehle tag-resource und untag-resource.

Löschen Sie ein VPC-Lattice-Dienstnetzwerk

Bevor Sie ein Dienstnetzwerk löschen können, müssen Sie zunächst alle Verknüpfungen löschen, die das Dienstnetzwerk möglicherweise mit einem Dienst, einer Ressourcenkonfiguration, einer VPC oder einem VPC-Endpunkt hat. Wenn Sie ein Dienstnetzwerk löschen, löschen wir auch alle Ressourcen, die sich auf das Dienstnetzwerk beziehen, z. B. die Ressourcenrichtlinie, die Authentifizierungsrichtlinie und die Abonnements für das Zugriffsprotokoll.

Um ein Servicenetzwerk mithilfe der Konsole zu löschen

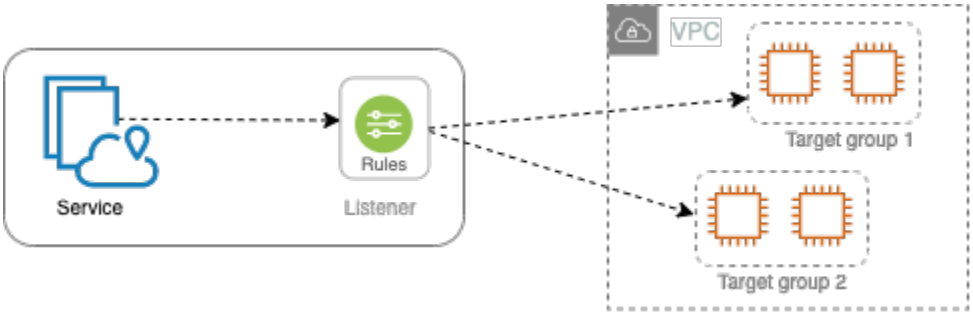
1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Service networks aus.
3. Aktivieren Sie das Kontrollkästchen für das Dienstnetzwerk und wählen Sie dann Aktionen, Dienstnetzwerk löschen aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Delete (Löschen) aus.

Um ein Servicenetzwerk mit dem zu löschen AWS CLI

Verwenden Sie den delete-service-network-Befehl.

Dienstleistungen in VPC Lattice

Ein Service innerhalb von VPC Lattice ist eine unabhängig einsetzbare Softwareeinheit, die eine bestimmte Aufgabe oder Funktion bereitstellt. Ein Dienst kann auf Instanzen, Containern oder als serverlose Funktionen innerhalb eines Kontos oder einer Virtual Private Cloud (VPC) ausgeführt werden. Ein Dienst verfügt über einen Listener, der Regeln, sogenannte Listener-Regeln, verwendet, die Sie konfigurieren können, um den Datenverkehr an Ihre Ziele weiterzuleiten. Zu den unterstützten Zieltypen gehören EC2 Instances, IP-Adressen, Lambda-Funktionen, Application Load Balancers, Amazon ECS-Aufgaben und Kubernetes Pods. Weitere Informationen finden Sie unter Zielgruppen in VPC Lattice. Sie können einen Service mehreren Servicenetzwerken zuordnen. Das folgende Diagramm zeigt die wichtigsten Komponenten eines typischen Dienstes innerhalb von VPC Lattice.



Sie können einen Dienst erstellen, indem Sie ihm einen Namen und eine Beschreibung geben. Um den Datenverkehr zu Ihrem Dienst zu kontrollieren und zu überwachen, ist es jedoch wichtig, dass Sie Zugriffseinstellungen und Überwachungsdetails angeben. Um Traffic von Ihrem Service an Ihre Ziele weiterzuleiten, müssen Sie einen Listener einrichten und Regeln konfigurieren. Damit der Datenverkehr vom Servicenetzwerk zu Ihrem Service fließen kann, müssen Sie Ihren Service mit dem Service-Netzwerk verknüpfen.

Es gibt ein Leerlauf-Timeout und ein Gesamt-Verbindungs-Timeout für Verbindungen zu Zielen. Das Timeout für Verbindungen im Leerlauf beträgt 1 Minute. Danach wird die Verbindung geschlossen. Die maximale Dauer beträgt 10 Minuten. Danach lassen wir keine neuen Streams über die Verbindung zu und beginnen mit dem Schließen der vorhandenen Streams.

Aufgaben

- Schritt 1: Erstellen Sie einen VPC Lattice-Dienst
- Schritt 2: Routing definieren
- Schritt 3: Netzwerkzuordnungen erstellen
- Schritt 4: Überprüfen und Erstellen

- Zuordnungen für einen VPC Lattice-Dienst verwalten
- Zugriffseinstellungen für einen VPC Lattice-Dienst bearbeiten
- Überwachungsdetails für einen VPC Lattice-Dienst bearbeiten
- Tags für einen VPC Lattice-Dienst verwalten
- Konfigurieren Sie einen benutzerdefinierten Domainnamen für Ihren VPC Lattice-Dienst
- Bringen Sie Ihr eigenes Zertifikat (BYOC) für VPC Lattice mit
- Löschen Sie einen VPC Lattice-Dienst

Schritt 1: Erstellen Sie einen VPC Lattice-Dienst

Erstellen Sie einen grundlegenden VPC Lattice-Dienst mit Zugriffseinstellungen und Überwachungsdetails. Der Dienst ist jedoch erst dann voll funktionsfähig, wenn Sie seine Routing-Konfiguration definieren und ihn einem Servicenetzwerk zuordnen.

Um einen Basisdienst 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 VPC Lattice die Option Services aus.
3. Wählen Sie Create service.
4. Gehen Sie für Identifikatoren wie folgt vor:

   a. Geben Sie einen Namen für den Dienst ein. Der Name muss zwischen 3 und 63 Zeichen lang sein und Kleinbuchstaben, Zahlen und Bindestriche enthalten. Er muss mit einem Buchstaben oder einer Zahl beginnen und enden. Verwenden Sie keine doppelten Bindestriche.

   b. (Optional) Geben Sie eine Beschreibung für das Servicenetzwerk ein. Sie können die Beschreibung während oder nach der Erstellung festlegen oder ändern. Die Beschreibung kann bis zu 256 Zeichen lang sein.
5. Um einen benutzerdefinierten Domainnamen für Ihren Service anzugeben, wählen Sie Benutzerdefinierte Domänenkonfiguration angeben aus und geben Sie den benutzerdefinierten Domainnamen ein.

   Für HTTPS-Listener können Sie das Zertifikat auswählen, das VPC Lattice für die TLS-Terminierung verwendet. Wenn Sie jetzt kein Zertifikat auswählen, können Sie es auswählen, wenn Sie einen HTTPS-Listener für den Dienst erstellen.

Für TCP-Listener müssen Sie einen benutzerdefinierten Domainnamen für Ihren Dienst angeben. Wenn Sie ein Zertifikat angeben, wird es nicht verwendet. Stattdessen führen Sie die TLS-Terminierung in Ihrer Anwendung durch.

6. Wählen Sie für Dienstzugriff die Option Keine aus, wenn Sie möchten, dass Clients in dem mit dem Service VPCs verbundenen Netzwerk auf Ihren Service zugreifen. Um eine Authentifizierungsrichtlinie zur Steuerung des Zugriffs auf den Dienst anzuwenden, wählen Sie AWS IAM. Um eine Ressourcenrichtlinie auf den Dienst anzuwenden, führen Sie für die Authentifizierungsrichtlinie einen der folgenden Schritte aus:
   - Geben Sie eine Richtlinie in das Eingabefeld ein. Wählen Sie beispielsweise Richtlinien, die Sie kopieren und einfügen können, aus.
   - Wählen Sie Richtlinienvorlage anwenden und wählen Sie die Vorlage Authentifizierten und nicht authentifizierten Zugriff zulassen aus. Mit dieser Vorlage kann ein Kunde von einem anderen Konto aus auf den Service zugreifen, indem er entweder die Anfrage signiert (d. h. authentifiziert) oder anonym (d. h. nicht authentifiziert).
   - Wählen Sie Richtlinienvorlage anwenden und wählen Sie die Vorlage Nur authentifizierten Zugriff zulassen aus. Mit dieser Vorlage kann ein Kunde von einem anderen Konto aus nur dann auf den Service zugreifen, wenn er die Anfrage signiert (d. h. authentifiziert).
7. (Optional) Um Zugriffsprotokolle zu aktivieren, schalten Sie den Schalter Zugriffsprotokolle ein und geben Sie wie folgt ein Ziel für Ihre Zugriffsprotokolle an:
   - Wählen Sie CloudWatch Protokollgruppe und wählen Sie eine CloudWatch Protokollgruppe aus. Um eine Protokollgruppe zu erstellen, wählen Sie Protokollgruppe erstellen in CloudWatch.
   - Wählen Sie S3-Bucket aus und geben Sie den S3-Bucket-Pfad einschließlich eines beliebigen Präfixes ein. Um Ihre S3-Buckets zu durchsuchen, wählen Sie Browse S3.
   - Wählen Sie Kinesis Data Firehose Delivery Stream und wählen Sie einen Delivery Stream aus. Um einen Delivery Stream zu erstellen, wählen Sie Create a delivery stream in Kinesis.
8. (Optional) Um Ihren Service mit anderen Konten zu teilen, wählen Sie unter Resource Shares eine AWS RAM Resource Share aus. Um eine Ressourcenfreigabe zu erstellen, wählen Sie in der RAM-Konsole die Option Ressourcenfreigabe erstellen aus.
9. Um Ihre Konfiguration zu überprüfen und den Service zu erstellen, wählen Sie Skip to review and create. Andernfalls wählen Sie Weiter, um die Routing-Konfiguration für Ihren Service zu definieren.

Schritt 2: Routing definieren

Definieren Sie Ihre Routing-Konfiguration mithilfe von Listenern, damit Ihr Service Traffic an die von Ihnen angegebenen Ziele senden kann.

Voraussetzung

Bevor Sie einen Listener hinzufügen können, müssen Sie eine VPC Lattice-Zielgruppe erstellen. Weitere Informationen finden Sie unter the section called “Erstellen einer Zielgruppe”.

Um das Routing für Ihren Service mithilfe der Konsole zu definieren

1. Wählen Sie Add listener (Listener hinzufügen) aus.
2. Für den Listener-Namen können Sie entweder einen benutzerdefinierten Listener-Namen angeben oder das Protokoll und den Port Ihres Listeners als Listener-Namen verwenden. Ein benutzerdefinierter Name, den Sie angeben, kann bis zu 63 Zeichen lang sein und muss für jeden Dienst in Ihrem Konto eindeutig sein. Die gültigen Zeichen sind a-z, 0-9 und Bindestriche (-). Sie können keinen Bindestrich als erstes oder letztes Zeichen oder unmittelbar nach einem anderen Bindestrich verwenden. Sie können den Namen eines Listeners nicht ändern, nachdem Sie ihn erstellt haben.
3. Wählen Sie ein Protokoll und geben Sie dann eine Portnummer ein.
4. Wählen Sie für Standardaktion die VPC Lattice-Zielgruppe aus, die Traffic empfangen soll, und wählen Sie die Gewichtung aus, die dieser Zielgruppe zugewiesen werden soll. Sie können optional eine weitere Zielgruppe für die Standardaktion hinzufügen. Wählen Sie Aktion hinzufügen und wählen Sie dann eine andere Zielgruppe aus und geben Sie deren Gewicht an.
5. (Optional) Um eine weitere Regel hinzuzufügen, wählen Sie Regel hinzufügen und geben Sie dann einen Namen, eine Priorität, eine Bedingung und eine Aktion für die Regel ein.

   Sie können jeder Regel eine Prioritätszahl zwischen 1 und 100 zuweisen. Ein Listener kann nicht über mehrere Regeln mit derselben Priorität verfügen. Regeln werden in der Reihenfolge ihrer Prioritäten bewertet, ausgehend vom niedrigsten Wert hin zum höchsten Wert. Die Standardregel wird zuletzt ausgewertet.

   Geben Sie unter Bedingung ein Pfadmuster für die Pfadübereinstimmungsbedingung ein. Die maximale Größe jeder Zeichenfolge beträgt 200 Zeichen. Beim Vergleich wird nicht zwischen Groß- und Kleinschreibung unterschieden.
6. (Optional) Um Tags hinzuzufügen, erweitern Sie Listener-Tags, wählen Sie Neues Tag hinzufügen aus und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.

7. Um Ihre Konfiguration zu überprüfen und den Service zu erstellen, wählen Sie Skip to review and create. Andernfalls wählen Sie Weiter, um Ihren Dienst einem Servicenetzwerk zuzuordnen.

Schritt 3: Netzwerkzuordnungen erstellen

Ordnen Sie Ihren Dienst einem Servicenetzwerk zu, damit Kunden mit ihm kommunizieren können.

So ordnen Sie mithilfe der Konsole einen Dienst einem Servicenetzwerk zu

1. Wählen Sie für VPC Lattice-Dienstnetzwerke das Dienstnetzwerk aus. Um ein Servicenetzwerk zu erstellen, wählen Sie Create a VPC Lattice network aus. Sie können Ihren Service mehreren Servicenetzwerken zuordnen.
2. (Optional) Um ein Tag hinzuzufügen, erweitern Sie Tags für die Zuordnung von Servicenetzwerken, wählen Sie Neues Tag hinzufügen aus und geben Sie einen Tagschlüssel und einen Tagwert ein.
3. Wählen Sie Weiter aus.

Schritt 4: Überprüfen und Erstellen

Um die Konfiguration zu überprüfen und den Dienst mithilfe der Konsole zu erstellen

1. Überprüfen Sie die Konfiguration für Ihren Dienst.
2. Wählen Sie Bearbeiten, wenn Sie einen Teil der Dienstkonfiguration ändern müssen.
3. Wenn Sie mit der Überprüfung oder Bearbeitung Ihrer Konfiguration fertig sind, wählen Sie Create VPC Lattice service aus.
4. Wenn Sie einen benutzerdefinierten Domänennamen für den Dienst angegeben haben, müssen Sie das DNS-Routing konfigurieren, nachdem der Dienst erstellt wurde. Weitere Informationen finden Sie unter the section called “Konfigurieren Sie einen benutzerdefinierten Domainnamen”.

Zuordnungen für einen VPC Lattice-Dienst verwalten

Wenn Sie einen Dienst mit dem Dienstnetzwerk verknüpfen, ermöglicht es Clients (Ressourcen in einer VPC, die dem Dienstnetzwerk zugeordnet ist), Anfragen an diesen Dienst zu stellen. Sie können Dienste zuordnen, die sich in Ihrem Konto befinden, oder Dienste, die von verschiedenen Konten aus mit Ihnen geteilt wurden. Dieser Schritt ist bei der Erstellung des Dienstes optional. Nach

der Erstellung kann der Dienst jedoch erst dann mit anderen Diensten kommunizieren, wenn Sie ihn einem Dienstnetzwerk zuordnen. Dienstinhaber können ihre Dienste dem Servicenetzwerk zuordnen, wenn ihr Konto über den erforderlichen Zugriff verfügt. Weitere Informationen finden Sie unter So funktioniert VPC Lattice.

Um Dienstnetzwerkzuordnungen mithilfe der Konsole zu verwalten

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Services aus.
3. Wählen Sie den Namen des Dienstes aus, um seine Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Dienstnetzwerkzuordnungen.
5. Gehen Sie wie folgt vor, um eine Zuordnung zu erstellen:
    a. Wählen Sie Verknüpfungen erstellen aus.
    b. Wählen Sie ein Servicenetzwerk aus den VPC Lattice-Dienstnetzwerken aus. Um ein Servicenetzwerk zu erstellen, wählen Sie Create a VPC Lattice network aus.
    c. (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.
    d. Wählen Sie Änderungen speichern aus.
6. Um eine Verbindung zu löschen, aktivieren Sie das Kontrollkästchen für die Zuordnung und wählen Sie dann Aktionen, Netzwerkzuordnungen 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-service-association.

Um eine Dienstnetzwerkverbindung mit dem zu löschen AWS CLI

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

Zugriffseinstellungen für einen VPC Lattice-Dienst bearbeiten

Mit den Zugriffseinstellungen können Sie den Clientzugriff auf einen Dienst konfigurieren und verwalten. Zu den Zugriffseinstellungen gehören der Authentifizierungstyp und die Authentifizierungsrichtlinien. Mithilfe von Authentifizierungsrichtlinien können Sie den Datenverkehr, der zu Diensten innerhalb von VPC Lattice fließt, authentifizieren und autorisieren.

Sie können Authentifizierungsrichtlinien auf Dienstnetzwerkebene, Serviceebene oder auf beiden Ebenen anwenden. Auf der Serviceebene können Dienstinhaber feinkörnige Kontrollen anwenden, die restriktiver sein können. In der Regel werden Authentifizierungsrichtlinien von den Netzwerkbesitzern oder Cloud-Administratoren angewendet. Sie können eine maßgeschneiderte Autorisierung implementieren, die beispielsweise authentifizierte Anrufe innerhalb der Organisation oder anonyme GET-Anfragen, die einer bestimmten Bedingung entsprechen, ermöglicht. Weitere Informationen finden Sie unter Steuern Sie den Zugriff auf VPC Lattice-Dienste mithilfe von Authentifizierungsrichtlinien.

Um Zugriffsrichtlinien mithilfe der Konsole hinzuzufügen oder zu aktualisieren

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Services aus.
3. Wählen Sie den Namen des Dienstes aus, um seine Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Zugriff, um die aktuellen Zugriffseinstellungen zu überprüfen.
5. Um die Zugriffseinstellungen zu aktualisieren, wählen Sie Zugriffseinstellungen bearbeiten.
6. Wenn Sie möchten, dass die Clients VPCs im zugehörigen Servicenetzwerk auf Ihren Service zugreifen, wählen Sie None als Authentifizierungstyp aus.
7. Um eine Ressourcenrichtlinie zur Steuerung des Zugriffs auf den Dienst anzuwenden, wählen Sie AWS IAM als Authentifizierungstyp und gehen Sie für Auth-Richtlinie wie folgt vor:
   - Geben Sie eine Richtlinie in das Eingabefeld ein. Wählen Sie beispielsweise Richtlinien, die Sie kopieren und einfügen können, aus.
   - Wählen Sie Richtlinienvorlage anwenden und wählen Sie die Vorlage Authentifizierten und nicht authentifizierten Zugriff zulassen aus. Mit dieser Vorlage kann ein Kunde von einem anderen Konto aus auf den Service zugreifen, indem er entweder die Anfrage signiert (d. h. authentifiziert) oder anonym (d. h. nicht authentifiziert).
   - Wählen Sie Richtlinienvorlage anwenden und wählen Sie die Vorlage Nur authentifizierten Zugriff zulassen aus. Mit dieser Vorlage kann ein Kunde von einem anderen Konto aus nur dann auf den Service zugreifen, wenn er die Anfrage signiert (d. h. authentifiziert).
8. Wählen Sie Änderungen speichern aus.

Um eine Zugriffsrichtlinie hinzuzufügen oder zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie den put-auth-policy-Befehl.

Überwachungsdetails für einen VPC Lattice-Dienst bearbeiten

VPC Lattice generiert Metriken und Protokolle für jede Anfrage und Antwort, sodass Anwendungen effizienter überwacht und Fehler behoben werden können.

Sie können Zugriffsprotokolle aktivieren und die Zielressource für Ihre Protokolle angeben. VPC Lattice kann Protokolle an die folgenden Ressourcen senden: CloudWatch Protokollgruppen, Firehose-Lieferstreams und S3-Buckets.

Um Zugriffsprotokolle zu aktivieren oder ein Protokollziel mithilfe der Konsole zu aktualisieren

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Services aus.
3. Wählen Sie den Namen des Dienstes aus, um seine Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Überwachung und dann Protokolle aus. Überprüfen Sie die Zugriffsprotokolle, um festzustellen, ob die Zugriffsprotokolle aktiviert sind.
5. Um Zugriffsprotokolle zu aktivieren oder zu deaktivieren, wählen Sie Zugriffsprotokolle bearbeiten und schalten Sie dann den Schalter Zugriffsprotokolle ein oder aus.
6. Wenn Sie Zugriffsprotokolle aktivieren, müssen Sie die Art des Lieferziels auswählen und dann das Ziel für die Zugriffsprotokolle erstellen oder auswählen. Sie können das Lieferziel auch jederzeit ändern. Zum Beispiel:
   - Wählen Sie CloudWatch Protokollgruppe und wählen Sie eine CloudWatch Protokollgruppe aus. Um eine Protokollgruppe zu erstellen, wählen Sie Protokollgruppe erstellen in CloudWatch.
   - Wählen Sie S3-Bucket aus und geben Sie den S3-Bucket-Pfad einschließlich eines beliebigen Präfixes ein. Um Ihre S3-Buckets zu durchsuchen, wählen Sie Browse S3.
   - Wählen Sie Kinesis Data Firehose Delivery Stream und wählen Sie einen Delivery Stream aus. Um einen Delivery Stream zu erstellen, wählen Sie Create a delivery stream in Kinesis.
7. Wählen Sie Änderungen speichern aus.

Um Zugriffsprotokolle zu aktivieren, verwenden Sie AWS CLI

Verwenden Sie den create-access-log-subscription-Befehl.

Um das Protokollziel zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie den update-access-log-subscription-Befehl.

Um Zugriffsprotokolle zu deaktivieren, verwenden Sie AWS CLI

Verwenden Sie den delete-access-log-subscription-Befehl.

Tags für einen VPC Lattice-Dienst verwalten

Mithilfe von Tags können Sie Ihren Service auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung.

Sie können jedem Service mehrere Tags hinzufügen. Tag-Schlüssel müssen für jeden Dienst eindeutig sein. Wenn Sie ein Tag mit einem Schlüssel hinzufügen, der dem Dienst bereits zugeordnet ist, wird der Wert dieses Tags aktualisiert. Sie können Zeichen wie Buchstaben, Leerzeichen, Zahlen (in UTF-8) und die folgenden Sonderzeichen verwenden: + - =. _ : / @. Verwenden Sie keine führenden oder nachgestellten Leerzeichen. Bei Tag-Werten muss die Groß- und Kleinschreibung beachtet werden.

Um Tags mit der Konsole hinzuzufügen oder zu löschen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Services aus.
3. Wählen Sie den Namen des Dienstes aus, um seine Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Tags aus.
5. Um ein Tag hinzuzufügen, wählen Sie Tags hinzufügen und geben Sie den Tag-Schlüssel und den Tag-Wert ein. Zum Hinzufügen eines weiteren Tags wählen Sie Neues Tag hinzufügen erneut aus. Wenn Sie fertig mit dem Hinzufügen der Tags sind, klicken Sie auf Save changes (Änderungen speichern).
6. Um ein Tag zu löschen, aktivieren Sie das Kontrollkästchen für das Tag und wählen Sie Löschen. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

Um Tags hinzuzufügen oder zu löschen, verwenden Sie AWS CLI

Verwenden Sie die Befehle tag-resource und untag-resource.

Konfigurieren Sie einen benutzerdefinierten Domainnamen für Ihren VPC Lattice-Dienst

Wenn Sie einen neuen Dienst erstellen, generiert VPC Lattice einen eindeutigen vollqualifizierten Domänennamen (FQDN) für den Dienst mit der folgenden Syntax.

```
service_name-service_id.partition_id.vpc-lattice-svcs.region.on.aws
```

Die von VPC Lattice bereitgestellten Domainnamen sind für Ihre Benutzer jedoch nicht leicht zu merken. Benutzerdefinierte Domainnamen sind einfacher und intuitiver und können Ihren URLs Benutzern zur Verfügung gestellt werden. Wenn Sie lieber einen benutzerdefinierten Domainnamen für Ihren Service verwenden möchten, z. B. `www.parking.example.com` anstelle des von VPC Lattice generierten DNS-Namens, können Sie ihn bei der Erstellung eines VPC Lattice-Dienstes konfigurieren. Wenn ein Client eine Anfrage mit Ihrem benutzerdefinierten Domainnamen stellt, löst der DNS-Server sie in den von VPC Lattice generierten Domainnamen auf.

Voraussetzungen

- Sie benötigen einen registrierten Domainnamen für Ihren Dienst. Wenn Sie noch keinen registrierten Domainnamen haben, können Sie einen über Amazon Route 53 oder einen anderen kommerziellen Registrar registrieren.
- Um HTTPS-Anfragen zu erhalten, müssen Sie Ihr eigenes Zertifikat angeben. AWS Certificate Manager VPC Lattice unterstützt kein Standardzertifikat als Fallback. Wenn Sie also kein SSL/TLS Zertifikat bereitstellen, das Ihrem benutzerdefinierten Domainnamen entspricht, schlagen alle HTTPS-Verbindungen zu Ihrem benutzerdefinierten Domainnamen fehl. Weitere Informationen finden Sie unter Bringen Sie Ihr eigenes Zertifikat (BYOC) für VPC Lattice mit.

Einschränkungen und Überlegungen

- Sie können nicht mehr als einen benutzerdefinierten Domainnamen für einen Dienst verwenden.
- Sie können den benutzerdefinierten Domainnamen nicht ändern, nachdem Sie den Dienst erstellt haben.
- Der benutzerdefinierte Domainname muss für ein Servicenetzwerk eindeutig sein. Das bedeutet, dass ein Dienst nicht mit einem benutzerdefinierten Domänennamen erstellt werden kann, der bereits (für einen anderen Dienst) im selben Dienstnetzwerk existiert.

Das folgende Verfahren zeigt, wie Sie einen benutzerdefinierten Domainnamen für Ihren Dienst konfigurieren.

AWS Management Console

So konfigurieren Sie einen benutzerdefinierten Domainnamen für Ihren Dienst

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Service aus.
3. Wählen Sie Service erstellen aus. Sie werden zu Schritt 1: Service erstellen weitergeleitet.
4. Wählen Sie im Abschnitt Benutzerdefinierte Domänenkonfiguration die Option Benutzerdefinierte Domänenkonfiguration angeben aus.
5. Geben Sie Ihren benutzerdefinierten Domainnamen ein.
6. Um HTTPS-Anfragen zu bearbeiten, wählen Sie unter Benutzerdefiniertes SSL/TLS Zertifikat das Zertifikat aus, das Ihrem benutzerdefinierten SSL/TLS Domainnamen entspricht. Wenn Sie noch kein Zertifikat haben oder jetzt keines hinzufügen möchten, können Sie bei der Erstellung Ihres HTTPS-Listeners ein Zertifikat hinzufügen. Ohne ein Zertifikat kann Ihr benutzerdefinierter Domainname jedoch keine HTTPS-Anfragen bearbeiten. Weitere Informationen finden Sie unter Hinzufügen eines HTTPS-Listeners.
7. Wenn Sie alle anderen Informationen für die Erstellung des Dienstes hinzugefügt haben, wählen Sie Erstellen aus.

AWS CLI

Um einen benutzerdefinierten Domainnamen für Ihren Service zu konfigurieren

Verwenden Sie den Befehl create-service.

```
aws vpc-lattice create-service --name service_name --custom-domain-
name your_custom_domain_name --type https --certificate-arn arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

Geben Sie im obigen Befehl für `--name` einen Namen für Ihren Dienst ein. Geben Sie für `--custom-domain-name` den Domainnamen Ihres Dienstes ein, `parking.example.com` z. B. Oder `--certificate-arn` geben Sie den ARN Ihres Zertifikats in ACM ein. Das Zertifikat ARN ist in Ihrem Konto unter verfügbar AWS Certificate Manager.

Ordnen Sie Ihrem Dienst einen benutzerdefinierten Domainnamen zu

Registrieren Sie zunächst Ihren benutzerdefinierten Domainnamen, falls Sie dies noch nicht getan haben. Die ICANN (Internet Corporation for Assigned Names and Numbers) verwaltet Domain-Namen im Internet. Sie registrieren einen Domain-Namen über eine Vergabestelle für Domain-Namen, eine von der ICANN autorisierte Organisation, die die Registrierung von Domain-Namen verwaltet. Die Website für Ihre Vergabestelle enthält genaue Anweisungen und Preise für die Registrierung des Domain-Namens. Weitere Informationen finden Sie in den folgenden Ressourcen:

- Um Amazon Route 53 zur Registrierung eines Domain-Namens zu verwenden, siehe Registrieren von Domain-Namen mit Route 53 im Amazon Route 53-Entwicklerhandbuch.
- Eine Liste autorisierter Vergabestellen finden Sie im Accredited Registrar Directory.

Verwenden Sie als Nächstes Ihren DNS-Dienst, z. B. Ihren Domain-Registrar, um einen Datensatz zu erstellen, um Anfragen an Ihren Dienst weiterzuleiten. Weitere Informationen finden Sie in der Dokumentation zu Ihrem DNS-Service. Alternativ dazu können Sie Route 53 als Ihren DNS-Service verwenden.

Wenn Sie Route 53 verwenden, können Sie einen Aliaseintrag oder einen CNAME-Eintrag verwenden, um Anfragen an Ihren Dienst weiterzuleiten. Es wird empfohlen, einen Aliaseintrag zu verwenden, da Sie einen Aliaseintrag am obersten Knoten eines DNS-Namespaces, der auch als Zonen-Apex bezeichnet wird, erstellen können.

Wenn Sie Route 53 verwenden, müssen Sie zunächst eine gehostete Zone erstellen, die Informationen darüber enthält, wie Sie den Verkehr für Ihre Domain im Internet weiterleiten. Nachdem Sie die private oder öffentlich gehostete Zone erstellt haben, erstellen Sie einen Datensatz, sodass Ihr benutzerdefinierter Domainname `parking.example.com` beispielsweise dem automatisch generierten VPC Lattice-Domainnamen zugeordnet wird, zum Beispiel. `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws` Ohne diese Zuordnung funktioniert Ihr benutzerdefinierter Domainname in VPC Lattice nicht.

Die folgenden Verfahren zeigen, wie Sie mithilfe von Route 53 eine private oder öffentliche gehostete Zone erstellen

AWS Management Console

Informationen zum Erstellen eines Aliasdatensatzes für die Weiterleitung von Anfragen an Ihren Service mithilfe von Route 53 finden Sie unter Weiterleiten von Datenverkehr an den Amazon VPC Lattice-Service-Domänenendpunkt.

Verwenden Sie den von VPC Lattice generierten Domainnamen für Ihren Service, z. B. **`my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`** für den Value. Sie finden diesen automatisch generierten Domainnamen in der VPC Lattice-Konsole auf Ihrer Serviceseite.

AWS CLI

Um einen Alias-Datensatz in Ihrer Hosting-Zone zu erstellen

1. Rufen Sie den von VPC Lattice generierten Domainnamen für Ihren Service (z. B.`my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`) und die Hosting-Zonen-ID ab, indem Sie den `get-service` Befehl ausführen.
2. Verwenden Sie den folgenden Befehl, um den Alias festzulegen.

```
aws route53 change-resource-record-sets --hosted-zone-id hosted-zone-id-for-your-service-domain --change-batch file://~/Desktop/change-set.json
```

Erstellen Sie für die `change-set.json` Datei eine JSON-Datei mit dem Inhalt des folgenden JSON-Beispiels und speichern Sie sie auf Ihrem lokalen Computer. Ersetzen Sie *`file://~/Desktop/change-set.json`* den obigen Befehl durch den Pfad der JSON-Datei, die auf Ihrem lokalen Computer gespeichert ist. Beachten Sie, dass „Type“ im folgenden JSON ein A- oder AAAA-Datensatztyp sein kann.

```
{
    "Comment": "my-service-domain.com alias",
    "Changes": [
        {
            "Action": "CREATE",
            "ResourceRecordSet": {
                "Name": "my-custom-domain-name.com",
                "Type": "alias-record-type",
                "AliasTarget": {
                    "HostedZoneId": "hosted-zone-id-for-your-service-domain",
                    "DNSName": "lattice-generated-domain-name",
                    "EvaluateTargetHealth": true
                }
            }
        }
    ]
}
```

Bringen Sie Ihr eigenes Zertifikat (BYOC) für VPC Lattice mit

Um HTTPS-Anfragen bearbeiten zu können, müssen Sie Ihr eigenes SSL/TLS Zertifikat AWS Certificate Manager (ACM) bereithalten, bevor Sie einen benutzerdefinierten Domainnamen einrichten können. Diese Zertifikate müssen einen Subject Alternate Name (SAN) oder Common Name (CN) haben, der dem benutzerdefinierten Domainnamen für Ihren Dienst entspricht. Wenn das SAN vorhanden ist, suchen wir nur nach einer Übereinstimmung in der SAN-Liste. Wenn das SAN nicht vorhanden ist, suchen wir im CN nach einer Übereinstimmung.

VPC Lattice bedient HTTPS-Anfragen mithilfe von Server Name Indication (SNI). DNS leitet die HTTPS-Anfrage auf der Grundlage des benutzerdefinierten Domainnamens und des Zertifikats, das diesem Domainnamen entspricht, an Ihren VPC Lattice-Dienst weiter. Informationen zum Anfordern eines SSL/TLS Zertifikats für einen Domainnamen in ACM oder zum Importieren eines Zertifikats in ACM finden Sie unter Ausstellen und Verwalten von Zertifikaten und Importieren von Zertifikaten im Benutzerhandbuch.AWS Certificate Manager Wenn Sie kein eigenes Zertifikat in ACM anfordern oder importieren können, verwenden Sie den von VPC Lattice generierten Domainnamen und das Zertifikat.

VPC Lattice akzeptiert nur ein benutzerdefiniertes Zertifikat pro Dienst. Sie können jedoch ein benutzerdefiniertes Zertifikat für mehrere benutzerdefinierte Domänen verwenden. Das bedeutet, dass Sie dasselbe Zertifikat für alle VPC Lattice-Dienste verwenden können, die Sie mit einem benutzerdefinierten Domainnamen erstellen.

Um Ihr Zertifikat mit der ACM-Konsole anzuzeigen, öffnen Sie Certificates und wählen Sie Ihre Zertifikat-ID aus. Sie sollten den VPC Lattice-Dienst, der diesem Zertifikat zugeordnet ist, unter Zugeordnete Ressource sehen.

Einschränkungen und Überlegungen

- VPC Lattice ermöglicht Platzhalterübereinstimmungen, die sich eine Ebene tief im Subject Alternate Name (SAN) oder Common Name (CN) des zugehörigen Zertifikats befinden. Dies ist beispielsweise der Fall, wenn Sie einen Dienst mit dem benutzerdefinierten Domainnamen erstellen `parking.example.com` und dem SAN Ihr eigenes Zertifikat zuordnen. `*.example.com` Wenn eine Anfrage eingeht`parking.example.com`, ordnet VPC Lattice das SAN einem beliebigen Domainnamen mit der Apex-Domäne zu. `example.com` Wenn Sie jedoch über die benutzerdefinierte Domäne `parking.different.example.com` und Ihr Zertifikat über das SAN verfügen`*.example.com`, schlägt die Anfrage fehl.

- VPC Lattice unterstützt eine Ebene der Wildcard-Domainübereinstimmung. Das bedeutet, dass ein Platzhalter nur als Subdomain der ersten Ebene verwendet werden kann und dass er nur eine Subdomänenebene schützt. Wenn das SAN Ihres Zertifikats beispielsweise aktiviert ist`*.example.com`, wird es nicht unterstützt. `parking.*.example.com`
- VPC Lattice unterstützt einen Platzhalter pro Domainnamen. Das bedeutet, dass das nicht gültig `*.*.example.com` ist. Weitere Informationen finden Sie im AWS Certificate Manager Benutzerhandbuch unter Anfordern eines öffentlichen Zertifikats.
- VPC Lattice unterstützt nur Zertifikate mit 2048-Bit-RSA-Schlüsseln.
- Das SSL/TLS Zertifikat in ACM muss sich in derselben Region befinden wie der VPC Lattice-Dienst, dem Sie es zuordnen.

Sicherung des privaten Schlüssels Ihres Zertifikats

Wenn Sie mit ACM ein SSL/TLS Zertifikat anfordern, generiert ACM ein public/private key pair. Das Schlüsselpaar wird beim Import eines Zertifikats generiert. Der öffentliche Schlüssel wird Teil des Zertifikats. Um den privaten Schlüssel sicher zu speichern, erstellt ACM einen weiteren Schlüssel, den so genannten KMS-Schlüssel AWS KMS, mit dem Alias aws/acm. AWS KMS verwendet diesen Schlüssel, um den privaten Schlüssel Ihres Zertifikats zu verschlüsseln. Weitere Informationen finden Sie unter Datenschutz im AWS Certificate Manager des AWS Certificate Manager -Benutzerhandbuchs.

VPC Lattice verwendet AWS TLS Connection Manager, einen Dienst, auf den nur Sie zugreifen können AWS-Services, um die privaten Schlüssel Ihres Zertifikats zu sichern und zu verwenden. Wenn Sie Ihr ACM-Zertifikat verwenden, um einen VPC Lattice-Dienst zu erstellen, ordnet VPC Lattice Ihr Zertifikat dem TLS Connection Manager zu. AWS Dazu erstellen wir einen Zuschuss für Ihren verwalteten Schlüssel. AWS KMS AWS Dieser Zuschuss ermöglicht es dem TLS Connection Manager AWS KMS , den privaten Schlüssel Ihres Zertifikats zu entschlüsseln. Der TLS-Verbindungsmanager verwendet das Zertifikat und den entschlüsselten privaten Schlüssel (Klartext), um eine sichere Verbindung (SSL/TLS-Sitzung) mit Clients von VPC Lattice-Diensten herzustellen. Wenn das Zertifikat von einem VPC Lattice-Dienst getrennt wird, wird der Grant zurückgezogen. Weitere Informationen finden Sie unter Berechtigungen im AWS Key Management Service -Entwicklerhandbuch.

Weitere Informationen finden Sie unter Verschlüsselung im Ruhezustand.

Löschen Sie einen VPC Lattice-Dienst

Um einen VPC Lattice-Dienst zu löschen, müssen Sie zunächst alle Verknüpfungen löschen, die der Dienst möglicherweise zu einem beliebigen Dienstnetzwerk hat. Wenn Sie einen Dienst löschen, werden auch alle Ressourcen gelöscht, die sich auf den Dienst beziehen, z. B. die Ressourcenrichtlinie, die Authentifizierungsrichtlinie, Listener, Listener-Regeln und Zugriffsprotokollabonnements.

Um einen Dienst 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 VPC Lattice die Option Service aus.
3. Wählen Sie auf der Seite Dienste den Service aus, den Sie löschen möchten, und klicken Sie dann auf Aktionen, Dienst löschen.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

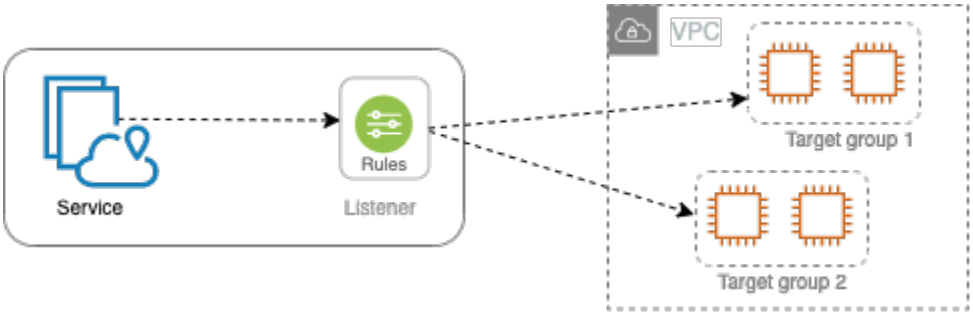
Um einen Dienst mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-service.

Zielgruppen in VPC Lattice

Eine VPC Lattice-Zielgruppe ist eine Sammlung von Zielen oder Rechenressourcen, auf denen Ihre Anwendung oder Ihr Dienst ausgeführt wird. Zu den unterstützten Zieltypen gehören EC2 Instances, IP-Adressen, Lambda-Funktionen, Application Load Balancers, Amazon ECS-Aufgaben und Kubernetes Pods. Sie können Ihren Zielgruppen auch bestehende Dienste zuordnen. Weitere Informationen zur Verwendung von Kubernetes mit VPC Lattice finden Sie im AWS Gateway API Controller User Guide.

Jede Zielgruppe wird verwendet, um Anfragen an ein oder mehrere registrierte Ziele weiterzuleiten. Wenn Sie eine Listener-Regel erstellen, geben Sie eine Zielgruppe und Bedingungen an. Wenn die Bedingung einer Regel erfüllt ist, wird der Datenverkehr an die entsprechende Zielgruppe weitergeleitet. Sie können unterschiedliche Zielgruppen für verschiedene Arten von Anfragen erstellen. Erstellen Sie beispielsweise eine Zielgruppe für allgemeine Anfragen und andere Zielgruppen für Anfragen, die bestimmte Regelbedingungen wie einen Pfad oder einen Header-Wert enthalten.



Sie definieren Zustandsprüfungseinstellungen für Ihren Service auf der Basis der einzelnen Zielgruppen. Jede Zielgruppe verwendet die standardmäßigen Zustandsprüfungseinstellungen, es sei denn, Sie überschreiben diese, wenn Sie die Zielgruppe erstellen, oder ändern sie später. Nachdem Sie eine Zielgruppe in einer Regel für einen Listener angegeben haben, überwacht der Dienst kontinuierlich den Zustand aller mit der Zielgruppe registrierten Ziele. Der Service leitet Anforderungen an die registrierten Ziele weiter, die in Ordnung sind.

Um eine Zielgruppe in einer Regel für einen Service-Listener anzugeben, muss sich die Zielgruppe im gleichen Konto wie der Dienst befinden.

Die Zielgruppen von VPC Lattice ähneln den Zielgruppen von Elastic Load Balancing, sind jedoch nicht austauschbar.

Inhalt

- Erstellen einer VPC-Lattice-Zielgruppe
- Registrieren von Zielen für eine VPC-Lattice-Zielgruppe
- Zustandsprüfungen für Ihre VPC Lattice-Zielgruppen
- Weiterleitungskonfiguration
- Weiterleitungsalgorithmus
- Zieltyp
- IP-Adresstyp
- HTTP-Ziele in VPC Lattice
- Lambda-Funktionen als Ziele in VPC Lattice
- Application Load Balancers als Ziele in VPC Lattice
- Protokollversion
- Tags für Ihre VPC Lattice-Zielgruppe
- Eine VPC-Lattice-Zielgruppe löschen

Erstellen einer VPC-Lattice-Zielgruppe

Sie registrieren Ihre Ziele bei einer Zielgruppe. Standardmäßig sendet der VPC Lattice-Dienst Anfragen an registrierte Ziele unter Verwendung des Ports und Protokolls, die Sie für die Zielgruppe angegeben haben. Sie können diesen Port überschreiben, wenn Sie jedes Ziel bei der Zielgruppe registrieren.

Um Datenverkehr an die Ziele in einer Zielgruppe weiterzuleiten, geben Sie die Zielgruppe in einer Aktion an, wenn Sie einen Listener erstellen oder eine Regel für den Listener erstellen. Weitere Informationen finden Sie unter Listener-Regeln für Ihren VPC Lattice-Service. Sie können dieselbe Zielgruppe in mehreren Listenern angeben, aber diese Listener müssen demselben Service angehören. Um eine Zielgruppe mit einem Dienst zu verwenden, müssen Sie sicherstellen, dass die Zielgruppe nicht von einem Listener verwendet wird, der einem anderen Dienst angehört.

Sie können jederzeit Ziele zu Ihrer Zielgruppe hinzufügen oder aus dieser entfernen. Weitere Informationen finden Sie unter Registrieren von Zielen für eine VPC-Lattice-Zielgruppe. Sie können auch die Zustandsprüfungseinstellungen für Ihre Zielgruppe ändern. Weitere Informationen finden Sie unter Zustandsprüfungen für Ihre VPC Lattice-Zielgruppen.

Erstellen einer Zielgruppe

Sie können eine Zielgruppe erstellen und optional Ziele registrieren.

Erstellen einer Zielgruppe mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Zielgruppen aus.
3. Wählen Sie Zielgruppe erstellen aus.
4. Führen Sie unter Wählen Sie einen Zieltyp aus einen der folgenden Schritte aus:
   - Wählen Sie Instances, um Ziele nach Instance-ID zu registrieren.
   - Wählen Sie IP-Adressen, um Ziele anhand der IP-Adresse zu registrieren.
   - Wählen Sie Lambda-Funktion, um eine Lambda-Funktion als Ziel zu registrieren.
   - Wählen Sie Application Load Balancer, um einen Application Load Balancer als Ziel zu registrieren.
5. Geben Sie unter Zielgruppenname einen Namen für die Zielgruppe ein. Dieser Name muss für Ihr Konto in jeder AWS Region eindeutig sein, darf maximal 32 Zeichen lang sein, darf nur alphanumerische Zeichen oder Bindestriche enthalten und darf nicht mit einem Bindestrich beginnen oder enden.
6. Für Protokoll und Port können Sie die Standardwerte nach Bedarf ändern. Das Standardprotokoll ist HTTPS und der Standardport ist 443.

   Wenn der Zieltyp eine Lambda-Funktion ist, können Sie weder ein Protokoll noch einen Port angeben.
7. Wählen Sie für den IP-Adresstyp aus IPv4, ob Ziele mit IPv4 Adressen registriert werden IPv6sollen oder ob Ziele mit IPv6 Adressen registriert werden sollen. Sie können diese Einstellung nicht ändern, nachdem die Zielgruppe erstellt wurde.

   Diese Option ist nur verfügbar, wenn der Zieltyp IP-Adressen ist.
8. Wählen Sie im Feld VPC eine Virtual Private Cloud (VPC) aus.

   Diese Option ist nicht verfügbar, wenn der Zieltyp eine Lambda-Funktion ist.
9. Ändern Sie für die Protokollversion den Standardwert nach Bedarf. Der Standardwert ist HTTP1.

   Diese Option ist nicht verfügbar, wenn der Zieltyp eine Lambda-Funktion ist.

10. Ändern Sie für Zustandsprüfungen die Standardeinstellungen nach Bedarf. Weitere Informationen finden Sie unter Zustandsprüfungen für Ihre VPC Lattice-Zielgruppen.

    Integritätsprüfungen sind nicht verfügbar, wenn der Zieltyp eine Lambda-Funktion ist.

11. Wählen Sie für die Version der Lambda-Ereignisstruktur eine Version aus. Weitere Informationen finden Sie unter the section called “Empfangen von Ereignissen vom VPC Lattice-Dienst”.

    Diese Option ist nur verfügbar, wenn der Zieltyp eine Lambda-Funktion ist

12. (Optional) Fügen Tags hinzu, indem Sie Tags auswählen, Neuen Tag hinzufügen auswählen und den Tag-Schlüssel und -Wert eingeben.
13. Wählen Sie Weiter aus.
14. Für Ziele registrieren können Sie diesen Schritt entweder überspringen oder Ziele wie folgt hinzufügen:
    - Wenn der Zieltyp Instances ist, wählen Sie die Instances aus, geben Sie die Ports ein und wählen Sie dann Schließen Sie die unten angeführten als ausstehend ein.
    - Wenn der Zieltyp IP-Adressen lautet, gehen Sie wie folgt vor:
        a. Behalten Sie unter Netzwerk auswählen die VPC bei, die Sie für die Zielgruppe ausgewählt haben, oder wählen Sie Andere private IP-Adresse.
        b. Geben Sie unter Ports angeben IPs und definieren die IP-Adresse ein und geben Sie die Ports ein. Der Standard-Port ist der Zielgruppenport.
        c. Wählen Sie Schließen Sie die unten angeführten als ausstehend ein aus.
    - Wenn der Zieltyp eine Lambda-Funktion ist, wählen Sie eine Lambda-Funktion aus. Um eine Lambda-Funktion zu erstellen, wählen Sie Neue Lambda-Funktion erstellen.
    - Wenn der Zieltyp ein Application Load Balancer ist, wählen Sie einen Application Load Balancer aus. Um einen Application Load Balancer zu erstellen, wählen Sie Application Load Balancer erstellen.
15. Wählen Sie Zielgruppe erstellen aus.

    Es kann einige Minuten dauern, bis VPC Lattice die Ziele registriert. Weitere Informationen finden Sie unter Warum dauert es so lange, bis meine DNS-Änderungen in Route 53 und öffentlichen Resolvern verbreitet werden?

Erstellen einer Zielgruppe mithilfe der AWS CLI

Verwenden Sie den create-target-groupBefehl, um die Zielgruppe zu erstellen, und den Befehl register-targets, um Ziele hinzuzufügen.

Gemeinsam genutzte Subnetze

Teilnehmer können VPC Lattice-Zielgruppen in einer freigegebenen VPC erstellen. Die folgenden Regeln gelten für gemeinsam genutzte Subnetze:

- Alle Teile eines VPC Lattice-Dienstes, wie Listener, Zielgruppen und Ziele, müssen mit demselben Konto erstellt werden. Sie können in Subnetzen erstellt werden, die dem Eigentümer des VPC Lattice-Dienstes gehören oder mit diesem gemeinsam genutzt werden.
- Die für eine Zielgruppe registrierten Ziele müssen mit demselben Konto wie die Zielgruppe erstellt werden.
- Nur der Besitzer einer VPC kann die VPC einem Servicenetzwerk zuordnen. Teilnehmerressourcen in einer gemeinsam genutzten VPC, die einem Servicenetzwerk zugeordnet ist, können Anforderungen an Services senden, die dem Servicenetzwerk zugeordnet sind. Der Administrator kann dies jedoch mithilfe von Sicherheitsgruppen ACLs, Netzwerk- oder Authentifizierungsrichtlinien verhindern.

Weitere Informationen über gemeinsam nutzbare Ressourcen für VPC Lattice finden Sie unter. VPC Lattice-Entitäten teilen

Registrieren von Zielen für eine VPC-Lattice-Zielgruppe

Ihr Service dient als zentraler Kontaktpunkt für Kunden und verteilt den eingehenden Datenverkehr an die fehlerfreien registrierten Ziele. Sie können jedes Ziel bei einer oder mehreren Zielgruppen registrieren.

Wenn die Nachfrage nach Ihrer Anwendung steigt, können Sie zusätzliche Ziele mit einer oder mehreren Zielgruppen registrieren, um die Nachfrage zu bewältigen. Der Service beginnt mit dem Routing von Anfragen an ein neu registriertes Ziel, sobald der Registrierungsprozess abgeschlossen ist und das Ziel die anfänglichen Zustandsprüfungen bestanden hat.

Wenn die Nachfrage nach Ihrer Anwendung sinkt oder Sie Ihre Ziele warten müssen, können Sie die Registrierung von Zielen bei Ihren Zielgruppen aufheben. Bei der Aufhebung der Registrierung eines Ziels wird es aus Ihrer Zielgruppe entfernt. Ansonsten hat dies keine Auswirkungen auf das Ziel. Der Service beendet das Routing von Anforderungen an ein Ziel, sobald es abgemeldet wird. Das Ziel

wechselt in den Zustand `DRAINING`, bis laufende Anfragen abgeschlossen wurden. Sie können das Ziel erneut bei der Zielgruppe registrieren, wenn es bereit ist, wieder Anfragen zu erhalten.

Der Zieltyp der Zielgruppe legt fest, wie Sie Ziele bei dieser Zielgruppe registrieren. Weitere Informationen finden Sie unter Zieltyp.

Verwenden Sie die folgenden Konsolenprozeduren, um Ziele zu registrieren oder deren Registrierung aufzuheben. Verwenden Sie alternativ die Befehle register-targets und deregister-targets aus dem. AWS CLI

Inhalt

- Ziele nach Instance-ID registrieren oder die Registrierung aufheben
- Ziele nach IP-Adresse registrieren oder die Registrierung aufheben
- Registrieren und Aufheben der Registrierung einer Lambda-Funktion
- Einen Application Load Balancer registrieren oder aufheben der Registrierung eines Application Load Balancer

Ziele nach Instance-ID registrieren oder die Registrierung aufheben

Die Zielinstanzen müssen sich in der Virtual Private Cloud (VPC) befinden, die Sie für die Zielgruppe angegeben haben. Die Instance muss sich auch im Status `running` befinden, wenn Sie sie registrieren.

Wenn Sie Ziele nach Instance-ID registrieren, können Sie Ihren Service mit einer Auto-Scaling-Gruppe verwenden. Nachdem Sie eine Zielgruppe einer Auto-Scaling-Gruppe zugeordnet haben und die Gruppe hochskaliert wird, werden die Instances, die die Auto-Scaling-Gruppe startet, automatisch bei der Zielgruppe registriert. Wenn Sie die Zielgruppe von der Auto-Scaling-Gruppe trennen, wird die Registrierung der Instances bei der Zielgruppe automatisch aufgehoben. Weitere Informationen finden Sie unter Weiterleitung des Datenverkehrs zu Ihrer Auto-Scaling-Gruppe mit einer VPC-Lattice-Zielgruppe im Benutzerhandbuch zu Amazon EC2 Auto Scaling.

So verfahren Sie zum Registrieren oder Aufheben der Registrierung von Zielen nach Instance-ID mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Zielgruppen aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.

4. Wählen Sie die Registerkarte Ziele.
5. Um Instances zu registrieren, wählen Sie Ziele registrieren. Wählen Sie die Instances aus, geben Sie den Instance-Instance-Standardport ein und wählen Sie dann Schließen Sie die unten angeführten als ausstehend ein. Wenn Sie mit dem Hinzufügen der Instances fertig sind, wählen Sie Ziele registrieren.
6. Um die Registrierung von Instances aufzuheben, wählen Sie die Instances aus und klicken Sie dann auf Abmelden.

Ziele nach IP-Adresse registrieren oder die Registrierung aufheben

Die Ziel-IP-Adressen müssen aus den Subnetzen der VPC stammen, die Sie für die Zielgruppe angegeben haben. Sie können die IP-Adressen eines anderen Dienstes nicht in derselben VPC registrieren. Sie können keine VPC-Endpoints oder öffentlich weiterleitungsfähigen IP-Adressen registrieren.

So verfahren Sie zum Registrieren oder Aufheben der Registrierung von Zielen nach IP-Adresse mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Zielgruppen aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Ziele.
5. Um IP-Adressen zu registrieren, wählen Sie Ziele registrieren. Wählen Sie für jede IP-Adresse das Netzwerk, die IP-Adresse und den Port aus und wählen Sie dann Schließen Sie die unten angeführten als ausstehend ein aus. Wenn Sie die Eingabe der Adressen abgeschlossen haben, wählen Sie Ziele registrieren.
6. Um die Registrierung von IP-Adressen aufzuheben, wählen Sie die IP-Adressen aus und klicken Sie dann auf Abmelden.

Registrieren und Aufheben der Registrierung einer Lambda-Funktion

Sie können eine einzelne Lambda-Funktion für die Zielgruppe registrieren. Wenn Sie zu Ihrer Lambda-Funktion keinen Datenverkehr mehr senden müssen, können Sie ihre Registrierung aufheben. Nachdem Sie die Registrierung einer Lambda-Funktion aufgehoben haben, schlagen

laufende Anfragen mit HTTP-5XX-Fehlermeldungen fehl. Es ist besser, eine neue Zielgruppe zu erstellen, anstatt die Lambda-Funktion für eine Zielgruppe zu ersetzen.

So verfahren Sie zum Registrieren und Aufheben der Registrierung einer Lambda-Funktion mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Zielgruppen aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Ziele.
5. Wenn keine Lambda-Funktion registriert ist, wählen Sie Ziel registrieren. Wählen Sie die Lambda-Funktion aus und wählen Sie Ziel registrieren.
6. Um die Registrierung einer Lambda-Funktion aufzuheben, wählen Sie Deregister (Registrierung aufheben). Wenn Sie zur Bestätigung aufgefordert werden, geben Sie ein **`confirm`** und wählen Sie dann Abmelden.

Einen Application Load Balancer registrieren oder aufheben der Registrierung eines Application Load Balancer

Sie können für jede Zielgruppe einen einzelnen Application Load Balancer registrieren. Wenn Sie keinen Datenverkehr mehr an Ihren Load Balancer senden müssen, können Sie ihn abmelden. Nachdem Sie einen Load Balancer deregistriert haben, schlagen In-Flight-Anfragen mit HTTP 5XX-Fehlern fehl. Es ist besser, eine neue Zielgruppe zu erstellen, anstatt den Application Load Balancer für eine Zielgruppe zu ersetzen.

So registrieren oder melden Sie einen Application Load Balancer mithilfe der Konsole an oder abmelden

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Zielgruppen aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Ziele.
5. Wenn kein Application Load Balancer registriert ist, wählen Sie Ziel registrieren. Wählen Sie den Application Load Balancer und anschließend Ziel registrieren aus.

6. Um die Registrierung eines Application Load Balancer aufzuheben, wählen Sie Deregister. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie ein **`confirm`** und wählen Sie dann Abmelden.

Zustandsprüfungen für Ihre VPC Lattice-Zielgruppen

Ihr Service sendet regelmäßig Anforderungen an die registrierten Ziele, um deren Status zu überprüfen. Diese Tests werden als Zustandsprüfungen bezeichnet.

Jeder VPC Lattice-Dienst leitet Anfragen nur an die fehlerfreien Ziele weiter. Jeder Service überprüft den Zustand jedes Ziels und verwendet dabei die Einstellungen für die Integritätsprüfung der Zielgruppen, bei denen das Ziel registriert ist. Nachdem Ihr Ziel registriert wurde, muss es die Zustandsprüfung fehlerfrei bestehen, um als stabil eingestuft zu werden. Nach Abschluss jeder Zustandsprüfung schließt der Dienst die Verbindung, die für die Zustandsprüfung hergestellt wurde.

Einschränkungen und Überlegungen

- Bei der Version des Zielgruppenprotokolls sind Integritätsprüfungen standardmäßig aktiviert. HTTP1
- Wenn die Zielgruppenprotokollversion ist HTTP2, sind Integritätsprüfungen standardmäßig nicht aktiviert. Sie können jedoch Integritätsprüfungen aktivieren und die Protokollversion manuell auf HTTP1 oder festlegen HTTP2.
- Health Checks unterstützen keine gRPC-Zielgruppen-Protokollversionen. Wenn Sie jedoch Integritätsprüfungen aktivieren, müssen Sie die Protokollversion für die Integritätsprüfung als HTTP1 oder HTTP2 angeben.
- Gesundheitschecks unterstützen keine Lambda-Zielgruppen.
- Health Checks unterstützen keine Application Load Balancer Balancer-Zielgruppen. Sie können jedoch mithilfe von Elastic Load Balancing Integritätsprüfungen für die Ziele Ihres Application Load Balancer aktivieren. Weitere Informationen finden Sie unter Zustandsprüfungen für Zielgruppen im Benutzerhandbuch für Application Load Balancers.

Zustandsprüfungseinstellungen

Sie können Zustandsprüfungen für die Ziele in einer Zielgruppe konfigurieren, wie in der folgenden Tabelle beschrieben. Die in der Tabelle verwendeten Einstellungsnamen sind die in der API verwendeten Namen. Der Dienst sendet unter Verwendung des angegeben Ports, Protokolls und

Ping-Pfads alle HealthCheckIntervalSecondsSekunden eine Zustandsprüfungs-Anforderung an jedes registrierte Ziel. Jede Anfrage nach einer Zustandsprüfung ist unabhängig und das Ergebnis hält über das gesamte Intervall an. Die Zeit, die das Ziel für die Antwort benötigt, hat keinen Einfluss auf das Intervall für die nächste Anfrage zur Zustandsprüfung. Wenn die Zustandsprüfungen UnhealthyThresholdCountaufeinanderfolgende Fehler überschreiten, nimmt der Dienst das Ziel aus dem Verkehr. Wenn die Zustandsprüfungen HealthyThresholdCountaufeinanderfolgende Erfolge überschreiten, nimmt der Dienst das Ziel wieder in Betrieb.

Einstellung	Beschreibung
HealthCheckProtocol	Das Protokoll, das der Service für die Zustandsprüfungen der Ziele verwendet. Möglichen Protokolle sind HTTP und HTTPS. Das Standardprotokoll ist HTTP.
HealthCheckPort	Der Port, den der Service für die Zustandsp rüfungen der Ziele verwendet. Standardmäßig wird der Port verwendet, auf dem jedes Ziel Datenverkehr vom Service empfängt.
HealthCheckPath	Das Ziel für Zustandsprüfungen der Ziele. Wenn die Protokollversion HTTP1 oder ist HTTP2, geben Sie einen gültigen URI an (/ Pfad? abfragen). Der Standardwert ist /.
HealthCheckTimeoutSeconds	Die Anzahl der Sekunden, in denen keine Antwort von einem Ziel bedeutet, dass die Zustandsprüfung fehlgeschlagen ist. Der Bereich liegt zwischen 1 und 120 Sekunden. Die Standardeinstellung ist 5 Sekunden, wenn der Zieltyp `INSTANCE` oder `IP` ist. Geben Sie 0 an, um diese Einstellung auf den Standardwert zurückzusetzen.
HealthCheckIntervalSeconds	Der etwaige Zeitraum in Sekunden zwischen den Zustandsprüfungen der einzelnen Ziele. Der Bereich liegt zwischen 5 und

Einstellung	Beschreibung
	300 Sekunden. Der Standardwert beträgt 30 Sekunden, wenn der Zieltyp `INSTANCE` oder ist`IP`. Geben Sie 0 an, um diese Einstellung auf den Standardwert zurückzusetzen.
HealthyThresholdCount	Die Anzahl der fortlaufenden erfolgreichen Zustandsprüfungen, die erforderlich sind, bevor ein fehlerhaftes Ziel als fehlerhaften Zustand bezeichnet wird. Der Bereich liegt zwischen 2 und 10. Der Standardwert ist 5. Geben Sie 0 an, um diese Einstellung auf den Standardwert zurückzusetzen.
UnhealthyThresholdCount	Die Anzahl der aufeinanderfolgenden Fehler bei der Zustandsprüfung, die erforderlich sind, bevor ein Ziel als fehlerhaft betrachtet wird. Der Bereich liegt zwischen 2 und 10. Der Standardwert ist 2. Geben Sie 0 an, um diese Einstellung auf den Standardwert zurückzus etzen.

Einstellung	Beschreibung
Matcher	Die Codes, die verwendet werden, um ein Ziel auf eine erfolgreiche Antwort zu überprüfen. Diese werden in der Konsole als Erfolgscodes bezeichnet. Wenn die Protokollversion HTTP1 oder ist HTTP2, liegen die möglichen Werte zwischen 200 und 499. Sie können mehrere Werte angeben (z. B. "200,202") oder einen Wertebereich (z. B. "200-299"). Der Standardwert ist 200. Die Health Check-Protokollversion für gRPC wird derzeit nicht unterstützt. Wenn Ihre Zielgruppen-Protokollversion jedoch gRPC ist, können Sie in Ihrer Health Check-Konfiguration HTTP1 oder HTTP2 Protokollversionen angeben.

Zustand der Ziele prüfen

Sie können den Zustand der Ziele, die in Ihren Zielgruppen registriert sind, überprüfen.

Überprüfen des Zustands Ihrer Ziele mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Zielgruppen aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. In der Registerkarte Ziele gibt die Spalte Zustandsstatus den Status der einzelnen Ziele wider. Wenn der Status einen anderen Wert als hat`Healthy`, enthält die Spalte Zustandstatusdetails weitere Informationen.

So überprüfen Sie den Zustand Ihrer Ziele mithilfe der AWS CLI

Verwenden Sie den Befehl list-targets. Die Ausgabe dieses Befehls enthält den Zustand des Ziels. Wenn der Status einen anderen Wert als `Healthy` aufweist, enthält die Ausgabe auch einen Ursachencode.

So erhalten Sie E-Mail-Benachrichtigungen über fehlerhafte Ziele

Verwenden Sie CloudWatch Alarme, um eine Lambda-Funktion zu starten, die Details zu fehlerhaften Zielen sendet.

Einstellungen für die Zustandsprüfung ändern

Sie können die Zustandsprüfungseinstellungen für Ihre Zielgruppe jederzeit ändern.

So ändern Sie die Einstellungen für die Zustandsprüfung mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Zielgruppen aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Integritätsprüfungen im Abschnitt Einstellungen Health Integritätsprüfungen die Option Bearbeiten aus.
5. Ändern Sie die Einstellungen für die Zustandsprüfung nach Bedarf.
6. Wählen Sie Änderungen speichern aus.

So ändern Sie die Einstellungen für die Zustandsprüfung mithilfe der AWS CLI

Verwenden Sie den update-target-group-Befehl.

Weiterleitungskonfiguration

Standardmäßig leitet ein Service Anforderungen an seine Ziele über das Protokoll und die Port-Nummer weiter, die Sie bei der Erstellung der Zielgruppe angegeben haben. Alternativ können Sie den für Weiterleitung von Datenverkehr zu einem Ziel verwendeten Port überschreiben, wenn Sie es bei der Zielgruppe registrieren.

Zielgruppen unterstützen die folgenden Protokolle und Ports:

- Protokolle: HTTP, HTTPS, TCP

- Ports: 1-65535

Wenn eine Zielgruppe mit dem HTTPS-Protokoll konfiguriert ist oder HTTPS-Zustandsprüfungen verwendet, verwenden TLS-Verbindungen zu den Zielen die Sicherheitsrichtlinie des Listeners. VPC Lattice stellt TLS-Verbindungen mit den Zielen her, wobei er die auf den Zielen installierten Zertifikate verwendet. VPC Lattice validiert diese Zertifikate nicht. Daher können Sie selbstsignierte Zertifikate oder Zertifikate verwenden, die abgelaufen sind. Der Datenverkehr zwischen VPC Lattice und den Zielen wird auf Paketebene authentifiziert, sodass kein Risiko von man-in-the-middle Angriffen oder Spoofing besteht, selbst wenn die Zertifikate auf den Zielen nicht gültig sind.

TCP-Zielgruppen werden nur mit TLS-Listenern unterstützt.

Weiterleitungsalgorithmus

Standardmäßig wird der Round-Robin-Routing-Algorithmus verwendet, um Anforderungen an fehlerfreie Ziele weiterzuleiten.

Wenn der VPC Lattice-Dienst eine Anfrage empfängt, verwendet er den folgenden Prozess:

1. Wertet die Listener-Regeln in der Reihenfolge ihrer Priorität aus, um zu bestimmen, welche Regel angewendet werden soll.
2. Wählt unter Verwendung des standardmäßigen Round-Robin-Algorithmus ein Ziel aus der Zielgruppe für die Regelaktion aus. Die Weiterleitung erfolgt unabhängig für jede Zielgruppe, auch wenn ein Ziel bei mehreren Zielgruppen registriert ist.

Wenn eine Zielgruppe nur fehlerhafte Ziele enthält, werden die Anfragen an alle Ziele weitergeleitet, unabhängig von ihrem Zustand. Das bedeutet, dass sich der VPC-Lattice-Service nicht öffnen lässt, wenn alle Ziele gleichzeitig die Zustandsprüfungen nicht bestehen. Das Fail-Open hat zur Folge, dass der Datenverkehr an alle Ziele unabhängig von deren Zustandsstatus auf der Grundlage des Round-Robin-Algorithmus aktiviert wird.

Zieltyp

Wenn Sie eine Zielgruppe erstellen, legen Sie ihren Zieltyp fest, wodurch festgelegt wird, welchen Zieltyp Sie beim Registrieren von Zielen bei dieser Zielgruppe angeben. Nachdem Sie eine Zielgruppe erstellt haben, können Sie ihren Zieltyp nicht mehr ändern.

Die folgenden Zieltypen sind möglich:

`INSTANCE`

Die Ziele werden nach Instance-ID angegeben.

`IP`

Die Ziele sind IP-Adressen.

`LAMBDA`

Das Ziel ist eine Lambda-Funktion.

`ALB`

Das Ziel ist ein Application Load Balancer.

Überlegungen

- Wenn der Zieltyp ist`IP`, müssen Sie IP-Adressen aus den Subnetzen der VPC für die Zielgruppe angeben. Wenn Sie IP-Adressen von außerhalb dieser VPC registrieren müssen, erstellen Sie eine Zielgruppe vom Typ `ALB` und registrieren Sie die IP-Adressen beim Application Load Balancer.
- Wenn der Zieltyp ist`IP`, können Sie keine VPC-Endpunkte oder öffentlich routbare IP-Adressen registrieren.
- Wenn der Zieltyp lautet`LAMBDA`, können Sie eine einzelne Lambda-Funktion registrieren. Wenn der Dienst eine Anfrage für die Lambda-Funktion erhält, ruft er die Lambda-Funktion auf. Wenn Sie mehrere Lambda-Funktionen für einen Dienst registrieren möchten, müssen Sie mehrere Zielgruppen verwenden.
- Wenn der Zieltyp ist`ALB`, können Sie einen einzelnen internen Application Load Balancer als Ziel für bis zu zwei VPC-Lattice-Services registrieren. Registrieren Sie dazu den Application Load Balancer bei zwei separaten Zielgruppen, die von zwei verschiedenen VPC-Lattice-Diensten verwendet werden. Darüber hinaus muss der angezielte Application Load Balancer mindestens einen Listener haben, dessen Port mit dem Zielgruppenport übereinstimmt.
- Sie können Ihre ECS-Aufgaben beim Start automatisch für eine VPC Lattice-Zielgruppe registrieren. Die Zielgruppe muss den Zieltyp aufweisen`IP`. Weitere Informationen finden Sie unter Verwenden von VPC Lattice mit Ihren Amazon ECS-Services im Developerhandbuch zum Amazon Elastic Container Service.

  Alternativ können Sie den Application Load Balancer für Ihren Amazon ECS-Service mit einer Zielgruppe vom Typ VPC Lattice registrieren. `ALB` Weitere Informationen finden Sie unter

Verwenden des Load-Balancings zur Verteilung des Datenverkehrs im Amazon Elastic Container Service-Entwicklerhandbuch.

- Um einen EKS-Pod als Ziel zu registrieren, verwenden Sie den AWS Gateway API Controller, der die IP-Adressen vom Kubernetes-Service bezieht.
- Wenn das Zielgruppenprotokoll TCP ist, sind die einzigen unterstützten Zieltypen `INSTANCE` und`IP`.

IP-Adresstyp

Wenn Sie eine Zielgruppe mit dem Zieltyp von erstellen`IP`, können Sie einen IP-Adresstyp für die Zielgruppe angeben. Dies gibt an, welche Art von Adressen der Load Balancer verwendet, um Anfragen und Zustandsprüfungen an Ziele zu senden. Die möglichen Werte sind `IPv4` und `IPv6`. Der Standardwert ist `IPV4`.

Überlegungen

- Wenn Sie eine Zielgruppe mit dem IP-Adresstyp erstellen`IPv6`, muss die VPC, die Sie für die Zielgruppe angeben, über einen IPv6 Adressbereich verfügen.
- Die IP-Adressen, die Sie bei einer Zielgruppe registrieren, müssen dem IP-Adresstyp der Zielgruppe entsprechen. Sie können beispielsweise keine IPv6 Adresse bei einer Zielgruppe registrieren, wenn ihr IP-Adresstyp ist`IPv4`.
- Die IP-Adressen, die Sie bei einer Zielgruppe registrieren, müssen innerhalb des IP-Adressbereichs der VPC liegen, den Sie für die Zielgruppe angegeben haben.

HTTP-Ziele in VPC Lattice

Die HTTP-Anforderungen und -Antworten verwenden Header-Felder, um Informationen über HTTP-Nachrichten zu senden. HTTP-Header werden automatisch hinzugefügt. Header-Felder sind durch einen Doppelpunkt getrennte Name/Wert-Paare, die durch eine Zeilenumschaltung und einen Zeilenvorschub getrennt sind. Ein Standardsatz von HTTP-Header-Feldern ist in RFC 2616, Nachrichten-Header definiert. Es sind auch Nicht-Standard-HTTP-Header verfügbar, die automatisch hinzugefügt und weithin von den Anwendungen verwendet werden. Beispielsweise gibt es nicht standardmäßige HTTP-Header mit dem Präfix. `x-forwarded`

x-forwardedHeader

Amazon VPC Lattice fügt die folgenden `x-forwarded` Header hinzu:

`x-forwarded-for`

Die Quell-IP-Adresse.

`x-forwarded-for-port`

Der Ziel-Port.

`x-forwarded-for-proto`

Das Verbindungsprotokoll (`http`|`https`).

Header zur Anruferidentität

Amazon VPC Lattice fügt die folgenden Header für Anruferidentitäten hinzu:

`x-amzn-lattice-identity`

Die Identitätsinformationen. Die folgenden Felder sind vorhanden, wenn die AWS Authentifizierung erfolgreich ist.

- `Principal`— Der authentifizierte Prinzipal.
- `PrincipalOrgID`— Die ID der Organisation für den authentifizierten Prinzipal.
- `SessionName`— Der Name der authentifizierten Sitzung.

Die folgenden Felder sind vorhanden, wenn die Roles Anywhere-Anmeldeinformationen verwendet werden und die Authentifizierung erfolgreich ist.

- `X509Issuer/OU`— Der Emittent (OU).
- `X509SAN/DNS`— Der alternative Name des Betreffs (DNS).
- `X509SAN/NameCN`— Der alternative Name des Emittenten (Name/CN).
- `X509SAN/URI`— Der alternative Name des Antragstellers (URI).
- `X509Subject/CN`— Der Betreffname (CN).

`x-amzn-lattice-network`

Die VPC. Das Format lautet wie folgt.

```
SourceVpcArn=arn:aws:ec2:region:account:vpc/id
```

`x-amzn-lattice-target`

Das Ziel. Das Format lautet wie folgt.

```
ServiceArn=arn;ServiceNetworkArn=arn;TargetGroupArn=arn
```

Informationen zur Ressource ARNs für VPC Lattice finden Sie unter Von Amazon VPC Lattice definierte Ressourcentypen.

Die Header der Anruferidentität können nicht gefälscht werden. VPC Lattice entfernt diese Header aus allen eingehenden Anfragen.

Lambda-Funktionen als Ziele in VPC Lattice

Sie können Ihre Lambda-Funktionen als Ziele bei einer VPC-Lattice-Zielgruppe registrieren und eine Listener-Regel konfigurieren, um Anfragen für Ihre Lambda-Funktion an die Zielgruppe weiterzuleiten. Wenn der Service die Anfrage an eine Zielgruppe mit einer Lambda-Funktion als Ziel weiterleitet, ruft er Ihre Lambda-Funktion auf und übergibt den Inhalt der Anfrage im JSON-Format an die Lambda-Funktion.

Einschränkungen

- Die Lambda-Funktion und die Zielgruppe müssen sich im gleichen Konto und in der gleichen Region befinden.
- Die maximale Größe des Anfragentextes, den Sie an eine Lambda-Funktion senden können, beträgt 6 MB.
- Die maximale Größe der JSON-Antwort, die die Lambda-Funktion senden kann, beträgt 6 MB.
- Das Protokoll muss HTTP oder HTTPS sein.

Vorbereiten der Lambda-Funktion

Die folgenden Empfehlungen gelten, wenn Sie Ihre Lambda-Funktion mit einem VPC-Lattice-Service verwenden.

Berechtigungen zum Aufrufen der Lambda-Funktion

Wenn Sie die Zielgruppe erstellen und die Lambda-Funktion mit dem AWS Management Console oder dem registrieren AWS CLI, fügt VPC Lattice in Ihrem Namen die erforderlichen Berechtigungen zu Ihrer Lambda-Funktionsrichtlinie hinzu.

Mithilfe des folgenden API-Aufrufs können Sie auch selbst Berechtigungen hinzufügen:

```
aws lambda add-permission \
  --function-name lambda-function-arn-with-alias-name \
  --statement-id vpc-lattice \
  --principal vpc-lattice.amazonaws.com \
  --action lambda:InvokeFunction \
  --source-arn target-group-arn
```

Versionsverwaltung der Lambda-Funktion

Sie können eine Lambda-Funktion pro Zielgruppe registrieren. Um sicherzustellen, dass Sie Ihre Lambda-Funktion ändern können und dass der VPC Lattice-Dienst immer die aktuelle Version der Lambda-Funktion aufruft, erstellen Sie einen Funktionsalias und nehmen Sie den Alias in den Funktions-ARN auf, wenn Sie die Lambda-Funktion beim VPC Lattice-Dienst registrieren. Weitere Informationen finden Sie unter Lambda-Funktionsversionen und Erstellen eines Alias für eine Lambda-Funktion im AWS Lambda Entwicklerhandbuch.

Erstellen Sie einer Zielgruppe für die Lambda-Funktion

Erstellen Sie eine Zielgruppe, die bei der Weiterleitung von Anforderungen verwendet wird. Wenn der Inhalt der Anfrage einer Listener-Regel mit einer Aktion zur Weiterleitung an diese Zielgruppe entspricht, ruft der VPC Lattice-Dienst die registrierte Lambda-Funktion auf.

So erstellen und registrieren Sie eine Zielgruppe und registrieren die Lambda-Funktion mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Zielgruppen aus.
3. Wählen Sie Zielgruppe erstellen aus.
4. Wählen Sie unter Zieltyp auswählen die Option Lambda-Funktion aus.
5. Geben Sie unter Zielgruppenname einen Namen für die Zielgruppe ein.
6. Wählen Sie für die Version der Lambda-Ereignisstruktur eine Version aus. Weitere Informationen finden Sie unter the section called “Empfangen von Ereignissen vom VPC Lattice-Dienst”.

7. (Optional) Fügen Tags hinzu, indem Sie Tags auswählen, Neuen Tag hinzufügen auswählen und den Tag-Schlüssel und -Wert eingeben.
8. Wählen Sie Weiter aus.
9. Führen Sie für Lambda function (Lambda-Funktion) einen der folgenden Schritte aus:
   - Wählen Sie eine bestehende Lambda-Funktion aus.
   - Erstellen Sie eine neue Lambda-Funktion und wählen Sie sie aus.
   - Registrieren Sie die Lambda-Funktion später.
10. Wählen Sie Zielgruppe erstellen aus.

So erstellen und registrieren Sie eine Zielgruppe und registrieren die Lambda-Funktion mithilfe der AWS CLI

Verwenden Sie die Befehle create-target-groupund register-targets.

Empfangen von Ereignissen vom VPC Lattice-Dienst

Der VPC-Lattice-Service unterstützt Lambda-Aufrufe für Anforderungen über HTTP und HTTPS. Der Dienst sendet ein Ereignis im JSON-Format und fügt den `X-Forwarded-For` Header zu jeder Anfrage hinzu.

Base64-Codierung

Der Dienst Base64 codiert den Hauptteil, wenn der `content-encoding` Header vorhanden ist und der Inhaltstyp keiner der folgenden ist:

- `text/*`
- `application/json`
- `application/xml`
- `application/javascript`

Wenn der `content-encoding`-Header nicht vorhanden ist, hängt die Base64-Codierung vom Inhaltstyp ab. Bei den oben genannten Inhaltstypen sendet der Dienst den Hauptteil unverändert, ohne Base64-Kodierung.

Ereignisstruktur

Wenn Sie eine Zielgruppe vom Typ erstellen oder aktualisierenLAMBDA, können Sie die Version der Ereignisstruktur angeben, die Ihre Lambda-Funktion empfängt. Die möglichen Versionen sind V1 undV2.

Example Beispielereignis: V2

```
{
    "version": "2.0",
    "path": "/",
    "method": "GET|POST|HEAD|...",
    "headers": {
        "header-key": ["header-value", ...],
        ...
    },
    "queryStringParameters": {
        "key": ["value", ...]
    },
    "body": "request-body",
    "isBase64Encoded": true|false,
    "requestContext": {
        "serviceNetworkArn": "arn:aws:vpc-
lattice:region:123456789012:servicenetwork/sn-0bf3f2882e9cc805a",
        "serviceArn": "arn:aws:vpc-
lattice:region:123456789012:service/svc-0a40eebed65f8d69c",
        "targetGroupArn": "arn:aws:vpc-
lattice:region:123456789012:targetgroup/tg-6d0ecf831eec9f09",
        "identity": {
            "sourceVpcArn":
 "arn:aws:ec2:region:123456789012:vpc/vpc-0b8276c84697e7339",
            "type": "AWS_IAM",
            "principal": "arn:aws:iam::123456789012:assumed-role/my-role/my-session",
            "principalOrgID": "o-50dc6c495c0c9188",
            "sessionName": "i-0c7de02a688bde9f7",
            "x509IssuerOu": "string",
            "x509SanDns": "string",
            "x509SanNameCn": "string",
            "x509SanUri": "string",
            "x509SubjectCn": "string"
        },
        "region": "region",
        "timeEpoch": "1690497599177430"
    }
}
```

`body`

Der Text der Anforderung. Nur vorhanden, wenn das Protokoll HTTP, HTTPS oder gRPC ist.

`headers`

Die HTTP-Header der Anforderung. Nur vorhanden, wenn das Protokoll HTTP, HTTPS oder gRPC ist.

`identity`

Die Identitätsinformationen. Folgende Felder sind möglich.

- `principal`— Der authentifizierte Principal. Nur vorhanden, wenn die AWS Authentifizierung erfolgreich ist.
- `principalOrgID`— Die ID der Organisation für den authentifizierten Prinzipal. Nur vorhanden, wenn die AWS Authentifizierung erfolgreich war.
- `sessionName`— Der Name der authentifizierten Sitzung. Nur vorhanden, wenn die AWS Authentifizierung erfolgreich ist.
- `sourceVpcArn`— Der ARN der VPC, von der die Anforderung stammt. Nur vorhanden, wenn die Quell-VPC identifiziert werden kann.
- `type`— Der Wert gibt an`AWS_IAM`, ob eine Authentifizierungsrichtlinie verwendet wird und die AWS Authentifizierung erfolgreich ist.

Wenn Roles Anywhere-Anmeldeinformationen verwendet werden und die Authentifizierung erfolgreich ist, sind die folgenden Felder möglich.

- `x509IssuerOu`— Der Emittent (OU).
- `x509SanDns`— Der alternative Name des Betreffs (DNS).
- `x509SanNameCn`— Der alternative Name des Emittenten (Name/CN).
- `x509SanUri`— Der alternative Name des Antragstellers (URI).
- `x509SubjectCn`— Der Betreffname (CN).

`isBase64Encoded`

Gibt an, ob der Text Base64-codiert war. Nur vorhanden, wenn das Protokoll HTTP, HTTPS oder gRPC ist und der Anforderungstext nicht bereits eine Zeichenfolge ist.

`method`

Die HTTP-Methode der Anforderung. Nur vorhanden, wenn das Protokoll HTTP, HTTPS oder gRPC ist.

`path`

Den Pfad der Anfrage. Nur vorhanden, wenn das Protokoll HTTP, HTTPS oder gRPC ist.

`queryStringParameters`

Die HTTP-Abfragezeichenfolge-Parameter. Nur vorhanden, wenn das Protokoll HTTP, HTTPS oder gRPC ist.

`serviceArn`

Der ARN des Dienstes, der die Anforderung empfängt.

`serviceNetworkArn`

Der ARN des Servicenetzwerks, das die Anforderung übermittelt.

`targetGroupArn`

Der ARN der Zielgruppe, die die Anforderung empfängt.

`timeEpoch`

Die Zeit, in Mikrosekunden.

Example Beispielereignis: V1

```
{
    "raw_path": "/path/to/resource",
    "method": "GET|POST|HEAD|...",
    "headers": {"header-key": "header-value", ... },
    "query_string_parameters": {"key": "value", ...},
    "body": "request-body",
    "is_base64_encoded": true|false
}
```

Antworten Sie auf den VPC Lattice-Dienst

Die Antwort von Ihrer Lambda-Funktion muss den Base64-codierten Status, Statuscode und die Header beinhalten. Sie können den Text weglassen.

Um den binären Inhalt in den Text der Antwort einzuschließen, müssen Sie den Inhalt mit Base64 codieren und `isBase64Encoded` auf `true` einstellen. Der Dienst dekodiert den Inhalt, um den binären Inhalt abzurufen, und sendet ihn im Hauptteil der HTTP-Antwort an den Client.

Der VPC Lattice-Dienst berücksichtigt keine hop-by-hop Header wie oder. `Connection` `Transfer-Encoding` Sie können den `Content-Length` Header auslassen, da der Dienst ihn berechnet, bevor er Antworten an Clients sendet.

Das folgende Beispiel ist eine Antwort von einer Lambda-Funktion:

```
{
    "isBase64Encoded": false,
    "statusCode": 200,
    "statusDescription": "200 OK",
    "headers": {
        "Set-cookie": "cookies",
        "Content-Type": "application/json"
    },
    "body": "Hello from Lambda (optional)"
}
```

Header mit mehreren Werten

VPC Lattice unterstützt Anfragen von einem Client oder Antworten von einer Lambda-Funktion, die Header mit mehreren Werten oder denselben Header mehrfach enthalten. VPC Lattice übergibt alle Werte an die Ziele.

Im folgenden Beispiel gibt es zwei Header, die header1 mit unterschiedlichen Werten benannt sind.

```
header1 = value1
header1 = value2
```

Bei einer V2-Ereignisstruktur sendet VPC Lattice die Werte in einer Liste. Zum Beispiel:

```
"header1": ["value1", "value2"]
```

Mit einer V1-Ereignisstruktur kombiniert VPC Lattice die Werte zu einer einzigen Zeichenfolge. Zum Beispiel:

```
"header1": "value1, value2"
```

Mehrwertparameter für Abfragezeichenfolge-Parameter

VPC Lattice unterstützt Abfrageparameter mit mehreren Werten für denselben Schlüssel.

Im folgenden Beispiel gibt es zwei Parameter, die QS1 mit unterschiedlichen Werten benannt sind.

```
http://www.example.com?&QS1=value1&QS1=value2
```

Bei einer V2-Ereignisstruktur sendet VPC Lattice die Werte in einer Liste. Zum Beispiel:

```
"QS1": ["value1", "value2"]
```

Bei einer V1-Ereignisstruktur verwendet VPC Lattice den zuletzt übergebenen Wert. Zum Beispiel:

```
"QS1": "value2"
```

Aufheben der Registrierung der Lambda-Funktion

Wenn Sie zu Ihrer Lambda-Funktion keinen Datenverkehr mehr senden müssen, können Sie ihre Registrierung aufheben. Nachdem Sie die Registrierung einer Lambda-Funktion aufgehoben haben, schlagen laufende Anfragen mit HTTP-5XX-Fehlermeldungen fehl.

Zum Ersetzen einer Lambda-Funktion wird empfohlen, eine neue Zielgruppe zu erstellen, die neue Funktion bei der neuen Zielgruppe zu registrieren und die Listener-Regeln so zu aktualisieren, dass anstatt der vorhandenen die neue Zielgruppe verwendet wird.

So heben Sie die Registrierung einer Lambda-Funktion mithilfe der Konsole auf

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Zielgruppen aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Klicken Sie auf der Registerkarte Targets (Ziele) auf Deregister (Registrierung aufheben).
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie ein **`confirm`** und wählen Sie dann Abmelden.

So heben Sie die Registrierung der Lambda-Funktion mithilfe der AWS CLI

Verwenden Sie den Befehl deregister-targets.

Application Load Balancers als Ziele in VPC Lattice

Sie können eine VPC-Lattice-Zielgruppe erstellen, einen einzelnen internen Application Load Balancer als Ziel registrieren und Ihren VPC-Lattice-Dienst so konfigurieren, dass er Datenverkehr an diese Zielgruppe weiterleitet. In diesem Szenario übernimmt der Application Load Balancer die Routing-Entscheidung, sobald der Datenverkehr ihn erreicht. Mit dieser Konfiguration können Sie das anforderungsbasierte Layer-7-Routing-Feature des Application Load Balancer in Kombination mit Funktionen verwenden, die VPC Lattice unterstützt, wie IAM-Authentifizierung und -Autorisierung sowie kontenübergreifende Konnektivität. VPCs

Einschränkungen

- Sie können einen einzelnen internen Application Load Balancer als Ziel in einer Zielgruppe vom Typ VPC Lattice registrieren. `ALB`
- Sie können einen Application Load Balancer als Ziel für bis zu zwei VPC Lattice-Zielgruppen registrieren, die von zwei verschiedenen VPC Lattice-Diensten verwendet werden.
- VPC Lattice bietet keine Gesundheitschecks für eine bestimmte Zielgruppe `ALB` an. Sie können jedoch Integritätsprüfungen unabhängig auf Load Balancer-Ebene für die Ziele in Elastic Load Balancing konfigurieren. Weitere Informationen finden Sie unter Zustandsprüfungen für Zielgruppen im Benutzerhandbuch für Application Load Balancers

Voraussetzungen

Erstellen Sie einen Application Load Balancer, um sich als Ziel für Ihre VPC Lattice-Zielgruppe zu registrieren. Der Load Balancer muss die folgenden Kriterien erfüllen:

- Das Load Balancer-Schema ist intern.
- Der Application Load Balancer muss sich in demselben Konto wie die VPC Lattice-Zielgruppe befinden und muss sich im Status Aktiv befinden.
- Der Application Load Balancer muss sich in derselben VPC wie die VPC Lattice-Zielgruppe befinden.
- Sie können HTTPS-Listener am Application Load Balancer verwenden, um TLS zu beenden, aber nur, wenn der VPC-Lattice-Dienst dasselbe SSL/TLS-Zertifikat verwendet wie der Load Balancer.
- Um die Client-IP des VPC Lattice-Dienstes im `X-Forwarded-For` Anforderungsheader beizubehalten, müssen Sie das Attribut für den Application Load `routing.http.xff_header_processing.mode` Balancer auf festlegen. `Preserve` Wenn

der Wert ist`Preserve`, behält der Load Balancer den `X-Forwarded-For` Header in der HTTP-Anforderung und sendet sie ohne Änderung an Ziele.

Weitere Informationen finden Sie unter Erstellen eines Application Load Balancer im Benutzerhandbuch für Application Load Balancer.

Schritt 1: Erstellen einer Zielgruppe vom Typ ALB

Gehen Sie wie folgt vor, um die Zielgruppe zu erstellen. Beachten Sie, dass VPC Lattice keine Gesundheitschecks für `ALB` Zielgruppen unterstützt. Sie können jedoch Zustandsprüfungen für die Zielgruppen Ihres Application Load Balancer konfigurieren. Weitere Informationen finden Sie unter Zustandsprüfungen für Zielgruppen im Benutzerhandbuch für Application Load Balancers.

Erstellen der Zielgruppe

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Zielgruppen aus.
3. Wählen Sie Zielgruppe erstellen aus.
4. Wählen Sie auf der Seite Zielgruppendetails angeben unter Grundkonfiguration Application Load Balancer als Zieltyp aus.
5. Geben Sie unter Zielgruppenname einen Namen für die Zielgruppe ein.
6. Wählen Sie für Protokoll **`HTTP`** oder **`HTTPS`** aus. Das Zielgruppenprotokoll muss mit dem Protokoll des Listeners für Ihren internen Application Load Balancer übereinstimmen.
7. Geben Sie als Port den Port für Ihre Zielgruppe an. Dieser Port muss mit dem Port des Listeners für Ihren internen Application Load Balancer übereinstimmen. Sie können alternativ einen Listener-Port auf dem internen Application Load Balancer hinzufügen, der dem Zielgruppenport entspricht, den Sie hier angeben.
8. Wählen Sie für VPC dieselbe Virtual Private Cloud (VPC) aus, die Sie bei der Erstellung des internen Application Load Balancer ausgewählt haben. Dies sollte die VPC sein, die Ihre VPC-Lattice-Ressourcen enthält.
9. Wählen Sie unter Protokollversion die Protokollversion aus, die Ihr Application Load Balancer unterstützt.
10. (Optional) Fügen Sie alle erforderlichen Tags hinzu.
11. Wählen Sie Weiter aus.

Schritt 2: Den Application Load Balancer als Ziel registrieren

Sie können den Load Balancer entweder jetzt oder später als Ziel registrieren.

So verfahren Sie zum Registrieren eines Application Load Balancer als Ziel

1. Wählen Sie Jetzt registrieren.
2. Wählen Sie als Application Load Balancer Ihren internen Application Load Balancer aus.
3. Behalten Sie für Port die Standardeinstellung bei oder geben Sie bei Bedarf einen anderen Port an. Dieser Port muss mit einem vorhandenen Listener-Port auf Ihrem Application Load Balancer übereinstimmen. Wenn Sie ohne einen passenden Port fortfahren, erreicht der Datenverkehr Ihren Application Load Balancer nicht.
4. Wählen Sie Zielgruppe erstellen aus.

Protokollversion

Standardmäßig senden Dienste Anforderungen an Ziele unter Verwendung von HTTP/1.1. Sie können die Protokollversion verwenden, um Anforderungen mit HTTP/2 oder gRPC an Ziele zu senden.

In der folgenden Tabelle sind die Ergebnisse für die Kombinationen aus Anforderungsprotokoll und Zielgruppen-Protokollversion zusammengefasst.

Anforderungsprotokoll	Protokollversion	Ergebnis
HTTP/1.1	HTTP/1.1	Herzlichen Glückwunsch
HTTP/2	HTTP/1.1	Herzlichen Glückwunsch
gRPC	HTTP/1.1	Fehler
HTTP/1.1	HTTP/2	Fehler
HTTP/2	HTTP/2	Herzlichen Glückwunsch
gRPC	HTTP/2	Erfolg, wenn Ziele gRPC unterstützen

Anforderungsprotokoll	Protokollversion	Ergebnis
HTTP/1.1	gRPC	Fehler
HTTP/2	gRPC	Erfolg bei einer POST-Anfo rderung
gRPC	gRPC	Herzlichen Glückwunsch

Überlegungen zur gRPC-Protokollversion

- Das einzige unterstützte Listener-Protokoll ist HTTPS.
- Die einzigen unterstützten Zieltypen sind `INSTANCE` und `IP`.
- Der Dienst analysiert gRPC-Anfragen und leitet gRPC-Aufrufe basierend auf dem Paket, dem Dienst und der Methode an die entsprechenden Zielgruppen weiter.
- Sie können keine Lambda-Funktionen als Ziel verwenden.

Überlegungen zur HTTP/2-Protokollversion

- Das einzige unterstützte Listener-Protokoll ist HTTPS. Sie können entweder HTTP oder HTTPS als Zielgruppenprotokoll wählen.
- Die einzigen unterstützten Listener-Regeln sind Forward und Fixed Response.
- Die einzigen unterstützten Zieltypen sind `INSTANCE` und `IP`.
- Der Dienst unterstützt Streaming von Clients. Der Service unterstützt kein Streaming zu den Zielen.

Tags für Ihre VPC Lattice-Zielgruppe

Tags helfen Ihnen, Ihre Zielgruppen auf unterschiedliche Weise zu kategorisieren, z.B. nach Zweck, Eigentümer oder Umgebung.

Sie können mehrere Tags für jede Zielgruppe hinzufügen. Tag-Schlüssel müssen für jede Zielgruppe eindeutig sein. Wenn Sie ein Tag mit einem Schlüssel hinzufügen, der der Zielgruppe bereits zugeordnet ist, ändert sich der Wert dieses Tags.

Wenn Sie ein Tag nicht mehr benötigen, können Sie es entfernen.

Einschränkungen

- Maximale Anzahl von Tags pro Ressource: 50
- Maximale Schlüssellänge: 127 Unicode-Zeichen
- Maximale Wertlänge: 255 Unicode-Zeichen
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden. Erlaubte Zeichen sind Buchstaben, Leerzeichen und Zahlen, die in UTF-8 darstellbar sind, sowie die folgenden Sonderzeichen: + - = _ : / @. Verwenden Sie keine führenden oder nachgestellten Leerzeichen.
- Verwenden Sie in Tag-Namen oder -Werten nicht das `aws:` Präfix, da es für die AWS -Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht als Ihre Tags pro Ressourcenlimit angerechnet.

So aktualisieren Sie die Tags für eine Zielgruppe mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Zielgruppen aus.
3. Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
4. Wählen Sie die Registerkarte Tags aus.
5. Um ein Tag hinzuzufügen, wählen Sie Tags hinzufügen und geben Sie dann den Tagschlüssel und -Wert ein. Zum Hinzufügen eines weiteren Tags wählen Sie Neues Tag hinzufügen erneut aus. Wenn Sie fertig mit dem Hinzufügen der Tags sind, klicken Sie auf Save changes (Änderungen speichern).
6. Um ein Tag zu löschen, aktivieren Sie das Kontrollkästchen für das Tag und wählen Sie Löschen. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

So aktualisieren Sie die Tags für eine Zielgruppe mithilfe der AWS CLI

Verwenden Sie die Befehle tag-resource und untag-resource.

Eine VPC-Lattice-Zielgruppe löschen

Sie können eine Zielgruppe löschen, wenn sie nicht von den Weiterleitungsaktionen der Listener-Regeln referenziert wird. Das Löschen einer Zielgruppe hat keine Auswirkungen auf die Ziele hat, die

bei der Zielgruppe registriert sind. Sie können eine registrierte EC2 Instance anhalten oder beenden, wenn Sie sie nicht mehr benötigen.

Löschen einer Zielgruppe mithilfe der Konsole

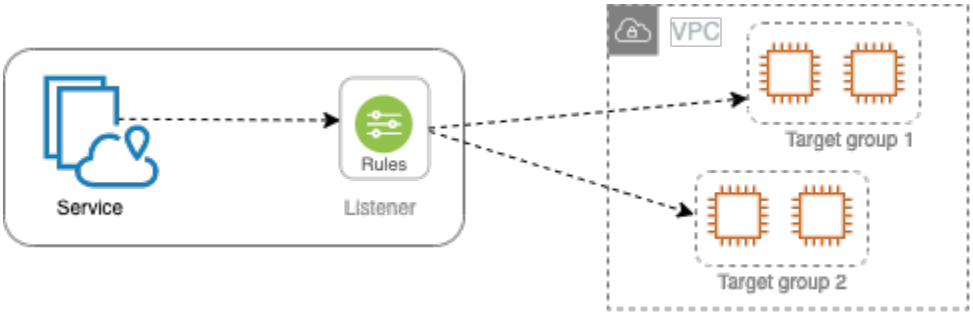
1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Targets (Zielgruppen) aus.
3. Aktivieren Sie das Kontrollkästchen für die Zielgruppe und wählen Sie dann Aktionen, Löschen aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

So löschen Sie eine Zielgruppe mithilfe der AWS CLI

Verwenden Sie den delete-target-group-Befehl.

Listener für Ihren VPC Lattice-Service

Bevor Sie Ihren VPC Lattice-Service verwenden können, müssen Sie einen Listener hinzufügen. Ein Listener ist ein Prozess, der mit dem Protokoll und dem Port, das bzw. den Sie konfigurieren, Verbindungsanforderungen prüft. Die Regeln, die Sie für einen Listener definieren, bestimmen, wie der Service Anfragen an seine registrierten Ziele weiterleitet.



Inhalt

Listener-Konfiguration

Listener unterstützen die folgenden Protokolle und Ports:

- Protokolle: HTTP, HTTPS, TLS
- Ports: 1-65535

Wenn das Listener-Protokoll HTTPS ist, stellt VPC Lattice ein TLS-Zertifikat bereit und verwaltet es, das dem von VPC Lattice generierten FQDN zugeordnet ist. VPC Lattice unterstützt TLS auf HTTP/1.1 und HTTP/2. Wenn Sie einen Dienst mit einem HTTPS-Listener konfigurieren, bestimmt VPC Lattice das HTTP-Protokoll automatisch mithilfe von Application-Layer Protocol Negotiation

(ALPN). Wenn ALPN nicht vorhanden ist, verwendet VPC Lattice standardmäßig HTTP/1.1. Weitere Informationen finden Sie unter HTTPS-Listener.

VPC Lattice kann HTTP, HTTPS, HTTP/1.1 und HTTP/2 abhören und mit Zielen in allen diesen Protokollen und Versionen kommunizieren. Wir setzen nicht voraus, dass die Protokolle für den Hörer und die Zielgruppe übereinstimmen. VPC Lattice verwaltet den gesamten Prozess des Upgrades und Downgrades zwischen Protokollen und Versionen. Weitere Informationen finden Sie unter Protokollversion.

Sie können einen TLS-Listener erstellen, um sicherzustellen, dass Ihre Anwendung den verschlüsselten Datenverkehr anstelle von VPC Lattice entschlüsselt. Weitere Informationen finden Sie unter TLS-Listener.

VPC Lattice unterstützt nicht. WebSockets

HTTP-Listener für VPC Lattice-Dienste

Ein Listener ist ein Prozess, der Verbindungsanfragen überprüft. Sie können einen Listener definieren, wenn Sie Ihren VPC Lattice-Dienst erstellen. Sie können Ihrem Service jederzeit Listener hinzufügen.

Die Informationen auf dieser Seite helfen Ihnen beim Erstellen eines HTTP-Listeners für Ihren Service. Hinweise zum Erstellen von Listenern, die andere Protokolle verwenden, finden Sie unter HTTPS-Listener und. TLS-Listener

Voraussetzungen

- Um der Standard-Listener-Regel eine Forward-Aktion hinzuzufügen, müssen Sie eine verfügbare VPC Lattice-Zielgruppe angeben. Weitere Informationen finden Sie unter Erstellen einer VPC-Lattice-Zielgruppe.
- Sie können dieselbe Zielgruppe in mehreren Listenern angeben, aber diese Listener müssen demselben Service angehören. Um eine Zielgruppe mit einem VPC-Lattice-Dienst zu verwenden, müssen Sie sicherstellen, dass sie nicht von einem Listener verwendet wird, der einem anderen VPC-Lattice-Dienst angehört.

Hinzufügen eines HTTP-Listeners

Sie können Ihrem Service jederzeit Listener und Regeln hinzufügen. Sie konfigurieren einen Listener mit einem Protokoll und einem Port für Verbindungen von Clients zum Service und eine VPC-

Lattice-Zielgruppe für die Standard-Listener-Regel. Weitere Informationen finden Sie unter Listener-Konfiguration.

So fügen Sie einen HTTP-Listener mithilfe der Konsole hinzu

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Services aus.
3. Wählen Sie den Namen des Dienstes aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Routing die Option Listener hinzufügen aus.
5. Als Listener-Name können Sie entweder einen benutzerdefinierten Listener-Namen angeben oder das Protokoll und den Port Ihres Listeners als Listener-Namen verwenden. Ein benutzerdefinierter Name, den Sie angeben, kann bis zu 63 Zeichen lang sein und muss für jeden Dienst in Ihrem Konto eindeutig sein. Gültige Zeichen sind a—z, 0—9 und Bindestriche (—). Sie können keinen Bindestrich als erstes oder letztes Zeichen oder unmittelbar nach einem anderen Bindestrich verwenden. Sie können den Namen nach der Erstellung nicht mehr ändern.
6. Wählen Sie für Protokoll: Port die Option HTTP und geben Sie eine Portnummer ein.
7. Wählen Sie für Standardaktion die VPC Lattice-Zielgruppe aus, die Traffic empfangen soll, und wählen Sie die Gewichtung aus, die dieser Zielgruppe zugewiesen werden soll. Die Gewichtung, die Sie einer Zielgruppe zuweisen, legt fest, dass sie Priorität beim Empfang von Traffic hat. Wenn beispielsweise zwei Zielgruppen dasselbe Gewicht haben, erhält jede Zielgruppe die Hälfte des Traffics. Wenn Sie nur eine Zielgruppe angegeben haben, werden 100 Prozent des Traffics an die eine Zielgruppe gesendet.

   Sie können optional eine weitere Zielgruppe für die Standardaktion hinzufügen. Wählen Sie Aktion hinzufügen und wählen Sie dann eine Zielgruppe aus und geben Sie deren Gewicht an.
8. (Optional) Um eine weitere Regel hinzuzufügen, wählen Sie Regel hinzufügen und geben Sie dann einen Namen, eine Priorität, eine Bedingung und eine Aktion für die Regel ein.

   Sie können jeder Regel eine Prioritätszahl zwischen 1 und 100 zuweisen. Ein Listener kann nicht über mehrere Regeln mit derselben Priorität verfügen. Regeln werden in der Reihenfolge ihrer Prioritäten bewertet, ausgehend vom niedrigsten Wert hin zum höchsten Wert. Die Standardregel wird zuletzt ausgewertet. Weitere Informationen finden Sie unter Listener-Regeln.
9. (Optional) Um Tags hinzuzufügen, erweitern Sie Listener-Tags, wählen Sie Neuen Tag hinzufügen und geben Sie einen Tag-Schlüssel und -Wert ein.
10. Überprüfen Sie Ihre Konfiguration und wählen Sie dann Hinzufügen.

Um einen HTTP-Listener hinzuzufügen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl create-listener, um einen Listener mit einer Standardregel zu erstellen, und den Befehl create-rule, um zusätzliche Listener-Regeln zu erstellen.

HTTPS-Listener für VPC Lattice-Dienste

Ein Listener ist ein Prozess, der Verbindungsanfragen überprüft. Sie definieren einen Listener, wenn Sie Ihren Service erstellen. Sie können Ihrem Service in VPC Lattice jederzeit Listener hinzufügen.

Sie können einen HTTS-Listener erstellen, der TLS-Version 1.2 oder TLS-Version 1.3 verwendet, um HTTPS-Verbindungen mit VPC Lattice direkt zu beenden. VPC Lattice stellt ein TLS-Zertifikat bereit und verwaltet es, das dem von VPC Lattice generierten vollqualifizierten Domainnamen (FQDN) zugeordnet ist. VPC Lattice unterstützt TLS auf HTTP/1.1 und HTTP/2. Wenn Sie einen Dienst mit einem HTTPS-Listener konfigurieren, bestimmt VPC Lattice das HTTP-Protokoll automatisch über Application-Layer Protocol Negotiation (ALPN). Wenn ALPN nicht vorhanden ist, verwendet VPC Lattice standardmäßig HTTP/1.1.

VPC Lattice verwendet eine Multi-Tenancy-Architektur, was bedeutet, dass es mehrere Dienste auf demselben Endpunkt hosten kann. VPC Lattice verwendet TLS mit Server Name Indication (SNI) für jede Client-Anfrage. Encrypted Client Hello (ECH) und Encrypted Server Name Indication (ESNI) werden nicht unterstützt.

VPC Lattice kann HTTP, HTTPS, HTTP/1.1 und HTTP/2 abhören und mit Zielen in allen diesen Protokollen und Versionen kommunizieren. Diese Listener- und Zielgruppenkonfigurationen müssen nicht übereinstimmen. VPC Lattice verwaltet den gesamten Prozess des Upgrades und Downgrades zwischen Protokollen und Versionen. Weitere Informationen finden Sie unter Protokollversion.

Um sicherzustellen, dass Ihre Anwendung den Datenverkehr entschlüsselt, erstellen Sie stattdessen einen TLS-Listener. Mit TLS-Passthrough beendet VPC Lattice TLS nicht. Weitere Informationen finden Sie unter TLS-Listener.

Inhalt

Sicherheitsrichtlinie

VPC Lattice verwendet eine Sicherheitsrichtlinie, die aus einer Kombination aus einem TLSv1 2.2-Protokoll und einer Liste von SSL/TLS-Chiffren besteht. Das Protokoll stellt eine sichere Verbindung zwischen einem Client und einem Server her und stellt sicher, dass alle Daten, die zwischen dem Client und Ihres Dienstes in VPC Lattice übertragen werden, privat sind. Ein Verschlüsselungsverfahren ist ein Algorithmus, der eine kodierte Nachricht mithilfe von Verschlüsselungsschlüsseln erstellt. Protokolle verwenden mehrere Chiffren, um Daten zu verschlüsseln. Während der Verbindungsaushandlung präsentieren der Client und VPC Lattice eine Liste mit Verschlüsselungsverfahren und Protokollen, die sie jeweils unterstützen, nach Priorität sortiert. Standardmäßig wird für die sichere Verbindung die erste Verschlüsselung auf der Liste des Servers ausgewählt, die mit einem der Verschlüsselungsverfahren des Clients übereinstimmt.

VPC Lattice verwendet die folgenden TLS 1.2 SSL/TLS-Chiffren in dieser Rangfolge:

- `ECDHE-RSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES128-SHA`
- `ECDHE-RSA-AES256-GCM-SHA384`
- `ECDHE-RSA-AES256-SHA`
- `AES128-GCM-SHA256`
- `AES128-SHA`
- `AES256-GCM-SHA384`
- `AES256-SHA`

VPC Lattice verwendet auch die folgenden TLS 1.3 SSL/TLS-Chiffren in dieser Reihenfolge der Präferenz:

- `TLS_AES_128_GCM_SHA256`
- `TLS_AES_256_GCM_SHA384`
- `TLS_CHACHA20_POLY1305_SHA256`

ALPN-Richtlinie

Application-Layer Protocol Negotiation (ALPN) ist eine TLS-Erweiterung, die bei den ersten TLS-Handshake-Hello-Nachrichten gesendet wird. ALPN ermöglicht es der Anwendungsebene

auszuhandeln, welche Protokolle über eine sichere Verbindung wie HTTP/1 und HTTP/2 verwendet werden sollen.

Wenn der Client eine ALPN-Verbindung initiiert, vergleicht der VPC Lattice-Dienst die ALPN-Einstellungsliste des Clients mit seiner ALPN-Richtlinie. Wenn der Client ein Protokoll aus der ALPN-Richtlinie unterstützt, stellt der VPC Lattice-Dienst die Verbindung auf der Grundlage der Präferenzliste der ALPN-Richtlinie her. Andernfalls verwendet der Dienst ALPN nicht.

VPC Lattice unterstützt die folgende ALPN-Richtlinie:

`HTTP2Preferred`

Bevorzugen Sie HTTP/2 gegenüber HTTP/1.1. Die ALPN-Einstellungsliste lautet h2, http/1.1.

Hinzufügen eines HTTPS-Listeners

Sie konfigurieren einen Listener mit einem Protokoll und einem Port für Verbindungen von Clients zum Dienst und einer Zielgruppe für die Standard-Listener-Regel. Weitere Informationen finden Sie unter Listener-Konfiguration.

Voraussetzungen

- Um der Standard-Listener-Regel eine Forward-Aktion hinzuzufügen, müssen Sie eine verfügbare VPC Lattice-Zielgruppe angeben. Weitere Informationen finden Sie unter Erstellen einer VPC-Lattice-Zielgruppe.
- Sie können dieselbe Zielgruppe in mehreren Listenern angeben, aber diese Listener müssen demselben VPC Lattice-Service angehören. Um eine Zielgruppe mit einem VPC-Lattice-Dienst zu verwenden, müssen Sie sicherstellen, dass sie nicht von einem Listener verwendet wird, der einem anderen VPC-Lattice-Dienst angehört.
- Sie können das von VPC Lattice bereitgestellte Zertifikat verwenden oder Ihr eigenes Zertifikat importieren. AWS Certificate Manager Weitere Informationen finden Sie unter the section called “BYOC”.

So fügen Sie einen HTTPS-Listeners mithilfe der Konsole hinzu

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Services aus.
3. Wählen Sie den Namen des Dienstes aus, um die Detailseite zu öffnen.

4. Wählen Sie auf der Registerkarte Routing die Option Listener hinzufügen aus.
5. Als Listener-Name können Sie entweder einen benutzerdefinierten Listener-Namen angeben oder das Protokoll und den Port Ihres Listeners als Listener-Namen verwenden. Ein benutzerdefinierter Name, den Sie angeben, kann bis zu 63 Zeichen lang sein und muss für jeden Dienst in Ihrem Konto eindeutig sein. Gültige Zeichen sind a—z, 0—9 und Bindestriche (—). Sie können keinen Bindestrich als erstes oder letztes Zeichen oder unmittelbar nach einem anderen Bindestrich verwenden. Sie können den Namen eines Listeners nach der Erstellung nicht mehr ändern.
6. Wählen Sie für Protocol: Port die Option HTTPS und geben Sie eine Portnummer ein.
7. Wählen Sie für Standardaktion die VPC Lattice-Zielgruppe aus, die Traffic empfangen soll, und wählen Sie die Gewichtung aus, die dieser Zielgruppe zugewiesen werden soll. Die Gewichtung, die Sie einer Zielgruppe zuweisen, legt fest, dass sie Priorität beim Empfang von Traffic hat. Wenn beispielsweise zwei Zielgruppen dasselbe Gewicht haben, erhält jede Zielgruppe die Hälfte des Traffics. Wenn Sie nur eine Zielgruppe angegeben haben, werden 100 Prozent des Traffics an die eine Zielgruppe gesendet.

   Sie können optional eine weitere Zielgruppe für die Standardaktion hinzufügen. Wählen Sie Aktion hinzufügen und wählen Sie dann eine Zielgruppe aus und geben Sie deren Gewicht an.
8. (Optional) Um eine weitere Regel hinzuzufügen, wählen Sie Regel hinzufügen und geben Sie dann einen Namen, eine Priorität, eine Bedingung und eine Aktion für die Regel ein.

   Sie können jeder Regel eine Prioritätszahl zwischen 1 und 100 zuweisen. Ein Listener kann nicht über mehrere Regeln mit derselben Priorität verfügen. Regeln werden in der Reihenfolge ihrer Prioritäten bewertet, ausgehend vom niedrigsten Wert hin zum höchsten Wert. Die Standardregel wird zuletzt ausgewertet. Weitere Informationen finden Sie unter Listener-Regeln.
9. (Optional) Um Tags hinzuzufügen, erweitern Sie Listener-Tags, wählen Sie Neuen Tag hinzufügen und geben Sie einen Tag-Schlüssel und -Wert ein.
10. Wenn Sie bei der Erstellung des Dienstes keinen benutzerdefinierten Domainnamen angegeben haben, generiert VPC Lattice für HTTPS-Listener-Zertifikatseinstellungen automatisch ein TLS-Zertifikat, um den über den Listener fließenden Datenverkehr zu sichern.

    Wenn Sie den Dienst mit einem benutzerdefinierten Domainnamen erstellt, aber kein passendes Zertifikat angegeben haben, können Sie dies jetzt tun, indem Sie das Zertifikat unter Benutzerdefiniertes SSL/TLS-Zertifikat auswählen. Andernfalls ist das Zertifikat, das Sie bei der Erstellung des Dienstes angegeben haben, bereits ausgewählt.
11. Überprüfen Sie Ihre Konfiguration und wählen Sie dann Hinzufügen.

So fügen Sie einen HTTPS-Listener mithilfe der AWS CLI

Verwenden Sie den Befehl create-listener, um einen Listener mit einer Standardregel zu erstellen, und den Befehl create-rule, um zusätzliche Listener-Regeln zu erstellen.

TLS-Listener für VPC Lattice-Dienste

Ein Listener ist ein Prozess, der Verbindungsanfragen überprüft. Sie können einen Listener definieren, wenn Sie Ihren VPC Lattice-Dienst erstellen. Sie können Ihrem Service jederzeit Listener hinzufügen.

Sie können einen TLS-Listener erstellen, sodass VPC Lattice verschlüsselten Datenverkehr an Ihre Anwendungen weiterleitet, ohne ihn zu entschlüsseln.

Wenn Sie es vorziehen, dass VPC Lattice verschlüsselten Datenverkehr entschlüsselt und unverschlüsselten Datenverkehr an Ihre Anwendungen sendet, erstellen Sie stattdessen einen HTTPS-Listener. Weitere Informationen finden Sie unter HTTPS-Listener.

Überlegungen

Für TLS-Listener gelten die folgenden Überlegungen:

- Der VPC Lattice-Dienst muss einen benutzerdefinierten Domainnamen haben. Der benutzerdefinierte Domänenname des Dienstes wird als Übereinstimmung mit Service Name Indication (SNI) verwendet. Wenn Sie bei der Erstellung des Dienstes ein Zertifikat angegeben haben, wird es nicht verwendet.
- Die einzige Regel, die für einen TLS-Listener zulässig ist, ist die Standardregel.
- Die Standardaktion für einen TLS-Listener muss eine Weiterleitungsaktion an eine TCP-Zielgruppe sein.
- Standardmäßig sind Integritätsprüfungen für TCP-Zielgruppen deaktiviert. Wenn Sie Integritätsprüfungen für eine TCP-Zielgruppe aktivieren, müssen Sie ein Protokoll und eine Protokollversion angeben.
- TLS-Listener leiten Anfragen mithilfe des SNI-Felds der Client-Hello-Nachricht weiter. Sie können Platzhalter- und SAN-Zertifikate für Ihre Ziele verwenden, wenn die entsprechende Bedingung exakt mit der Client-Hello übereinstimmt.
- Da der gesamte Datenverkehr vom Client zum Ziel verschlüsselt bleibt, kann VPC Lattice die HTTP-Header nicht lesen und keine HTTP-Header einfügen oder entfernen. Daher gelten bei einem TLS-Listener die folgenden Einschränkungen:

  - Die Verbindungsdauer ist auf 10 Minuten begrenzt
  - Authentifizierungsrichtlinien sind auf anonyme Prinzipale beschränkt
  - Lambda-Ziele werden nicht unterstützt
- Encrypted Client Hello (ECH) wird nicht unterstützt.
- Encrypted Server Name Indication (ESNI) wird nicht unterstützt.

Hinzufügen eines TLS-Listeners

Sie konfigurieren einen Listener mit einem Protokoll und einem Port für Verbindungen von Clients zum Dienst und einer Zielgruppe für die Standard-Listener-Regel. Weitere Informationen finden Sie unter Listener-Konfiguration.

So fügen Sie mithilfe der Konsole einen TLS-Listener hinzu

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Services aus.
3. Wählen Sie den Namen des Dienstes aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Routing die Option Listener hinzufügen aus.
5. Als Listener-Name können Sie entweder einen benutzerdefinierten Listener-Namen angeben oder das Protokoll und den Port Ihres Listeners als Listener-Namen verwenden. Ein benutzerdefinierter Name, den Sie angeben, kann bis zu 63 Zeichen lang sein und muss für jeden Dienst in Ihrem Konto eindeutig sein. Gültige Zeichen sind a—z, 0—9 und Bindestriche (—). Sie können keinen Bindestrich als erstes oder letztes Zeichen oder unmittelbar nach einem anderen Bindestrich verwenden. Sie können den Namen eines Listeners nach der Erstellung nicht mehr ändern.
6. Wählen Sie als Protokoll TLS aus. Geben Sie für Port eine Portnummer ein.
7. Wählen Sie für An Zielgruppe weiterleiten eine VPC-Lattice-Zielgruppe aus, die das TCP-Protokoll für den Empfang des Datenverkehrs verwendet, und wählen Sie die Gewichtung aus, die dieser Zielgruppe zugewiesen werden soll. Sie können optional eine weitere Zielgruppe hinzufügen. Wählen Sie Zielgruppe hinzufügen und wählen Sie dann eine Zielgruppe aus und geben Sie deren Gewicht ein.
8. (Optional) Um Tags hinzuzufügen, erweitern Sie Listener-Tags, wählen Sie Neuen Tag hinzufügen und geben Sie einen Tag-Schlüssel und -Wert ein.
9. Überprüfen Sie Ihre Konfiguration und wählen Sie dann Hinzufügen.

Um einen TLS-Listener hinzuzufügen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl create-listener, um einen Listener mit einer Standardregel zu erstellen. Geben Sie das TLS_PASSTHROUGH-Protokoll an.

Listener-Regeln für Ihren VPC Lattice-Service

Jeder Listener hat eine Standardregel und zusätzliche Regeln, die Sie definieren können. Jede Rolle besteht aus einer Priorität, mindestens einer Aktion und mindestens einer Bedingung. Sie können jederzeit Regel hinzufügen oder bearbeiten.

Inhalt

Standardregeln

Beim Erstellen eines Listeners definieren Sie Aktionen für die Standardregel. Standardregeln können keine Bedingungen aufweisen. Wenn für die Regeln eines Listeners keine Bedingungen erfüllt werden, wird die Aktion für die Standardregel durchgeführt.

Priorität der Regel

Jede Regel hat eine Priorität. Regeln werden in der Reihenfolge ihrer Prioritäten bewertet, ausgehend vom niedrigsten Wert hin zum höchsten Wert. Die Standardregel wird zuletzt ausgewertet. Sie können die Priorität einer nicht standardmäßigen Regel jederzeit ändern. Sie können die Priorität der Standardregel nicht ändern.

Regelaktion

Listener für VPC Lattice-Dienste unterstützen Forward-Aktionen und Fixed-Response-Aktionen.

Weiterleitungsaktionen

Sie können `forward` Aktionen verwenden, um Anfragen an eine oder mehrere VPC Lattice-Zielgruppen weiterzuleiten. Wenn Sie mehrere Zielgruppen für eine `forward`-Aktion angeben, müssen Sie für jede Zielgruppe eine Gewichtung angeben. Jede Zielgruppengewichtung ist ein Wert zwischen 0 und 999. Anforderungen, die einer Listener-Regel mit gewichteten Zielgruppen entsprechen, werden basierend auf ihren Gewichtungen an diese Zielgruppen verteilt. Wenn Sie beispielsweise zwei Zielgruppen mit einer Gewichtung von 10 angeben, erhält jede Zielgruppe die Hälfte der Anforderungen. Wenn Sie zwei Zielgruppen angeben, eine mit einer Gewichtung von 10 und die andere mit einer Gewichtung von 20, erhält die Zielgruppe mit der Gewichtung von 20 doppelt so viele Anforderungen wie die andere Zielgruppe.

Aktionen mit feststehender Antwort

Verwenden Sie `fixed-response`-Aktionen, um Client-Anforderungen zu verwerfen und eine benutzerdefinierte HTTP-Antwort zurückzugeben. Sie können diese Aktion verwenden, um einen 404- oder 500-Antwortcode zurückzugeben.

Example Beispiel einer festgelegten Antwortaktion für die AWS CLI

Sie können beim Erstellen oder Aktualisieren einer Regel eine Aktion angeben. Die folgende Aktion sendet eine feste Antwort mit dem angegebenen Statuscode.

```
"action": {
    "fixedResponse": {
        "statusCode": 404
},
```

Regelbedingungen

Jede Regelbedingung weist einen Typ und Bedingungsinformationen auf. Wenn die Bedingungen für eine Regel erfüllt sind, wird die dazugehörige Aktion durchgeführt.

Im Folgenden sind die unterstützten Übereinstimmungskriterien für eine Regel aufgeführt:

Header-Übereinstimmung

Das Routing basiert auf den HTTP-Headern für jede Anfrage. Mit HTTP-Header-Bedingungen können Sie Regeln konfigurieren, mit denen Anforderungen auf Grundlage der HTTP-Header für die Anforderung weitergeleitet werden. Sie können die Namen der standardmäßigen

oder benutzerdefinierten HTTP-Header-Felder angeben. Beim Headernamen und der Übereinstimmungsauswertung wird nicht zwischen Groß- und Kleinschreibung unterschieden. Sie können diese Einstellung ändern, indem Sie die Berücksichtigung von Groß- und Kleinschreibung aktivieren. Platzhalterzeichen werden im Header-Namen nicht unterstützt. Die Übereinstimmungen von Präfix, Exakt und Enthält werden beim Header-Abgleich unterstützt.

Methodenübereinstimmung

Das Routing basiert auf der HTTP-Anforderungsmethode jeder Anfrage.

Mit Bedingungen für HTTP-Anforderungsmethoden können Sie Regeln konfigurieren, mit denen Anforderungen auf Grundlage der HTTP-Anforderungsmethode der Anforderung weitergeleitet werden. Sie können standardmäßige oder benutzerdefinierte HTTP-Methoden angeben. Die Methode match unterscheidet zwischen Groß- und Kleinschreibung. Der Methodenname muss eine exakte Übereinstimmung sein. Platzhalterzeichen werden nicht unterstützt.

Pfadübereinstimmung

Das Routing basiert auf dem Abgleich der Pfadmuster in der Anfrage URLs.

Sie können Pfadbedingungen verwenden, um Regeln zu definieren, die Anfragen auf der Grundlage der URL in der Anfrage weiterleiten. Platzhalterzeichen werden nicht unterstützt. Präfix und exakte Übereinstimmung im Pfad werden unterstützt.

Hinzufügen einer Regel

Sie können jederzeit eine Listener-Regel hinzufügen.

Hinzufügen einer Listener-Regel mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Services aus.
3. Wählen Sie den Namen des Dienstes aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Routing die Option Listener bearbeiten aus.
5. Erweitern Sie Listener-Regeln und wählen Sie Regel hinzufügen aus.
6. Geben Sie für Rule name (Regelname) einen Namen für die Regel ein.
7. Geben Sie für Priorität eine Priorität zwischen 1 und 100 ein. Regeln werden in der Reihenfolge ihrer Prioritäten bewertet, ausgehend vom niedrigsten Wert hin zum höchsten Wert. Die Standardregel wird zuletzt ausgewertet.

8. Geben Sie unter Bedingung ein Pfadmuster für die Pfadübereinstimmungsbedingung ein. Die Maximalgröße jeder Zeichenfolge beträgt 200 Zeichen. Bei diesem Vergleich wird nicht zwischen Groß- und Kleinschreibung unterschieden. Platzhalterzeichen werden nicht unterstützt.

   Verwenden Sie das oder ein AWS SDK, um eine Regelbedingung für den Header AWS CLI - oder Methodenabgleich hinzuzufügen.
9. Wählen Sie für Action eine VPC Lattice-Zielgruppe aus.
10. Wählen Sie Änderungen speichern aus.

Hinzufügen einer Regel mithilfe der AWS CLI

Verwenden Sie den Befehl create-rule.

Aktualisieren einer Regel

Sie können eine Listener-Regel jederzeit aktualisieren. Sie können die Priorität, den Zustand, die Zielgruppe und die Gewichtung der einzelnen Zielgruppen ändern. Sie können den Namen der Regel nicht ändern.

So aktualisieren Sie eine Listener-Regel mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Services aus.
3. Wählen Sie den Namen des Dienstes aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Routing die Option Listener bearbeiten aus.
5. Ändern Sie die Regelprioritäten, -bedingungen und -aktionen nach Bedarf.
6. Überprüfen Sie Ihre Aktualisierungen und wählen Sie Änderungen speichern.

So aktualisieren Sie eine Regel mithilfe der AWS CLI

Verwenden Sie den Befehl update-rule.

Löschen einer Regel

Sie können die nicht standardmäßigen Regeln für einen Listener jederzeit löschen. Sie können die Standardregel für einen Listener nicht löschen. Wenn Sie einen Listener löschen, werden alle seine Regeln gelöscht.

Löschen einer Listener-Regel mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Services aus.
3. Wählen Sie den Namen des Dienstes aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Routing die Option Listener bearbeiten aus.
5. Suchen Sie die Regel und wählen Sie Entfernen aus.
6. Wählen Sie Änderungen speichern aus.

Löschen einer Regel mithilfe der AWS CLI

Verwenden Sie den Befehl delete-rule.

Löschen eines Listeners für Ihren VPC Lattice-Service

Sie können einen Listener jederzeit löschen. Wenn Sie einen Listener löschen, werden alle seine Regeln automatisch gelöscht.

Löschen eines Listener mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Services aus.
3. Wählen Sie den Namen des Dienstes aus, um die Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte Routing die Option Listener löschen aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

Um einen Listener mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-listener.

VPC-Ressourcen in Amazon VPC Lattice

Sie können VPC-Ressourcen mit anderen Teams in Ihrer Organisation oder mit externen unabhängigen Softwareanbietern (ISV) teilen. Eine VPC-Ressource kann eine AWS-native Ressource sein, z. B. eine Amazon RDS-Datenbank, ein Domainname oder eine IP-Adresse. Die Ressource kann sich in Ihrer VPC oder Ihrem lokalen Netzwerk befinden und muss nicht mit einem Lastenausgleich ausgestattet werden. Sie verwenden AWS RAM , um die Prinzipale anzugeben, die auf die Ressource zugreifen können. Sie erstellen ein Ressourcen-Gateway, über das auf Ihre Ressource zugegriffen werden kann. Sie erstellen auch eine Ressourcenkonfiguration, die die Ressource oder eine Gruppe von Ressourcen darstellt, die Sie gemeinsam nutzen möchten.

Die Principals, mit denen Sie die Ressource teilen, können über VPC-Endpunkte privat auf diese Ressourcen zugreifen. Sie können einen Ressourcen-VPC-Endpunkt verwenden, um auf eine Ressource zuzugreifen oder mehrere Ressourcen in einem VPC-Lattice-Dienstnetzwerk zu bündeln, und über einen VPC-Endpunkt des Servicenetzwerks auf das Servicenetzwerk zugreifen.

In den folgenden Abschnitten wird erklärt, wie VPC-Ressourcen in VPC Lattice erstellt und verwaltet werden:

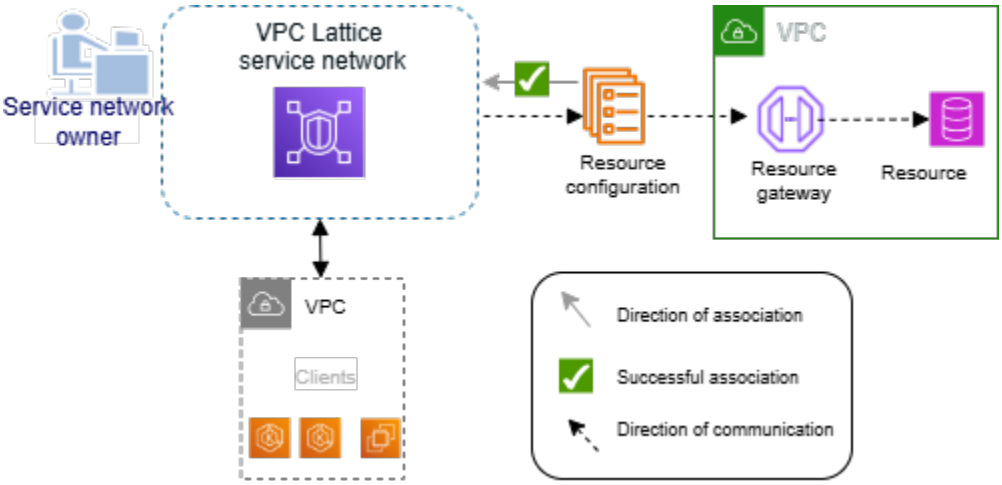
Themen

Ressourcen-Gateways in VPC Lattice

Ein Ressourcen-Gateway ist der Punkt, der Datenverkehr in die VPC empfängt, in der 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-Adresse des Datenverkehrs ist die IP-Adresse des Ressourcen-Gateways in einer Availability Zone. An ein Ressourcengateway können mehrere Ressourcenkonfigurationen mit jeweils mehreren Ressourcen angehängt werden.

Das folgende Diagramm zeigt, wie ein Client über das Resource Gateway auf eine Ressource zugreift:



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.

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

IP-Adresstypen

Ein Ressourcen-Gateway kann Dual-Stack-Adressen IPv6 oder Dual-Stack-Adressen haben 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 Resource 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 Resource 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 Resource IPv4 IPv6 Gateway-Netzwerkschnittstellen sowohl als auch Adressen zu. Diese Option wird nur unterstützt, wenn alle ausgewählten Subnetze sowohl als auch IPv6 Adressbereiche haben IPv4 und die Ressource entweder eine IPv4 Oder-Adresse hat. IPv6

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

Erstellen Sie ein Ressourcen-Gateway in VPC Lattice

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

Voraussetzung

Um ein Resource Gateway zu erstellen, muss in einem Subnetz ein /28-Block verfügbar sein.

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 IP-Typ für das Ressourcen-Gateway.
6. Wählen Sie die VPC aus, in der sich die Ressource befindet.
7. Wählen Sie bis zu fünf Sicherheitsgruppen aus, um den eingehenden Verkehr von der VPC zum Servicenetzwerk zu kontrollieren.
8. (Optional) Sie fügen ein Tag hinzu, indem Sie neues Tag hinzufügen auswählen und den Schlüssel und den Wert für das Tag eingeben.
9. Wählen Sie Create Resource Gateway aus.

Um ein Ressourcen-Gateway mit dem zu erstellen AWS CLI

Verwenden Sie den create-resource-gateway-Befehl.

Löschen Sie ein Ressourcen-Gateway in VPC Lattice

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

Um ein Ressourcen-Gateway mit der Konsole zu löschen

1. Öffnen Sie die 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 zu löschen, verwenden Sie AWS CLI

Verwenden Sie den delete-resource-gateway-Befehl.

Ressourcenkonfigurationen 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. Damit auf eine Ressource von einer anderen VPC aus zugegriffen werden kann, muss sie über eine Ressourcenkonfiguration verfügen.

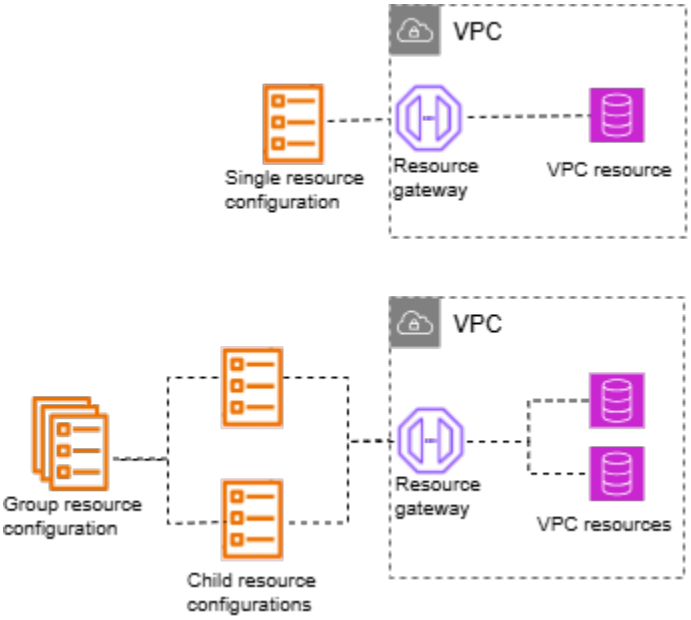
Inhalt

Arten von Ressourcenkonfigurationen

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

- Konfiguration einer einzelnen Ressource: Stellt eine IP-Adresse oder einen Domainnamen dar. Es kann unabhängig gemeinsam genutzt werden.
- Konfiguration von Gruppenressourcen: Es handelt sich um eine Sammlung von Konfigurationen untergeordneter Ressourcen. Es kann verwendet werden, um eine Gruppe von DNS- und IP-Adressendpunkten darzustellen.
- Konfiguration untergeordneter Ressourcen: Sie ist 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 einer Gruppe hinzugefügt und aus ihr 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 Jede Beziehung zwischen Gruppe und Kind wird automatisch berücksichtigt.

Die folgende Abbildung zeigt eine Konfiguration mit einer einzelnen Ressource, einer untergeordneten Ressource und einer Gruppenressource:



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 von den IP-Adressen des Ressourcen-Gateways in dieser VPC kommt.

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: Sie können jeden Domainnamen verwenden, 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.

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

Gemeinsame Nutzung von Ressourcenkonfigurationen über AWS RAM

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

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

Um von einer anderen 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 Sie eine Ressourcenkonfiguration in VPC Lattice

Verwenden Sie die Konsole, um eine Ressourcenkonfiguration zu erstellen.

Um eine Ressourcenkonfiguration mit der Konsole zu erstellen

1. Öffnen Sie die 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. Wählen Sie den Bezeichner für die Ressource aus, die diese Ressourcenkonfiguration darstellen soll.
8. Wählen Sie die Portbereiche aus, über die Sie die Ressource gemeinsam nutzen möchten.
9. Geben Sie unter Zuordnungseinstellungen an, ob diese Ressourcenkonfiguration mit gemeinsam nutzbaren Dienstnetzwerken verknüpft werden kann.
10. Wählen Sie unter Konfiguration gemeinsam genutzter Ressourcen die Ressourcenfreigaben aus, anhand derer die Prinzipale identifiziert werden, die auf diese Ressource zugreifen können.

11. (Optional) Aktivieren Sie unter Überwachung die Option Ressourcenzugriffsprotokolle und das Zustellungsziel, wenn Sie Anfragen und Antworten an und von der Ressourcenkonfiguration überwachen möchten.
12. (Optional) Sie fügen ein Tag hinzu, indem Sie neues Tag hinzufügen auswählen und den Schlüssel und den Wert für das Tag eingeben.
13. Wählen Sie „Ressourcenkonfiguration erstellen“.

Um eine Ressourcenkonfiguration mit dem zu erstellen AWS CLI

Verwenden Sie den create-resource-configuration-Befehl.

Zuordnungen für eine VPC-Lattice-Ressourcenkonfiguration verwalten

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

Verwalten Sie Dienstnetzwerkzuordnungen

Erstellen oder löschen Sie eine Dienstnetzwerkverbindung.

> **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. Wählen Sie Änderungen speichern aus.
9. Um eine Zuordnung zu löschen, aktivieren Sie das Kontrollkästchen für die Verknüpfung und wählen Sie dann Aktionen, Löschen aus. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Löschen aus.

Um eine Dienstnetzwerkverbindung mit dem zu erstellen AWS CLI

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

Um eine Dienstnetzwerkverbindung mit dem zu löschen AWS CLI

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

VPC-Endpunktzuordnungen verwalten

Verwalten Sie eine VPC-Endpunktverknüpfung.

So verwalten Sie eine VPC-Endpunktverknüpfung mithilfe der Konsole

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 Endpunktzuordnungen.
5. Wählen Sie die Zuordnungs-ID aus, um die zugehörige Detailseite zu öffnen. Von hier aus können Sie die Zuordnung ändern oder löschen.
6. Um eine neue Endpunktzuordnung zu erstellen, gehen Sie im linken Navigationsbereich zu PrivateLink und Lattice und wählen Sie Endpoints aus.
7. Wählen Sie Endpunkte erstellen aus.

8. Wählen Sie die Ressourcenkonfiguration aus, die Sie mit Ihrer VPC verbinden möchten.
9. Wählen Sie die VPC, Subnetze und Sicherheitsgruppen aus.
10. (Optional) Um VPC VPC-Endpunkt zu taggen, wählen Sie Neues Tag hinzufügen aus und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
11. Wählen Sie Endpunkt erstellen aus.

So erstellen Sie eine VPC-Endpunktzuweisung mit dem AWS CLI

Verwenden Sie den create-vpc-endpoint-Befehl.

Um eine VPC-Endpunktverknüpfung mit dem AWS CLI

Verwenden Sie den delete-vpc-endpoint-Befehl.

Teilen Sie Ihre VPC Lattice-Entitäten

Amazon VPC Lattice ist in AWS Resource Access Manager (AWS RAM) integriert, um die gemeinsame Nutzung von Services, Ressourcenkonfigurationen und Servicenetzwerken zu ermöglichen. AWS RAM ist ein Service, der es Ihnen ermöglicht, einige VPC Lattice-Entitäten mit anderen AWS-Konten oder durch andere zu teilen. AWS Organizations Mit können Sie Entitäten AWS RAM, die Ihnen gehören, gemeinsam nutzen, indem Sie eine Ressourcenfreigabe erstellen. Eine Ressourcenfreigabe gibt die Entitäten an, die gemeinsam genutzt werden sollen, und die Verbraucher, mit denen sie geteilt werden sollen. Zu den Verbrauchern können folgende Angaben zählen:

- AWS-Konten Spezifisch innerhalb oder außerhalb seiner Organisation in AWS Organizations.
- Eine Organisationseinheit innerhalb seiner Organisation in AWS Organizations.
- Eine ganze Organisation in AWS Organizations.

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

Inhalt

Voraussetzungen für die gemeinsame Nutzung von VPC Lattice-Entitäten

- Um eine Entität gemeinsam zu nutzen, müssen Sie sie in Ihrem besitzen. AWS-Konto Das bedeutet, dass die Entität Ihrem Konto zugewiesen oder bereitgestellt werden muss. Sie können eine Entität, die mit Ihnen geteilt wurde, nicht teilen.
- Um eine Entität mit Ihrer Organisation oder einer Organisationseinheit in zu teilen AWS Organizations, müssen Sie das Teilen mit aktivieren AWS Organizations. Weitere Informationen finden Sie unter Ressourcenfreigabe für AWS Organizations aktivieren im AWS RAM - Benutzerhandbuch.

VPC Lattice-Entitäten teilen

Um eine Entität gemeinsam zu nutzen, erstellen Sie zunächst eine gemeinsame Ressource mit AWS Resource Access Manager. Eine Ressourcenfreigabe gibt an, welche Entitäten gemeinsam genutzt werden sollen, mit welchen Verbrauchern sie geteilt werden und welche Aktionen Principals ausführen können.

Wenn Sie eine VPC Lattice-Entität, die Sie besitzen, mit anderen teilen AWS-Konten, ermöglichen Sie diesen Konten, ihre Entitäten mit Entitäten in Ihrem Konto zu verknüpfen. Wenn Sie eine Zuordnung für eine gemeinsam genutzte Entität erstellen, generieren wir einen Amazon-Ressourcennamen (ARN) im Konto des Rechtsträgers und in dem Konto, das die Zuordnung erstellt hat. Daher können sowohl der Eigentümer der Entität als auch das Konto, das die Zuordnung erstellt hat, die Zuordnung löschen.

Wenn Sie Teil einer Organisation sind AWS Organizations und das Teilen innerhalb Ihrer Organisation aktiviert ist, erhalten Verbraucher in Ihrer Organisation automatisch Zugriff auf die gemeinsam genutzte Entität. Andernfalls erhalten Verbraucher eine Einladung, dem Resource Share beizutreten, und erhalten nach Annahme der Einladung Zugriff auf die gemeinsame Entität.

Überlegungen

- Sie können drei Arten von VPC-Lattice-Entitäten gemeinsam nutzen: Dienstnetzwerke, Dienste und Ressourcenkonfigurationen.
- Sie können Ihre VPC Lattice-Entitäten mit allen teilen. AWS-Konto
- Sie können Ihre VPC Lattice-Entitäten nicht mit einzelnen IAM-Benutzern und -Rollen teilen.
- VPC Lattice unterstützt vom Kunden verwaltete Berechtigungen für Dienste, Ressourcenkonfigurationen und Servicenetzwerke.

So teilen Sie eine Entität, die Ihnen gehört, mithilfe der VPC Lattice-Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice Services, Service Networks oder Resource Configurations aus.
3. Wählen Sie den Namen der Entität aus, um deren Detailseite zu öffnen, und wählen Sie dann auf der Registerkarte Sharing Service, Share service network oder Share resource configuration aus.

4. Wählen Sie die AWS RAM Ressourcenfreigaben unter Ressourcenfreigaben aus.
   Um eine Ressourcenfreigabe zu erstellen, wählen Sie in der RAM-Konsole die Option Ressourcenfreigabe erstellen.
5. Wählen Sie „Dienst teilen“, „Dienstnetzwerk teilen“ oder „Ressourcenkonfiguration teilen“.

Um eine Entität, die Ihnen gehört, mithilfe der AWS RAM Konsole zu teilen

Verwenden Sie das unter Erstellen einer Ressourcenfreigabe im AWS RAM Benutzerhandbuch beschriebene Verfahren.

Um eine Entität, die Ihnen gehört, zu teilen, verwenden Sie den AWS CLI

Verwenden Sie den associate-resource-share-Befehl.

Beenden Sie die gemeinsame Nutzung von VPC-Lattice-Entitäten

Um die gemeinsame Nutzung einer VPC Lattice-Entität, die Sie besitzen, zu beenden, müssen Sie sie aus der Ressourcenfreigabe entfernen. Bestehende Verknüpfungen bleiben bestehen, nachdem Sie die gemeinsame Nutzung Ihrer Entität beendet haben. Neue Verknüpfungen zu einer zuvor gemeinsam genutzten Entität sind nicht zulässig. Wenn entweder der Entitätsbesitzer oder der Zuordnungsbesitzer eine Verknüpfung löscht, wird sie aus beiden Konten gelöscht. Wenn ein Kontoinhaber eine Ressourcenfreigabe verlassen möchte, muss er den Eigentümer der Ressourcenfreigabe bitten, sein Konto aus der Liste der Konten zu entfernen, mit denen diese Ressource geteilt wurde.

So beenden Sie die gemeinsame Nutzung einer Entität, die Ihnen gehört, mithilfe der VPC Lattice-Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice Services, Service Networks oder Resource Configurations aus.
3. Wählen Sie den Namen der Entität, um ihre Detailseite zu öffnen.
4. Aktivieren Sie auf der Registerkarte Freigabe das Kontrollkästchen für die Ressourcenfreigabe und wählen Sie dann Entfernen aus.

Um die gemeinsame Nutzung einer Entität, deren Eigentümer Sie sind, über die AWS RAM Konsole zu beenden

Weitere Informationen finden Sie unter Aktualisieren einer Ressourcenfreigabe im AWS RAM Benutzerhandbuch.

Um die gemeinsame Nutzung einer Entität zu beenden, die Ihnen gehört, verwenden Sie den AWS CLI

Verwenden Sie den disassociate-resource-share-Befehl.

Zuständigkeiten und Genehmigungen

Die folgenden Verantwortlichkeiten und Berechtigungen gelten für die Verwendung gemeinsam genutzter VPC Lattice-Entitäten.

Eigentümer von Entitäten

- Der Besitzer des Servicenetzwerks kann einen von einem Verbraucher erstellten Dienst nicht ändern.
- Der Besitzer des Dienstnetzwerks kann einen von einem Verbraucher erstellten Dienst nicht löschen.
- Der Besitzer des Servicenetzwerks kann alle Dienstzuordnungen für das Servicenetzwerk beschreiben.
- Der Besitzer des Servicenetzwerks kann jeden Dienst, der dem Servicenetzwerk zugeordnet ist, trennen, unabhängig davon, wer die Zuordnung erstellt hat.
- Der Besitzer des Servicenetzwerks kann alle VPC-Zuordnungen für das Dienstnetzwerk beschreiben.
- Der Besitzer des Servicenetzwerks kann jede VPC trennen, die ein Verbraucher dem Servicenetzwerk zugeordnet hat.
- Der Besitzer des Servicenetzwerks kann alle Ressourcenkonfigurationszuordnungen für das Dienstnetzwerk beschreiben.
- Der Besitzer des Dienstnetzwerks kann die Zuordnung zu jeder Ressourcenkonfiguration aufheben, die dem Dienstnetzwerk zugeordnet ist, unabhängig davon, wer die Zuordnung erstellt hat.
- Der Besitzer des Servicenetzwerks kann alle Endpunktzuordnungen für das Dienstnetzwerk beschreiben.
- Der Besitzer des Servicenetzwerks kann die Zuordnung aller Endpunkte, die dem Servicenetzwerk zugeordnet sind, aufheben, unabhängig davon, wer die Zuordnung erstellt hat.

- Der Dienstbesitzer kann alle Dienstnetzwerkzuordnungen mit dem Dienst beschreiben.
- Der Dienstbesitzer kann einen Dienst von jedem Dienstnetzwerk trennen, dem er zugeordnet ist.
- Der Besitzer der Ressourcenkonfiguration kann alle Netzwerkzuordnungen mit der Ressourcenkonfiguration beschreiben.
- Der Besitzer der Ressourcenkonfiguration kann eine Ressourcenkonfiguration von jedem Dienstnetzwerk trennen, dem sie zugeordnet ist.
- Der Besitzer des VPC-Endpunkts kann das Servicenetzwerk beschreiben, dem er zugeordnet ist.
- Der VPC-Endpunktbesitzer kann einen Endpunkt vom Servicenetzwerk trennen.
- Nur das Konto, das eine Zuordnung erstellt hat, kann die Zuordnung zwischen dem Servicenetzwerk und der VPC aktualisieren.

Verbraucher von Entitäten

- Der Verbraucher kann eine Service- oder Ressourcenkonfiguration, die er nicht erstellt hat, nicht löschen.
- Der Verbraucher kann nur die Dienste oder Ressourcenkonfigurationen trennen, die er einem Dienstnetzwerk zugeordnet hat.
- Der Verbraucher und der Netzwerkbesitzer können alle Verknüpfungen zwischen einem Dienstnetzwerk und einer Dienst- oder Ressourcenkonfiguration beschreiben.
- Der Verbraucher kann keine Dienstinformationen eines Dienstes oder Informationen zur Ressourcenkonfiguration einer Ressourcenkonfiguration abrufen, die ihm nicht gehört.
- Der Verbraucher kann alle Dienstzuordnungen und Ressourcenkonfigurationen beschreiben, die mit einem gemeinsamen Servicenetzwerk verknüpft sind.
- Der Verbraucher kann einen Dienst oder eine Ressourcenkonfiguration einem Shared-Servicenetzwerk zuordnen.
- Der Verbraucher kann alle VPC-Zuordnungen zu einem Shared Service Network sehen.
- Der Verbraucher kann eine VPC einem Shared Service Network zuordnen.
- Der Verbraucher kann nur das trennen VPCs , was er einem Servicenetzwerk zugeordnet hat.
- Der Verbraucher kann einen VPC-Endpunkt für ein Servicenetzwerk erstellen, um seine VPC mit einem Shared Service Network zu verbinden.
- Der Verbraucher kann nur den VPC-Endpunkt des Servicenetzwerks löschen, den er erstellt hat, um seine VPC mit einem Shared Service Network zu verbinden.

- Der Nutzer eines Shared Service kann einen Service nicht einem Service-Netzwerk zuordnen, das ihm nicht gehört.
- Der Nutzer eines Shared-Service-Netzwerks kann keine VPC oder einen Service zuordnen, den er nicht besitzt.
- Der Nutzer einer Konfiguration mit gemeinsam genutzten Ressourcen kann eine Ressourcenkonfiguration keinem Servicenetzwerk zuordnen, das ihm nicht gehört.
- Der Nutzer eines Shared Service Network kann keine VPC-, Service- oder Ressourcenkonfiguration zuordnen, die er nicht besitzt.
- Der Verbraucher kann eine Service-, Service-, Netzwerk- oder Ressourcenkonfiguration beschreiben, die mit ihm gemeinsam genutzt wird.
- Der Verbraucher kann zwei Entitäten nicht zuordnen, wenn beide mit ihm gemeinsam genutzt werden.

Kontoübergreifende Ereignisse

Wenn Eigentümer und Verbraucher von Entitäten Aktionen an einer gemeinsamen Entität ausführen, werden diese Aktionen als kontoübergreifende Ereignisse in AWS CloudTrail aufgezeichnet.

`CreateServiceNetworkResourceAssociationBySharee`

Wird an den Eigentümer der Entität gesendet, wenn ein Nutzer der Entität CreateServiceNetworkResourceAssociation mit einer gemeinsam genutzten Entität anruft. Wenn der Anrufer Eigentümer der Ressourcenkonfiguration ist, wird das Ereignis an den Besitzer des Dienstnetzwerks gesendet. Wenn der Anrufer Eigentümer des Dienstnetzwerks ist, wird das Ereignis an den Besitzer der Ressourcenkonfiguration gesendet.

`CreateServiceNetworkServiceAssociationBySharee`

Wird an den Eigentümer der Entität gesendet, wenn ein Entitätsnutzer CreateServiceNetworkServiceAssociationmit einer gemeinsam genutzten Entität anruft. Wenn der Dienst dem Anrufer gehört, wird das Ereignis an den Besitzer des Dienstnetzwerks gesendet. Wenn der Anrufer Eigentümer des Dienstnetzwerks ist, wird das Ereignis an den Eigentümer des Dienstes gesendet.

`CreateServiceNetworkVpcAssociationBySharee`

Wird an den Eigentümer der Entität gesendet, wenn ein Nutzer der Entität CreateServiceNetworkVpcAssociationüber ein Shared Service Network anruft.

`DeleteServiceNetworkResourceAssociationByOwner`

Wird an den Eigentümer der Assoziation gesendet, wenn der Eigentümer der Entität DeleteServiceNetworkResourceAssociation mit einer gemeinsam genutzten Entität anruft. Wenn der Anrufer Eigentümer der Ressourcenkonfiguration ist, wird das Ereignis an den Besitzer der Dienstnetzwerkzuordnung gesendet. Wenn der Anrufer Eigentümer des Dienstnetzwerks ist, wird das Ereignis an den Besitzer der Ressourcenzuordnung gesendet.

`DeleteServiceNetworkResourceAssociationBySharee`

Wird an den Eigentümer der Entität gesendet, wenn ein Entitätsnutzer DeleteServiceNetworkResourceAssociation mit einer gemeinsam genutzten Entität anruft. Wenn der Anrufer Eigentümer der Ressourcenkonfiguration ist, wird das Ereignis an den Besitzer des Dienstnetzwerks gesendet. Wenn der Anrufer Eigentümer des Dienstnetzwerks ist, wird das Ereignis an den Besitzer der Ressourcenkonfiguration gesendet.

`DeleteServiceNetworkServiceAssociationByOwner`

Wird an den Eigentümer der Assoziation gesendet, wenn der Eigentümer der Entität DeleteServiceNetworkServiceAssociationmit einer gemeinsam genutzten Entität anruft. Wenn der Dienst dem Anrufer gehört, wird das Ereignis an den Besitzer der Dienstnetzwerkverbindung gesendet. Wenn der Anrufer Eigentümer des Dienstnetzwerks ist, wird das Ereignis an den Eigentümer der Dienstverbindung gesendet.

`DeleteServiceNetworkServiceAssociationBySharee`

Wird an den Eigentümer der Entität gesendet, wenn ein Benutzer der Entität DeleteServiceNetworkServiceAssociationmit einer gemeinsam genutzten Entität anruft. Wenn der Dienst dem Anrufer gehört, wird das Ereignis an den Besitzer des Dienstnetzwerks gesendet. Wenn der Anrufer Eigentümer des Dienstnetzwerks ist, wird das Ereignis an den Eigentümer des Dienstes gesendet.

`DeleteServiceNetworkVpcAssociationByOwner`

Wird an den Eigentümer der Assoziation gesendet, wenn der Eigentümer der Entität über ein gemeinsames Servicenetzwerk anruft DeleteServiceNetworkVpcAssociation.

`DeleteServiceNetworkVpcAssociationBySharee`

Wird an den Eigentümer der Entität gesendet, wenn ein Nutzer der Entität DeleteServiceNetworkVpcAssociationüber ein Shared-Service-Netzwerk anruft.

`GetServiceBySharee`

Wird an den Eigentümer der Entität gesendet, wenn ein Nutzer der Entität über einen GetServicegemeinsam genutzten Dienst anruft.

`GetServiceNetworkBySharee`

Wird an den Eigentümer der Entität gesendet, wenn ein Nutzer der Entität GetServiceNetworküber ein Shared Service-Netzwerk anruft.

`GetServiceNetworkResourceAssociationBySharee`

Wird an den Eigentümer der Entität gesendet, wenn ein Entitätsverbraucher GetServiceNetworkResourceAssociation mit einer gemeinsam genutzten Entität anruft. Wenn der Anrufer Eigentümer der Ressourcenkonfiguration ist, wird das Ereignis an den Besitzer des Dienstnetzwerks gesendet. Wenn der Anrufer Eigentümer des Dienstnetzwerks ist, wird das Ereignis an den Besitzer der Ressourcenkonfiguration gesendet.

`GetServiceNetworkServiceAssociationBySharee`

Wird an den Eigentümer der Entität gesendet, wenn ein Entitätsnutzer GetServiceNetworkServiceAssociationmit einer gemeinsam genutzten Entität anruft. Wenn der Dienst dem Anrufer gehört, wird das Ereignis an den Besitzer des Dienstnetzwerks gesendet. Wenn der Anrufer Eigentümer des Dienstnetzwerks ist, wird das Ereignis an den Eigentümer des Dienstes gesendet.

`GetServiceNetworkVpcAssociationBySharee`

Wird an den Eigentümer der Entität gesendet, wenn ein Nutzer der Entität GetServiceNetworkVpcAssociationüber ein Shared Service Network anruft.

Im Folgenden finden Sie ein Beispiel für einen Eintrag für das `CreateServiceNetworkServiceAssociationBySharee` Ereignis.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
```

```
    },
    "eventTime": "2023-04-27T17:12:46Z",
    "eventSource": "vpc-lattice.amazonaws.com",
    "eventName": "CreateServiceNetworkServiceAssociationBySharee",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "vpc-lattice.amazonaws.com",
    "userAgent": "ec2.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "callerAccountId": "111122223333"
    },
    "requestID": "ddabb0a7-70c6-4f70-a6c9-00cbe8a6a18b",
    "eventID": "bd03cdca-7edd-4d50-b9c9-eaa89f4a47cd",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::VpcLattice::ServiceNetworkServiceAssociation",
            "ARN": "arn:aws:vpc-
lattice:region:123456789012:servicenetworkserviceassociation/snsa-0d5ea7bc72EXAMPLE"
        }
    ],
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

VPC Lattice für Oracle Database@AWS

VPC Lattice unterstützt AWS Managed Service Integrations for Oracle Database@AWS(ODB) und bietet Ihnen eine vereinfachte Konnektivität zwischen dem ODB-Netzwerk und vor Ort. AWS VPCs Um diese Konnektivität zu unterstützen, stellt VPC Lattice in Ihrem Namen die folgenden Entitäten bereit:

Standard-Servicenetzwerk

Das Standarddienstenetzwerk verwendet die Namenskonvention `default-odb-network-randomHash`

Standard-Endpunkt für das Servicenetzwerk

Es gibt keinen Namen für diese AWS Ressource.

Ressourcen-Gateway

Das Ressourcen-Gateway verwendet die Namenskonvention `default-odb-network-randomHash`

VPC Lattice unterstützt AWS verwaltete Service-Integrationen, die als verwaltete Integrationen in Ihr ODB-Netzwerk bezeichnet werden. Standardmäßig ist Oracle Cloud Infrastructure (OCI) Managed Backup to Amazon S3 aktiviert. Sie können wählen, ob Sie den selbstverwalteten Zugriff auf Amazon S3 aktivieren möchten.

Sobald Sie Ihr ODB-Netzwerk erstellt haben, können Sie die bereitgestellten Ressourcen mithilfe von oder anzeigen. AWS Management Console AWS CLI Der folgende Beispielbefehl listet die verwalteten Standardintegrationen des ODB-Netzwerks und alle anderen Ressourcen auf, die Sie möglicherweise für dieses Servicenetzwerk haben:

```
aws vpc-lattice list-service-network-resource-associations \
        --service-network-identifier default-odb-network-randomHash
```

Überlegungen

Die folgenden Überlegungen gelten für VPC Lattice für: Oracle Database@AWS

- Sie können das Standarddienstenetzwerk, den Servicenetzwerkendpunkt, das Ressourcen-Gateway oder andere von VPC Lattice bereitgestellte ODB-verwaltete Integrationen nicht

löschen. Um diese Entitäten zu löschen, löschen Sie Ihr ODB-Netzwerk oder deaktivieren Sie die verwalteten Integrationen.

- Clients können nur auf die verwalteten Integrationen im ODB-Netzwerk zugreifen. Clients außerhalb des ODB-Netzwerks, z. B. in Ihrem VPCs, können diese verwalteten Integrationen nicht für den Zugriff auf S3 verwenden.
- Sie können keine Verbindung zu einer der verwalteten Integrationen außerhalb des von VPC Lattice bereitgestellten ODB-Netzwerks herstellen.
- Der gesamte Datenverkehr zu Amazon S3 wird über den Standard-Endpunkt des Service-Netzwerks abgewickelt, und es fallen die üblichen Bearbeitungsgebühren für den Zugriff auf Ressourcen an. Weitere Informationen finden Sie unter Preise für VPC Lattice.
- Für Oracle Database@AWS verwaltete Integrationen fallen keine Stundengebühren an.
- Sie können die von VPC Lattice bereitgestellten Ressourcen wie jedes andere Servicenetzwerk verwalten. Sie können das Standarddienstnetzwerk mit anderen AWS-Konten oder Organisationen gemeinsam nutzen und dem Standardnetzwerk neue Endpunkte, VPC-Zuordnungen, VPC Lattice-Dienste und Ressourcen hinzufügen.
- Die folgenden Berechtigungen sind erforderlich, damit VPC Lattice Ressourcen bereitstellen Oracle Database@AWS kann:

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
         "Sid": "AllowODBEC2andLatticeActions",
         "Action": [
             "ec2:DescribeVpcs",
             "ec2:CreateTags",
             "ec2:DescribeAvailabilityZones",
             "ec2:CreateOdbNetworkPeering",
             "ec2:DeleteOdbNetworkPeering",
             "ec2:ModifyOdbNetworkPeering",
             "ec2:DescribeVpcEndpointAssociations",
             "ec2:CreateVpcEndpoint",
             "ec2:DeleteVpcEndpoints",
             "ec2:DescribeVpcEndpoints",
             "vpc-lattice:CreateServiceNetwork",
             "vpc-lattice:DeleteServiceNetwork",
             "vpc-lattice:GetServiceNetwork",
             "vpc-lattice:CreateServiceNetworkResourceAssociation",
             "vpc-lattice:DeleteServiceNetworkResourceAssociation",
```

```
                "vpc-lattice:GetServiceNetworkResourceAssociation",
                "vpc-lattice:CreateResourceGateway",
                "vpc-lattice:DeleteResourceGateway",
                "vpc-lattice:GetResourceGateway",
                "vpc-lattice:CreateServiceNetworkVpcEndpointAssociation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
    "Sid": "AllowSLRActionsForLattice",
    "Effect": "Allow",
    "Action": [
     "iam:CreateServiceLinkedRole"
    ],
    "Resource": "*",
     "Condition": {
      "StringEquals": {
       "iam:AWSServiceName": [
        "vpc-lattice.amazonaws.com"
       ]
      }
     }
   }
    ]
}
```

Um VPC Lattice für zu verwenden, empfehlen wir Oracle Database@AWS, dass Sie mit Servicenetzwerken, Dienstnetzwerkzuordnungen und Ressourcen-Gateways in VPC Lattice vertraut sind.

Themen

- the section called “Von Oracle Cloud Infrastructure (OCI) verwaltetes Backup auf Amazon S3”
- the section called “Amazon S3 S3-Zugriff”
- the section called “Greifen Sie auf VPC Lattice-Entitäten zu und teilen Sie sie”

Von Oracle Cloud Infrastructure (OCI) verwaltetes Backup auf Amazon S3

Wenn Sie eine Oracle Database@AWS Datenbank erstellen, erstellt VPC Lattice eine Ressourcenkonfiguration namens. `odb-managed-s3-backup-access` Diese Ressourcenkonfiguration stellt ein OCI-verwaltetes Backup Ihrer Datenbanken auf Amazon S3 dar und ermöglicht nur die Konnektivität zu Amazon S3 S3-Buckets, die OCI gehören. Der Verkehr zwischen dem ODB-Netzwerk und S3 verlässt niemals das Amazon-Netzwerk.

Amazon S3 S3-Zugriff

Zusätzlich zum OCI Managed Backup to Amazon S3 können Sie eine verwaltete Integration erstellen, die den Zugriff auf Amazon S3 vom ODB-Netzwerk aus ermöglicht. Wenn Sie das Oracle Database@AWS Netzwerk ändern, um die verwaltete Amazon S3 Access-Integration zu aktivieren, stellt VPC Lattice eine Ressourcenkonfiguration bereit, die `odb-s3-access` im Standard-Servicenetzwerk aufgerufen wird. Sie können diese Integration verwenden, um für Ihre eigenen Bedürfnisse auf Amazon S3 zuzugreifen, einschließlich selbstverwalteter Backups oder Wiederherstellungen. Sie können die Perimeterkontrolle einrichten, indem Sie eine Authentifizierungsrichtlinie angeben.

Überlegungen

Die folgenden Überlegungen gelten für die verwaltete Amazon S3 Access-Integration:

- Sie können nur eine verwaltete Amazon S3 Access-Integration für das ODB-Netzwerk erstellen.
- Diese verwaltete Integration ermöglicht den Zugriff auf Amazon S3 nur über das ODB-Netzwerk und nicht über andere VPC-Zuordnungen oder Service-Netzwerk-Endpunkte im Standard-Servicenetzwerk.
- Sie können nicht auf S3-Buckets in verschiedenen Regionen zugreifen. AWS

Aktivieren Sie die verwaltete Amazon S3 Access-Integration

Verwenden Sie den folgenden Befehl, um die verwaltete Amazon S3 Access-Integration zu aktivieren:

```
aws odb modify-odb-network --enable-s3-access
```

Sicherer Zugriff mit einer Authentifizierungsrichtlinie

Sie können den Zugriff auf S3-Buckets sichern, indem Sie mithilfe der ODB-API eine Authentifizierungsrichtlinie definieren. Die folgende Beispielrichtlinie gewährt Zugriff auf bestimmte S3-Buckets, die einer bestimmten Organisation gehören.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1515115909152",
  "Statement": [
    {
      "Sid": "GrantAccessToMyOrgS3",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::awsexamplebucket1",
        "arn:aws:s3:::awsexamplebucket1/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceOrgID": "o-abcd1234"
        }
      }
    }
  ]
}
```

> **Note**
>
> Die `aws:VpcSourceIp` Bedingungsschlüssel `aws:SourceVpcaws:SourceVpce`, und werden für S3-Bucket-Richtlinien nicht unterstützt, wenn ODB-verwaltete Integrationen verwendet werden.

Greifen Sie auf VPC Lattice-Entitäten zu und teilen Sie sie

Sie können Ihr ODB-Netzwerk auch mit Diensten, Ressourcen und anderen Clients verbinden, VPCs indem Sie VPC Lattice verwenden. Diese Konnektivitätsoptionen werden über das

Standarddienstenetzwerk, das Ressourcen-Gateway und den von VPC Lattice bereitgestellten Servicenetzwerk-Endpunkt bereitgestellt.

Greifen Sie auf VPC Lattice-Dienste und -Ressourcen zu

Um auf andere Entitäten zuzugreifen, ordnen Sie Dienste oder Ressourcen, die Ihnen gehören oder die Sie mit Ihnen gemeinsam nutzen, dem Standarddienstnetzwerk zu. Clients im ODB-Netzwerk können über den Standard-Endpunkt des Dienstnetzwerks auf die Dienste oder Ressourcen zugreifen.

Überlegungen

Im Folgenden finden Sie Überlegungen zum Herstellen einer Verbindung zu anderen VPC Lattice-Entitäten:

- Sie können dem Dienstnetzwerk neue Dienstnetzwerkendpunkte, VPC-Zuordnungen, VPC-Lattice-Ressourcen und -Dienste hinzufügen, aber Sie können die von VPC Lattice im Namen des ODB-Netzwerks bereitgestellten Ressourcen nicht ändern. Diese Oracle Database@AWS APIs müssen über den verwaltet werden.

Teilen Sie Ihr ODB-Netzwerk über VPC Lattice

Sie können Ihre ODB-Netzwerkressourcen mit Kunden in anderen VPCs Konten oder vor Ort teilen. Erstellen Sie zunächst eine Ressourcenkonfiguration für die Ressourcen, die Sie gemeinsam nutzen möchten. Die Ressourcenkonfigurationen müssen das Standard-Ressourcen-Gateway für Ihr ODB-Netzwerk verwenden. Anschließend können Sie die Ressourcen Ihrem Standarddienstenetzwerk zuordnen.

Clients in anderen Ländern VPCs oder mit AWS-Konten denen Sie Ihr Servicenetzwerk geteilt haben, können über ihre eigenen Servicenetzwerk-Endpunkte oder VPC-Zuordnungen auf diese Ressourcen zugreifen. Weitere Informationen finden Sie unter the section called “Verknüpfungen verwalten”.

Überlegungen

Im Folgenden finden Sie Hinweise zur gemeinsamen Nutzung Ihres ODB-Netzwerks:

- Wir empfehlen, ODB-Netzwerkinstanzen nur als IP-basierte Ressourcen gemeinsam zu nutzen.
- VPC Lattice unterstützt den Single Client Access Name (SCAN) -Listener-DNS von OCI nicht.

Sicherheit in Amazon VPC Lattice

Cloud-Sicherheit hat höchste AWS Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, in der AWS Dienste ausgeführt werden. AWS Cloud AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon VPC Lattice gelten, finden Sie unter AWS Services im Bereich nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Sie sind dafür verantwortlich, die Kontrolle über Ihre Inhalte zu behalten, die auf dieser Infrastruktur gehostet werden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von VPC Lattice anwenden können. In den folgenden Themen erfahren Sie, wie Sie VPC Lattice konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS Dienste verwenden, die Ihnen helfen, Ihren VPC Lattice-Dienst, Ihre Servicenetzwerke und Ressourcenkonfigurationen zu überwachen und zu sichern.

Inhalt

Zugriff auf VPC Lattice-Dienste verwalten

VPC Lattice ist standardmäßig sicher, da Sie explizit angeben müssen, auf welche Dienste und Ressourcenkonfigurationen Sie Zugriff gewähren möchten und mit welchen. VPCs Sie können über eine VPC-Zuordnung oder einen VPC-Endpunkt vom Typ Dienstnetzwerk auf Dienste zugreifen. In Szenarien mit mehreren Konten können Sie Dienste, Ressourcenkonfigurationen und Dienstnetzwerke über Kontogrenzen hinweg gemeinsam nutzen AWS Resource Access Manager.

VPC Lattice bietet ein Framework, mit dem Sie eine defense-in-depth Strategie auf mehreren Ebenen des Netzwerks implementieren können.

- Erste Ebene — Die Verbindung zwischen Dienst, Ressource, VPC und VPC-Endpunkt mit einem Servicenetzwerk. Eine VPC kann entweder über eine Assoziation oder über einen VPC-Endpunkt mit einem Servicenetzwerk verbunden sein. Wenn eine VPC nicht mit einem Dienstnetzwerk verbunden ist, können Clients in der VPC nicht auf die Dienst- und Ressourcenkonfigurationen zugreifen, die dem Dienstnetzwerk zugeordnet sind.
- Zweite Ebene — Optionaler Sicherheitsschutz auf Netzwerkebene für das Servicenetzwerk, z. B. Sicherheitsgruppen und Netzwerk. ACLs Mit diesen können Sie den Zugriff auf bestimmte Gruppen von Clients in einer VPC statt auf alle Clients in der VPC zulassen.
- Dritte Ebene — Optionale VPC Lattice-Authentifizierungsrichtlinie. Sie können eine Authentifizierungsrichtlinie auf Dienstnetzwerke und einzelne Dienste anwenden. In der Regel wird die Authentifizierungsrichtlinie im Servicenetzwerk vom Netzwerk- oder Cloud-Administrator verwaltet, und sie implementieren eine grobe Autorisierung. Beispielsweise werden nur authentifizierte Anfragen von einer bestimmten Organisation zugelassen. AWS Organizations Bei einer Authentifizierungsrichtlinie auf Dienstebene legt der Dienstbesitzer in der Regel detaillierte Kontrollen fest, die möglicherweise restriktiver sind als die grobkörnige Autorisierung, die auf Dienstnetzwerkebene angewendet wird.

> **Note**
>
> Die Authentifizierungsrichtlinie im Servicenetzwerk gilt nicht für Ressourcenkonfigurationen im Servicenetzwerk.

Methoden der Zugriffskontrolle

- Authentifizierungsrichtlinien

- Sicherheitsgruppen
- Netzwerk ACLs

Steuern Sie den Zugriff auf VPC Lattice-Dienste mithilfe von Authentifizierungsrichtlinien

VPC Lattice-Authentifizierungsrichtlinien sind IAM-Richtliniendokumente, die Sie an Dienstnetzwerke oder Dienste anhängen, um zu steuern, ob ein bestimmter Principal Zugriff auf eine Gruppe von Diensten oder einen bestimmten Dienst hat. Sie können jedem Dienstnetzwerk oder Dienst, auf den Sie den Zugriff kontrollieren möchten, eine Authentifizierungsrichtlinie hinzufügen.

> **Note**
>
> Die Authentifizierungsrichtlinie im Servicenetzwerk gilt nicht für Ressourcenkonfigurationen im Servicenetzwerk.

Authentifizierungsrichtlinien unterscheiden sich von identitätsbasierten IAM-Richtlinien. Identitätsbasierte IAM-Richtlinien sind IAM-Benutzern, -Gruppen oder -Rollen zugeordnet und definieren, welche Aktionen diese Identitäten auf welchen Ressourcen ausführen können. Authentifizierungsrichtlinien sind an Dienste und Dienstnetzwerke angehängt. Damit die Autorisierung erfolgreich ist, müssen sowohl Authentifizierungsrichtlinien als auch identitätsbasierte Richtlinien explizite Zulassungsanweisungen enthalten. Weitere Informationen finden Sie unter Wie funktioniert die Autorisierung.

Sie können die AND-Konsole verwenden, um Authentifizierungsrichtlinien für Dienste AWS CLI und Dienstnetzwerke anzuzeigen, hinzuzufügen, zu aktualisieren oder zu entfernen. Wenn Sie eine Authentifizierungsrichtlinie hinzufügen, aktualisieren oder entfernen, kann es einige Minuten dauern, bis sie fertig ist. Stellen Sie bei der Verwendung von sicher AWS CLI, dass Sie sich in der richtigen Region befinden. Sie können entweder die Standardregion für Ihr Profil ändern oder den `--region` Parameter zusammen mit dem Befehl verwenden.

Inhalt

- Allgemeine Elemente einer Authentifizierungsrichtlinie
- Ressourcenformat für Authentifizierungsrichtlinien
- Bedingungsschlüssel, die in Authentifizierungsrichtlinien verwendet werden können

- Anonyme (nicht authentifizierte) Prinzipale
- Beispiel für Authentifizierungsrichtlinien
- Wie funktioniert die Autorisierung

Um mit Authentifizierungsrichtlinien zu beginnen, folgen Sie dem Verfahren zum Erstellen einer Authentifizierungsrichtlinie, die für ein Dienstnetzwerk gilt. Für restriktivere Berechtigungen, die Sie nicht auf andere Dienste anwenden möchten, können Sie optional Authentifizierungsrichtlinien für einzelne Dienste festlegen.

Verwalten Sie den Zugriff auf ein Servicenetzwerk mit Authentifizierungsrichtlinien

Die folgenden AWS CLI Aufgaben zeigen Ihnen, wie Sie den Zugriff auf ein Servicenetzwerk mithilfe von Authentifizierungsrichtlinien verwalten. Anweisungen zur Verwendung der Konsole finden Sie unterServicenetzwerke in VPC Lattice.

Aufgaben

- Fügen Sie einem Dienstnetzwerk eine Authentifizierungsrichtlinie hinzu
- Ändern Sie den Authentifizierungstyp eines Servicenetzwerks
- Entfernen Sie eine Authentifizierungsrichtlinie aus einem Servicenetzwerk

Fügen Sie einem Dienstnetzwerk eine Authentifizierungsrichtlinie hinzu

Folgen Sie den Schritten in diesem Abschnitt, um Folgendes AWS CLI zu verwenden:

- Aktivieren Sie die Zugriffskontrolle in einem Servicenetzwerk mithilfe von IAM.
- Fügen Sie dem Dienstnetzwerk eine Authentifizierungsrichtlinie hinzu. Wenn Sie keine Authentifizierungsrichtlinie hinzufügen, wird für den gesamten Datenverkehr die Fehlermeldung „Zugriff verweigert“ angezeigt.

Um die Zugriffskontrolle zu aktivieren und eine Authentifizierungsrichtlinie zu einem neuen Servicenetzwerk hinzuzufügen

1. Um die Zugriffskontrolle in einem Dienstnetzwerk zu aktivieren, sodass dieses eine Authentifizierungsrichtlinie verwenden kann, verwenden Sie den create-service-network Befehl mit der `--auth-type` Option und dem Wert von. `AWS_IAM`

```
aws vpc-lattice create-service-network --name Name --auth-type AWS_IAM [--
tags TagSpecification]
```

Bei erfolgreicher Ausführung gibt der Befehl eine Ausgabe zurück, die in etwa wie folgt aussieht:

```
{
   "arn": "arn",
   "authType": "AWS_IAM",
   "id": "sn-0123456789abcdef0",
   "name": "Name"
}
```

2. Verwenden Sie den put-auth-policy Befehl und geben Sie die ID des Dienstnetzwerks an, dem Sie die Authentifizierungsrichtlinie hinzufügen möchten, sowie die Authentifizierungsrichtlinie, die Sie hinzufügen möchten.

   Verwenden Sie beispielsweise den folgenden Befehl, um eine Authentifizierungsrichtlinie für das Dienstnetzwerk mit der ID zu erstellen. *sn-0123456789abcdef0*

   ```
   aws vpc-lattice put-auth-policy --resource-identifier sn-0123456789abcdef0 --
   policy file://policy.json
   ```

   Verwenden Sie JSON, um eine Richtliniendefinition zu erstellen. Weitere Informationen finden Sie unter Allgemeine Elemente einer Authentifizierungsrichtlinie.

   Bei erfolgreicher Ausführung gibt der Befehl eine Ausgabe zurück, die in etwa wie folgt aussieht:

   ```
   {
      "policy": "policy",
      "state": "Active"
   }
   ```

Um die Zugriffskontrolle zu aktivieren und einem vorhandenen Servicenetzwerk eine Authentifizierungsrichtlinie hinzuzufügen

1. Um die Zugriffskontrolle in einem Dienstnetzwerk zu aktivieren, sodass dieses eine Authentifizierungsrichtlinie verwenden kann, verwenden Sie den update-service-network Befehl mit der `--auth-type` Option und dem Wert von. `AWS_IAM`

```
aws vpc-lattice update-service-network --service-network-
identifier sn-0123456789abcdef0 --auth-type AWS_IAM
```

Bei erfolgreicher Ausführung gibt der Befehl eine Ausgabe zurück, die in etwa wie folgt aussieht:

```
{
   "arn": "arn",
   "authType": "AWS_IAM",
   "id": "sn-0123456789abcdef0",
   "name": "Name"
}
```

2. Verwenden Sie den put-auth-policy Befehl und geben Sie die ID des Dienstnetzwerks an, dem Sie die Authentifizierungsrichtlinie hinzufügen möchten, sowie die Authentifizierungsrichtlinie, die Sie hinzufügen möchten.

```
aws vpc-lattice put-auth-policy --resource-identifier sn-0123456789abcdef0 --
policy file://policy.json
```

Verwenden Sie JSON, um eine Richtliniendefinition zu erstellen. Weitere Informationen finden Sie unter Allgemeine Elemente einer Authentifizierungsrichtlinie.

Bei erfolgreicher Ausführung gibt der Befehl eine Ausgabe zurück, die in etwa wie folgt aussieht:

```
{
   "policy": "policy",
   "state": "Active"
}
```

Ändern Sie den Authentifizierungstyp eines Servicenetzwerks

Um die Authentifizierungsrichtlinie für ein Servicenetzwerk zu deaktivieren

Verwenden Sie den update-service-network Befehl mit der `--auth-type` Option und dem Wert. `NONE`

```
aws vpc-lattice update-service-network --service-network-
identifier sn-0123456789abcdef0 --auth-type NONE
```

Wenn Sie die Authentifizierungsrichtlinie später erneut aktivieren müssen, führen Sie diesen Befehl mit den für die `--auth-type` Option `AWS_IAM` angegebenen Werten aus.

Entfernen Sie eine Authentifizierungsrichtlinie aus einem Servicenetzwerk

Um eine Authentifizierungsrichtlinie aus einem Servicenetzwerk zu entfernen

Verwenden Sie den delete-auth-policy-Befehl.

```
aws vpc-lattice delete-auth-policy --resource-identifier sn-0123456789abcdef0
```

Die Anforderung schlägt fehl, wenn Sie eine Authentifizierungsrichtlinie entfernen, bevor Sie den Authentifizierungstyp eines Dienstnetzwerks in ändern. `NONE`

Verwalten Sie den Zugriff auf einen Dienst mit Authentifizierungsrichtlinien

Die folgenden AWS CLI Aufgaben zeigen Ihnen, wie Sie den Zugriff auf einen Dienst mithilfe von Authentifizierungsrichtlinien verwalten. Anweisungen zur Verwendung der Konsole finden Sie unterDienstleistungen in VPC Lattice.

Aufgaben

- Fügen Sie einem Dienst eine Authentifizierungsrichtlinie hinzu
- Ändern Sie den Authentifizierungstyp eines Dienstes
- Entfernen Sie eine Authentifizierungsrichtlinie aus einem Dienst

Fügen Sie einem Dienst eine Authentifizierungsrichtlinie hinzu

Gehen Sie wie folgt vor, um das AWS CLI zu verwenden:

- Aktivieren Sie die Zugriffskontrolle für einen Dienst mithilfe von IAM.
- Fügen Sie dem Dienst eine Authentifizierungsrichtlinie hinzu. Wenn Sie keine Authentifizierungsrichtlinie hinzufügen, wird für den gesamten Datenverkehr die Fehlermeldung „Zugriff verweigert“ angezeigt.

Um die Zugriffskontrolle zu aktivieren und einem neuen Dienst eine Authentifizierungsrichtlinie hinzuzufügen

1. Um die Zugriffskontrolle für einen Dienst zu aktivieren, sodass dieser eine Authentifizierungsrichtlinie verwenden kann, verwenden Sie den create-service Befehl mit der `--auth-type` Option und dem Wert von. `AWS_IAM`

   ```
   aws vpc-lattice create-service --name Name --auth-type AWS_IAM [--
   tags TagSpecification]
   ```

   Bei erfolgreicher Ausführung gibt der Befehl eine Ausgabe zurück, die in etwa wie folgt aussieht:

   ```
   {
      "arn": "arn",
      "authType": "AWS_IAM",
      "dnsEntry": {
         ...
      },
      "id": "svc-0123456789abcdef0",
      "name": "Name",
      "status": "CREATE_IN_PROGRESS"
   }
   ```

2. Verwenden Sie den put-auth-policy Befehl und geben Sie die ID des Dienstes an, dem Sie die Authentifizierungsrichtlinie hinzufügen möchten, sowie die Authentifizierungsrichtlinie, die Sie hinzufügen möchten.

   Verwenden Sie beispielsweise den folgenden Befehl, um eine Authentifizierungsrichtlinie für den Dienst mit der ID zu erstellen. *svc-0123456789abcdef0*

   ```
   aws vpc-lattice put-auth-policy --resource-identifier svc-0123456789abcdef0 --
   policy file://policy.json
   ```

   Verwenden Sie JSON, um eine Richtliniendefinition zu erstellen. Weitere Informationen finden Sie unter Allgemeine Elemente einer Authentifizierungsrichtlinie.

   Bei erfolgreicher Ausführung gibt der Befehl eine Ausgabe zurück, die in etwa wie folgt aussieht:

   ```
   {
      "policy": "policy",
   ```

```
   "state": "Active"
}
```

Um die Zugriffskontrolle zu aktivieren und einem vorhandenen Dienst eine Authentifizierungsrichtlinie hinzuzufügen

1. Um die Zugriffskontrolle für einen Dienst zu aktivieren, sodass dieser eine Authentifizierungsrichtlinie verwenden kann, verwenden Sie den update-service Befehl mit der `--auth-type` Option und dem Wert von. `AWS_IAM`

   ```
   aws vpc-lattice update-service --service-identifier svc-0123456789abcdef0 --auth-type AWS_IAM
   ```

   Bei erfolgreicher Ausführung gibt der Befehl eine Ausgabe zurück, die in etwa wie folgt aussieht:

   ```
   {
      "arn": "arn",
      "authType": "AWS_IAM",
      "id": "svc-0123456789abcdef0",
      "name": "Name"
   }
   ```

2. Verwenden Sie den put-auth-policy Befehl und geben Sie die ID des Dienstes an, dem Sie die Authentifizierungsrichtlinie hinzufügen möchten, sowie die Authentifizierungsrichtlinie, die Sie hinzufügen möchten.

   ```
   aws vpc-lattice put-auth-policy --resource-identifier svc-0123456789abcdef0 --policy file://policy.json
   ```

   Verwenden Sie JSON, um eine Richtliniendefinition zu erstellen. Weitere Informationen finden Sie unter Allgemeine Elemente einer Authentifizierungsrichtlinie.

   Bei erfolgreicher Ausführung gibt der Befehl eine Ausgabe zurück, die in etwa wie folgt aussieht:

   ```
   {
      "policy": "policy",
      "state": "Active"
   }
   ```

Ändern Sie den Authentifizierungstyp eines Dienstes

Um die Authentifizierungsrichtlinie für einen Dienst zu deaktivieren

Verwenden Sie den update-service Befehl mit der `--auth-type` Option und dem Wert. `NONE`

```
aws vpc-lattice update-service --service-identifier svc-0123456789abcdef0 --auth-type
 NONE
```

Wenn Sie die Authentifizierungsrichtlinie später erneut aktivieren müssen, führen Sie diesen Befehl mit den für die `--auth-type` Option `AWS_IAM` angegebenen Werten aus.

Entfernen Sie eine Authentifizierungsrichtlinie aus einem Dienst

Um eine Authentifizierungsrichtlinie aus einem Dienst zu entfernen

Verwenden Sie den delete-auth-policy-Befehl.

```
aws vpc-lattice delete-auth-policy --resource-identifier svc-0123456789abcdef0
```

Die Anforderung schlägt fehl, wenn Sie eine Authentifizierungsrichtlinie entfernen, bevor Sie den Authentifizierungstyp des Dienstes in ändern. `NONE`

Wenn Sie Authentifizierungsrichtlinien aktivieren, die authentifizierte Anfragen an einen Dienst erfordern, müssen alle Anfragen an diesen Dienst eine gültige Anforderungssignatur enthalten, die mit Signature Version 4 (Sigv4) berechnet wurde. Weitere Informationen finden Sie unter SIGv4 authentifizierte Anfragen für Amazon VPC Lattice.

Allgemeine Elemente einer Authentifizierungsrichtlinie

VPC Lattice-Authentifizierungsrichtlinien werden mit derselben Syntax wie IAM-Richtlinien angegeben. Weitere Informationen finden Sie unter Identitätsbasierte Richtlinien und ressourcenbasierte Richtlinien im IAM-Benutzerhandbuch.

Eine Authentifizierungsrichtlinie enthält die folgenden Elemente:

- Schulleiter — Die Person oder Anwendung, der Zugriff auf die Aktionen und Ressourcen in der Anweisung gewährt wird. In einer Authentifizierungsrichtlinie ist der Principal die IAM-Entität, die der Empfänger dieser Berechtigung ist. Der Principal wird als IAM-Entität authentifiziert, um

Anfragen an eine bestimmte Ressource oder eine Gruppe von Ressourcen zu stellen, wie dies bei Diensten in einem Dienstnetzwerk der Fall ist.

Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder Dienste umfassen. AWS Weitere Informationen finden Sie unter AWS JSON-Richtlinienelemente: Principal im IAM-Benutzerhandbuch.

- Effekt — Der Effekt, wenn der angegebene Principal die bestimmte Aktion anfordert. Dies kann entweder `Allow` oder `Denysein`. Wenn Sie die Zugriffskontrolle für einen Dienst oder ein Dienstnetzwerk mithilfe von IAM aktivieren, sind Prinzipale standardmäßig nicht berechtigt, Anfragen an den Dienst oder das Dienstnetzwerk zu stellen.
- Aktionen — Die spezifische API-Aktion, für die Sie die Erlaubnis erteilen oder verweigern. VPC Lattice unterstützt Aktionen, die das Präfix verwenden. `vpc-lattice-svcs` Weitere Informationen finden Sie unter Von Amazon VPC Lattice Services definierte Aktionen in der Service Authorization Reference.
- Ressourcen — Die Dienste, die von der Aktion betroffen sind.
- Bedingung — Die Bedingungen sind optional. Sie können sie verwenden, um zu kontrollieren, wann Ihre Richtlinie in Kraft tritt. Weitere Informationen finden Sie unter Bedingungsschlüssel für Amazon VPC Lattice Services in der Service Authorization Reference.

Wenn Sie Authentifizierungsrichtlinien erstellen und verwalten, möchten Sie möglicherweise den IAM-Richtliniengenerator verwenden.

Anforderung

Die Richtlinie in JSON darf keine neuen Zeilen oder Leerzeilen enthalten.

Ressourcenformat für Authentifizierungsrichtlinien

Sie können den Zugriff auf bestimmte Ressourcen einschränken, indem Sie eine Authentifizierungsrichtlinie erstellen, die ein passendes Schema mit einem `<serviceARN>/<path>` Muster verwendet und das `Resource` Element codiert, wie in den folgenden Beispielen gezeigt.

Protokoll	Beispiele
HTTP	• `"Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:ser`

Protokoll	Beispiele
	vice/svc-0123456789abcdef0/rates" • "Resource": "*/rates" • "Resource": "*/*"
gRPC	• "Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/api.parking/GetRates" • "Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/api.parking/*" • "Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/*"

Verwenden Sie das folgende Amazon Resource Name (ARN) -Ressourcenformat für<serviceARN>:

```
arn:aws:vpc-lattice:region:account-id:service/service-id
```

Zum Beispiel:

```
"Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0"
```

Bedingungsschlüssel, die in Authentifizierungsrichtlinien verwendet werden können

Der Zugriff kann durch Bedingungsschlüssel im Element Bedingung der Authentifizierungsrichtlinien weiter gesteuert werden. Diese Bedingungsschlüssel stehen je nach Protokoll und davon, ob die Anfrage mit Signature Version 4 (Sigv4) signiert oder anonym ist, zur Auswertung zur Verfügung. Bei Bedingungsschlüsseln wird die Groß- und Kleinschreibung beachtet.

AWS stellt globale Bedingungsschlüssel bereit, mit denen Sie den Zugriff steuern können, z. B. `aws:PrincipalOrgID` und`aws:SourceIp`. Eine Liste der AWS globalen Bedingungsschlüssel finden Sie im IAM-Benutzerhandbuch unter Kontextschlüssel für AWS globale Bedingungen.

In der folgenden Tabelle sind die VPC Lattice-Bedingungsschlüssel aufgeführt. Weitere Informationen finden Sie unter Bedingungsschlüssel für Amazon VPC Lattice Services in der Service Authorization Reference.

Bedingungsschlüssel	Beschreibung	Beispiel	Verfügbar für anonyme (nicht authentifizierte) Anrufer?	Verfügbar für gRPC?
`vpc-lattice-svcs:Port`	Filtert den Zugriff nach dem Service-Port, an den die Anfrage gestellt wird	80	Ja	Ja
`vpc-lattice-svcs:RequestMethod`	Filtert den Zugriff nach der Methode der Anfrage	GET	Ja	Immer POSTEN
`vpc-lattice-svcs:RequestHeader/` *`header-name`* `:` *`value`*	Filtert den Zugriff nach einem Header-Name-Wert-Paar in den Anforderungsheadern	content-type: application/json	Ja	Ja
`vpc-lattice-svcs:RequestQueryString/` *`key-name`*`:` *`value`*	Filtert den Zugriff nach den Schlüssel-Wert-Paaren der Abfragezeichenfolge in der Anforderungs-URL	quux: [corge, grault]	Ja	Nein
`vpc-lattice-svcs:ServiceNetworkArn`	Filtert den Zugriff nach dem ARN des Servicenetzwerks des Dienstes, der die Anfrage empfängt	arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/sn-01	Ja	Ja

Bedingungsschlüssel	Beschreibung	Beispiel	Verfügbar für anonyme (nicht authentifizierte) Anrufer?	Verfügbar für gRPC?
		23456789abcdef0		
`vpc-lattice-svcs:ServiceArn`	Filtert den Zugriff nach dem ARN des Dienstes, der die Anfrage empfängt	arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0	Ja	Ja
`vpc-lattice-svcs:SourceVpc`	Filtert den Zugriff nach der VPC, von der aus die Anfrage gestellt wird	vpc-1a2b3c4d	Ja	Ja
`vpc-lattice-svcs:SourceVpcOwnerAccount`	Filtert den Zugriff durch das eigene Konto der VPC, von der aus die Anfrage gestellt wird	123456789012	Ja	Ja

Anonyme (nicht authentifizierte) Prinzipale

Anonyme Principals sind Anrufer, die ihre AWS Anfragen nicht mit Signature Version 4 (Sigv4) signieren und sich in einer VPC befinden, die mit dem Servicenetzwerk verbunden ist. Anonyme Prinzipale können nicht authentifizierte Anfragen an Dienste im Servicenetzwerk stellen, sofern eine Authentifizierungsrichtlinie dies zulässt.

Beispiel für Authentifizierungsrichtlinien

Im Folgenden finden Sie Beispiele für Authentifizierungsrichtlinien, bei denen Anfragen von authentifizierten Prinzipalen gestellt werden müssen.

Alle Beispiele verwenden die `us-west-2` Region und enthalten ein fiktives Konto. IDs

Beispiel 1: Beschränken Sie den Zugriff auf Dienste durch eine bestimmte Organisation AWS

Das folgende Beispiel für eine Authentifizierungsrichtlinie gewährt jeder authentifizierten Anfrage Berechtigungen für den Zugriff auf alle Dienste im Dienstnetzwerk, für die die Richtlinie gilt. Die Anfrage muss jedoch von Prinzipalen stammen, die zu der in der Bedingung angegebenen AWS Organisation gehören.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "vpc-lattice-svcs:Invoke",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "aws:PrincipalOrgID": [
                  "o-123456example"
               ]
            }
         }
      }
   ]
}
```

Beispiel 2: Beschränken Sie den Zugriff auf einen Service durch eine bestimmte IAM-Rolle

Das folgende Beispiel für eine Authentifizierungsrichtlinie gewährt Berechtigungen für jede authentifizierte Anfrage, die die IAM-Rolle verwendet, `rates-client` um HTTP-GET-Anfragen für den im Element angegebenen Dienst zu stellen. `Resource` Die Ressource im `Resource` Element entspricht dem Dienst, an den die Richtlinie angehängt ist.

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

```
   "Statement":[
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": [
               "arn:aws:iam::123456789012:role/rates-client"
            ]
         },
         "Action": "vpc-lattice-svcs:Invoke",
         "Resource": [
            "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0/
*"
         ],
         "Condition": {
            "StringEquals": {
               "vpc-lattice-svcs:RequestMethod": "GET"
            }
         }
      }
   ]
}
```

Beispiel 3: Beschränken Sie den Zugriff auf Dienste durch authentifizierte Principals in einer bestimmten VPC

Das folgende Beispiel für eine Authentifizierungsrichtlinie erlaubt nur authentifizierte Anfragen von Prinzipalen in der VPC, deren VPC-ID lautet. *vpc-1a2b3c4d*

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "vpc-lattice-svcs:Invoke",
         "Resource": "*",
         "Condition": {
            "StringNotEquals": {
               "aws:PrincipalType": "Anonymous"
            },
            "StringEquals": {
               "vpc-lattice-svcs:SourceVpc": "vpc-1a2b3c4d"
            }
```

```
            }
        }
    ]
}
```

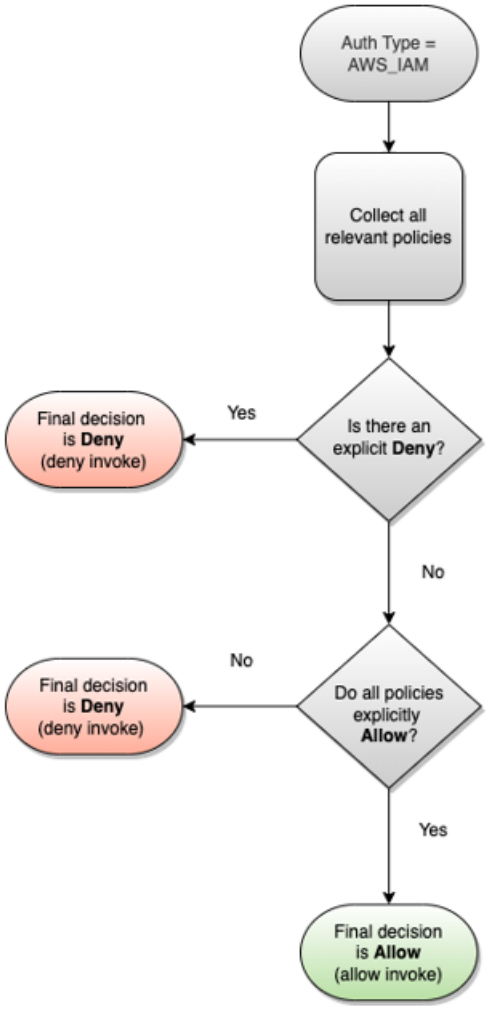
Wie funktioniert die Autorisierung

Wenn ein VPC Lattice-Dienst eine Anfrage erhält, bewertet der AWS Durchsetzungscode alle relevanten Berechtigungsrichtlinien zusammen, um zu bestimmen, ob die Anfrage autorisiert oder abgelehnt werden soll. Bei der Autorisierung werden alle identitätsbasierten IAM-Richtlinien und Authentifizierungsrichtlinien bewertet, die im Anforderungskontext gelten. Standardmäßig werden alle Anfragen implizit verweigert, wenn der Authentifizierungstyp ist. `AWS_IAM` Eine ausdrückliche Zulassung durch alle relevanten Richtlinien hat Vorrang vor der Standardeinstellung.

Die Autorisierung beinhaltet:

- Erfassung aller relevanten identitätsbasierten IAM-Richtlinien und Authentifizierungsrichtlinien.
- Bewertung der daraus resultierenden Richtlinien:
  - Es wird überprüft, ob der Anforderer (z. B. ein IAM-Benutzer oder eine IAM-Rolle) berechtigt ist, den Vorgang von dem Konto aus durchzuführen, zu dem der Anforderer gehört. Wenn es keine ausdrückliche Zulassungsanweisung gibt, wird die Anfrage AWS nicht autorisiert.
  - Es wird überprüft, ob die Anforderung gemäß der Authentifizierungsrichtlinie für das Dienstnetzwerk zulässig ist. Wenn eine Authentifizierungsrichtlinie aktiviert ist, es aber keine ausdrückliche Zulassungsanweisung gibt, wird die Anfrage AWS nicht autorisiert. Wenn es eine explizite Allow-Anweisung gibt oder der Authentifizierungstyp es ist`NONE`, wird der Code fortgesetzt.
  - Es wird überprüft, ob die Anforderung gemäß der Authentifizierungsrichtlinie für den Dienst zulässig ist. Wenn eine Authentifizierungsrichtlinie aktiviert ist, es aber keine ausdrückliche Zulassungsanweisung gibt, wird die Anfrage AWS nicht autorisiert. Wenn es eine explizite Erlaubnis-Anweisung gibt oder der Authentifizierungstyp „Zulassen“ ist**`NONE`**, gibt der Erzwingungscode die endgültige Entscheidung „Zulassen“ zurück.
  - Eine explizite Zugriffsverweigerung überschreibt jede Zugriffserlaubnis in einer Richtlinie.

Das Diagramm zeigt den Autorisierungsablauf. Wenn eine Anfrage gestellt wird, erlauben oder verweigern die entsprechenden Richtlinien der Anfrage den Zugriff auf einen bestimmten Dienst.



Steuern Sie den Verkehr in VPC Lattice mithilfe von Sicherheitsgruppen

AWS Sicherheitsgruppen agieren als virtuelle Firewalls und kontrollieren den Netzwerkverkehr zu und von den Entitäten, denen sie zugeordnet sind. Mit VPC Lattice können Sie Sicherheitsgruppen erstellen und sie der VPC-Zuordnung zuweisen, die eine VPC mit einem Servicenetzwerk verbindet, um zusätzliche Sicherheitsvorkehrungen auf Netzwerkebene für Ihr Servicenetzwerk durchzusetzen. Wenn Sie eine VPC über einen VPC-Endpunkt mit einem Servicenetzwerk verbinden, können Sie dem VPC-Endpunkt auch Sicherheitsgruppen zuweisen. Ebenso können Sie Ressourcen-Gateways, die Sie erstellen, Sicherheitsgruppen zuweisen, um den Zugriff auf Ressourcen in Ihrer VPC zu ermöglichen.

Inhalt

- Sicherheitsgruppen für eine VPC-Zuordnung verwalten

Liste der verwalteten Präfixe

VPC Lattice stellt verwaltete Präfixlisten bereit, die die IP-Adressen enthalten, die für die Weiterleitung des Datenverkehrs über das VPC-Lattice-Netzwerk verwendet werden, wenn Sie eine Dienstnetzwerkverbindung verwenden, um Ihre VPC mithilfe einer VPC-Zuordnung mit einem Servicenetzwerk zu verbinden. Dabei handelt es sich entweder um private Verbindungen, um lokale Verbindungen oder um öffentliche Verbindungen, die nicht IPs geroutet werden können. IPs IPs

Sie können in Ihren Sicherheitsgruppenregeln auf die von VPC Lattice verwalteten Präfixlisten verweisen. Dadurch kann der Datenverkehr von den Clients über das VPC-Lattice-Dienstnetzwerk zu den VPC-Lattice-Dienstzielen fließen.

Nehmen wir beispielsweise an, Sie haben eine EC2 Instance als Ziel in der Region USA West (Oregon) registriert (). `us-west-2` Sie können der Instanz-Sicherheitsgruppe eine Regel hinzufügen, die eingehenden HTTPS-Zugriff aus der Liste der verwalteten VPC Lattice-Präfixe ermöglicht, sodass der VPC-Lattice-Verkehr in dieser Region die Instance erreichen kann. Wenn Sie alle anderen Regeln für eingehenden Datenverkehr aus der Sicherheitsgruppe entfernen, können Sie verhindern, dass jeder andere Datenverkehr als VPC-Lattice-Verkehr die Instance erreicht.

Die Namen der verwalteten Präfixlisten für VPC Lattice lauten wie folgt:

- com.amazonaws. *region*.vpc-Gitter
- com.amazonaws. *region*.ipv6.vpc-Gitter

Weitere Informationen finden Sie im Abschnitt zur AWS-verwalteten Präfixliste im Amazon-VPC-Benutzerhandbuch.

Windows- und MacOS-Clients

Die Adressen in den VPC Lattice-Präfixlisten sind verknüpfungslokale Adressen und nicht routbare öffentliche Adressen. Wenn Sie von diesen Clients aus eine Verbindung zu VPC Lattice herstellen, müssen Sie deren Konfigurationen aktualisieren, sodass die IP-Adressen in der Liste der verwalteten Präfixe an die primäre IP-Adresse des Clients weitergeleitet werden. Im Folgenden finden Sie einen Beispielbefehl, der die Konfiguration des Windows-Clients aktualisiert, wobei sich eine der Adressen in der Liste der verwalteten Präfixe 169.254.171.0 befindet.

```
C:\> route add 169.254.171.0 mask 255.255.255.0 primary-ip-address
```

Im Folgenden finden Sie einen Beispielbefehl, der die Konfiguration des macOS-Clients aktualisiert, wobei 169.254.171.0 sich eine der Adressen in der Liste der verwalteten Präfixe befindet.

```
sudo route -n add -net 169.254.171.0 primary-ip-address 255.255.255.0
```

Um die Erstellung einer statischen Route zu vermeiden, empfehlen wir, einen Servicenetzwerkendpunkt in einer VPC zu verwenden, um Konnektivität herzustellen. Weitere Informationen finden Sie unter the section called “VPC-Endpunktzuordnungen verwalten”.

Sicherheitsgruppenregeln

Die Verwendung von VPC Lattice mit oder ohne Sicherheitsgruppen hat keine Auswirkungen auf Ihre bestehende VPC-Sicherheitsgruppenkonfiguration. Sie können jedoch jederzeit Ihre eigenen Sicherheitsgruppen hinzufügen.

Die wichtigsten Überlegungen

- Sicherheitsgruppenregeln für Clients steuern den ausgehenden Datenverkehr zu VPC Lattice.
- Sicherheitsgruppenregeln für Ziele steuern den eingehenden Datenverkehr von VPC Lattice zu den Zielen, einschließlich des Zustandsprüfverkehrs.
- Sicherheitsgruppenregeln für die Verbindung zwischen dem Servicenetzwerk und der VPC steuern, welche Clients auf das VPC-Lattice-Dienstnetzwerk zugreifen können.
- Sicherheitsgruppenregeln für das Ressourcen-Gateway steuern den ausgehenden Verkehr vom Ressourcen-Gateway zu den Ressourcen.

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

Damit der Datenverkehr vom Ressourcen-Gateway zu den Ressourcen fließen kann, müssen Sie ausgehende Regeln für die offenen Ports und akzeptierte Listener-Protokolle für die Ressourcen erstellen.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich	Kommentar
CIDR range for resource	*TCP*	*3306*	Lassen Sie den Datenverkehr vom

Bestimmungsort	Protocol (Protokoll)	Port-Bereich	Kommentar
			Ressourcen-Gateway zu den Datenbanken zu

Empfohlene Regeln für eingehende Zugriffe für Dienstnetzwerk- und VPC-Zuordnungen

Damit der Datenverkehr vom Client VPCs zu den Diensten fließen kann, die dem Servicenetzwerk zugeordnet sind, müssen Sie Regeln für eingehenden Datenverkehr für die Listener-Ports und Listener-Protokolle für die Dienste erstellen.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentar
VPC CIDR	*listener*	*listener*	Datenverkehr von Clients zu VPC Lattice zulassen

Empfohlene ausgehende Regeln für den Datenverkehr, der von Client-Instances zu VPC Lattice fließt

Standardmäßig gestatten Sicherheitsgruppen allen ausgehenden Datenverkehr. Wenn Sie jedoch benutzerdefinierte Regeln für ausgehenden Datenverkehr haben, müssen Sie ausgehenden Datenverkehr zum VPC Lattice-Präfix für Listener-Ports und Protokolle zulassen, damit Client-Instances eine Verbindung zu allen Diensten herstellen können, die dem VPC Lattice-Dienstnetzwerk zugeordnet sind. Sie können diesen Verkehr zulassen, indem Sie auf die ID der Präfixliste für VPC Lattice verweisen.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich	Kommentar
ID of the VPC Lattice prefix list	*listener*	*listener*	Datenverkehr von Clients zu VPC Lattice zulassen

Empfohlene Regeln für eingehenden Datenverkehr von VPC Lattice zu Ziel-Instances

Sie können die Client-Sicherheitsgruppe nicht als Quelle für die Sicherheitsgruppen Ihres Ziels verwenden, da der Datenverkehr von VPC Lattice fließt. Sie können auf die ID der Präfixliste für VPC Lattice verweisen.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentar
ID of the VPC Lattice prefix list	*target*	*target*	Verkehr von VPC Lattice zu Zielen zulassen
ID of the VPC Lattice prefix list	*health check*	*health check*	Health Check-Verkehr von VPC Lattice zu Zielen zulassen

Sicherheitsgruppen für eine VPC-Zuordnung verwalten

Sie können die verwenden, AWS CLI um Sicherheitsgruppen auf der VPC anzuzeigen, hinzuzufügen oder zu aktualisieren, um die Netzwerkverbindung zu verwalten. Denken Sie bei der Verwendung von daran AWS CLI, dass Ihre Befehle in der für Ihr Profil AWS-Region konfigurierten Version ausgeführt werden. Wenn Sie die Befehle in einer anderen Region ausführen möchten, ändern Sie entweder die Standardregion für Ihr Profil, oder verwenden Sie den `--region`-Parameter mit dem Befehl.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die Sicherheitsgruppe in derselben VPC wie die VPC erstellt haben, die Sie dem Dienstnetzwerk hinzufügen möchten. Weitere Informationen finden Sie unter Steuern des Datenverkehrs zu Ihren Ressourcen mithilfe von Sicherheitsgruppen im Amazon VPC-Benutzerhandbuch.

So fügen Sie eine Sicherheitsgruppe hinzu, wenn Sie eine VPC-Zuordnung mithilfe der Konsole erstellen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Service networks aus.
3. Wählen Sie den Namen des Servicenetzwerks aus, um dessen Detailseite zu öffnen.
4. Wählen Sie auf der Registerkarte VPC-Zuordnungen erstellen und dann VPC-Zuordnung hinzufügen aus.
5. Wählen Sie eine VPC und bis zu fünf Sicherheitsgruppen aus.
6. Wählen Sie Änderungen speichern aus.

So fügen Sie Sicherheitsgruppen für eine bestehende VPC-Zuordnung mithilfe der Konsole hinzu oder aktualisieren sie

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Service networks aus.
3. Wählen Sie den Namen des Servicenetzwerks aus, um dessen Detailseite zu öffnen.
4. Aktivieren Sie auf der Registerkarte VPC-Zuordnungen das Kontrollkästchen für die Zuordnung und wählen Sie dann Aktionen, Sicherheitsgruppen bearbeiten aus.
5. Fügen Sie nach Bedarf Sicherheitsgruppen hinzu und entfernen Sie sie.
6. Wählen Sie Änderungen speichern aus.

Um eine Sicherheitsgruppe hinzuzufügen, wenn Sie eine VPC-Zuordnung mit dem AWS CLI

Verwenden Sie den Befehl create-service-network-vpc-association und geben Sie die ID der VPC für die VPC-Zuordnung und die ID der hinzuzufügenden Sicherheitsgruppen an.

```
aws vpc-lattice create-service-network-vpc-association \
    --service-network-identifier sn-0123456789abcdef0 \
    --vpc-identifier vpc-1a2b3c4d \
    --security-group-ids sg-7c2270198example
```

Bei erfolgreicher Ausführung gibt der Befehl eine Ausgabe zurück, die in etwa wie folgt aussieht:

```
{
  "arn": "arn",
  "createdBy": "464296918874",
  "id": "snva-0123456789abcdef0",
  "status": "CREATE_IN_PROGRESS",
  "securityGroupIds": ["sg-7c2270198example"]
}
```

Um Sicherheitsgruppen für eine bestehende VPC-Zuordnung hinzuzufügen oder zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl update-service-network-vpc-association und geben Sie die ID des Dienstnetzwerks und IDs der Sicherheitsgruppen an. Diese Sicherheitsgruppen haben Vorrang vor allen zuvor verknüpften Sicherheitsgruppen. Definieren Sie mindestens eine Sicherheitsgruppe, wenn Sie die Liste aktualisieren.

```
aws vpc-lattice update-service-network-vpc-association
    --service-network-vpc-association-identifier sn-903004f88example \
    --security-group-ids sg-7c2270198example sg-903004f88example
```

> **Warning**
>
> Sie können nicht alle Sicherheitsgruppen entfernen. Stattdessen müssen Sie zuerst die VPC-Zuordnung löschen und dann die VPC-Zuordnung ohne Sicherheitsgruppen neu erstellen. Seien Sie vorsichtig, wenn Sie die VPC-Zuordnung löschen. Dadurch wird verhindert, dass der Datenverkehr Dienste erreicht, die sich in diesem Dienstnetzwerk befinden.

Steuern Sie den Verkehr zu VPC Lattice über das Netzwerk ACLs

Eine Netzwerk-Zugriffssteuerungsliste (ACL) erlaubt oder verweigert bestimmten eingehenden oder ausgehenden Datenverkehr auf der Subnetzebene. Die Standard-Netzwerk-ACL lässt den gesamten ein- und ausgehenden Datenverkehr zu. Sie können ein benutzerdefiniertes Netzwerk ACLs für Ihre Subnetze erstellen, um eine zusätzliche Sicherheitsebene bereitzustellen. Weitere Informationen finden Sie unter Netzwerk ACLs im Amazon VPC-Benutzerhandbuch.

Inhalt

Netzwerk ACLs für Ihre Client-Subnetze

Das Netzwerk ACLs für Client-Subnetze muss den Verkehr zwischen Clients und VPC Lattice zulassen. Sie können die zulässigen IP-Adressbereiche aus der Liste der verwalteten Präfixe für VPC Lattice abrufen.

Im Folgenden finden Sie ein Beispiel für eine Regel für eingehenden Datenverkehr.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentar
vpc_lattice_cidr_block	TCP	1025-65535	Verkehr von VPC Lattice zu Clients zulassen

Es folgt ein Beispiel für eine Outbound-Regel.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich	Kommentar
vpc_latti ce_cidr_block	*listener*	*listener*	Datenverkehr von Clients zu VPC Lattice zulassen

Netzwerk ACLs für Ihre Zielsubnetze

Das Netzwerk ACLs für Zielsubnetze muss den Datenverkehr zwischen Zielen und VPC Lattice sowohl am Zielport als auch am Health Check-Port zulassen. Sie können die zulässigen IP-Adressbereiche aus der Liste der verwalteten Präfixe für VPC Lattice abrufen.

Im Folgenden finden Sie ein Beispiel für eine Regel für eingehenden Datenverkehr.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentar
vpc_latti ce_cidr_block	*target*	*target*	Verkehr von VPC Lattice zu Zielen zulassen
vpc_latti ce_cidr_block	*health check*	*health check*	Health Check-Verkehr von VPC Lattice zu Zielen zulassen

Es folgt ein Beispiel für eine Outbound-Regel.

Bestimmungsort	Protocol (Protokoll)	Port-Bereich	Kommentar
vpc_latti ce_cidr_block	*target*	1024 - 65535	Datenverkehr von Zielen zu VPC Lattice zulassen
vpc_latti ce_cidr_block	*health check*	1024 - 65535	Zustandsprüfungsve rkehr von Zielen zu VPC Lattice zulassen

SIGv4 authentifizierte Anfragen für Amazon VPC Lattice

VPC Lattice verwendet Signature Version 4 (SIGv4) oder Signature Version 4A (SIGv4A) für die Client-Authentifizierung. Weitere Informationen finden Sie unter AWS Signature Version 4 für API-Anfragen im IAM-Benutzerhandbuch.

Überlegungen

- VPC Lattice versucht, jede Anfrage zu authentifizieren, die mit oder A signiert ist. SIGv4 SIGv4 Die Anfrage schlägt ohne Authentifizierung fehl.
- VPC Lattice unterstützt keine Payload-Signierung. Sie müssen einen `x-amz-content-sha256` Header mit dem Wert auf senden. `"UNSIGNED-PAYLOAD"`

Beispiele

- Python
- Java
- Node.js
- Golang
- Golang - GRPC

Python

In diesem Beispiel werden die signierten Anfragen über eine sichere Verbindung an einen im Netzwerk registrierten Dienst gesendet. Wenn Sie Anfragen bevorzugen, vereinfacht das Botocore-Paket den Authentifizierungsprozess, ist aber nicht unbedingt erforderlich. Weitere Informationen finden Sie in der Boto3-Dokumentation unter Anmeldeinformationen.

Verwenden Sie den folgenden Befehl, um die `awscrt` Pakete `botocore` und zu installieren. Weitere Informationen finden Sie unter AWS CRT Python.

```
pip install botocore awscrt
```

Wenn Sie die Client-Anwendung auf Lambda ausführen, installieren Sie die erforderlichen Module mithilfe von Lambda-Schichten oder nehmen Sie sie in Ihr Bereitstellungspaket auf.

Ersetzen Sie im folgenden Beispiel die Platzhalterwerte durch Ihre eigenen Werte.

SIGv4

```
from botocore import crt
import requests
from botocore.awsrequest import AWSRequest
import botocore.session

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtSigV4Auth(session.get_credentials(), 'vpc-lattice-svcs',
 'us-west-2')
    endpoint = 'https://data-svc-022f67d3a42.1234abc.vpc-lattice-svcs.us-
west-2.on.aws'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json', 'x-amz-content-sha256':
 'UNSIGNED-PAYLOAD'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["payload_signing_enabled"] = False
    signer.add_auth(request)

    prepped = request.prepare()

    response = requests.post(prepped.url, headers=prepped.headers, data=data)
    print(response.text)
```

SIGv4A

```
from botocore import crt
import requests
from botocore.awsrequest import AWSRequest
import botocore.session

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtSigV4AsymAuth(session.get_credentials(), 'vpc-lattice-
svcs', '*')
    endpoint = 'https://data-svc-022f67d3a42.1234abc.vpc-lattice-svcs.us-
west-2.on.aws'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json', 'x-amz-content-sha256':
 'UNSIGNED-PAYLOAD'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["payload_signing_enabled"] = False
```

```
    signer.add_auth(request)

    prepped = request.prepare()

    response = requests.post(prepped.url, headers=prepped.headers, data=data)
    print(response.text)
```

Java

Dieses Beispiel zeigt, wie Sie das Signieren von Anfragen mithilfe benutzerdefinierter Interzeptoren durchführen können. Es verwendet die standardmäßige Anbieterklasse für Anmeldeinformationen von AWS SDK for Java 2.x, die die richtigen Anmeldeinformationen für Sie abruft. Wenn Sie lieber einen bestimmten Anbieter für Anmeldeinformationen verwenden möchten, können Sie einen aus der AWS SDK for Java 2.xauswählen. Das AWS SDK für Java erlaubt nur unsignierte Payloads über HTTPS. Sie können den Unterzeichner jedoch so erweitern, dass er unsignierte Payloads über HTTP unterstützt.

SIGv4

```
package com.example;

import software.amazon.awssdk.http.auth.aws.signer.AwsV4HttpSigner;
import software.amazon.awssdk.http.auth.spi.signer.SignedRequest;

import software.amazon.awssdk.http.SdkHttpMethod;
import software.amazon.awssdk.http.SdkHttpClient;
import software.amazon.awssdk.identity.spi.AwsCredentialsIdentity;
import software.amazon.awssdk.http.SdkHttpRequest;
import software.amazon.awssdk.http.apache.ApacheHttpClient;
import software.amazon.awssdk.http.HttpExecuteRequest;
import software.amazon.awssdk.http.HttpExecuteResponse;
import java.io.IOException;
import java.net.URI;

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

public class sigv4 {

    public static void main(String[] args) {
        AwsV4HttpSigner signer = AwsV4HttpSigner.create();
```

```
        AwsCredentialsIdentity credentials =
 DefaultCredentialsProvider.create().resolveCredentials();

        if (args.length < 2) {
            System.out.println("Usage: sample <url> <region>");
            System.exit(1);
        }
        // Create the HTTP request to be signed
        var url = args[0];
        SdkHttpRequest httpRequest = SdkHttpRequest.builder()
                .uri(URI.create(url))
                .method(SdkHttpMethod.GET)
                .build();

        SignedRequest signedRequest = signer.sign(r -> r.identity(credentials)
                .request(httpRequest)
                .putProperty(AwsV4HttpSigner.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")
                .putProperty(AwsV4HttpSigner.PAYLOAD_SIGNING_ENABLED, false)
                .putProperty(AwsV4HttpSigner.REGION_NAME, args[1]));

        System.out.println("[*] Raw request headers:");
        signedRequest.request().headers().forEach((key, values) -> {
            values.forEach(value -> System.out.println("  " + key + ": " + value));
        });

        try (SdkHttpClient httpClient = ApacheHttpClient.create()) {
            HttpExecuteRequest httpExecuteRequest = HttpExecuteRequest.builder()
                    .request(signedRequest.request())
                    .contentStreamProvider(signedRequest.payload().orElse(null))
                    .build();

            System.out.println("[*] Sending request to: " + url);

            HttpExecuteResponse httpResponse =
 httpClient.prepareRequest(httpExecuteRequest).call();

            System.out.println("[*] Request sent");

            System.out.println("[*] Response status code: " +
 httpResponse.httpResponse().statusCode());
            // Read and print the response body
            httpResponse.responseBody().ifPresent(inputStream -> {
                try {
```

```
                    String responseBody = new String(inputStream.readAllBytes());
                    System.out.println("[*] Response body: " + responseBody);
                } catch (IOException e) {
                    System.err.println("[*] Failed to read response body");
                    e.printStackTrace();
                } finally {
                    try {
                        inputStream.close();
                    } catch (IOException e) {
                        System.err.println("[*] Failed to close input stream");
                        e.printStackTrace();
                    }
                }
            });
        } catch (IOException e) {
            System.err.println("[*] HTTP Request Failed.");
            e.printStackTrace();
        }

    }
}
```

SIGv4A

Dieses Beispiel erfordert eine zusätzliche Abhängigkeit von. `software.amazon.awssdk:http-auth-aws-crt`

```
package com.example;


import software.amazon.awssdk.http.auth.aws.signer.AwsV4aHttpSigner;
import software.amazon.awssdk.http.auth.aws.signer.RegionSet;
import software.amazon.awssdk.http.auth.spi.signer.SignedRequest;

import software.amazon.awssdk.http.SdkHttpMethod;
import software.amazon.awssdk.http.SdkHttpClient;
import software.amazon.awssdk.identity.spi.AwsCredentialsIdentity;
import software.amazon.awssdk.http.SdkHttpRequest;
import software.amazon.awssdk.http.apache.ApacheHttpClient;
import software.amazon.awssdk.http.HttpExecuteRequest;
import software.amazon.awssdk.http.HttpExecuteResponse;
import java.io.IOException;
import java.net.URI;
```

```
import java.util.Arrays;

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

public class sigv4a {

    public static void main(String[] args) {
        AwsV4aHttpSigner signer = AwsV4aHttpSigner.create();

        AwsCredentialsIdentity credentials =
 DefaultCredentialsProvider.create().resolveCredentials();

        if (args.length < 2) {
            System.out.println("Usage: sample <url> <regionset>");
            System.exit(1);
        }
        // Create the HTTP request to be signed
        var url = args[0];
        SdkHttpRequest httpRequest = SdkHttpRequest.builder()
                .uri(URI.create(url))
                .method(SdkHttpMethod.GET)
                .build();

        SignedRequest signedRequest = signer.sign(r -> r.identity(credentials)
                .request(httpRequest)
                .putProperty(AwsV4aHttpSigner.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")
                .putProperty(AwsV4aHttpSigner.PAYLOAD_SIGNING_ENABLED, false)
                .putProperty(AwsV4aHttpSigner.REGION_SET,
 RegionSet.create(String.join(" ",Arrays.copyOfRange(args, 1, args.length)))));

        System.out.println("[*] Raw request headers:");
        signedRequest.request().headers().forEach((key, values) -> {
            values.forEach(value -> System.out.println("  " + key + ": " + value));
        });

        try (SdkHttpClient httpClient = ApacheHttpClient.create()) {
            HttpExecuteRequest httpExecuteRequest = HttpExecuteRequest.builder()
                    .request(signedRequest.request())
                    .contentStreamProvider(signedRequest.payload().orElse(null))
                    .build();

            System.out.println("[*] Sending request to: " + url);
```

```
            HttpExecuteResponse httpResponse =
 httpClient.prepareRequest(httpExecuteRequest).call();

            System.out.println("[*] Request sent");

            System.out.println("[*] Response status code: " +
 httpResponse.httpResponse().statusCode());
            // Read and print the response body
            httpResponse.responseBody().ifPresent(inputStream -> {
                try {
                    String responseBody = new String(inputStream.readAllBytes());
                    System.out.println("[*] Response body: " + responseBody);
                } catch (IOException e) {
                    System.err.println("[*] Failed to read response body");
                    e.printStackTrace();
                } finally {
                    try {
                        inputStream.close();
                    } catch (IOException e) {
                        System.err.println("[*] Failed to close input stream");
                        e.printStackTrace();
                    }
                }
            });
        } catch (IOException e) {
            System.err.println("[*] HTTP Request Failed.");
            e.printStackTrace();
        }
    }
}
```

Node.js

In diesem Beispiel werden NodeJS-Bindungen vom Typ aws-crt verwendet, um eine signierte Anfrage über HTTPS zu senden.

Verwenden Sie den folgenden Befehl, um das `aws-crt` Paket zu installieren.

```
npm -i aws-crt
```

Wenn die `AWS_REGION` Umgebungsvariable existiert, verwendet das Beispiel die von angegebene Region`AWS_REGION`. Die Standardregion ist`us-east-1`.

SIGv4

```
const https = require('https')
const crt = require('aws-crt')
const { HttpRequest } = require('aws-crt/dist/native/http')

function sigV4Sign(method, endpoint, service, algorithm) {
    const host = new URL(endpoint).host
    const request = new HttpRequest(method, endpoint)
    request.headers.add('host', host)
    // crt.io.enable_logging(crt.io.LogLevel.INFO)
    const config = {
        service: service,
        region: process.env.AWS_REGION ? process.env.AWS_REGION : 'us-east-1',
        algorithm: algorithm,
        signature_type: crt.auth.AwsSignatureType.HttpRequestViaHeaders,
        signed_body_header: crt.auth.AwsSignedBodyHeaderType.XAmzContentSha256,
        signed_body_value: crt.auth.AwsSignedBodyValue.UnsignedPayload,
        provider: crt.auth.AwsCredentialsProvider.newDefault()
    }

    return crt.auth.aws_sign_request(request, config)
}

if (process.argv.length === 2) {
  console.error(process.argv[1] + ' <url>')
  process.exit(1)
}

const algorithm = crt.auth.AwsSigningAlgorithm.SigV4;

sigV4Sign('GET', process.argv[2], 'vpc-lattice-svcs', algorithm).then(
  httpResponse => {
    var headers = {}

    for (const sigv4header of httpResponse.headers) {
      headers[sigv4header[0]] = sigv4header[1]
    }

    const options = {
      hostname: new URL(process.argv[2]).host,
      path: new URL(process.argv[2]).pathname,
      method: 'GET',
      headers: headers
```

```
    }

    req = https.request(options, res => {
      console.log('statusCode:', res.statusCode)
      console.log('headers:', res.headers)
      res.on('data', d => {
        process.stdout.write(d)
      })
    })
    req.on('error', err => {
      console.log('Error: ' + err)
    })
    req.end()
  }
)
```

SIGv4A

```
const https = require('https')
const crt = require('aws-crt')
const { HttpRequest } = require('aws-crt/dist/native/http')

function sigV4Sign(method, endpoint, service, algorithm) {
    const host = new URL(endpoint).host
    const request = new HttpRequest(method, endpoint)
    request.headers.add('host', host)
    // crt.io.enable_logging(crt.io.LogLevel.INFO)
    const config = {
        service: service,
        region: process.env.AWS_REGION ? process.env.AWS_REGION : 'us-east-1',
        algorithm: algorithm,
        signature_type: crt.auth.AwsSignatureType.HttpRequestViaHeaders,
        signed_body_header: crt.auth.AwsSignedBodyHeaderType.XAmzContentSha256,
        signed_body_value: crt.auth.AwsSignedBodyValue.UnsignedPayload,
        provider: crt.auth.AwsCredentialsProvider.newDefault()
    }

    return crt.auth.aws_sign_request(request, config)
}

if (process.argv.length === 2) {
  console.error(process.argv[1] + ' <url>')
  process.exit(1)
```

```
}

const algorithm = crt.auth.AwsSigningAlgorithm.SigV4Asymmetric;

sigV4Sign('GET', process.argv[2], 'vpc-lattice-svcs', algorithm).then(
  httpResponse => {
    var headers = {}

    for (const sigv4header of httpResponse.headers) {
      headers[sigv4header[0]] = sigv4header[1]
    }

    const options = {
      hostname: new URL(process.argv[2]).host,
      path: new URL(process.argv[2]).pathname,
      method: 'GET',
      headers: headers
    }

    req = https.request(options, res => {
      console.log('statusCode:', res.statusCode)
      console.log('headers:', res.headers)
      res.on('data', d => {
        process.stdout.write(d)
      })
    })
    req.on('error', err => {
      console.log('Error: ' + err)
    })
    req.end()
  }
)
```

Golang

In diesem Beispiel werden die Smithy-Codegeneratoren für Go und das AWS SDK für die Programmiersprache Go verwendet, um Anfragen zum Signieren von Anfragen zu verarbeiten. Das Beispiel erfordert eine Go-Version von 1.21 oder höher.

SIGv4

```
package main
```

```
import (
        "context"
        "flag"
        "fmt"
        "io"
        "log"
        "net/http"
        "net/http/httputil"
        "os"
        "strings"

        "github.com/aws/aws-sdk-go-v2/aws"
        "github.com/aws/aws-sdk-go-v2/config"
        "github.com/aws/smithy-go/aws-http-auth/credentials"
        "github.com/aws/smithy-go/aws-http-auth/sigv4"
        v4 "github.com/aws/smithy-go/aws-http-auth/v4"
)

type nopCloser struct {
        io.ReadSeeker
}

func (nopCloser) Close() error {
        return nil
}

type stringFlag struct {
        set   bool
        value string
}



        flag.PrintDefaults()
        os.Exit(1)
}

func main() {
        flag.Parse()
        if !url.set || !region.set {
                Usage()
        }
```

```
	cfg, err := config.LoadDefaultConfig(context.TODO(),
config.WithClientLogMode(aws.LogSigning))
	if err != nil {
		log.Fatalf("failed to load SDK configuration, %v", err)
	}

	if len(os.Args) < 2 {
		log.Fatalf("Usage: go run main.go  <url>")
	}

	// Retrieve credentials from an SDK source, such as the instance profile
	sdkCreds, err := cfg.Credentials.Retrieve(context.TODO())
	if err != nil {
		log.Fatalf("Unable to retrieve credentials from SDK, %v", err)
	}

	creds := credentials.Credentials{
		AccessKeyID:     sdkCreds.AccessKeyID,
		SecretAccessKey: sdkCreds.SecretAccessKey,
		SessionToken:    sdkCreds.SessionToken,
	}

	// Add a payload body, which will not be part of the signature calculation
	body := nopCloser{strings.NewReader(`Example payload body`)}

	req, _ := http.NewRequest(http.MethodPost, url.value, body)

	// Create a sigv4a signer with specific options
	signer := sigv4.New(func(o *v4.SignerOptions) {
		o.DisableDoublePathEscape = true
		// This will add the UNSIGNED-PAYLOAD sha256 header
		o.AddPayloadHashHeader = true
		o.DisableImplicitPayloadHashing = true
	})

	// Perform the signing on req, using the credentials we retrieved from the
SDK
	err = signer.SignRequest(&sigv4.SignRequestInput{
		Request:     req,
		Credentials: creds,
		Service:     "vpc-lattice-svcs",
		Region: region.String(),
	})
```

```
        if err != nil {
                log.Fatalf("%s", err)
        }

        res, err := httputil.DumpRequest(req, true)

        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Raw request\n%s\n", string(res))

        log.Printf("[*] Sending request to %s\n", url.value)

        resp, err := http.DefaultClient.Do(req)
        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Request sent\n")

        log.Printf("[*] Response status code: %d\n", resp.StatusCode)

        respBody, err := io.ReadAll(resp.Body)
        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Response body: \n%s\n", respBody)
}
```

SIGv4A

```
package main

import (
        "context"
        "flag"
        "fmt"
        "io"
        "log"
        "net/http"
        "net/http/httputil"
```

```
        "os"
        "strings"

        "github.com/aws/aws-sdk-go-v2/aws"
        "github.com/aws/aws-sdk-go-v2/config"
        "github.com/aws/smithy-go/aws-http-auth/credentials"
        "github.com/aws/smithy-go/aws-http-auth/sigv4a"
        v4 "github.com/aws/smithy-go/aws-http-auth/v4"
)

type nopCloser struct {
        io.ReadSeeker
}

func (nopCloser) Close() error {
        return nil
}

type stringFlag struct {

func main() {
        flag.Parse()
        if !url.set || !regionSet.set {
                Usage()
        }

        cfg, err := config.LoadDefaultConfig(context.TODO(),
 config.WithClientLogMode(aws.LogSigning))
        if err != nil {
                log.Fatalf("failed to load SDK configuration, %v", err)
        }

        if len(os.Args) < 2 {
                log.Fatalf("Usage: go run main.go <url>")
        }

        // Retrieve credentials from an SDK source, such as the instance profile
        sdkCreds, err := cfg.Credentials.Retrieve(context.TODO())
        if err != nil {
                log.Fatalf("Unable to retrieve credentials from SDK, %v", err)
        }

        creds := credentials.Credentials{
                AccessKeyID:     sdkCreds.AccessKeyID,
```

```
                SecretAccessKey: sdkCreds.SecretAccessKey,
                SessionToken:    sdkCreds.SessionToken,
        }

        // Add a payload body, which will not be part of the signature calculation
        body := nopCloser{strings.NewReader(`Example payload body`)}

        req, _ := http.NewRequest(http.MethodPost, url.value, body)

        // Create a sigv4a signer with specific options
        signer := sigv4a.New(func(o *v4.SignerOptions) {
                o.DisableDoublePathEscape = true
                // This will add the UNSIGNED-PAYLOAD sha256 header
                o.AddPayloadHashHeader = true
                o.DisableImplicitPayloadHashing = true
        })

        // Create a slice out of the provided regionset
        rs := strings.Split(regionSet.value, ",")

        // Perform the signing on req, using the credentials we retrieved from the
SDK
        err = signer.SignRequest(&sigv4a.SignRequestInput{
                Request:     req,
                Credentials: creds,
                Service:     "vpc-lattice-svcs",
                RegionSet: rs,
        })

        if err != nil {
                log.Fatalf("%s", err)
        }

        res, err := httputil.DumpRequest(req, true)

        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Raw request\n%s\n", string(res))

        log.Printf("[*] Sending request to %s\n", url.value)

        resp, err := http.DefaultClient.Do(req)
```

```
        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Request sent\n")

        log.Printf("[*] Response status code: %d\n", resp.StatusCode)

        respBody, err := io.ReadAll(resp.Body)
        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Response body: \n%s\n", respBody)
}
```

Golang - GRPC

In diesem Beispiel wird das AWS SDK für die Programmiersprache Go verwendet, um das Signieren von Anfragen für GRPC-Anfragen zu handhaben. Dies kann mit dem Echo-Server aus dem GRPC-Beispielcode-Repository verwendet werden.

```
package main

import (
    "context"
    "crypto/tls"
    "crypto/x509"

    "flag"
    "fmt"
    "log"
    "net/http"
    "net/url"
    "strings"
    "time"

    "google.golang.org/grpc"
    "google.golang.org/grpc/credentials"

    "github.com/aws/aws-sdk-go-v2/aws"
    v4 "github.com/aws/aws-sdk-go-v2/aws/signer/v4"
```

```
    "github.com/aws/aws-sdk-go-v2/config"

    ecpb "google.golang.org/grpc/examples/features/proto/echo"
)

const (
    headerContentSha    = "x-amz-content-sha256"
    headerSecurityToken = "x-amz-security-token"
    headerDate          = "x-amz-date"
    headerAuthorization = "authorization"
    unsignedPayload     = "UNSIGNED-PAYLOAD"
)

type SigV4GrpcSigner struct {
    service      string
    region       string
    credProvider aws.CredentialsProvider
    signer       *v4.Signer
}

func NewSigV4GrpcSigner(service string, region string, credProvider
 aws.CredentialsProvider) *SigV4GrpcSigner {
    signer := v4.NewSigner()
    return &SigV4GrpcSigner{
        service:      service,
        region:       region,
        credProvider: credProvider,
        signer:       signer,
    }
}

func (s *SigV4GrpcSigner) GetRequestMetadata(ctx context.Context, uri ...string)
 (map[string]string, error) {
    ri, _ := credentials.RequestInfoFromContext(ctx)
    creds, err := s.credProvider.Retrieve(ctx)
    if err != nil {
        return nil, fmt.Errorf("failed to load credentials: %w", err)
    }

    // The URI we get here is scheme://authority/service/ - for siging we want to
 include the RPC name
    // But RequestInfoFromContext only has the combined /service/rpc-name - so read the
 URI, and
    // replace the Path with what we get from RequestInfo.
```

```
    parsed, err := url.Parse(uri[0])
    if err != nil {
        return nil, err
    }
    parsed.Path = ri.Method

    // Build a request for the signer.
    bodyReader := strings.NewReader("")
    req, err := http.NewRequest("POST", uri[0], bodyReader)
    if err != nil {
        return nil, err
    }
    date := time.Now()
    req.Header.Set(headerContentSha, unsignedPayload)
    req.Header.Set(headerDate, date.String())
    if creds.SessionToken != "" {
        req.Header.Set(headerSecurityToken, creds.SessionToken)
    }
    // The signer wants this as //authority/path
    // So get this by triming off the scheme and the colon before the first slash.
    req.URL.Opaque = strings.TrimPrefix(parsed.String(), parsed.Scheme+":")

    err = s.signer.SignHTTP(context.Background(), creds, req, unsignedPayload,
 s.service, s.region, date)
    if err != nil {
        return nil, fmt.Errorf("failed to sign request: %w", err)
    }

    // Pull the relevant headers out of the signer, and return them to get
    // included in the request we make.
    reqHeaders := map[string]string{
        headerContentSha:    req.Header.Get(headerContentSha),
        headerDate:          req.Header.Get(headerDate),
        headerAuthorization: req.Header.Get(headerAuthorization),
    }
    if req.Header.Get(headerSecurityToken) != "" {
        reqHeaders[headerSecurityToken] = req.Header.Get(headerSecurityToken)
    }

    return reqHeaders, nil
}

func (c *SigV4GrpcSigner) RequireTransportSecurity() bool {
    return true
```

```
}

var addr = flag.String("addr", "some-lattice-service:443", "the address to connect to")
var region = flag.String("region", "us-west-2", "region")

func callUnaryEcho(client ecpb.EchoClient, message string) {
    ctx, cancel := context.WithTimeout(context.Background(), 10*time.Second)
    defer cancel()
    resp, err := client.UnaryEcho(ctx, &ecpb.EchoRequest{Message: message})
    if err != nil {
        log.Fatalf("client.UnaryEcho(_) = _, %v: ", err)
    }
    fmt.Println("UnaryEcho: ", resp.Message)
}

func main() {
    flag.Parse()
    cfg, err := config.LoadDefaultConfig(context.TODO(),
 config.WithClientLogMode(aws.LogSigning))
    if err != nil {
        log.Fatalf("failed to load SDK configuration, %v", err)
    }

    pool, _ := x509.SystemCertPool()
    tlsConfig := &tls.Config{
        RootCAs: pool,
    }

    authority, _, _ := strings.Cut(*addr, ":") // Remove the port from the addr
    opts := []grpc.DialOption{
        grpc.WithTransportCredentials(credentials.NewTLS(tlsConfig)),

        // Lattice needs both the Authority to be set (without a port), and the SigV4
 signer
        grpc.WithAuthority(authority),
        grpc.WithPerRPCCredentials(NewSigV4GrpcSigner("vpc-lattice-svcs", *region,
 cfg.Credentials)),
    }

    conn, err := grpc.Dial(*addr, opts...)

    if err != nil {
        log.Fatalf("did not connect: %v", err)
    }
```

```
    defer conn.Close()
    rgc := ecpb.NewEchoClient(conn)

    callUnaryEcho(rgc, "hello world")
}
```

Datenschutz in Amazon VPC Lattice

Das AWS Modell der gilt für den Datenschutz in Amazon VPC Lattice. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen. AWS Cloud Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Dieser Inhalt enthält die Sicherheitskonfigurations- und Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services . Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Verschlüsselung während der Übertragung

VPC Lattice ist ein vollständig verwalteter Service, der aus einer Steuerungsebene und einer Datenebene besteht. Jede Ebene dient einem bestimmten Zweck im Service. Die Steuerungsebene stellt die administrative Ebene bereit, die zum Erstellen, Lesen/Beschreiben, Aktualisieren, Löschen und Auflisten (CRUDL) von Ressourcen APIs verwendet wird (z. B. `CreateService` und). `UpdateService` Die Kommunikation mit der VPC-Lattice-Steuerebene ist während der Übertragung durch TLS geschützt. Die Datenebene ist die VPC Lattice Invoke API, die die Verbindung zwischen Diensten bereitstellt. TLS verschlüsselt die Kommunikation mit der VPC Lattice-Datenebene, wenn Sie HTTPS oder TLS verwenden. Die Cipher Suite und die Protokollversion verwenden die von VPC Lattice bereitgestellten Standardeinstellungen und sind nicht konfigurierbar. Weitere Informationen finden Sie unter HTTPS-Listener für VPC Lattice-Dienste.

Verschlüsselung im Ruhezustand

Standardmäßig trägt die Verschlüsselung ruhender Daten dazu bei, den betrieblichen Aufwand und die Komplexität beim Schutz sensibler Daten zu reduzieren. Gleichzeitig können Sie damit sichere Anwendungen erstellen, die strenge Verschlüsselungsvorschriften und gesetzliche Auflagen erfüllen.

Inhalt

- Serverseitige Verschlüsselung mit in AWS KMS (SSE-KMS) gespeicherten AWS KMS Schlüsseln

Serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3)

Wenn Sie eine serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) verwenden, wird jedes Objekt wird mit einem eindeutigen Schlüssel verschlüsselt. Als zusätzliche Sicherheitsmaßnahme verschlüsseln wir den Schlüssel selbst mit einem Stammschlüssel, den wir regelmäßig wechseln. Die serverseitige Amazon-S3-Verschlüsselung verwendet zum Verschlüsseln Ihrer Daten eine der stärksten verfügbaren Blockverschlüsselungen, 256-bit Advanced Encryption Standard (AES-256) GCM. Für Objekte, die vor AES-GCM verschlüsselt wurden, wird AES-CBC zum Entschlüsseln dieser Objekte weiterhin unterstützt. Weitere Informationen finden Sie unter Serverseitige Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) verwenden.

Wenn Sie die serverseitige Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) für Ihren S3-Bucket für VPC Lattice-Zugriffsprotokolle aktivieren, verschlüsseln wir automatisch jede Zugriffsprotokolldatei, bevor sie in Ihrem S3-Bucket gespeichert wird. Weitere Informationen finden Sie unter An Amazon S3 gesendete Logs im CloudWatch Amazon-Benutzerhandbuch.

Serverseitige Verschlüsselung mit in AWS KMS (SSE-KMS) gespeicherten AWS KMS Schlüsseln

Die serverseitige Verschlüsselung mit AWS KMS Schlüsseln (SSE-KMS) ähnelt SSE-S3, bietet jedoch zusätzliche Vorteile und Gebühren für die Nutzung dieses Dienstes. Es gibt separate Berechtigungen für den AWS KMS Schlüssel, der zusätzlichen Schutz vor unbefugtem Zugriff auf Ihre Objekte in Amazon S3 bietet. SSE-KMS bietet Ihnen auch einen Prüfpfad, aus dem hervorgeht, wann und von AWS KMS wem Ihr Schlüssel verwendet wurde. Weitere Informationen finden Sie unter Serverseitige Verschlüsselung mit AWS Key Management Service (SSE-KMS) verwenden.

Inhalt

- Verschlüsselung und Entschlüsselung Ihres privaten Zertifikatschlüssels
- Verschlüsselungskontext für VPC Lattice
- Überwachung Ihrer Verschlüsselungsschlüssel für VPC Lattice

Verschlüsselung und Entschlüsselung Ihres privaten Zertifikatschlüssels

Ihr ACM-Zertifikat und Ihr privater Schlüssel werden mit einem AWS verwalteten KMS-Schlüssel verschlüsselt, der den Alias aws/acm hat. Sie können die Schlüssel-ID mit diesem Alias in der AWS KMS Konsole unter Verwaltete Schlüssel einsehen.AWS

VPC Lattice greift nicht direkt auf Ihre ACM-Ressourcen zu. Es verwendet den AWS TLS Connection Manager, um die privaten Schlüssel für Ihr Zertifikat zu sichern und darauf zuzugreifen. Wenn Sie Ihr ACM-Zertifikat verwenden, um einen VPC Lattice-Dienst zu erstellen, ordnet VPC Lattice Ihr Zertifikat dem TLS Connection Manager zu. AWS Dazu erstellen Sie eine Grant-ID für Ihren AWS verwalteten Schlüssel mit dem AWS KMS Präfix aws/acm. Eine Erteilung ist ein Richtlinieninstrument, das es TLS Connection Manager erlaubt, KMS-Schlüssel in kryptografischen Operationen zu verwenden. Die Erteilung erlaubt es dem Empfänger-Prinzipal (TLS Connection Manager), die angegebenen Genehmigungsoperationen für den KMS-Schlüssel aufzurufen, um den privaten Schlüssel Ihres Zertifikats zu entschlüsseln. Der TLS-Verbindungsmanager verwendet dann das Zertifikat und den entschlüsselten privaten Schlüssel (Klartext), um eine sichere Verbindung (SSL/TLS-Sitzung) mit Clients von VPC Lattice-Diensten herzustellen. Wenn das Zertifikat von einem VPC Lattice-Dienst getrennt wird, wird der Grant zurückgezogen.

Wenn Sie den Zugriff auf den KMS-Schlüssel entziehen möchten, empfehlen wir, das Zertifikat mit dem `update-service` Befehl oder aus dem Dienst zu ersetzen AWS Management Console oder zu löschen. AWS CLI

Verschlüsselungskontext für VPC Lattice

Ein Verschlüsselungskontext ist ein optionaler Satz von Schlüssel-Wert-Paaren, die kontextbezogene Informationen darüber enthalten, wofür Ihr privater Schlüssel verwendet werden könnte. AWS KMS bindet den Verschlüsselungskontext an die verschlüsselten Daten und verwendet ihn als zusätzliche authentifizierte Daten, um die authentifizierte Verschlüsselung zu unterstützen.

Wenn Ihre TLS-Schlüssel mit VPC Lattice und dem TLS Connection Manager verwendet werden, ist der Name Ihres VPC Lattice-Dienstes in dem Verschlüsselungskontext enthalten, der zur Verschlüsselung Ihres Schlüssels im Ruhezustand verwendet wird. Sie können überprüfen, für welchen VPC Lattice-Dienst Ihr Zertifikat und Ihr privater Schlüssel verwendet werden, indem Sie sich den Verschlüsselungskontext in Ihren CloudTrail Protokollen ansehen, wie im nächsten Abschnitt gezeigt, oder indem Sie in der ACM-Konsole die Registerkarte Zugeordnete Ressourcen aufrufen.

Zur Entschlüsselung von Daten wird derselbe Verschlüsselungskontext in der Anforderung übergeben. VPC Lattice verwendet bei allen kryptografischen AWS KMS-Vorgängen denselben

Verschlüsselungskontext, wobei der Schlüssel `aws:vpc-lattice:arn` und der Wert der Amazon-Ressourcenname (ARN) des VPC Lattice-Dienstes ist.

Im folgenden Beispiel sehen Sie den Verschlüsselungskontext in der Ausgabe einer Operation wie `CreateGrant`.

```
"encryptionContextEquals": {
    "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-west-2:111122223333:service/
svc-0b23c1234567890ab"
}
```

Überwachung Ihrer Verschlüsselungsschlüssel für VPC Lattice

Wenn Sie einen AWS verwalteten Schlüssel mit Ihrem VPC Lattice-Dienst verwenden, können Sie damit Anfragen verfolgen, AWS CloudTrailan die VPC Lattice sendet. AWS KMS

CreateGrant

Wenn Sie Ihr ACM-Zertifikat zu einem VPC Lattice-Dienst hinzufügen, wird in Ihrem Namen eine `CreateGrant` Anfrage gesendet, dass TLS Connection Manager den mit Ihrem ACM-Zertifikat verknüpften privaten Schlüssel entschlüsseln kann.

Sie können den **`CreateGrant`** Vorgang als Ereignis in CloudTrail, Ereignisverlauf, anzeigen. CreateGrant

Im Folgenden finden Sie ein Beispiel für einen Ereignisdatensatz im CloudTrail Ereignisverlauf für den `CreateGrant` Vorgang.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "IAMUser",
                "principalId": "EX_PRINCIPAL_ID",
                "arn": "arn:aws:iam::111122223333:user/Alice",
```

```
                "accountId": "111122223333",
                "userName": "Alice"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-02-06T23:30:50Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "acm.amazonaws.com"
    },
    "eventTime": "2023-02-07T00:07:18Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "acm.amazonaws.com",
    "userAgent": "acm.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "tlsconnectionmanager.amazonaws.com",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "operations": [
            "Decrypt"
        ],
        "constraints": {
            "encryptionContextEquals": {
                "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-
west-2:111122223333:service/svc-0b23c1234567890ab"
            }
        },
        "retiringPrincipal": "acm.us-west-2.amazonaws.com"
    },
    "responseElements": {
        "grantId": "f020fe75197b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "ba178361-8ab6-4bdd-9aa2-0d1a44b2974a",
    "eventID": "8d449963-1120-4d0c-9479-f76de11ce609",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
```

```
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Im obigen `CreateGrant` Beispiel ist der Principal des Empfängers TLS Connection Manager, und der Verschlüsselungskontext hat den VPC-Lattice-Dienst-ARN.

ListGrants

Sie können Ihre KMS-Schlüssel-ID und Ihre Konto-ID verwenden, um die API aufzurufen. `ListGrants` Dadurch erhalten Sie eine Liste aller Grants für den angegebenen KMS-Schlüssel. Weitere Informationen finden Sie unter ListGrants.

Verwenden Sie den folgenden `ListGrants` Befehl in AWS CLI , um die Details aller Zuschüsse anzuzeigen.

```
aws kms list-grants –key-id your-kms-key-id
```

Es folgt eine Beispielausgabe.

```
{
    "Grants": [
        {
            "Operations": [
                "Decrypt"
            ],
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "Name": "IssuedThroughACM",
            "RetiringPrincipal": "acm.us-west-2.amazonaws.com",
            "GranteePrincipal": "tlsconnectionmanager.amazonaws.com",
            "GrantId":
 "f020fe75197b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "CreationDate": "2023-02-06T23:30:50Z",
```

```
            "Constraints": {
                "encryptionContextEquals": {
                  "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                  "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-
west-2:111122223333:service/svc-0b23c1234567890ab"
                }
            }
        }
    ]
}
```

Im obigen `ListGrants` Beispiel ist der Principal des Empfängers TLS Connection Manager und der Verschlüsselungskontext hat den VPC-Lattice-Dienst-ARN.

Decrypt

VPC Lattice verwendet den TLS Connection Manager, um den `Decrypt` Vorgang zum Entschlüsseln Ihres privaten Schlüssels aufzurufen, um TLS-Verbindungen in Ihrem VPC Lattice-Dienst bereitzustellen. Sie können den **`Decrypt`** Vorgang im Ereignisverlauf unter Decrypt als Ereignis anzeigen. CloudTrail

Im Folgenden finden Sie ein Beispiel für einen Ereignisdatensatz im CloudTrail Ereignisverlauf für den `Decrypt` Vorgang.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "tlsconnectionmanager.amazonaws.com"
    },
    "eventTime": "2023-02-07T00:07:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "tlsconnectionmanager.amazonaws.com",
    "userAgent": "tlsconnectionmanager.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-west-2:111122223333:service/
svc-0b23c1234567890ab"
```

```
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "12345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "eventCategory": "Management"
}
```

Identitäts- und Zugriffsmanagement für Amazon VPC Lattice

In den folgenden Abschnitten wird beschrieben, wie Sie AWS Identity and Access Management (IAM) zur Sicherung Ihrer VPC Lattice-Ressourcen verwenden können, indem Sie steuern, wer VPC Lattice-API-Aktionen ausführen kann.

Themen

- So funktioniert Amazon VPC Lattice mit IAM
- Amazon VPC Lattice API-Berechtigungen
- Identitätsbasierte Richtlinien für Amazon VPC Lattice
- Verwenden von serviceverknüpften Rollen für Amazon VPC Lattice
- AWS verwaltete Richtlinien für Amazon VPC Lattice

So funktioniert Amazon VPC Lattice mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf VPC Lattice zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Verwendung mit VPC Lattice verfügbar sind.

IAM-Feature	VPC-Lattice-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie VPC Lattice und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für VPC Lattice

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. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien innerhalb von VPC Lattice

Unterstützt ressourcenbasierte Richtlinien: Ja

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. AWS In AWS Diensten, die ressourcenbasierte Richtlinien unterstützen, können Dienstadministratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource dieses Dienstes zu steuern. AWS 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.

VPC Lattice unterstützt Authentifizierungsrichtlinien, eine ressourcenbasierte Richtlinie, mit der Sie den Zugriff auf Dienste in Ihrem Servicenetzwerk steuern können. Weitere Informationen finden Sie unter Steuern Sie den Zugriff auf VPC Lattice-Dienste mithilfe von Authentifizierungsrichtlinien.

VPC Lattice unterstützt auch ressourcenbasierte Berechtigungsrichtlinien für die Integration mit. AWS Resource Access Manager Sie können diese ressourcenbasierten Richtlinien verwenden, um anderen AWS Konten oder Organisationen die Erlaubnis zur Verwaltung der Konnektivität für Dienste, Ressourcenkonfigurationen und Dienstnetzwerke zu erteilen. Weitere Informationen finden Sie unter Teilen Sie Ihre VPC Lattice-Entitäten.

Politische Maßnahmen für VPC Lattice

Unterstützt Richtlinienaktionen: Ja

In einer IAM-Richtlinienanweisung können Sie jede API-Aktion von jedem Service, der IAM unterstützt, angeben. Verwenden Sie für VPC Lattice das folgende Präfix mit dem Namen der API-Aktion:. `vpc-lattice:` Beispiel: `vpc-lattice:CreateService`, `vpc-lattice:CreateTargetGroup` und `vpc-lattice:PutAuthPolicy`.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommas:

```
"Action": [ "vpc-lattice:action1", "vpc-lattice:action2" ]
```

Sie können auch mehrere Aktionen mittels Platzhaltern angeben. Sie können beispielsweise alle Aktionen, deren Namen mit dem Wort beginnen`Get`, wie folgt angeben:

```
"Action": "vpc-lattice:Get*"
```

Eine vollständige Liste der VPC Lattice-API-Aktionen finden Sie unter Von Amazon VPC Lattice definierte Aktionen in der Service Authorization Reference.

Politische Ressourcen für VPC Lattice

Unterstützt Richtlinienressourcen: Ja

In einer IAM-Richtlinienanweisung gibt das `Resource`-Element das Objekt oder die Objekte an, für die die Anweisung gilt. Für VPC Lattice gilt jede IAM-Richtlinienanweisung für die Ressourcen, die Sie mithilfe ihrer angeben. ARNs

Das spezifische Format des Amazon Resource Name (ARN) hängt von der Ressource ab. Wenn Sie einen ARN angeben, ersetzen Sie den *`italicized`* Text durch Ihre ressourcenspezifischen Informationen.

- Abonnements für Zugriffsprotokolle:

  ```
  "Resource": "arn:aws:vpc-lattice:region:account-id:accesslogsubscription/access-log-subscription-id"
  ```

- Zuhörer:

  ```
  "Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id/
  listener/listener-id"
  ```

- Ressourcen-Gateways

  ```
  "Resource": "arn:aws:vpc-lattice:region:account-id:resourcegateway/resource-gateway-id"
  ```

- Konfiguration der Ressourcen

  ```
  "Resource": "arn:aws:vpc-lattice:region:account-id:resourceconfiguration/resource-configuration-id"
  ```

- Regeln:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id/
listener/listener-id/rule/rule-id"
```

- Services:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id"
```

- Servicenetzwerke:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:servicenetwork/service-network-id"
```

- Verbände von Servicenetzwerken:

```
"Resource": "arn:aws:vpc-lattice:region:account-
id:servicenetworkserviceassociation/service-network-service-association-id"
```

- Zuordnungen zur Konfiguration von Dienstnetzwerkressourcen

```
"Resource": "arn:aws:vpc-lattice:region:account-
id:servicenetworkresourceassociation/service-network-resource-association-id"
```

- VPC-Zuordnungen für das Servicenetzwerk:

```
"Resource": "arn:aws:vpc-lattice:region:account-
id:servicenetworkvpcassociation/service-network-vpc-association-id"
```

- Zielgruppen:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:targetgroup/target-group-id"
```

Schlüssel für Richtlinienbedingungen für VPC Lattice

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

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

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte

Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

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

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

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

Eine Liste der VPC Lattice-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon VPC Lattice in der Service Authorization Reference.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Informationen zu AWS globalen Bedingungsschlüsseln finden Sie unter Kontext-Schlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Zugriffskontrolllisten (ACLs) in VPC Lattice

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.

Attributbasierte Zugriffskontrolle (ABAC) mit VPC Lattice

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden diese Attribute als Tags AWS bezeichnet. Sie

können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

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

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

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

Weitere Informationen zu ABAC finden Sie unter 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.

Temporäre Anmeldeinformationen mit VPC Lattice verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

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

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden

AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Servicerollen für VPC Lattice

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.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von VPC Lattice beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn VPC Lattice eine Anleitung dazu bereitstellt.

Serviceverknüpfte Rollen für VPC Lattice

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte 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.

Informationen zum Erstellen oder Verwalten von dienstverknüpften VPC Lattice-Rollen finden Sie unter. Verwenden von serviceverknüpften Rollen für Amazon VPC Lattice

Amazon VPC Lattice API-Berechtigungen

Sie müssen IAM-Identitäten (wie Benutzern oder Rollen) die Berechtigung erteilen, die benötigten VPC Lattice API-Aktionen aufzurufen, wie unter beschrieben. Politische Maßnahmen für VPC Lattice Darüber hinaus müssen Sie für einige VPC Lattice-Aktionen IAM-Identitäten die Erlaubnis erteilen, bestimmte Aktionen von anderen aus aufzurufen. AWS APIs

Erforderliche Berechtigungen für die API

Wenn Sie die folgenden Aktionen über die API aufrufen, müssen Sie IAM-Benutzern die Erlaubnis erteilen, die angegebenen Aktionen aufzurufen.

`CreateResourceConfiguration`

- `vpc-lattice:CreateResourceConfiguration`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`
- `rds:DescribeDBClusters`

`CreateResourceGateway`

- `vpc-lattice:CreateResourceGateway`
- `ec2:AssignPrivateIpAddresses`
- `ec2:AssignIpv6Addresses`
- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`

`DeleteResourceGateway`

- `vpc-lattice:DeleteResourceGateway`
- `ec2:DeleteNetworkInterface`

`UpdateResourceGateway`

- `vpc-lattice:UpdateResourceGateway`
- `ec2:AssignPrivateIpAddresses`
- `ec2:AssignIpv6Addresses`
- `ec2:UnassignPrivateIpAddresses`
- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:DeleteNetworkInterface`

- ec2:DescribeNetworkInterfaces
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:ModifyNetworkInterfaceAttribute

CreateServiceNetworkResourceAssociation

- vpc-lattice:CreateServiceNetworkResourceAssociation
- ec2:AssignIpv6Addresses
- ec2:CreateNetworkInterface
- ec2:CreateNetworkInterfacePermission
- ec2:DescribeNetworkInterfaces

CreateServiceNetworkVpcAssociation

- vpc-lattice:CreateServiceNetworkVpcAssociation
- ec2:DescribeVpcs
- ec2:DescribeSecurityGroups(Nur erforderlich, wenn Sicherheitsgruppen bereitgestellt werden)

UpdateServiceNetworkVpcAssociation

- vpc-lattice:UpdateServiceNetworkVpcAssociation
- ec2:DescribeSecurityGroups(Wird nur benötigt, wenn Sicherheitsgruppen bereitgestellt werden)

CreateTargetGroup

- vpc-lattice:CreateTargetGroup
- ec2:DescribeVpcs

RegisterTargets

- vpc-lattice:RegisterTargets
- ec2:DescribeInstances(Wird nur benötigt, wenn der Zielgruppentyp angegeben INSTANCE ist)
- ec2:DescribeVpcs(Wird nur benötigt, wenn INSTANCE oder IP ist der Zielgruppentyp)
- ec2:DescribeSubnets(Wird nur benötigt, wenn INSTANCE oder der Zielgruppentyp IP ist)
- lambda:GetFunction(Wird nur benötigt, wenn der Zielgruppentyp LAMBDA ist)
- lambda:AddPermission(Nur erforderlich, wenn die Zielgruppe noch nicht berechtigt ist, die angegebene Lambda-Funktion aufzurufen)

`DeregisterTargets`

- `vpc-lattice:DeregisterTargets`

`CreateAccessLogSubscription`

- `vpc-lattice:CreateAccessLogSubscription`
- `logs:GetLogDelivery`
- `logs:CreateLogDelivery`

`DeleteAccessLogSubscription`

- `vpc-lattice:DeleteAccessLogSubscription`
- `logs:DeleteLogDelivery`

`UpdateAccessLogSubscription`

- `vpc-lattice:UpdateAccessLogSubscription`
- `logs:UpdateLogDelivery`

Identitätsbasierte Richtlinien für Amazon VPC Lattice

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

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

Einzelheiten zu den von VPC Lattice definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon VPC Lattice in der Service Authorization Reference.

Inhalt

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand VPC Lattice-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Für den vollen Zugriff sind zusätzliche Berechtigungen erforderlich

Um andere AWS Dienste, in die VPC Lattice integriert ist, und die gesamte Suite von VPC Lattice-Funktionen nutzen zu können, benötigen Sie spezielle zusätzliche Berechtigungen. Diese Berechtigungen sind nicht in der `VPCLatticeFullAccess` verwalteten Richtlinie enthalten, da das Risiko besteht, dass die Rechte eines unübersichtlichen Stellvertreters eskalieren.

Sie müssen Ihrer Rolle die folgende Richtlinie hinzufügen und sie zusammen mit der `VPCLatticeFullAccess` verwalteten Richtlinie verwenden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "firehose:TagDeliveryStream",
                "lambda:AddPermission",
                "s3:PutBucketPolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutResourcePolicy"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": [
                        "vpc-lattice.amazonaws.com"
```

```
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/vpc-
lattice.amazonaws.com/AWSServiceRoleForVpcLattice"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery*"
        }
    ]
}
```

Diese Richtlinie bietet die folgenden zusätzlichen Berechtigungen:

- `iam:AttachRolePolicy`: Ermöglicht das Anhängen der angegebenen verwalteten Richtlinie an die angegebene IAM-Rolle.
- `iam:PutRolePolicy`: Ermöglicht das Hinzufügen oder Aktualisieren eines Inline-Richtliniendokuments, das in die angegebene IAM-Rolle eingebettet ist.
- `s3:PutBucketPolicy`: Ermöglicht es Ihnen, eine Bucket-Richtlinie auf einen Amazon S3 S3-Bucket anzuwenden.
- `firehose:TagDeliveryStream`: Ermöglicht das Hinzufügen oder Aktualisieren von Tags für Firehose-Lieferstreams.

Beispiele für identitätsbasierte Richtlinien für VPC Lattice

Themen

- Beispielrichtlinie: VPC-Zuordnungen zu einem Servicenetzwerk verwalten

- Beispielrichtlinie: Dienstzuordnungen zu einem Dienstnetzwerk erstellen
- Beispielrichtlinie: Hinzufügen von Tags zu Ressourcen
- Beispielrichtlinie: Erstellen Sie eine serviceverknüpfte Rolle

Beispielrichtlinie: VPC-Zuordnungen zu einem Servicenetzwerk verwalten

Das folgende Beispiel zeigt eine Richtlinie, die Benutzern mit dieser Richtlinie die Berechtigung erteilt, die VPC-Zuordnungen zu einem Dienstnetzwerk zu erstellen, zu aktualisieren und zu löschen, jedoch nur für die in der Bedingung angegebene VPC und das Dienstnetzwerk. Weitere Informationen zur Angabe von Bedingungsschlüssel finden Sie unter Schlüssel für Richtlinienbedingungen für VPC Lattice.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:CreateServiceNetworkVpcAssociation",
            "vpc-lattice:UpdateServiceNetworkVpcAssociation",
            "vpc-lattice:DeleteServiceNetworkVpcAssociation"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "StringEquals": {
               "vpc-lattice:ServiceNetworkArn": "arn:aws:vpc-lattice:us-
west-2:123456789012:servicenetwork/sn-903004f88example",
               "vpc-lattice:VpcId": "vpc-1a2b3c4d"
            }
         }
      }
   ]
}
```

Beispielrichtlinie: Dienstzuordnungen zu einem Dienstnetzwerk erstellen

Wenn Sie keine Bedingungsschlüssel verwenden, um den Zugriff auf VPC-Lattice-Ressourcen zu steuern, können Sie stattdessen die Anzahl ARNs der Ressourcen in dem `Resource` Element angeben, um den Zugriff zu kontrollieren.

Das folgende Beispiel zeigt eine Richtlinie, die die Dienstzuordnungen auf ein Dienstnetzwerk beschränkt, das Benutzer mit dieser Richtlinie erstellen können, indem sie den ARNs Dienst und das Dienstnetzwerk angeben, die mit der `CreateServiceNetworkServiceAssociation` API-Aktion verwendet werden können. Weitere Hinweise zur Angabe der ARN-Werte finden Sie unterPolitische Ressourcen für VPC Lattice.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:CreateServiceNetworkServiceAssociation"
         ],
         "Resource": [
            "arn:aws:vpc-lattice:us-
west-2:123456789012:servicenetworkserviceassociation/*",
            "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-04d5cc9b88example",
            "arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/
sn-903004f88example"
         ]
      }
   ]
}
```

Beispielrichtlinie: Hinzufügen von Tags zu Ressourcen

Das folgende Beispiel zeigt eine Richtlinie, die Benutzern mit dieser Richtlinie die Berechtigung gibt, Tags auf VPC-Lattice-Ressourcen zu erstellen.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:TagResource"
         ],
         "Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:*/*"
      }
   ]
}
```

Beispielrichtlinie: Erstellen Sie eine serviceverknüpfte Rolle

VPC Lattice benötigt Berechtigungen zum Erstellen einer serviceverknüpften Rolle, wenn ein Benutzer in Ihrem Unternehmen zum ersten Mal VPC AWS-Konto Lattice-Ressourcen erstellt. Wenn die serviceverknüpfte Rolle noch nicht existiert, erstellt VPC Lattice sie in Ihrem Konto. Die serviceverknüpfte Rolle erteilt VPC Lattice Berechtigungen, sodass sie in AWS-Services Ihrem Namen andere Personen anrufen kann. Weitere Informationen finden Sie unter the section called “Verwenden von serviceverknüpften Rollen”.

Damit diese automatische Rollenerstellung möglich ist, müssen Benutzer über Berechtigungen für die Aktion `iam:CreateServiceLinkedRole` verfügen.

```
"Action": "iam:CreateServiceLinkedRole"
```

Das folgende Beispiel zeigt eine Richtlinie, die Benutzern mit dieser Richtlinie die Berechtigung gibt, eine dienstverknüpfte Rolle für VPC Lattice zu erstellen.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName":"vpc-lattice.amazonaws.com"
            }
         }
      }
   ]
}
```

Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für Amazon VPC Lattice

Amazon VPC Lattice verwendet eine serviceverknüpfte Rolle für die Berechtigungen, die erforderlich sind, um andere in AWS-Services Ihrem Namen anzurufen. Weitere Informationen finden Sie unter Serviceverknüpfte Rollen im IAM-Benutzerhandbuch.

VPC Lattice verwendet die mit dem Dienst verknüpfte Rolle namens. AWSServiceRoleForVpcLattice

Dienstbezogene Rollenberechtigungen für VPC Lattice

Die serviceverknüpfte Rolle AWSServiceRoleForVpcLattice vertraut darauf, dass der folgende Service die Rolle annimmt:

- `vpc-lattice.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie AWSVpcLatticeServiceRolePolicy ermöglicht es VPC Lattice, CloudWatch Metriken im Namespace zu veröffentlichen. `AWS/VpcLattice` Weitere Informationen finden Sie AWSVpcLatticeServiceRolePolicyin der Referenz zu AWS verwalteten Richtlinien.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter the section called “Beispielrichtlinie: Erstellen Sie eine serviceverknüpfte Rolle”.

Eine serviceverknüpfte Rolle für VPC Lattice erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie VPC-Lattice-Ressourcen in der AWS Management Console, der oder der AWS API erstellen AWS CLI, erstellt VPC Lattice die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie VPC Lattice-Ressourcen erstellen, erstellt VPC Lattice die serviceverknüpfte Rolle erneut für Sie.

Eine serviceverknüpfte Rolle für VPC Lattice bearbeiten

Sie können die Beschreibung der Verwendung von AWSServiceRoleForVpcLatticeIAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer servicebezogenen Rollenbeschreibung im IAM-Benutzerhandbuch.

Löschen Sie eine serviceverknüpfte Rolle für VPC Lattice

Wenn Sie Amazon VPC Lattice nicht mehr verwenden müssen, empfehlen wir Ihnen, Amazon VPC Lattice zu löschen. AWSServiceRoleForVpcLattice

Sie können diese serviceverknüpfte Rolle erst löschen, nachdem Sie alle VPC Lattice-Ressourcen in Ihrem gelöscht haben. AWS-Konto

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die dienstverknüpfte Rolle zu löschen. AWSServiceRoleForVpcLattice Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Löschen einer serviceverknüpften Rolle.

Nachdem Sie eine serviceverknüpfte Rolle gelöscht haben, erstellt VPC Lattice die Rolle erneut, wenn Sie VPC Lattice-Ressourcen in Ihrem erstellen. AWS-Konto

Unterstützte Regionen für serviceverknüpfte Rollen mit VPC Lattice

VPC Lattice unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist.

AWS verwaltete Richtlinien für Amazon VPC Lattice

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

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie 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 verwaltete Richtlinie: VPCLattice FullAccess

Diese Richtlinie bietet vollen Zugriff auf Amazon VPC Lattice und eingeschränkten Zugriff auf andere abhängige Dienste. Sie beinhaltet Berechtigungen für Folgendes:

- ACM — Rufen Sie den SSL/TLS Zertifikat-ARN für benutzerdefinierte Domainnamen ab.
- CloudWatch — Zugriffsprotokolle und Überwachungsdaten anzeigen.
- CloudWatch Protokolle — Richten Sie Zugriffsprotokolle ein und senden Sie sie an CloudWatch Logs.
- Amazon EC2 — Netzwerkschnittstellen konfigurieren und Informationen über EC2 Instances abrufen und VPCs. Dies wird verwendet, um Ressourcenkonfigurationen, Ressourcen-Gateways und Zielgruppen zu erstellen, VPC Lattice-Entitätszuordnungen zu konfigurieren und Ziele zu registrieren.
- Elastic Load Balancing — Rufen Sie Informationen über einen Application Load Balancer ab, um ihn als Ziel zu registrieren.
- Firehose — Ruft Informationen zu Lieferströmen ab, die zum Speichern von Zugriffsprotokollen verwendet werden.
- Lambda — Ruft Informationen über eine Lambda-Funktion ab, um sie als Ziel zu registrieren.
- Amazon RDS — Rufen Sie Informationen über RDS-Cluster und -Instances ab.
- Amazon S3 — Rufen Sie Informationen über S3-Buckets ab, die zum Speichern von Zugriffsprotokollen verwendet werden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter VPCLatticeFullAccess in der Referenz zu von AWS verwalteten Richtlinien.

Um andere AWS Dienste, in die VPC Lattice integriert ist, und die gesamte Suite von VPC Lattice-Funktionen nutzen zu können, benötigen Sie spezielle zusätzliche Berechtigungen. Diese Berechtigungen sind nicht in der `VPCLatticeFullAccess` verwalteten Richtlinie enthalten, da das Risiko besteht, dass die Rechte eines unübersichtlichen Stellvertreters eskalieren. Weitere Informationen finden Sie unter Für den vollen Zugriff sind zusätzliche Berechtigungen erforderlich.

AWS verwaltete Richtlinie: VPCLattice ReadOnlyAccess

Diese Richtlinie bietet Lesezugriff auf Amazon VPC Lattice und eingeschränkten Zugriff auf andere abhängige Dienste. Sie umfasst Berechtigungen für Folgendes:

- ACM — Rufen Sie den SSL/TLS Zertifikat-ARN für benutzerdefinierte Domainnamen ab.

- CloudWatch — Zugriffsprotokolle und Überwachungsdaten anzeigen.
- CloudWatch Protokolle — Zeigt Informationen zur Protokollzustellung für Zugriffsprotokollabonnements an.
- Amazon EC2 — Informationen über EC2 Instances abrufen und VPCs Zielgruppen erstellen und Ziele registrieren.
- Elastic Load Balancing — Ruft Informationen über einen Application Load Balancer ab.
- Firehose — Ruft Informationen zu Lieferströmen für die Zugriffs-Log-Zustellung ab.
- Lambda — Informationen zu einer Lambda-Funktion anzeigen.
- Amazon RDS — Rufen Sie Informationen über RDS-Cluster und -Instances ab.
- Amazon S3 — Rufen Sie Informationen zu S3-Buckets für die Zustellung von Zugriffsprotokollen ab.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter VPCLatticeReadOnlyAccess in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: VPCLattice ServicesInvokeAccess

Diese Richtlinie ermöglicht den Zugriff auf Amazon VPC Lattice-Dienste.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter VPCLatticeServicesInvokeAccess in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSVpc LatticeServiceRolePolicy

Diese Richtlinie ist einer dienstbezogenen Rolle zugeordnet, die so benannt ist AWSServiceRoleForVpcLattice, dass VPC Lattice Aktionen in Ihrem Namen ausführen kann. Sie können diese Richtlinie nicht mit Ihren IAM-Entitäten verknüpfen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon VPC Lattice.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSVpcLatticeServiceRolePolicy in der Referenz zu von AWS verwalteten Richtlinien.

VPC Lattice-Updates für verwaltete Richtlinien AWS

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für VPC Lattice an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed für das VPC Lattice User Guide, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
VPCLatticeFullAccess	VPC Lattice fügt Nur-Lese-Berechtigungen zur Beschreibung von Amazon RDS-Clustern und -Instances hinzu.	01. Dezember 2024
VPCLatticeReadOnlyAccess	VPC Lattice fügt Nur-Lese-Berechtigungen zur Beschreibung von Amazon RDS-Clustern und -Instances hinzu.	01. Dezember 2024
AWSVpcLatticeServiceRolePolicy	VPC Lattice fügt Berechtigungen hinzu, damit VPC Lattice eine vom Anforderer verwaltete Netzwerkschnittstelle erstellen kann.	01. Dezember 2024
VPCLatticeFullAccess	VPC Lattice fügt eine neue Richtlinie hinzu, um Berechtigungen für vollen Zugriff auf Amazon VPC Lattice und eingeschränkten Zugriff auf andere abhängige Dienste zu gewähren.	31. März 2023
VPCLatticeReadOnlyAccess	VPC Lattice fügt eine neue Richtlinie hinzu, um Berechtigungen für schreibgeschützten Zugriff auf Amazon VPC Lattice und eingeschränkten Zugriff auf andere abhängige Dienste zu gewähren.	31. März 2023
VPCLatticeServicesInvokeAccess	VPC Lattice fügt eine neue Richtlinie hinzu, um Zugriff auf den Aufruf von Amazon VPC Lattice-Diensten zu gewähren.	31. März 2023
AWSVpcLatticeServiceRolePolicy	VPC Lattice fügt seiner serviceverknüpften Rolle Berechtigungen hinzu, damit VPC Lattice Metriken im Namespace veröffentlichen CloudWatch kann. `AWS/`	5. Dezember 2022

Änderung	Beschreibung	Datum
	`VpcLattice` Die `AWSVpcLatticeServiceRolePolicy` Richtlinie beinhaltet die Erlaubnis, die API-Aktion aufzurufen. CloudWatch PutMetricData Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon VPC Lattice.	
VPC Lattice hat begonnen, Änderungen zu verfolgen	VPC Lattice begann, Änderungen an seinen AWS verwalteten Richtlinien zu verfolgen.	5. Dezember 2022

Konformitätsvalidierung für Amazon VPC Lattice

Externe Prüfer bewerten die Sicherheit und Konformität von Amazon VPC Lattice im Rahmen mehrerer AWS Compliance-Programme.

Informationen darüber, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services Umfang nach Compliance-Programm unter Umfang nach Compliance-Programm AWS-Services das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Greifen Sie über Schnittstellenendpunkte auf Amazon VPC Lattice zu ()AWS PrivateLink

Sie können eine private Verbindung zwischen Ihrer VPC und Amazon VPC Lattice herstellen, indem Sie einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellenendpunkte werden mit einer Technologie betrieben AWS PrivateLink, die es Ihnen ermöglicht, privat auf VPC Lattice APIs ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder Verbindung zuzugreifen. AWS Direct Connect Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit VPC Lattice zu kommunizieren. APIs

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Netzwerkschnittstellen in Ihren Subnetzen repräsentiert.

Überlegungen zu VPC-Endpunkten mit Schnittstellen

Bevor Sie einen VPC-Schnittstellen-Endpunkt für VPC Lattice einrichten, stellen Sie sicher, dass Sie Access AWS-Services through AWS PrivateLink im Leitfaden lesen.AWS PrivateLink

VPC Lattice unterstützt Aufrufe aller API-Aktionen von Ihrer VPC aus.

Erstellen eines VPC-Schnittstellen-Endpunkts für VPC Lattice

Sie können einen VPC-Endpunkt für den VPC Lattice-Service entweder mit der Amazon VPC-Konsole oder mit () erstellen. AWS Command Line Interface AWS CLI Weitere Informationen finden Sie im AWS PrivateLink Handbuch unter Erstellen eines Schnittstellen-VPC-Endpunkts.

Erstellen Sie einen VPC-Endpunkt für VPC Lattice mit dem folgenden Dienstnamen:

`com.amazonaws.region.vpc-lattice`

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an VPC Lattice stellen, indem Sie den Standard-DNS-Namen für die Region verwenden, z. B. `vpc-lattice.us-east-1.amazonaws.com`

Resilienz in Amazon VPC Lattice

Die AWS globale Infrastruktur basiert AWS-Regionen auf Availability Zones.

AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind.

Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Infrastruktursicherheit in Amazon VPC Lattice

Als verwalteter Service ist Amazon VPC Lattice durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf VPC Lattice zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Überwachung von Amazon VPC Lattice

Verwenden Sie die Funktionen in diesem Abschnitt, um Ihre Amazon VPC Lattice-Servicenetzwerke, Dienste, Zielgruppen und VPC-Verbindungen zu überwachen.

Inhalt

CloudWatch Metriken für Amazon VPC Lattice

Amazon VPC Lattice sendet Daten in Bezug auf Ihre Zielgruppen und Services an Amazon CloudWatch und verarbeitet sie in lesbare Metriken nahezu in Echtzeit. Diese Metriken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Amazon VPC Lattice verwendet eine serviceverknüpfte Rolle in Ihrem AWS Konto, um Messwerte an Amazon zu senden. CloudWatch Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon VPC Lattice.

Inhalt

Anzeigen von CloudWatch Amazon-Metriken

Sie können die CloudWatch Amazon-Metriken für Ihre Zielgruppen und Dienste über die CloudWatch Konsole oder anzeigen AWS CLI.

So zeigen Sie Metriken mithilfe der CloudWatch -Konsole an

1. Öffnen Sie die CloudWatch Amazon-Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den `AWS/VpcLattice`-Namespace.
4. (Optional) Um eine Metrik in allen Dimensionen anzuzeigen, geben Sie den Namen in das Suchfeld ein.
5. (Optional) Um nach Maß zu filtern, wählen Sie einen der folgenden Schritte aus:
   - Um nur die für Ihre Zielgruppen gemeldeten Kennzahlen anzuzeigen, wählen Sie Zielgruppen aus. Um die Metriken für eine einzelne Zielgruppe anzuzeigen, geben Sie den Namen in das Suchfeld ein.
   - Um nur die für Ihre Dienste gemeldeten Metriken anzuzeigen, wählen Sie Dienste. Um die Metriken für einen einzelnen Service anzuzeigen, geben Sie den Namen in das Suchfeld ein.

Um Metriken anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den folgenden CloudWatch list-metrics AWS CLI -Befehl, um die verfügbaren Metriken aufzuführen:

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

Informationen zu den einzelnen Metriken und ihren Dimensionen finden Sie unter Zielgruppen-Metriken und. Servicemetriken

Zielgruppen-Metriken

VPC Lattice speichert automatisch Kennzahlen zu Zielgruppen im `AWS/VpcLattice` CloudWatch Amazon-Namespace. Weitere Informationen zu Zielgruppen finden Sie unterZielgruppen in VPC Lattice.

Dimensionen

Verwenden Sie die nachstehenden Dimensionen, um die Metriken nach Zielgruppen zu filtern:

- `AvailabilityZone`
- `TargetGroup`

Metrik	Beschreibung
`TotalConnectionCount`	Verbindungen insgesamt. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Traffic empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.
`ActiveConnectionCount`	Aktive Verbindungen. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Traffic empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.
`ConnectionErrorCount`	Verbindungsfehler insgesamt.

Metrik	Beschreibung
	Kriterien für die Berichterstattung • Wird immer ab dem Zeitpunkt gemeldet, zu dem die Ressource Datenverkehr empfängt (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.
`HTTP1_ConnectionCount`	HTTP/1.1-Verbindungen insgesamt. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Traffic empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.

Metrik	Beschreibung
`HTTP2_ConnectionCount`	HTTP/2-Verbindungen insgesamt. Kriterien für die Berichterstattung • Wird immer (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt) ab dem Zeitpunkt gemeldet, zu dem die Ressource Datenverkehr empfängt. Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.
`ConnectionTimeoutCount`	Gesamtzahl der Timeouts bei Verbindungsverbindungen. Kriterien für die Berichterstattung • Wird immer ab dem Zeitpunkt gemeldet, zu dem die Ressource Datenverkehr empfängt (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.

Metrik	Beschreibung
`TotalReceivedConnectionBytes`	Gesamtzahl der empfangenen Verbindungsbytes. Kriterien für die Berichterstattung • Wird immer (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt) ab dem Zeitpunkt gemeldet, zu dem die Ressource Datenverkehr empfängt. Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.
`TotalSentConnectionBytes`	Gesamtzahl der gesendeten Verbindungsbytes. Kriterien für die Berichterstattung • Wird immer (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt) ab dem Zeitpunkt gemeldet, zu dem die Ressource Datenverkehr empfängt. Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.

Metrik	Beschreibung
`TotalRequestCount`	Anfragen insgesamt. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Traffic empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.
`ActiveRequestCount`	Gesamtzahl der aktiven Anfragen. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Traffic empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einem Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.

Metrik	Beschreibung
`RequestTime`	Anforderungszeit bis zum letzten Byte in Millisekunden. Kriterien für die Berichterstattung • Wird immer ab dem Zeitpunkt gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt), sobald die Ressource Traffic empfängt. Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichsten Statistiken sind `Average` und `pNN.NN` (Perzentile).
`HTTPCode_2XX_Count`, `HTTPCode_3XX_Count`, `HTTPCode_4XX_Count`, `HTTPCode_5XX_Count`	Aggregieren Sie HTTP-Antwortcodes. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Traffic empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einem Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist`Sum`.

Metrik	Beschreibung
`TLSConnectionErrorCount`	Gesamtzahl der TLS-Verbindungsfehler ohne fehlgeschlagene Zertifikatsüberprüfungen. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Datenverkehr empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.
`TotalTLSConnectionHandshakeCount`	Gesamtzahl der erfolgreichen TLS-Verbindungs-Handshakes. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Datenverkehr empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.

Servicemetriken

VPC Lattice speichert automatisch Metriken zu Services im `AWS/VpcLattice` CloudWatch Amazon-Namespace. Weitere Informationen zu -Services finden Sie unterDienstleistungen in VPC Lattice.

Dimensionen

Verwenden Sie die nachstehenden Dimensionen, um die Metriken nach Zielgruppen zu filtern:

- `AvailabilityZone`
- `Service`

Metrik	Beschreibung
`RequestTimeoutCount`	Gesamtzahl der Anfragen, bei denen das Timeout beim Warten auf eine Antwort überschritten wurde. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Traffic empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist`Sum`.
`TotalRequestCount`	Anfragen insgesamt. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Traffic empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt).

Metrik	Beschreibung
	Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.
`RequestTime`	Anforderungszeit in Millisekunden. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Traffic empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einen Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichsten Statistiken sind `Average` und `pNN.NN` (Perzentile).

Metrik	Beschreibung
`HTTPCode_2XX_Count`, `HTTPCode_3XX_Count`, `HTTPCode_4XX_Count`, `HTTPCode_5XX_Count`	Aggregieren Sie HTTP-Antwortcodes. Kriterien für die Berichterstattung • Wird ab dem Zeitpunkt, zu dem die Ressource Traffic empfängt, immer gemeldet (unabhängig davon, ob es sich um einen Wert von Null oder einem Wert ungleich Null handelt). Häufigkeit von Bereinigungen • Einmal pro Minute. Statistiken • Die nützlichste Statistik ist `Sum`.

Zugriffsprotokolle für Amazon VPC Lattice

Zugriffsprotokolle erfassen detaillierte Informationen zu Ihren VPC Lattice-Diensten und Ressourcenkonfigurationen. Sie können diese Zugriffsprotokolle verwenden, um Verkehrsmuster zu analysieren und alle Dienste im Netzwerk zu überprüfen. Für VPC Lattice-Dienste veröffentlichen wir `VpcLatticeAccessLogs` und für Ressourcenkonfigurationen veröffentlichen wir, `VpcLatticeResourceAccessLogs` was separat konfiguriert werden muss.

Zugriffsprotokolle sind optional und standardmäßig deaktiviert. Nachdem Sie die Zugriffsprotokolle aktiviert haben, können Sie sie jederzeit deaktivieren.

Preisgestaltung

Bei der Veröffentlichung von Zugriffsprotokollen fallen Gebühren an. Protokolle, die AWS nativ in Ihrem Namen veröffentlicht werden, werden als verkaufte Protokolle bezeichnet. Weitere Informationen zu den Preisen für verkaufte Logs finden Sie unter CloudWatch Amazon-Preise, wählen Sie Logs und sehen Sie sich die Preise unter Verkaufte Logs an.

Inhalt

- Ziele der Zugriffsprotokolle
- Aktivieren der Zugriffsprotokolle
- Inhalt des Zugriffsprotokolls
- Inhalt des Ressourcenzugriffsprotokolls
- Problembehandlung bei Zugriffsprotokollen

Für die Aktivierung von Zugriffsprotokollen sind IAM-Berechtigungen erforderlich

Um Zugriffsprotokolle zu aktivieren und die Protokolle an ihre Ziele zu senden, muss die Richtlinie dem IAM-Benutzer, der Gruppe oder der Rolle, die Sie verwenden, die folgenden Aktionen zugeordnet haben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Sid": "ManageVPCLatticeAccessLogSetup",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:GetLogDelivery",
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "vpc-lattice:CreateAccessLogSubscription",
                "vpc-lattice:GetAccessLogSubscription",
                "vpc-lattice:UpdateAccessLogSubscription",
                "vpc-lattice:DeleteAccessLogSubscription",
                "vpc-lattice:ListAccessLogSubscriptions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Informationen finden Sie im Abschnitt Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im AWS Identity and Access Management -Benutzerhandbuch.

Nachdem Sie die Richtlinie aktualisiert haben, die dem IAM-Benutzer, der Gruppe oder der Rolle zugeordnet ist, die Sie verwenden, gehen Sie zu. Aktivieren der Zugriffsprotokolle

Ziele der Zugriffsprotokolle

Sie können Zugriffsprotokolle an die folgenden Ziele senden.

CloudWatch Amazon-Protokolle

- VPC Lattice übermittelt Logs in der Regel innerhalb von 2 CloudWatch Minuten an Logs. Beachten Sie jedoch, dass die tatsächliche Protokollzustellung nach bestem Wissen erfolgt und es zu zusätzlicher Latenz kommen kann.
- Eine Ressourcenrichtlinie wird automatisch erstellt und der CloudWatch Protokollgruppe hinzugefügt, wenn die Protokollgruppe nicht über bestimmte Berechtigungen verfügt. Weitere Informationen finden Sie unter An Logs sent to CloudWatch Logs im CloudWatch Amazon-Benutzerhandbuch.
- Zugriffsprotokolle, an die gesendet werden, finden Sie in der CloudWatch Konsole CloudWatch unter Protokollgruppen. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter An CloudWatch Logs gesendete Protokolldaten anzeigen.

Amazon S3

- VPC Lattice übermittelt Protokolle in der Regel innerhalb von 6 Minuten an Amazon S3. Beachten Sie jedoch, dass die tatsächliche Protokollzustellung nach bestem Wissen erfolgt und es zu zusätzlicher Latenz kommen kann.
- Eine Bucket-Richtlinie wird automatisch erstellt und Ihrem Amazon S3 S3-Bucket hinzugefügt, falls der Bucket nicht über bestimmte Berechtigungen verfügt. Weitere Informationen finden Sie unter An Amazon S3 gesendete Logs im CloudWatchAmazon-Benutzerhandbuch.
- Zugriffsprotokolle, die an Amazon S3 gesendet werden, verwenden die folgende Benennungskonvention:

```
[bucket]/[prefix]/AWSLogs/[accountId]/VpcLattice/AccessLogs/[region]/[YYYY/
MM/DD]/[resource-id]/[accountId]_VpcLatticeAccessLogs_[region]_[resource-
id]_YYYYMMDDTHHmmZ_[hash].json.gz
```

- VpcLatticeResourceAccessLogs die an Amazon S3 gesendet werden, verwenden die folgende Namenskonvention:

```
[bucket]/[prefix]/AWSLogs/[accountId]/VpcLattice/ResourceAccessLogs/[region]/[YYYY/
MM/DD]/[resource-id]/[accountId]_VpcLatticeResourceAccessLogs_[region]_[resource-
id]_YYYYMMDDTHHmmZ_[hash].json.gz
```

Amazon Data Firehose

- VPC Lattice liefert Logs in der Regel innerhalb von 2 Minuten an Firehose. Beachten Sie jedoch, dass die tatsächliche Protokollzustellung nach bestem Wissen erfolgt und es zu zusätzlichen Latenzen kommen kann.
- Es wird automatisch eine serviceverknüpfte Rolle erstellt, die VPC Lattice die Erlaubnis erteilt, Zugriffsprotokolle an zu senden. Amazon Data Firehose Damit die automatische Rollenerstellung erfolgreich ist, müssen die Benutzer über die Berechtigung für die Aktion `iam:CreateServiceLinkedRole` verfügen. Weitere Informationen finden Sie unter Gesendete Logs Amazon Data Firehose im CloudWatch Amazon-Benutzerhandbuch.
- Weitere Informationen zum Anzeigen der gesendeten Protokolle finden Sie unter Monitoring Amazon Kinesis Data Streams im Amazon Data Firehose Developer Guide. Amazon Data Firehose

Aktivieren der Zugriffsprotokolle

Gehen Sie wie folgt vor, um die Zugriffsprotokolle so zu konfigurieren, dass Zugriffsprotokolle erfasst und an das von Ihnen gewählte Ziel gesendet werden.

Inhalt

Aktivieren Sie die Zugriffsprotokolle mithilfe der Konsole

Sie können während der Erstellung Zugriffsprotokolle für ein Dienstnetzwerk, einen Dienst oder eine Ressourcenkonfiguration aktivieren. Sie können Zugriffsprotokolle auch aktivieren, nachdem Sie eine Dienstnetzwerk-, Dienst- oder Ressourcenkonfiguration erstellt haben, wie im folgenden Verfahren beschrieben.

Um einen Basisdienst mit der Konsole zu erstellen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie das Dienstnetzwerk, den Dienst oder die Ressourcenkonfiguration aus.
3. Wählen Sie Aktionen, Protokolleinstellungen bearbeiten aus.
4. Schalten Sie den Schalter Zugriffsprotokolle ein.
5. Fügen Sie wie folgt ein Lieferziel für Ihre Zugriffsprotokolle hinzu:
   - Wählen Sie CloudWatch Protokollgruppe und wählen Sie eine Protokollgruppe aus. Um eine Protokollgruppe zu erstellen, wählen Sie Protokollgruppe erstellen in CloudWatch.
   - Wählen Sie S3-Bucket aus und geben Sie den S3-Bucket-Pfad einschließlich eines beliebigen Präfixes ein. Um Ihre S3-Buckets zu durchsuchen, wählen Sie Browse S3.
   - Wählen Sie Kinesis Data Firehose Delivery Stream und wählen Sie einen Delivery Stream aus. Um einen Delivery Stream zu erstellen, wählen Sie Create a delivery stream in Kinesis.
6. Wählen Sie Änderungen speichern aus.

Aktivieren Sie die Zugriffsprotokolle mit dem AWS CLI

Verwenden Sie den CLI-Befehl create-access-log-subscription, um Zugriffsprotokolle für Servicenetzwerke oder Dienste zu aktivieren.

Inhalt des Zugriffsprotokolls

Die folgende Tabelle beschreibt die Felder eines Zugriffsprotokolleintrags.

Feld	Beschreibung	Format
`hostHeader`	Der Autoritätsheader der Anfrage.	Zeichenfolge
`sslCipher`	Der OpenSSL-Name für den Satz von Chiffren, der zum Herstellen der Client-TLS-Verbindung verwendet wird.	Zeichenfolge
`serviceNetworkArn`	Das Servicenetzwerk ARN.	arn:aws:vpc-lattice: ::service network/ *region account id*

Feld	Beschreibung	Format
`resolvedUser`	Der ARN des Benutzers, wenn die Authentifizierung aktiviert ist und die Authentifizierung abgeschlossen ist.	null | ARN | „Anonym“ | „Unbekannt“
`authDeniedReason`	Der Grund, warum der Zugriff verweigert wird, wenn die Authentifizierung aktiviert ist.	null | „Dienst“ | „Netzwerk“ | „Identität“
`requestMethod`	Der Methodenheader der Anfrage.	Zeichenfolge
`targetGroupArn`	Die Zielhostgruppe, zu der der Zielhost gehört.	Zeichenfolge
`tlsVersion`	Die TLS-Version.	TLSv*x*
`userAgent`	Der User-Agent-Header.	Zeichenfolge
`ServerNameIndication`	[Nur HTTPS] Der auf dem SSL-Verbindungs-Socket für Server Name Indication (SNI) festgelegte Wert.	Zeichenfolge
`destinationVpcId`	Die Ziel-VPC-ID.	vpc- *xxxxxxxx*
`sourceIpPort`	Die IP-Adresse und:Port der Quelle.	*ip*:*port*
`targetIpPort`	Die IP-Adresse und der Port des Ziels.	*ip*:*port*
`serviceArn`	Der Dienst ARN.	arn:aws:vpc-lattice: ::service/ *region account id*
`sourceVpcId`	Die Quell-VPC-ID.	vpc- *xxxxxxxx*
`requestPath`	Den Pfad der Anfrage.	LatticePath?:*path*

Feld	Beschreibung	Format
`startTime`	Die Startzeit der Anfrage.	*YYYY*- *MM* - *DD* T *HHMM*: *SS* Z
`protocol`	Das Protokoll. Derzeit entweder HTTP/1.1 oder HTTP/2.	Zeichenfolge
`responseCode`	Der HTTP-Antwort-Code. Nur der Antwortcode für die endgültigen Header wird protokolliert. Weitere Informationen finden Sie unter Problembehandlung bei Zugriffsprotokollen.	Ganzzahl
`bytesReceived`	Die empfangenen Text- und Header-Bytes.	Ganzzahl
`bytesSent`	Die gesendeten Text- und Header-Bytes.	Ganzzahl
`duration`	Gesamtdauer der Anfrage in Millisekunden von der Startzeit bis zum letzten ausgehenden Byte.	Ganzzahl
`requestToTargetDuration`	Gesamtdauer der Anfrage in Millisekunden von der Startzeit bis zum letzten an das Ziel gesendeten Byte.	Ganzzahl
`responseFromTargetDuration`	Gesamtdauer der Anfrage in Millisekunden vom ersten vom Zielhost gelesenen Byte bis zum letzten an den Client gesendeten Byte.	Ganzzahl

Feld	Beschreibung	Format
`grpcResponseCode`	Der gRPC-Antwortcode. Weitere Informationen finden Sie unter Statuscodes und ihre Verwendung in gRPC. Dieses Feld wird nur protokolliert, wenn der Dienst gRPC unterstützt.	Ganzzahl
`callerPrincipal`	Der authentifizierte Prinzipal.	Zeichenfolge
`callerX509SubjectCN`	Der Name des Antragstellers (CN).	Zeichenfolge
`callerX509IssuerOU`	Der Emittent (OU).	Zeichenfolge
`callerX509SANNameCN`	Die Alternative des Emittenten (Name/CN).	Zeichenfolge
`callerX509SANDNS`	Der alternative Name des Antragstellers (DNS).	Zeichenfolge
`callerX509SANURI`	Der alternative Name (URI) des Antragstellers.	Zeichenfolge
`sourceVpcArn`	Der ARN der VPC, von der die Anfrage stammt.	arn:aws:ec2: ::vpc/ *region account id*

Beispiel

Es folgt ein Beispiel für einen Protokolleintrag.

```
{
    "hostHeader": "example.com",
    "sslCipher": "-",
    "serviceNetworkArn": "arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/
svn-1a2b3c4d",
    "resolvedUser": "Unknown",
    "authDeniedReason": "null",
```

```
    "requestMethod": "GET",
    "targetGroupArn": "arn:aws:vpc-lattice:us-west-2:123456789012:targetgroup/
tg-1a2b3c4d",
    "tlsVersion": "-",
    "userAgent": "-",
    "serverNameIndication": "-",
    "destinationVpcId": "vpc-0abcdef1234567890",
    "sourceIpPort": "178.0.181.150:80",
    "targetIpPort": "131.31.44.176:80",
    "serviceArn": "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-1a2b3c4d",
    "sourceVpcId": "vpc-0abcdef1234567890",
    "requestPath": "/billing",
    "startTime": "2023-07-28T20:48:45Z",
    "protocol": "HTTP/1.1",
    "responseCode": 200,
    "bytesReceived": 42,
    "bytesSent": 42,
    "duration": 375,
    "requestToTargetDuration": 1,
    "responseFromTargetDuration": 1,
    "grpcResponseCode": 1
}
```


Inhalt des Ressourcenzugriffsprotokolls

In der folgenden Tabelle werden die Felder eines Protokolleintrags für den Ressourcenzugriff beschrieben.

Feld	Beschreibung	Format
`serviceNetworkArn`	Das Servicenetzwerk ARN.	arn: *partition* vpc-latti ce: ::servicenetwork/ *region account id*
`serviceNetworkReso urceAssociationId`	Die Ressourcen-ID des Dienstnetzwerks.	*snra-xxx*
`vpcEndpointId`	Die Endpunkt-ID, die für den Zugriff auf die Ressource verwendet wurde.	Zeichenfolge

Feld	Beschreibung	Format
`sourceVpcArn`	Der Quell-VPC-ARN oder die VPC, von der aus die Verbindung initiiert wurde.	Zeichenfolge
`resourceConfigurationArn`	Der ARN der Ressourcenkonfiguration, auf die zugegriffen wurde.	Zeichenfolge
`protocol`	Das Protokoll, das für die Kommunikation mit der Ressourcenkonfiguration verwendet wird. Derzeit wird nur TCP unterstützt.	Zeichenfolge
`sourceIpPort`	Die IP-Adresse und der Port der Quelle, die die Verbindung initiiert hat.	*ip*:*port*
`destinationIpPort`	Die IP-Adresse und der Port, über die die Verbindung initiiert wurde. Dies wird die IP von SN-E/SN-A sein.	*ip*:*port*
`gatewayIpPort`	Die IP-Adresse und der Port, die vom Ressourcen-Gateway für den Zugriff auf die Ressource verwendet werden.	*ip*:*port*
`resourceIpPort`	Die IP-Adresse und der Port der Ressource.	*ip*:*port*

Beispiel

Es folgt ein Beispiel für einen Protokolleintrag.

```
{
    "eventTimestamp": "2024-12-02T10:10:10.123Z",
    "serviceNetworkArn": "arn:aws:vpc-lattice:us-west-2:1234567890:servicenetwork/
sn-1a2b3c4d",
    "serviceNetworkResourceAssociationId": "snra-1a2b3c4d",
    "vpcEndpointId": "vpce-01a2b3c4d",
    "sourceVpcArn": "arn:aws:ec2:us-west-2:1234567890:vpc/vpc-01a2b3c4d",
    "resourceConfigurationArn": "arn:aws:vpc-lattice:us-
west-2:0987654321:resourceconfiguration/rcfg-01a2b3c4d",
    "protocol": "tcp",
    "sourceIpPort": "172.31.23.56:44076",
    "destinationIpPort": "172.31.31.226:80",
    "gatewayIpPort": "10.0.28.57:49288",
    "resourceIpPort": "10.0.18.190:80"
}
```

Problembehandlung bei Zugriffsprotokollen

Dieser Abschnitt enthält eine Erläuterung der HTTP-Fehlercodes, die Sie möglicherweise in Zugriffsprotokollen sehen.

Fehlercode	Mögliche Ursachen
HTTP 400: Bad Request (Schlechte Anfrage)	• Der Client hat eine falsch formatierte Anfrage gesendet, die nicht der HTTP-Spezifikation entspricht. • Der Anforderungsheader hat für den gesamten Anforderungsheader oder mehr als 100 Header mehr als 60 KB überschritten. • Der Client hat die Verbindung beendet, bevor er den vollständigen Anfragetext gesendet hat.
HTTP 403: Forbidden (Verboten)	Die Authentifizierung wurde für den Dienst konfiguriert, aber die eingehende Anfrage ist weder authentifiziert noch autorisiert.
HTTP 404: Dienst existiert nicht	Sie versuchen, eine Verbindung zu einem Dienst herzustellen, der nicht existiert oder der nicht im richtigen Dienstnetzwerk registriert ist.

Fehlercode	Mögliche Ursachen
HTTP 500: Internal Server Error (Interner Serverfehler)	Bei VPC Lattice ist ein Fehler aufgetreten, z. B. konnte keine Verbindung zu Zielen hergestellt werden.
HTTP 502: Bad Gateway	Bei VPC Lattice ist ein Fehler aufgetreten.

CloudTrail Protokolle für Amazon VPC Lattice

Amazon VPC Lattice ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem ausgeführten Aktionen bereitstellt. AWS-Service CloudTrail erfasst alle API-Aufrufe für VPC Lattice als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der VPC Lattice-Konsole und Codeaufrufen für die VPC-Lattice-API-Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an VPC Lattice gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wann sie gestellt wurde, und weitere Details ermitteln.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.
- Die Anforderung wurde im Namen eines IAM-Identity-Center-Benutzers erstellt.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS Management Console sind regionsübergreifend. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten AWS-Regionen in Ihrem Konto erfassen. Wenn Sie einen Einzel-Region-Trail erstellen, können Sie nur die Ereignisse anzeigen, die im AWS-Region des Trails protokolliert wurden. Weitere Informationen zu Trails finden Sie unter Erstellen eines Trails für Ihr AWS-Konto und Erstellen eines Trails für eine Organisation im AWS CloudTrail -Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3 – Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail Lake im AWS CloudTrail Benutzerhandbuch.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur Preisgestaltung finden Sie unter CloudTrail AWS CloudTrail Preisgestaltung.

Verwenden Sie Zugriffsprotokolle, um zusätzliche Aktionen zu überwachen. Weitere Informationen finden Sie unter Zugriffsprotokolle.

VPC-Lattice-Management-Ereignisse in CloudTrail

Verwaltungsereignisse enthalten Informationen zu Verwaltungsvorgängen, die für Ressourcen in Ihrem ausgeführt werden. AWS-Konto Sie werden auch als Vorgänge auf Steuerebene bezeichnet. In der Standardeinstellung werden Verwaltungsereignisse CloudTrail protokolliert.

Amazon VPC Lattice protokolliert den Betrieb der VPC Lattice-Kontrollebene als Verwaltungsereignisse. Eine Liste der Vorgänge auf der Amazon VPC Lattice-Kontrollebene, bei denen sich VPC Lattice anmeldet CloudTrail, finden Sie in der Amazon VPC Lattice API-Referenz.

Beispiele für VPC Lattice-Ereignisse

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über den angeforderten API-Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt ein CloudTrail Ereignis für den CreateServiceVorgang.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "accountId": "abcdef01234567890",
    "accessKeyId": "abcdef01234567890",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "abcdef01234567890",
            "arn": "arn:abcdef01234567890",
            "accountId": "abcdef01234567890",
            "userName": "abcdef01234567890"
        },
        "webIdFederationData": {},
        "attributes": {
            "creationDate": "2022-08-16T03:34:54Z",
            "mfaAuthenticated": "false"
        }
    }
  },
```

```
  "eventTime": "2022-08-16T03:36:12Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "CreateService",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "abcdef01234567890",
  "userAgent": "abcdef01234567890",
  "requestParameters": {
    "name": "rates-service"
  },
  "responseElements": {
    "name": "rates-service",
    "id": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "status": "CREATE_IN_PROGRESS"
  },
  "requestID": "abcdef01234567890",
  "eventID": "abcdef01234567890",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "abcdef01234567890",
  "eventCategory": "Management"
}
```


Das folgende Beispiel zeigt ein CloudTrail Ereignis für den DeleteServiceVorgang.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "abcdef01234567890",
    "arn": "arn:ABCXYZ123456",
    "accountId": "abcdef01234567890",
    "accessKeyId": "abcdef01234567890",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "abcdef01234567890",
            "arn": "arn:aws:iam::AIDACKCEVSQ6C2EXAMPLE:role/Admin",
            "accountId": "abcdef01234567890",
            "userName": "Admin"
        },
        "webIdFederationData": {},
```

```
        "attributes": {
            "creationDate": "2022-10-27T17:42:36Z",
            "mfaAuthenticated": "false"
        }
    }
  },
  "eventTime": "2022-10-27T17:56:41Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "DeleteService",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "72.21.198.64",
  "userAgent": "abcdef01234567890",
  "requestParameters": {
    "serviceIdentifier": "abcdef01234567890"
  },
  "responseElements": {
    "name": "test",
    "id": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "status": "DELETE_IN_PROGRESS"
  },
  "requestID": "abcdef01234567890",
  "eventID": "abcdef01234567890",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "abcdef01234567890",
  "eventCategory": "Management"
}
```


Informationen zu CloudTrail Datensatzinhalten finden Sie im AWS CloudTrail Benutzerhandbuch unter CloudTrailDatensatzinhalt.

Kontingente für Amazon VPC Lattice

Ihr AWS-Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jedes Kontingent. AWS-Service Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Für einige Kontingente können Sie Erhöhungen beantragen, während andere Kontingente nicht erhöht werden können.

Um die Kontingente für VPC Lattice anzuzeigen, öffnen Sie die Konsole Service Quotas. Wählen AWS-Servicesund wählen Sie im Navigationsbereich VPC Lattice aus.

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

Ihr AWS-Konto hat die folgenden Kontingente in Bezug auf VPC Lattice.

Name	Standard	Anpas	Beschreibung
Größe der Authentifizierungsrichtlinie	Jede unterstützte Region: 10 Kilobyte	Nein	Die maximale Größe einer JSON-Datei in einer Auth-Richtlinie.
Konfigurationen untergeordneter Ressourcen pro Gruppenressourcenkonfiguration	Jede unterstützte Region: 40	Ja	Die maximale Anzahl von Konfigurationen untergeordneter Ressourcen in einer Gruppenressourcenkonfiguration. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den AWS Support.
Zuhörer pro Dienst	Jede unterstützte Region: 2	Ja	Die maximale Anzahl von Listenern, die Sie für einen Dienst erstellen können. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den AWS Support.

Name	Standard	Anpas	Beschreibung
Ressourcenkonfigurationen pro Servicenetzwerk	Jede unterstützte Region: 100	Yes (Ja)	Die maximale Anzahl von Ressourcenkonfigurationen, die einem Servicenetzwerk zugeordnet sind. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den AWS Support.
Ressourcenkonfigurationen pro AWS Region	Jede unterstützte Region: 500	Ja	Die maximale Anzahl von Ressourcenkonfigurationen, die ein AWS Konto pro AWS Region haben kann. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den AWS Support.
Ressourcen-Gateways pro VPC	Jede unterstützte Region: 100	Yes (Ja)	Die maximale Anzahl von Ressourcen-Gateways in einer VPC. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den AWS Support.
Regeln pro Zuhörer	Jede unterstützte Region: 5	Yes (Ja)	Die maximale Anzahl von Regeln, die Sie für Ihren Service-Listener definieren können. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den AWS Support.

Name	Standard	Anpas	Beschreibung
Sicherheitsgruppen pro Verband	Jede unterstützte Region: 5	Nein	Die maximale Anzahl von Sicherheitsgruppen, die Sie zu einer Zuordnung zwischen einer VPC und einem Dienstnetzwerk hinzufügen können.
Dienstzuordnungen pro Dienstnetzwerk	Jede unterstützte Region: 500	Ja	Die maximale Anzahl von Diensten, die Sie einem einzelnen Dienstnetzwerk zuordnen können. Für zusätzliche Kapazität s- und Limiterhöhungen wenden Sie sich an den AWS Support.
Servicenetzwerke pro Region	Jede unterstützte Region: 10	Yes (Ja)	Die maximale Anzahl von Servicenetzwerken pro Region. Für zusätzliche Kapazitäts- und Limiterhö hungen wenden Sie sich an den AWS Support.
Dienstleistungen pro Region	Jede unterstützte Region: 500	Ja	Die maximale Anzahl von Diensten pro Region. Für zusätzliche Kapazität s- und Limiterhöhungen wenden Sie sich an den AWS Support.

Name	Standard	Anpas	Beschreibung
Zielgruppen pro Region	Jede unterstützte Region: 500	Ja	Die maximale Anzahl von Zielgruppen pro Region. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den AWS Support.
Zielgruppen pro Service	Jede unterstützte Region: 5	Yes (Ja)	Die maximale Anzahl von Zielgruppen, die Sie einem Service zuordnen können. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den AWS Support.
Ziele pro Zielgruppe	Jede unterstützte Region: 1 000	Ja	Die maximale Anzahl von Zielen, die Sie einer einzelnen Zielgruppe zuordnen können. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den AWS Support.
VPC-Zuordnungen pro Servicenetzwerk	Jede unterstützte Region: 500	Ja	Die maximale Anzahl davon VPCs , die Sie einem einzelnen Dienstnetzwerk zuordnen können. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den AWS Support.

Name	Standard	Anpas	Beschreibung
VPC-Endpunkte vom Typ Servicenetzwerk pro Servicenetzwerk	Jede unterstützte Region: 50	Ja	Die maximale Anzahl von Dienstnetzwerkendpunkten, die einem Dienstnetzwerk zugeordnet sind. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den AWS Support.

Die folgenden Availability Zones werden für VPC Lattice nicht unterstützt:`use1-az3`,`usw1-az2`,`apne1-az3`,`apne2-az2`,, `euc1-az2euw1-az4`,`cac1-az3`. `ilc1-az2`

Die folgenden Beschränkungen gelten ebenfalls.

Limit	Wert	Beschreibung
Bandbreite pro Dienst pro Availability Zone	10 Gbit/s	Die maximale Bandbreite, die pro Dienst pro Availability Zone zugewiesen wird.
Bandbreite pro Ressourcen-Gateway pro Availability Zone	100 Gbit/s	Die maximale Bandbreite, die pro Ressourcen-Gateway pro Availability Zone zugewiesen wird.
Maximale Übertragungseinheit (MTU) pro Verbindung	8500 Byte	Die Größe des größten Datenpakets, das ein Dienst akzeptieren kann.
Anfragen pro Sekunde pro Dienst pro Availability Zone	10.000	Für HTTP-Dienste ist dies die maximale Anzahl von Anfragen pro Sekunde pro Dienst pro Availability Zone.
Leerlaufzeit der Verbindung pro Verbindung	1 Minute	Die maximale Zeit, die eine Verbindung ohne aktive Anfragen (für HTTP und GRPC) oder ohne aktive

Limit	Wert	Beschreibung
		Datenübertragung (für TLS-PASSTHROUGH) inaktiv sein kann.
Maximale Verbindungslebensdauer pro Verbindung	10 Minuten	Die maximale Zeit, während der eine Verbindung geöffnet sein kann.
Servicenetzwerk pro VPC	1 Servicenetzwerk	Sie können eine VPC über eine Zuordnung nur mit einem Servicenetzwerk verbinden. Um eine VPC mit mehreren Servicenetzwerken zu verbinden, können Sie VPC-Endpunkte vom Typ Dienstnetzwerk verwenden.

Dokumentenverlauf für das Amazon VPC Lattice-Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für VPC Lattice beschrieben.

Änderung	Beschreibung	Datum
VPC Lattice hinzugefügt für Oracle Database@AWS	VPC Lattice für Oracle Database@AWS veröffentlicht.	26. Juni 2025
Dual-Stack-Unterstützung für Management-Endpunkte hinzugefügt	VPC Lattice unterstützt jetzt Dual-Stack IPv4 - (und IPv6) Endpoints für das gesamte VPC-Lattice-Management. APIs	30. April 2025
Ressourcen teilen und darauf zugreifen	VPC Lattice unterstützt jetzt die gemeinsame Nutzung und den Zugriff auf Ressourcen über VPC- und Kontogrenzen hinweg. Dies beinhaltet Aktualisierungen der VPCLatticeReadOnlyAccessRichtlinien und. VPCLatticeFullAccess	01. Dezember 2024
TLS-Passthrough	VPC Lattice unterstützt jetzt TLS-Passthrough, sodass Sie die TLS-Terminierung in Ihrer Anwendung zur Authentifizierung durchführen können. end-to-end	14. Mai 2024

Version der Lambda-Ereignisstruktur	VPC Lattice unterstützt jetzt eine neue Version der Lambda-Ereignisstruktur.	07. September 2023
Support für Shared VPCs	Die Teilnehmer können VPC Lattice-Zielgruppen in einer gemeinsam genutzten VPC erstellen.	5. Juli 2023
Version für allgemeine Verfügbarkeit	Die Veröffentlichung des VPC Lattice User Guide for General Availability (GA)	31. März 2023
VPC Lattice meldet jetzt Änderungen an seinen verwalteten Richtlinien AWS	Änderungen an verwalteten Richtlinien werden unter „AWS Verwaltete Richtlinien für VPC Lattice“ im Kapitel „Sicherheit“ beschrieben.	29. März 2023
Support für den Application Load Balancer Balancer-Zieltyp	VPC Lattice unterstützt jetzt die Erstellung einer Zielgruppe vom Typ Application Load Balancer.	29. März 2023
Support für alle Instance-Typen	VPC Lattice unterstützt jetzt alle Instance-Typen.	27. März 2023
IPv6 Unterstützung	VPC Lattice unterstützt jetzt IPv4 sowohl IPv6 IP-Zielgruppen.	27. März 2023
HTTP2 Protokollversion für Zustandsprüfungen	Integritätsprüfungen werden jetzt unterstützt, wenn die Zielgruppenprotokollversion aktiviert ist HTTP2.	27. März 2023

Die Antwortaktion für Listener-Regeln wurde behoben	Listener für VPC Lattice-Dienste unterstützen jetzt zusätzlich zu Forward-Aktionen auch feste Antwortaktionen.	27. März 2023
Support für benutzerdefinierte Domainnamen	Sie können jetzt einen benutzerdefinierten Domainnamen für Ihren VPC Lattice-Dienst konfigurieren	14. Februar 2023
Support für BYOC (Bring Your Own Certificate)	VPC Lattice unterstützt die Verwendung Ihres eigenen SSL/TLS Zertifikats in ACM für benutzerdefinierte Domainnamen.	14. Februar 2023
VPC Lattice meldet jetzt eine aktualisierte Liste der nicht unterstützten Instance-Typen	Drei weitere Instanzen wurden zur Liste der nicht unterstützten Instanzen hinzugefügt.	26. Januar 2023
VPC Lattice meldet jetzt Änderungen an seinen verwalteten Richtlinien AWS	Ab dem 5. Dezember 2022 werden Änderungen an verwalteten Richtlinien im Thema „AWS Verwaltete Richtlinien für VPC Lattice“ im Kapitel „Sicherheit“ beschrieben. Die erste aufgeführte Änderung ist das Hinzufügen von Berechtigungen, die für CloudWatch die Überwachung erforderlich sind.	5. Dezember 2022
Erstversion	Erste Version des VPC Lattice User Guide	5. Dezember 2022

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.