



Benutzerhandbuch

Amazon VPC Lattice



Amazon VPC Lattice: Benutzerhandbuch

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist Amazon VPC Lattice?	1
Zentrale Komponenten	1
Rollen und Zuständigkeiten	3
Features	4
So funktioniert VPC Lattice	5
Zugreifen auf VPC Lattice	9
Preisgestaltung	9
Servicenetze	10
Erstellen Sie ein Servicenetzwerk	11
Verknüpfungen verwalten	13
Dienstzuordnungen verwalten	13
VPC-Zuordnungen verwalten	14
Zugriffseinstellungen bearbeiten	15
Bearbeiten Sie die Überwachungsdetails	17
Verwalten von Tags	18
Löschen Sie ein Servicenetzwerk	19
Services	20
Schritt 1: Erstellen Sie einen VPC Lattice-Dienst	21
Schritt 2: Routing definieren	23
Schritt 3: Netzwerkzuordnungen erstellen	24
Schritt 4: Überprüfen und Erstellen	24
Zuordnungen verwalten	24
Zugriffseinstellungen bearbeiten	25
Bearbeiten Sie die Überwachungsdetails	27
Verwalten von Tags	28
Konfigurieren Sie einen benutzerdefinierten Domainnamen	29
Ordnen Sie Ihrem Dienst einen benutzerdefinierten Domainnamen zu	31
BYOC	34
Den privaten Schlüssel Ihres Zertifikats sichern	35
Einen Service löschen	36
Zielgruppen	37
Erstellen einer Zielgruppe	38
Erstellen einer Zielgruppe	38
Gemeinsam genutzte Subnetze	40

Ziele registrieren	41
Instanz-IDs	42
IP-Adressen	43
Lambda-Funktionen	43
Application Load Balancer	44
Konfigurieren von Zustandsprüfungen	44
Zustandsprüfungseinstellungen	45
Zustand der Ziele prüfen	47
Ändern Sie die Einstellungen für die Zustandsprüfung	48
Weiterleitungskonfiguration	48
Weiterleitungsalgorithmus	49
Zieltyp	50
IP-Adresstyp	51
HTTP-Ziele	51
x-forwardedHeader	52
Header zur Anruferidentität	52
Lambda-Funktionen als Ziele	53
Vorbereiten der Lambda-Funktion	53
Erstellen Sie einer Zielgruppe für die Lambda-Funktion	43
Empfangen von Ereignissen vom VPC Lattice-Dienst	55
Antworten Sie auf den VPC Lattice-Dienst	58
Header mit mehreren Werten	59
Aufheben der Registrierung der Lambda-Funktion	60
Application Load Balancers als Ziele	60
Voraussetzungen	61
Schritt 1: Erstellen Sie eine Zielgruppe vom Typ ALB	62
Schritt 2: Registrieren Sie den Application Load Balancer als Ziel	62
Protokollversion	63
Aktualisieren der Tags	64
Löschen einer Zielgruppe	65
Listener	67
Listener-Konfiguration	67
Erstellen eines Listeners	68
HTTP-Listener	68
Voraussetzungen	69
Hinzufügen eines HTTP-Listeners	69

HTTPS-Listener	70
Sicherheitsrichtlinie	71
ALPN-Richtlinie	72
Hinzufügen eines HTTPS-Listeners	72
TLS-Listener	74
Überlegungen	74
Fügen Sie einen TLS-Listener hinzu	75
Listener-Regeln	76
Standardregeln	76
Priorität der Regel	77
Regelaktion	77
Regelbedingungen	78
Hinzufügen einer Regel	78
Aktualisieren Sie eine Regel	79
Löschen einer Regel	80
Aktualisieren eines Listeners	80
Löschen eines Listeners	81
VPC Lattice-Ressourcen teilen	82
Voraussetzungen	82
Ressourcen teilen	83
Beenden Sie das Teilen von Ressourcen	84
Zuständigkeiten und Genehmigungen	85
Besitzer von Ressourcen	85
Nutzer von Ressourcen	85
Kontoübergreifende Ereignisse	86
Sicherheit	89
Zugriff auf Dienste verwalten	90
Authentifizierungsrichtlinien	90
Sicherheitsgruppen	106
Netzwerk-ACLs	111
Authentifizierte Anfragen	113
Datenschutz	121
Verschlüsselung während der Übertragung	122
Verschlüsselung im Ruhezustand	122
Identity and Access Management	129
So funktioniert Amazon VPC Lattice mit IAM	129

API-Berechtigungen	136
Identitätsbasierte Richtlinien	138
Verwenden von serviceverknüpften Rollen	144
AWS verwaltete Richtlinien	146
Compliance-Validierung	149
AWS PrivateLink	151
Überlegungen zu VPC-Endpunkten mit Schnittstellen	151
Erstellen eines VPC-Schnittstellen-Endpunkts für VPC Lattice	151
Ausfallsicherheit	152
Sicherheit der Infrastruktur	152
Überwachung	154
CloudWatch Metriken	154
CloudWatch Amazon-Metriken anzeigen	154
Kennzahlen für Zielgruppen	155
Servicemetriken	168
Zugriffsprotokolle	171
Für die Aktivierung von Zugriffsprotokollen sind IAM-Berechtigungen erforderlich	172
Ziele der Zugriffsprotokolle	173
Aktivieren der Zugriffsprotokolle	174
Inhalt des Zugriffsprotokolls	175
Beheben Sie Probleme mit Zugriffsprotokollen	179
CloudTrail Logs	180
Die Einträge in der VPC Lattice-Protokolldatei verstehen	180
Kontingente	184
Dokumentverlauf	188
.....	cxc

Was ist Amazon VPC Lattice?

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

Moderne Anwendungen können aus mehreren kleinen und modularen Diensten bestehen, die oft als Microservices bezeichnet werden. Die Modernisierung hat zwar ihre Vorteile, kann aber auch zu Netzwerkkomplexitäten und Herausforderungen führen, wenn Sie diese Microservices verbinden. Wenn die Entwickler beispielsweise auf verschiedene Teams verteilt sind, können sie Microservices für mehrere Konten oder VPCs entwickeln und bereitstellen.

In VPC Lattice bezeichnen wir einen Microservice als Service. Dies ist der Wortlaut, den Sie in der VPC Lattice-Dokumentation finden.

Inhalt

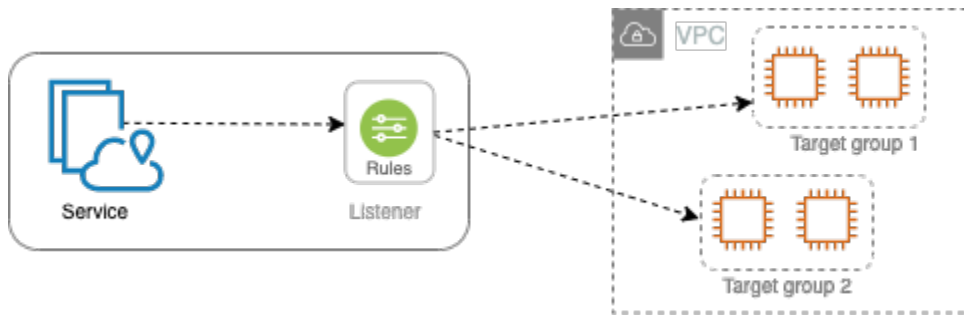
- [Zentrale Komponenten](#)
- [Rollen und Zuständigkeiten](#)
- [Features](#)
- [So funktioniert VPC Lattice](#)
- [Zugreifen auf VPC Lattice](#)
- [Preisgestaltung](#)

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-Instances oder ECS-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. [Ziele können EC2-Instances, IP-Adressen, Lambda-Funktionen, Application Load Balancer oder Kubernetes-Pods sein.](#) Diese ähneln den Zielgruppen, die Elastic Load Balancing bietet, sind jedoch nicht austauschbar.

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.

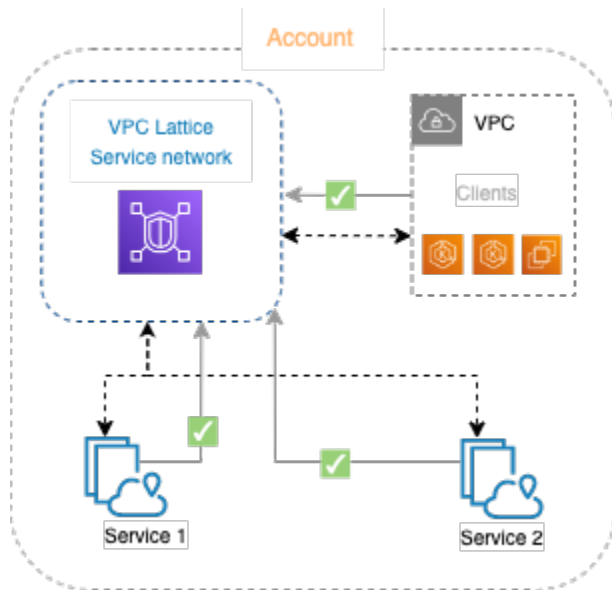
Regel

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.

Servicenetzwerk

Eine logische Grenze für eine Sammlung von Diensten. Ein Client ist jede Ressource, die in einer VPC bereitgestellt wird und dem Servicenetzwerk zugeordnet ist. Clients und Dienste, die demselben Servicenetzwerk zugeordnet sind, können miteinander kommunizieren, wenn 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 die Sie über AWS Resource Access Manager (AWS RAM) mit Ihrem Konto teilen.

Richtlinien für die Authentifizierung

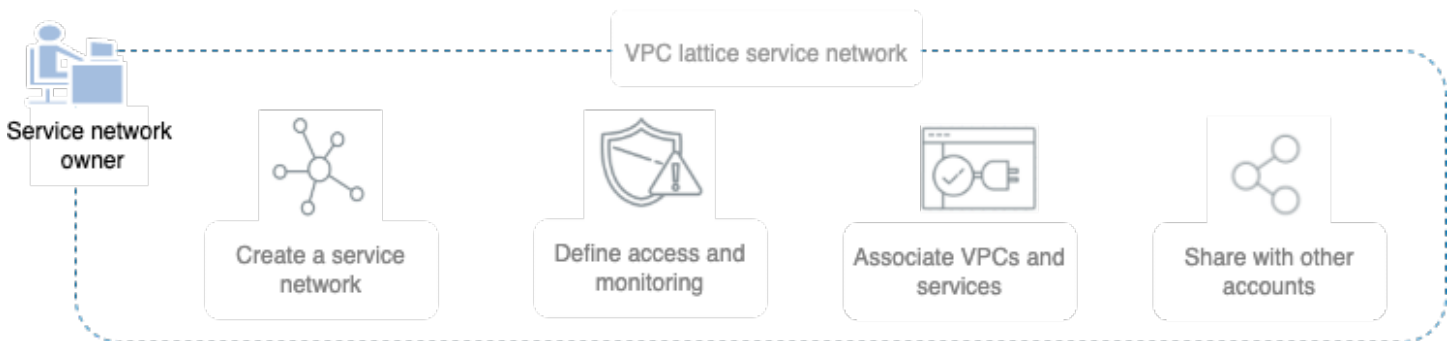
Detaillierte Autorisierungsrichtlinien, mit denen der Zugriff auf Dienste definiert werden kann. Sie können einzelnen Diensten oder dem Servicenetzwerk separate Authentifizierungsrichtlinien zuordnen. Sie können beispielsweise eine Richtlinie dafür erstellen, wie ein Zahlungsdienst, der auf einer Auto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

Rollen und Zuständigkeiten

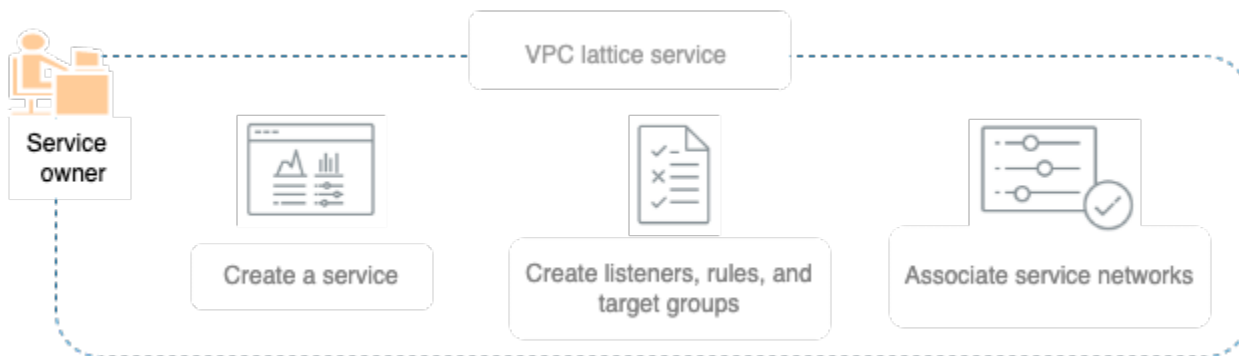
Eine Rolle bestimmt, wer für die Einrichtung und den Informationsfluss innerhalb von Amazon VPC Lattice verantwortlich ist. In der Regel gibt es zwei Rollen, den Eigentümer des Servicenetzwerks und den Eigentümer des Dienstes, und ihre Zuständigkeiten können sich überschneiden.

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 Dienste mithilfe von Authentifizierungs- und Autorisierungsrichtlinien zu verwalten. Der Besitzer des Dienstnetzwerks kann dem Dienstnetzwerk auch einen Dienst zuordnen, wenn der Dienst mit dem Konto des Dienstnetzwerkbesitzers 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.



Features

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

Serviceerkennung

Alle Clients und Dienste in VPCs, die dem Servicenetzwerk zugeordnet sind, können mit anderen Diensten innerhalb desselben Dienstnetzwerks 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

Die Client-to-service C-Konnektivität wird mithilfe der VPC Lattice-Datenebene innerhalb der AWS Netzwerkinfrastruktur hergestellt. Wenn Sie eine VPC mit dem Servicenetzwerk verknüpfen, kann sich jeder Client innerhalb der VPC mit Diensten im Servicenetzwerk verbinden, sofern er über den erforderlichen Zugriff verfügt.

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 veröffentlicht VPC Lattice Metriken im Dienstbesitzerkonto und bietet Ihnen die Möglichkeit, die Protokollierung zu aktivieren. Wenn die Clients auch demselben Dienstnetzwerk zugeordnet sind, erhält der Eigentümer des Dienstnetzwerks Protokolle für alle Dienste, die dem Dienstnetzwerk zugeordnet sind. Der Dienstbesitzer erhält Protokolle für alle Clients, die Anfragen an seinen Dienst stellen.

VPC Lattice arbeitet mit den folgenden Tools, um Sie bei der Überwachung und Fehlerbehebung Ihrer Dienste zu unterstützen: CloudWatch Protokollgruppen, Firehose-Lieferdatenströme und S3-Buckets.

Sicherheit

VPC Lattice bietet ein Framework, mit dem Sie eine Verteidigungsstrategie auf mehreren Ebenen des Netzwerks implementieren können. Die erste Ebene ist die Service- und VPC-Assoziation. Ohne eine VPC und eine Dienstverbindung können Kunden nicht auf den Service 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.

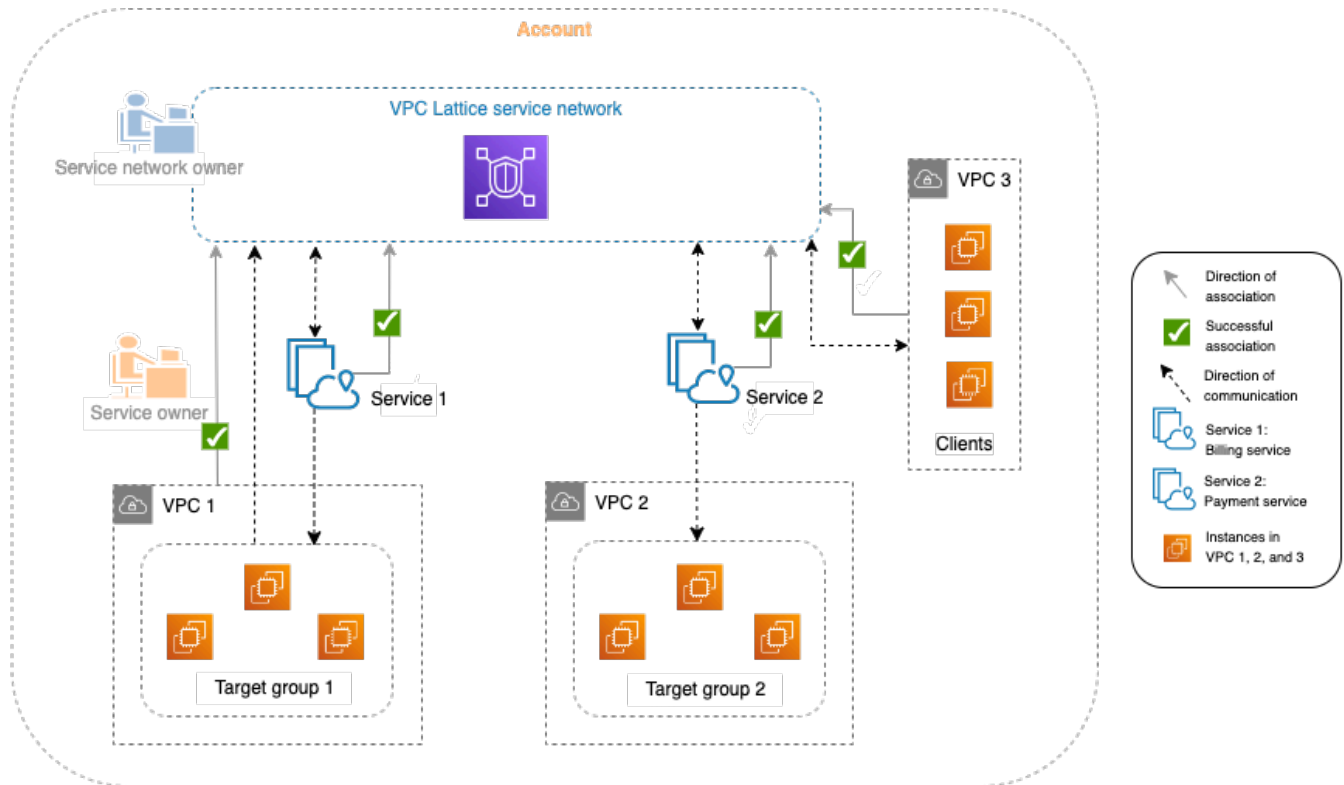
So funktioniert VPC Lattice

VPC Lattice wurde entwickelt, um Ihnen dabei zu helfen, alle darin enthaltenen Dienste 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:

- Dienste, die dem Dienstnetzwerk zugeordnet sind, können Anfragen von Clients empfangen, deren VPCs ebenfalls dem Dienstnetzwerk zugeordnet sind.
- Ein Client kann Anfragen an Dienste senden, die einem Servicenetzwerk zugeordnet sind, nur wenn er sich in einer VPC befindet, die demselben Servicenetzwerk zugeordnet ist. Client-Datenverkehr, der eine VPC-Peering-Verbindung oder ein Transit-Gateway durchquert, wird verweigert.
- Ein Client kann keine Anfragen an Clients in anderen VPCs senden, die dem Servicenetzwerk zugeordnet sind.
- Ziele von Diensten in VPCs, die dem Dienstnetzwerk zugeordnet sind, sind ebenfalls Clients und können Anfragen an andere Dienste senden, die dem Dienstnetzwerk zugeordnet sind.
- Ziele von Diensten in VPCs, die nicht mit dem Servicenetzwerk verknüpft sind, sind keine Clients und können keine Anfragen an andere Dienste 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 drei VPCs wurden unter demselben Konto wie das Dienstnetzwerk 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 Instanzen läuft, die bei Zielgruppe 2 in VPC 2 registriert sind. VPC 3 befindet sich im selben Konto und hat Kunden, aber keine Dienste.

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 Zielressourcen angeben, auf denen die Dienste ausgeführt werden, z. B. Instanzen. Sie geben auch die VPCs an, in denen sich diese Ziele befinden.

Im obigen Diagramm stellen die gepunkteten Pfeile, die auf die Zielgruppen der Dienste zeigen, den Verkehr dar, der von jedem Dienst zur jeweiligen Zielgruppe fließt. Die gepunkteten Pfeile stellen die Kommunikationsrichtung zwischen dem Dienst und der Zielgruppe dar.

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 Dienstnetzwerk zuordnen, wird dieser Dienst für andere Dienste und Clients in den VPCs, die dem Dienstnetzwerk zugeordnet sind, auffindbar.

Die bidirektionalen gepunkteten Pfeile zwischen dem Dienst und dem Dienstnetzwerk stellen die bidirektionale Kommunikation dar, die sich aus der Zuordnung ergibt. Die gepunkteten Pfeile vom Servicenetzwerk zu den Diensten stehen für Dienste, die Anfragen von Clients empfangen. Die gepunkteten Pfeile in der entgegengesetzten Richtung, d. h. von den Diensten zum Dienstnetzwerk, stehen für Dienste, die auf Kundenanfragen über das Dienstnetzwerk antworten.

5. Ordnen Sie VPCs dem Servicenetzwerk zu

Der Besitzer des Servicenetzes ordnet VPC 1 und VPC 3 dem Servicenetzwerk zu. Den Zuordnungen werden Pfeile mit Häkchen angezeigt, die auf das Servicenetzwerk zeigen. Mit diesen Zuordnungen werden die Ziele in diesen VPCs zu Clients und können Anfragen an die zugehörigen Dienste stellen. Der bidirektionale gepunktete Pfeil zwischen VPC 3 und dem Servicenetzwerk steht für eine bidirektionale Kommunikation zwischen den Clients (z. B. Instanzen) in VPC 3 und dem Servicenetzwerk als Ergebnis der Zuordnung. In ähnlicher Weise steht der gepunktete Pfeil, der von Zielgruppe 1 zum Servicenetzwerk zeigt, für Clients, die Anfragen an andere Dienste stellen, die mit dem Servicenetzwerk verbunden sind.

Beachten Sie, dass VPC 2 weder einen Pfeil noch ein Häkchen hat, die für eine Zuordnung stehen. 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.

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 den APIs finden Sie unter [Amazon VPC Lattice API Reference](#).
- **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](#).

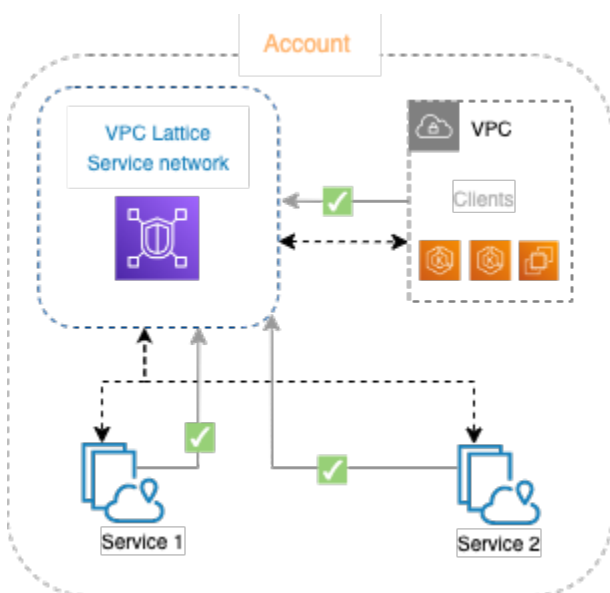
Preisgestaltung

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. Weitere Informationen finden Sie unter [Amazon VPC Lattice Pricing](#).

Servicenetze in VPC Lattice

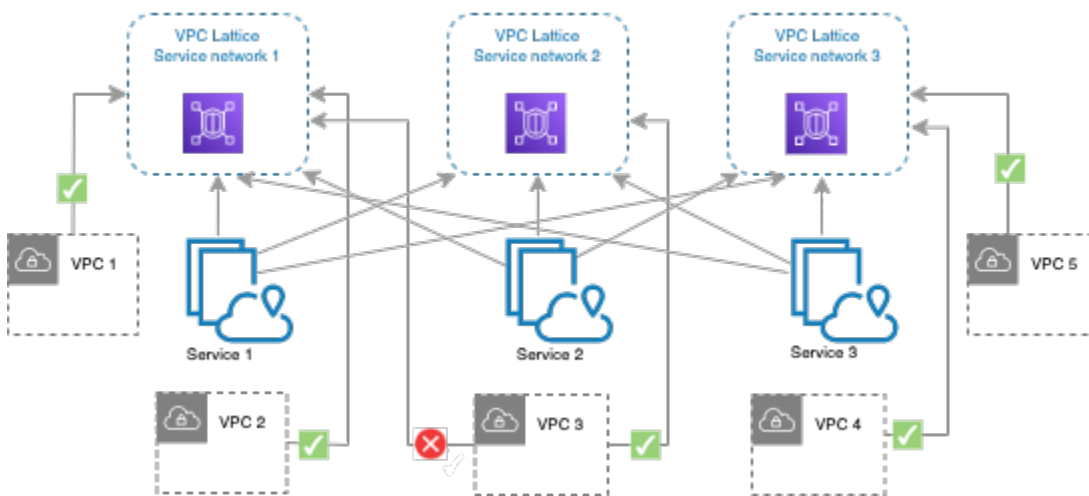
Ein Servicenetzwerk ist eine logische Grenze für eine Sammlung von Diensten. Mit dem Netzwerk verbundene Dienste können im Hinblick auf Erkennung, Konnektivität, Zugänglichkeit und Beobachtbarkeit autorisiert werden. Um Anfragen an Dienste im Netzwerk stellen zu können, muss sich Ihr Service oder Client in einer VPC befinden, die mit dem Dienstnetzwerk verknüpft ist.

Das folgende Diagramm zeigt die wichtigsten Komponenten eines typischen Servicenetzes 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 einen oder mehrere Dienste mehreren Servicenetzen zuordnen. Sie können auch mehrere VPCs einem Dienstnetzwerk zuordnen. Jede VPC kann jedoch nur einem Servicenetzwerk zugeordnet werden.

In der folgenden Abbildung stellen die Pfeile die Zuordnungen zwischen Diensten und Dienstnetzwerken sowie die Verknüpfungen zwischen den VPCs und Dienstnetzwerken dar. Sie können sehen, dass mehrere Dienste mehreren Dienstnetzwerken zugeordnet sind und dass jedem Dienstnetzwerk mehrere VPCs zugeordnet sind. Das rote X im Diagramm zeigt jedoch, dass jede VPC nicht mehr als eine Zuordnung zu einem Servicenetzwerk haben kann.



Weitere Informationen finden Sie unter [Kontingente für Amazon VPC Lattice](#).

Erstellen Sie ein Servicenetzwerk

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 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.

Informationen zum Zuordnen von VPCs, nachdem Sie das Dienstnetzwerk erstellt haben, finden Sie alternativ unter [the section called "VPC-Zuordnungen verwalten"](#).

7. Für den Netzwerkzugriff können Sie den Standardauthentifizierungstyp None beibehalten, wenn Sie möchten, dass die Clients in den zugehörigen 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 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).
8. (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.
9. (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.
10. 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. Mit diesem Befehl wird nur das grundlegende Servicenetzwerk erstellt. 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-Servicenetzwerk

Wenn Sie einen Service mit dem Service-Netzwerk verknüpfen, ermöglicht es Clients (Ressourcen in einer VPC, die dem Service-Netzwerk zugeordnet ist), Anfragen an den Service zu stellen. Wenn Sie eine VPC dem Servicenetzwerk zuordnen, können alle Ziele innerhalb dieser VPC Clients sein und mit anderen Diensten im Servicenetzwerk kommunizieren.

Inhalt

- [Dienstzuordnungen verwalten](#)
- [VPC-Zuordnungen verwalten](#)

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 [So funktioniert 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 die zugehörige 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 Dienstzuordnung mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl [create-service-network-service-association](#).

Um eine Dienstverknüpfung mit dem AWS CLI

Verwenden Sie den Befehl [delete-service-network-service-association](#).

VPC-Zuordnungen verwalten

Clients können Anfragen an Dienste senden, die dem Servicenetzwerk zugeordnet sind, nur wenn sie sich in VPCs befinden, die dem Dienstnetzwerk zugeordnet sind. Client-Datenverkehr, der eine VPC-Peering-Verbindung oder ein Transit-Gateway durchquert, wird verweigert.

Das Zuordnen einer VPC ist ein optionaler Schritt, wenn Sie ein Servicenetzwerk erstellen. Das Servicenetzwerk ist jedoch erst dann voll funktionsfähig, wenn Sie eine VPC zuordnen. Netzwerkbesitzer können VPCs einem Servicenetzwerk zuordnen, wenn ihr Konto über den erforderlichen Zugriff verfügt. Weitere Informationen finden Sie unter [So funktioniert VPC Lattice](#).

Wenn Sie eine VPC-Zuordnung löschen, können Clients in den VPCs 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 die zugehörige Detailseite zu öffnen.
4. Wählen Sie die Registerkarte VPC-Zuordnungen.
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-Zuordnung zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl [update-service-network-vpc-association](#).

Um eine VPC-Assoziation mit dem AWS CLI

Verwenden Sie den Befehl [delete-service-network-vpc-association](#).

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.

Sie können Authentifizierungsrichtlinien auf Dienstnetzwerkebene, Serviceebene oder auf beiden Ebenen anwenden. In der Regel werden Authentifizierungsrichtlinien von den Netzwerkbesitzern oder Cloud-Administratoren angewendet. Sie können eine kursspezifische 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 die zugehörige 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 in den zugehörigen VPCs auf die Dienste in diesem Dienstnetzwerk zugreifen, wählen Sie None als Authentifizierungstyp aus.
7. Um eine Ressourcenrichtlinie auf das Dienstnetzwerk 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 die zugehörige 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. Beispielsweise:
 - 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 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 die zugehörige 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 Servicenetzwerk

Bevor Sie ein Dienstnetzwerk löschen können, müssen Sie zunächst alle Verknüpfungen löschen, die das Dienstnetzwerk möglicherweise mit einem Dienst oder einer VPC 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 Zugriffsprotokolle.

Um ein Servicenetzwerk mithilfe der Konsole zu löschen

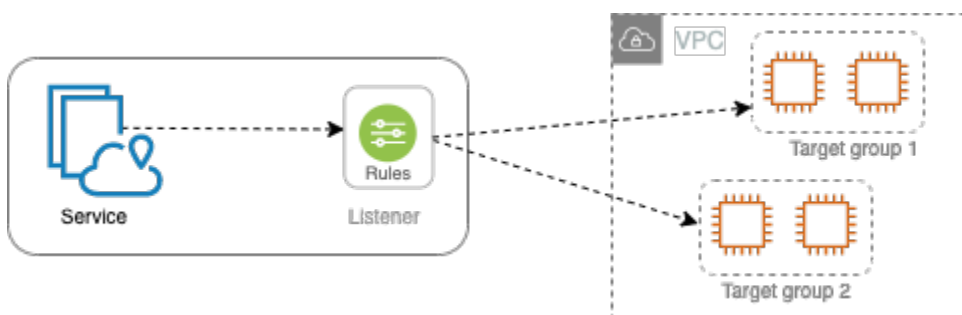
1. Öffnen Sie die Amazon VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich unter VPC Lattice die Option Service networks aus.
3. Aktivieren Sie das Kontrollkästchen für das Dienstnetzwerk und wählen Sie dann Aktionen, Dienstnetzwerk löschen aus.
4. Wenn Sie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

Um ein Servicenetzwerk zu löschen, verwenden Sie 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. [Ziele können EC2-Instances, IP-Adressen, serverlose Lambda-Funktionen, Application Load Balancer oder Kubernetes-Pods sein.](#) Weitere Informationen finden Sie unter [Zielgruppen in VPC Lattice](#). Sie können einen Dienst 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](#)
- [Einen Service löschen](#)

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 den VPCs, die dem Dienstnetzwerk zugeordnet sind, auf Ihren Service zugreifen. Um eine [Authentifizierungsrichtlinie](#) zur Steuerung des Zugriffs auf den Service 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 Domännennamen 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 zu erstellen, verwenden Sie 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 der Dienstnetzwerkebene, der 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 in VPCs im zugehörigen Dienstnetzwerk auf Ihren Service zugreifen, wählen Sie None als Authentifizierungstyp aus.
7. Um eine Ressourcenrichtlinie zur Steuerung des Zugriffs auf den Service 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 authentifizierte 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 authentifizierte 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. Beispielsweise:
 - 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 einfachere und intuitivere URLs, die Sie Ihren Benutzern zur Verfügung stellen können. 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. Dies geschieht jedoch nur, wenn Sie Ihren benutzerdefinierten Domainnamen dem von VPC Lattice generierten Domainnamen mit einem CNAME-Eintrag zuordnen, um Anfragen an Ihren Service weiterzuleiten. Weitere Informationen finden Sie unter [Ordnen Sie Ihrem Dienst einen benutzerdefinierten Domainnamen zu](#).

Voraussetzungen

- Sie müssen über einen registrierten Domainnamen für Ihren Service verfügen. 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 Domännennamen erstellt werden kann, der bereits (für einen anderen Dienst) im selben Dienstnetzwerk existiert.

Um einen benutzerdefinierten Domainnamen für Ihren Dienst zu konfigurieren, verwenden Sie AWS Management Console

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 SSL/TLS-Zertifikat aus, das Ihrem benutzerdefinierten 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.

Um einen benutzerdefinierten Domainnamen für Ihren Service zu konfigurieren, verwenden Sie AWS CLI

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.

Wenn Sie kein eigenes SSL-/TLS-Zertifikat in AWS Certificate Manager (ACM) haben, können Sie eines erstellen oder importieren, bevor Sie einen benutzerdefinierten Domainnamen einrichten. Das Zertifikat ist jedoch nur erforderlich, wenn Sie HTTPS-Anfragen mit Ihrem benutzerdefinierten Domainnamen bearbeiten möchten. Weitere Informationen finden Sie unter [Bringen Sie Ihr eigenes Zertifikat \(BYOC\) für VPC Lattice mit](#).

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 CNAME-Eintrag 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, müssen Sie zunächst eine gehostete Zone erstellen, die Informationen zur Weiterleitung des Datenverkehrs im Internet für Ihre Domain enthält. Nachdem Sie die private oder öffentlich gehostete Zone erstellt haben, erstellen Sie einen CNAME-Eintrag, sodass Ihr benutzerdefinierter Domainname beispielsweise dem automatisch generierten Domainnamen von VPC Lattice zugeordnet wird `parking.example.com`, 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. Weitere Informationen finden Sie unter [Erstellen von Datensätzen mithilfe der Amazon Route 53 53-Konsole](#) im Amazon Route 53-Entwicklerhandbuch. Darüber hinaus können Sie anhand der folgenden Schritte eine gehostete Zone und einen CNAME-Eintrag erstellen, um Ihren benutzerdefinierten Domainnamen dem VPC-Lattice-Endpunkt zuzuordnen.

So erstellen Sie mit der Amazon Route 53-Konsole eine private oder öffentlich gehostete Zone mit einem CNAME-Eintrag

1. Öffnen Sie die Route 53-Konsole unter <https://console.aws.amazon.com/route53/>.
2. Wählen Sie im Navigationsbereich Hosted Zones und dann Create Hosted Zone aus.
3. Wählen Sie unter Domainname den Namen der gehosteten Zone aus, die Sie verwenden möchten, um den Datenverkehr an Ihren VPC Lattice-Dienst weiterzuleiten. Wenn Ihr benutzerdefinierter Domainname beispielsweise `parking.example.com` (`http://parking.example.com/`) lautet, lautet der Domainname für Ihre gehostete Zone `example.com` (`http://example.com/`), auch bekannt als Apex-Domänenname. Anschließend können Sie einen CNAME-Eintrag für diese gehostete Zone erstellen, um den Datenverkehr an Ihren VPC Lattice-Dienst weiterzuleiten. Hinweis: Sie können den Namen einer gehosteten Zone nicht mehr ändern, nachdem Sie sie erstellt haben.
4. Wählen Sie für Typ je nach Bedarf Private Hosted Zone oder Public Hosted Zone aus.
5. Wählen Sie Ihre Region und wählen Sie die VPC-ID für eine VPC aus, die Sie mit dieser gehosteten Zone verknüpfen möchten.
6. Fügen Sie bei Bedarf Tags hinzu und wählen Sie Create Hosted Zone aus. Nach der Erstellung wird Ihre gehostete Zone unter Gehostete Zonen aufgeführt.
7. Um einen CNAME-Eintrag in der Hosting-Zone zu erstellen, die Sie gerade erstellt haben, wählen Sie die Hosting-Zone und dann Eintrag erstellen aus.
8. Geben Sie unter Datensatz erstellen die folgenden Werte an:
 - a. Geben Sie unter Datensatzname den Namen ein, den Sie als Ihren benutzerdefinierten Domainnamen verwenden möchten. Wenn Sie `parking.example.com` (`http://acme.example.com/`) als Ihren benutzerdefinierten Domainnamen verwenden möchten, geben Sie `parking *` ein. Das bedeutet, dass Sie den Namen der Subdomain eingeben würden, `parking` jedoch ohne den Domainnamen der gehosteten Zone `example.com` (`http://example.com/`).
 - b. Wählen Sie als Datensatztyp die Option CNAME aus.
 - c. Lassen Sie Alias ausgeschaltet.
 - d. Geben Sie unter Value den VPC Lattice ein, der den Domainnamen für Ihren Service generiert hat (z. B. `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`). Sie finden diesen automatisch generierten Domainnamen in der VPC Lattice-Konsole auf Ihrer Serviceseite. Wenn Sie den verwenden AWS CLI, gibt

die Ausgabe der `list-services` Befehle `create-service` oder diesen automatisch generierten Domainnamen zurück.

- e. Akzeptieren Sie für TTL (Sekunden) den Standardwert 300.
 - f. Wählen Sie unter Routing-Richtlinie die entsprechende Routing-Richtlinie aus. Weitere Informationen finden Sie unter [Auswahl einer Routing-Richtlinie](#) im Amazon Route 53-Entwicklerhandbuch.
9. Wählen Sie Create records (Datensätze erstellen).

Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Weitergabe abgeschlossen ist, können Sie den Datenverkehr mithilfe des benutzerdefinierten Domainnamens an Ihren Service weiterleiten.

Um einen Aliaseintrag in Ihrer gehosteten Zone zu erstellen, verwenden Sie AWS CLI

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` im 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.

Den privaten Schlüssel Ihres Zertifikats sichern

Wenn Sie mit ACM ein SSL/TLS-Zertifikat anfordern, generiert ACM ein öffentliches/privates key pair. Wenn Sie ein Zertifikat importieren, generieren Sie das key pair. 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 AWS Certificate Manager im AWS Certificate Manager Benutzerhandbuch](#).

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 [Grants im Developer Guide](#).AWS Key Management Service

Weitere Informationen finden Sie unter [Verschlüsselung im Ruhezustand](#).

Einen Service löschen

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).

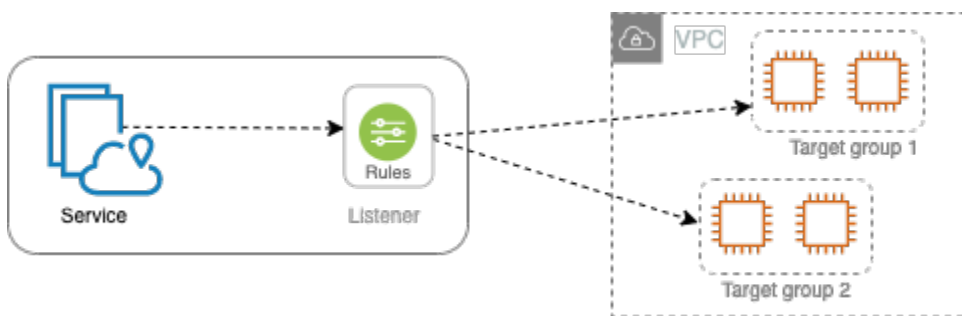
Um einen Dienst mit dem zu löschen AWS CLI

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. Ziele können EC2-Instances, IP-Adressen, Lambda-Funktionen, Application Load Balancer oder Kubernetes-Pods sein. 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 die Einstellungen für die Zustandsprüfung für Ihren Service auf Zielgruppenbasis. Jede Zielgruppe verwendet die standardmäßigen Zustandsprüfungseinstellungen, es sei denn, Sie überschreiben diese, wenn Sie die Zielgruppe erstellen, oder ändern sie später. Nachdem Sie in einer Regel für einen Listener eine Zielgruppe angegeben haben, überwacht der Service kontinuierlich den Zustand aller Ziele, die bei der Zielgruppe registriert sind. Der Service leitet Anfragen an die registrierten Ziele weiter, die fehlerfrei sind.

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

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

Inhalt

- [Erstellen Sie eine VPC-Lattice-Zielgruppe](#)

- [Ziele bei einer VPC Lattice-Zielgruppe registrieren](#)
- [Gesundheitschecks für Ihre VPC Lattice-Zielgruppen](#)
- [Weiterleitungskonfiguration](#)
- [Weiterleitungsalgorithmus](#)
- [Zieltyp](#)
- [IP-Adresstyp](#)
- [HTTP-Ziele in VPC Lattice](#)
- [Lambda fungiert als Ziele in VPC Lattice](#)
- [Application Load Balancer als Ziele in VPC Lattice](#)
- [Protokollversion](#)
- [Tags für Ihre VPC Lattice-Zielgruppe](#)
- [Löschen Sie eine VPC Lattice-Zielgruppe](#)

Erstellen Sie eine VPC-Lattice-Zielgruppe

Sie registrieren Ihre Ziele bei einer Zielgruppe. Standardmäßig sendet der VPC Lattice-Dienst Anfragen an registrierte Ziele und verwendet dabei den Port und das Protokoll, 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 Dienst angehören. Um eine Zielgruppe mit einem Dienst zu verwenden, müssen Sie sicherstellen, dass die Zielgruppe nicht von einem Listener für einen anderen Dienst verwendet wird.

Sie können jederzeit Ziele zu Ihrer Zielgruppe hinzufügen oder aus dieser entfernen. Weitere Informationen finden Sie unter [Ziele bei einer VPC Lattice-Zielgruppe registrieren](#). Sie können auch die Zustandsprüfungseinstellungen für Ihre Zielgruppe ändern. Weitere Informationen finden Sie unter [Gesundheitschecks für Ihre VPC Lattice-Zielgruppen](#).

Erstellen einer Zielgruppe

Sie können eine Zielgruppe erstellen und optional Ziele wie folgt 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 aus, um Ziele nach Instance-ID zu registrieren.
 - Wählen Sie IP-Adressen aus, um Ziele nach 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 als IP-Adresstyp IPv4 aus, um Ziele mit IPv4-Adressen zu registrieren, oder wählen Sie IPv6, um Ziele mit IPv6-Adressen zu registrieren. 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. Die Standardeinstellung ist HTTP1.

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

10. Ändern Sie für Integritätsprüfungen die Standardeinstellungen nach Bedarf. Weitere Informationen finden Sie unter [Gesundheitschecks 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) Um Tags hinzuzufügen, erweitern Sie Tags, wählen Sie Neues Tag hinzufügen aus und geben Sie den Tag-Schlüssel und den Tag-Wert ein.
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 „IP-Adressen angeben und Ports definieren“ die IP-Adresse ein und geben Sie die Ports ein. Der Standardport 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. Um eine Lambda-Funktion zu erstellen, wählen Sie Create a new Lambda-Funktion.
 - 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.

Um eine Zielgruppe mit dem zu erstellen AWS CLI

Verwenden Sie den [create-target-group](#) Befehl, um die Zielgruppe zu erstellen, und den Befehl [register-targets](#), um Ziele hinzuzufügen.

Gemeinsam genutzte Subnetze

Die Teilnehmer können VPC Lattice-Zielgruppen in einer gemeinsam genutzten 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 Dienstnetzwerk zugeordnet ist, können Anfragen an Dienste senden, die dem Dienstnetzwerk zugeordnet sind. Der Administrator kann dies jedoch mithilfe von Sicherheitsgruppen, Netzwerk-ACLs oder Authentifizierungsrichtlinien verhindern.

Weitere Informationen zu den gemeinsam nutzbaren Ressourcen für VPC Lattice finden Sie unter.

[VPC Lattice-Ressourcen teilen](#)

Ziele bei einer VPC Lattice-Zielgruppe registrieren

Ihr Service dient als zentrale Anlaufstelle für Kunden und verteilt den eingehenden Traffic auf seine fehlerfreien registrierten Ziele. Sie können jedes Ziel bei einer oder mehreren Zielgruppen registrieren.

Wenn die Nachfrage nach Ihrer Anwendung steigt, können Sie zusätzliche Ziele bei einer oder mehreren Zielgruppen registrieren, um der Nachfrage gerecht zu werden. Der Service leitet Anfragen an ein neu registriertes Ziel weiter, sobald der Registrierungsprozess abgeschlossen ist und das Ziel die ersten 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 Dienst beendet die Weiterleitung von Anfragen an ein Ziel, sobald es deregistriert ist. 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 deregistrieren](#)

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 anhand der Instanz-ID registrieren, können Sie Ihren Service mit einer Auto Scaling Scaling-Gruppe verwenden. Nachdem Sie eine Zielgruppe an eine Auto Scaling-Gruppe angehängt haben und die Gruppe skaliert wird, werden die Instances, die die Auto Scaling 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 [Weiterleiten von Traffic an Ihre Auto Scaling Scaling-Gruppe mit einer VPC Lattice-Zielgruppe](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

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-Port ein und wählen Sie dann unten Als ausstehend einbeziehen aus. Wenn Sie mit dem Hinzufügen von Instances fertig sind, wählen Sie Ziele registrieren.
6. Um die Registrierung von Instances aufzuheben, wählen Sie die Instances aus und klicken Sie dann auf Deregister.

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-Endpunkte oder öffentlich routbare 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 mit der Angabe von Adressen fertig sind, wählen Sie Ziele registrieren aus.
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 bei der 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 registrieren oder deregistrieren Sie eine 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.

- Um die Registrierung einer Lambda-Funktion aufzuheben, wählen Sie **Deregister** (Registrierung aufheben). Wenn Sie zur Bestätigung aufgefordert werden, geben Sie die Taste ein **confirm** und wählen Sie dann **Abmelden**.

Einen Application Load Balancer registrieren oder deregistrieren

Sie können für jede Zielgruppe einen einzelnen Application Load Balancer registrieren. Wenn Sie keinen Traffic 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 deregistrieren Sie einen Application Load Balancer mithilfe der Konsole

- Öffnen Sie die Amazon VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
- Wählen Sie im Navigationsbereich unter VPC Lattice die Option **Zielgruppen** aus.
- Wählen Sie den Namen der Zielgruppe aus, um deren Detailseite zu öffnen.
- Wählen Sie die Registerkarte **Ziele**.
- Wenn kein Application Load Balancer registriert ist, wählen Sie **Ziel registrieren**. Wählen Sie den Application Load Balancer und anschließend **Ziel registrieren** aus.
- Um die Registrierung eines Application Load Balancer aufzuheben, wählen Sie **Deregister**. Wenn Sie zur Bestätigung aufgefordert werden, geben **confirm** Sie die Eingabe ein und wählen Sie dann **Abmelden**.

Gesundheitschecks für Ihre VPC Lattice-Zielgruppen

Ihr Service sendet regelmäßig Anfragen an seine registrierten Ziele, um deren Status zu testen. 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

- Wenn die Zielgruppenprotokollversion HTTP1 ist, sind Integritätsprüfungen standardmäßig aktiviert.
- Wenn die Zielgruppenprotokollversion HTTP2 ist, sind Integritätsprüfungen standardmäßig nicht aktiviert. Sie können jedoch Integritätsprüfungen aktivieren und die Protokollversion manuell auf HTTP1 oder HTTP2 festlegen.
- 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 [Zielgruppenstatus](#) 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 alle `HealthCheckIntervalSeconds` Sekunden eine Anfrage zur Integritätsprüfung an jedes registrierte Ziel. Dabei werden der angegebene Port, das Protokoll und der angegebene Ping-Pfad verwendet. 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 mehrere `UnhealthyThresholdCount` aufeinanderfolgende Fehler überschreiten, nimmt der Dienst das Ziel außer Betrieb. Wenn die Zustandsprüfungen mehr als `HealthyThresholdCount` aufeinanderfolgende Erfolge aufweisen, nimmt der Service das Ziel wieder in Betrieb.

Einstellung	Beschreibung
<code>HealthCheckProtocol</code>	Das Protokoll, das der Dienst bei der Durchführung von Zustandsprüfungen an Zielen verwendet. Möglichen Protokolle sind HTTP und HTTPS. Das Standardprotokoll ist HTTP.
<code>HealthCheckPort</code>	Der Port, den der Dienst bei der Durchführung von Zustandsprüfungen an Zielen verwendet

Einstellung	Beschreibung
	. Standardmäßig wird der Port verwendet, über den jedes Ziel Datenverkehr vom Dienst empfängt.
HealthCheckPath	Das Ziel für Zustandsprüfungen der Ziele. Wenn die Protokollversion HTTP1 oder HTTP2 ist, geben Sie einen gültigen URI (/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—120 Sekunden. Die Standardeinstellung ist 5 Sekunden, wenn der Zieltyp INSTANCE oder IP ist. Geben Sie 0 an, um diese Einstellung auf ihren Standardwert zurückzusetzen.
HealthCheckIntervalSeconds	Der etwaige Zeitraum in Sekunden zwischen den Zustandsprüfungen der einzelnen Ziele. Der Bereich liegt zwischen 5 und 300 Sekunden. Die Standardeinstellung ist 30 Sekunden, wenn der Zieltyp INSTANCE oder istIP. Geben Sie 0 an, um diese Einstellung auf ihren Standardwert zurückzusetzen.
HealthyThresholdCount	Die Anzahl der aufeinanderfolgenden erfolgreichen Zustandsprüfungen, die erforderlich sind, bevor ein fehlerhaftes Ziel als fehlerfrei eingestuft wird. Der Bereich liegt zwischen 2 und 10. Der Standardwert ist 5. Geben Sie 0 an, um diese Einstellung auf den Standardwert zurückzusetzen.

Einstellung	Beschreibung
UnhealthyThresholdCount	<p>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 ihren Standardwert zurückzusetzen.</p>
Matcher	<p>Die Codes, die verwendet werden, um ein Ziel auf eine erfolgreiche Antwort zu überprüfen. Diese werden in der Konsole als Erfolgscodes bezeichnet.</p> <p>Wenn die Protokollversion HTTP1 oder HTTP2 ist, 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.</p> <p>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.</p>

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 ein anderer Wert ist als `Healthy`, enthält die Spalte mit den Gesundheitsstatusdetails weitere Informationen.

Um den Zustand Ihrer Ziele zu überprüfen, verwenden Sie 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 initiieren, um Details über fehlerhafte Ziele zu senden.

Ändern Sie die Einstellungen für die Zustandsprüfung

Sie können die Zustandsprüfungseinstellungen für Ihre Zielgruppe jederzeit ändern.

Um die Einstellungen für die Integritätsprüfung mit der Konsole zu ändern

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 für die Integritätsprüfung die Option Bearbeiten aus.
5. Ändern Sie die Einstellungen für die Integritätsprüfung nach Bedarf.
6. Wählen Sie Änderungen speichern aus.

Um die Einstellungen für die Integritätsprüfung zu ändern, verwenden Sie AWS CLI

Verwenden Sie den [update-target-group](#)-Befehl.

Weiterleitungskonfiguration

Standardmäßig leitet ein Dienst Anfragen an seine Ziele weiter und verwendet dabei das Protokoll und die Portnummer, 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-Integritätsprüfungen verwendet, verwenden die TLS-Verbindungen zu den Zielen die Sicherheitsrichtlinie des Listeners. VPC Lattice stellt mithilfe von Zertifikaten, die Sie auf den Zielen installieren, TLS-Verbindungen zu den Zielen her. 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-Listern unterstützt.](#)

Weiterleitungsalgorithmus

Standardmäßig wird der Round-Robin-Routing-Algorithmus verwendet, um Anfragen 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 deren Gesundheitsstatus. Das bedeutet, dass der VPC Lattice-Dienst nicht geöffnet werden kann, wenn alle Ziele gleichzeitig die Zustandsprüfungen nicht bestehen. Das Fail-Open hat zur Folge, dass der Datenverkehr auf der Grundlage des Round-Robin-Algorithmus zu allen Zielen unabhängig von deren Integritätsstatus zugelassen 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 istIP, 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 istIP, können Sie keine VPC-Endpunkte oder öffentlich routbare IP-Adressen registrieren.
- Wenn der Zieltyp istLAMBDA, 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 istALB, können Sie einen einzelnen internen Application Load Balancer als Ziel von bis zu zwei VPC Lattice Services registrieren. Registrieren Sie dazu den Application Load Balancer für zwei separate Zielgruppen, die von zwei verschiedenen VPC-Lattice-Diensten verwendet werden. Darüber hinaus muss der Ziel-Application Application Load Balancer mindestens einen Listener haben, dessen Port mit dem Zielgruppenport übereinstimmt.

- Um eine ECS-Aufgabe als Ziel zu registrieren, verwenden Sie den ALB Zieltyp und registrieren Sie den Application Load Balancer für Ihren Amazon ECS-Service. Weitere Informationen finden Sie unter [Service – Load Balancing](#) 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 INSTANCE die einzigen unterstützten Zieltypen und IP

IP-Adresstyp

Wenn Sie eine Zielgruppe mit dem Zieltyp von erstellenIP, 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 einem IP-Adresstyp von erstellen, muss die VPCIPv6, 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, deren IP-Adresstyp istIPv4.
- 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 authentifzierten Prinzipal.
- `SessionName`— Der Name der authentifzierten 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 Name des Subjekts (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 zu den Ressourcen-ARNs für VPC Lattice finden Sie unter [Von Amazon VPC Lattice definierte Ressourcentypen](#).

Lambda fungiert 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. Weitere Informationen finden Sie unter [Using AWS Lambda with Amazon VPC Lattice](#) im AWS Lambda Developer Guide.

Einschränkungen

- Die Lambda-Funktion und die Zielgruppe müssen sich im gleichen Konto und in der gleichen Region befinden.
- Die maximale Größe des Anforderungstexts, den Sie an eine Lambda-Funktion senden können, beträgt 6 MB.
- Die maximale Größe der Antwort-JSON, 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-Dienst 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.

Um eine Zielgruppe zu erstellen und die Lambda-Funktion über die Konsole zu registrieren

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) Um Tags hinzuzufügen, erweitern Sie Tags, wählen Sie Neues Tag hinzufügen aus und geben Sie den Tag-Schlüssel und den Tag-Wert ein.

8. Wählen Sie Weiter aus.
9. Führen Sie für Lambda function (Lambda-Funktion) einen der folgenden Schritte aus:
 - Wählen Sie eine vorhandene 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-group](#) und [register-targets](#).

Empfangen von Ereignissen vom VPC Lattice-Dienst

Der VPC Lattice-Dienst unterstützt Lambda-Aufrufe für Anfragen sowohl über HTTP als auch über 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.

Format der Ereignisstruktur

Wenn Sie eine Zielgruppe vom Typ erstellen oder aktualisieren LAMBDA, können Sie die Version der Ereignisstruktur angeben, die Ihre Lambda-Funktion empfängt. Die möglichen Versionen sind V1 und V2.

Example Beispiereignis: 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 Anfrage. Nur vorhanden, wenn das Protokoll HTTP, HTTPS oder gRPC ist.

identity

Die Identitätsinformationen. Die folgenden Felder sind möglich.

- `principal`— Der authentifizierte Principal. Nur vorhanden, wenn die AWS Authentifizierung erfolgreich ist.
- `principalOrgID`— Die ID der Organisation für den authentifzierten Prinzipal. Nur vorhanden, wenn die AWS Authentifizierung erfolgreich war.
- `sessionName`— Der Name der authentifzierten Sitzung. Nur vorhanden, wenn die AWS Authentifizierung erfolgreich ist.
- `sourceVpcArn`— Der ARN der VPC, von der die Anfrage 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 Name des Subjekts (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 Parameter der HTTP-Abfragezeichenfolge. Nur vorhanden, wenn das Protokoll HTTP, HTTPS oder gRPC ist.

serviceArn

Der ARN des Dienstes, der die Anfrage empfängt.

serviceNetworkArn

Der ARN des Servicenetzwerks, das die Anfrage zustellt.

targetGroupArn

Der ARN der Zielgruppe, die die Anfrage erhält.

timeEpoch

Die Zeit in Mikrosekunden.

Example Beispiereignis: 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 weglassen, da der Service ihn berechnet, bevor er Antworten an Clients sendet.

Im Folgenden finden Sie ein Beispiel für eine Antwort aus 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

Standardmäßig unterstützt VPC Lattice Anfragen von einem Client oder Antworten von einer Lambda-Funktion, die Header mit mehreren Werten enthält oder denselben Header mehrfach enthält. VPC Lattice unterstützt auch Abfrageparameter mit mehreren Werten für denselben Schlüssel.

Wenn bei Anforderungsheadern mehrere Parameter denselben Namen haben, übergibt VPC Lattice beide Werte an die Ziele. Im Folgenden finden Sie ein Beispiel für den Namen von zwei separaten Headern: `header 1`

```
header1 = foo
header1 = bar
```

Dann sendet VPC Lattice beide Werte an die Ziele:

```
"header1": ["foo", "bar"]
```

Wenn bei Abfragezeichenfolgen mehrere Parameter denselben Namen haben, gewinnt der letzte Wert. Das bedeutet, dass Parameter `_not_ coalesced` in einem einzigen Wert zusammengefasst werden, wenn sie denselben Schlüsselnamen haben.

Im Folgenden finden Sie ein Beispiel, bei dem `foo` und die Werte der Parameter mit demselben Namen `bar` sind^{Q51}:

```
http://www.example.com?&Q51=foo&Q51=bar
```

Dann sendet VPC Lattice den letzten Wert an die Ziele:

```
"QS1": "bar"
```

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 deregistrieren Sie eine 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. Klicken Sie auf der Registerkarte Targets (Ziele) auf Deregister (Registrierung aufheben).
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie die Eingabe ein **confirm** und wählen Sie dann Abmelden aus.

Um die Registrierung der Lambda-Funktion mit dem AWS CLI

Verwenden Sie den Befehl [deregister-targets](#).

Application Load Balancer 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 Traffic an diese Zielgruppe weiterleitet. In diesem Szenario übernimmt der Application Load Balancer die Routing-Entscheidung, sobald der Verkehr ihn erreicht. Mit dieser Konfiguration können Sie die anforderungsbasierte Layer-7-Routing-Funktion des Application Load Balancer in Kombination mit Funktionen verwenden, die VPC Lattice unterstützt, wie IAM-Authentifizierung und -Autorisierung sowie Konnektivität zwischen VPCs und Konten.

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 [Gesundheitschecks für Ihre Zielgruppen](#) im Benutzerhandbuch für Application Load Balancers

Voraussetzungen

Erstellen Sie einen Application Load Balancer, um sich als Ziel bei Ihrer 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 auf dem Application Load Balancer verwenden, um TLS zu beenden, aber nur, wenn der VPC Lattice-Dienst dasselbe SSL/TLS-Zertifikat wie der Load Balancer verwendet.
- 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-Anfrage bei und sendet ihn ohne Änderung an Ziele. Weitere Informationen finden Sie unter [X-Forwarded-For im Benutzerhandbuch für Application Load Balancers](#).

Weitere Informationen finden Sie unter [Erstellen eines Application Load Balancer](#) im Benutzerhandbuch für Application Load Balancers.

Schritt 1: Erstellen Sie eine 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 Integritätsprüfungen für die Zielgruppen Ihres Application Load Balancer konfigurieren. Weitere Informationen finden Sie unter [Zielgruppenstatus](#) im Benutzerhandbuch für Application Load Balancers.

Um die Zielgruppe 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 Zielgruppen aus.
3. Wählen Sie Zielgruppe erstellen aus.
4. Wählen Sie auf der Seite Zielgruppendedetails 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 unter 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: Registrieren Sie den Application Load Balancer als Ziel

Sie können den Load Balancer entweder jetzt oder zu einem späteren Zeitpunkt als Ziel registrieren.

So registrieren Sie einen Application Load Balancer als Ziel

1. Wählen Sie Jetzt registrieren.

2. Wählen Sie für 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 Anfragen über HTTP/1.1 an Ziele. 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
HTTP/1.1	gRPC	Fehler
HTTP/2	gRPC	Erfolg bei einer POST-Anforderung
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 die gRPC-Aufrufe auf der Grundlage des Pakets, des Dienstes und der Methode an die entsprechenden Zielgruppen weiter.
- Sie können Lambda-Funktionen nicht als Ziele 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 Dienst 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 das `aws :` Präfix nicht in Ihren Tagnamen oder -Werten, da es für AWS die 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 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 die Tags für eine Zielgruppe zu aktualisieren, verwenden Sie AWS CLI

Verwenden Sie die Befehle [tag-resource](#) und [untag-resource](#).

Löschen Sie eine VPC Lattice-Zielgruppe

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, die bei der Zielgruppe registriert sind. Wenn Sie die registrierte EC2-Instance nicht mehr benötigen, können Sie sie anhalten oder beenden.

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 Zielgruppen aus.
3. Aktivieren Sie das Kontrollkästchen für die Zielgruppe und wählen Sie dann Aktionen, Löschen aus.

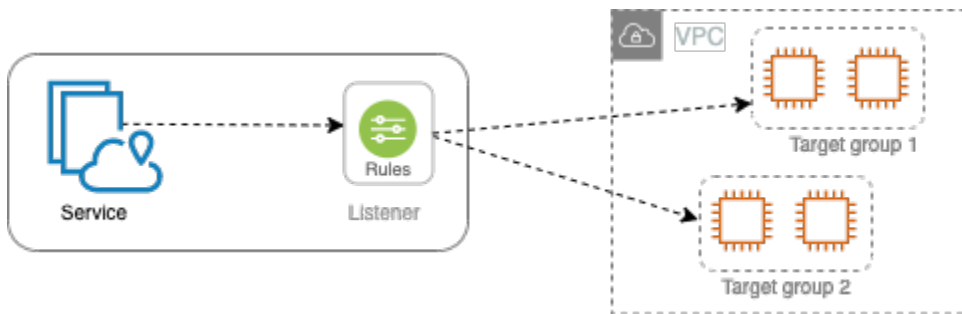
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **confirm** ein und wählen Sie dann Löschen aus.

Um eine Zielgruppe zu löschen, verwenden Sie AWS CLI

Verwenden Sie den [delete-target-group](#)-Befehl.

Listener für Ihren VPC Lattice-Service

Bevor Sie Ihren VPC Lattice-Dienst 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](#)
- [Erstellen eines Listeners](#)
- [HTTP-Listener für VPC Lattice-Dienste](#)
- [HTTPS-Listener für VPC Lattice-Dienste](#)
- [TLS-Listener für VPC Lattice-Dienste](#)
- [Listener-Regeln für Ihren VPC Lattice-Service](#)
- [Aktualisieren eines Listeners](#)
- [Löschen eines Listeners](#)

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

Erstellen eines Listeners

Sie können Listener für Ihren VPC Lattice-Dienst erstellen. Wenn Sie einen Listener erstellen, müssen Sie einen Namen, eine Standardaktion und ein Protokoll angeben. Ein Listener wird mit einer Standardregel geliefert. Sie können auch zusätzliche Regeln für Ihren Listener erstellen.

Um einen Listener mit der Konsole zu erstellen

- [the section called “Hinzufügen eines HTTP-Listeners”](#)
- [the section called “Hinzufügen eines HTTPS-Listeners”](#)
- [the section called “Fügen Sie einen TLS-Listener hinzu”](#)
- [the section called “Hinzufügen einer Regel”](#)

Um einen Listener mit dem zu erstellen AWS CLI

[Verwenden Sie die Befehle create-listener und create-rule.](#)

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 dabei, einen HTTP-Listener für Ihren Service zu erstellen. 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 Sie eine VPC-Lattice-Zielgruppe](#).
- Sie können dieselbe Zielgruppe in mehreren Listenern angeben, aber diese Listener müssen demselben Dienst angehören. Um eine Zielgruppe mit einem VPC Lattice-Dienst zu verwenden, müssen Sie sicherstellen, dass sie nicht von einem Listener für einen anderen VPC Lattice-Dienst verwendet wird.

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 seine 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. 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 nicht ändern, nachdem Sie ihn erstellt haben.
6. Wählen Sie für Protokoll: Port die Option HTTP und geben Sie eine Portnummer ein.

- 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.

- (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](#).

- (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.
- Überprüfen Sie Ihre Konfiguration und wählen Sie dann Hinzufügen.

Um einen HTTP-Listener hinzuzufügen, verwenden Sie 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 HTTPS-Listener erstellen, der TLS Version 1.2 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.

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](#)
- [ALPN-Richtlinie](#)
- [Hinzufügen eines HTTPS-Listeners](#)

Sicherheitsrichtlinie

VPC Lattice verwendet eine Sicherheitsrichtlinie, die eine Kombination aus dem TLSv1.2-Protokoll und einer Liste von SSL/TLS-Chiffren ist. Das Protokoll stellt eine sichere Verbindung zwischen einem Client und einem Server her und trägt dazu bei, dass alle Daten, die zwischen dem Client und Ihrem Dienst 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 des Verbindungsaushandlungsprozesses präsentieren der Client und VPC Lattice eine Liste von Chiffren und Protokollen, die sie jeweils unterstützen, in der Reihenfolge ihrer Präferenz. 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 das TLSv1.2-Protokoll und die folgenden SSL/TLS-Chiffren in dieser Reihenfolge der Präferenz:

- 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

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 Sie eine VPC-Lattice-Zielgruppe](#).
- Sie können dieselbe Zielgruppe in mehreren Listenern angeben, aber diese Listener müssen demselben VPC Lattice-Dienst angehören. Um eine Zielgruppe mit einem VPC Lattice-Dienst zu

verwenden, müssen Sie sicherstellen, dass sie nicht von einem Listener für einen anderen VPC Lattice-Dienst verwendet wird.

- Sie können das von VPC Lattice bereitgestellte Zertifikat verwenden oder Ihr eigenes Zertifikat in 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 seine 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. 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.
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 Neues Tag hinzufügen aus und geben Sie einen Tag-Schlüssel und einen Tag-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.

Um einen HTTPS-Listener hinzuzufügen, verwenden Sie 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

Die folgenden Überlegungen gelten für TLS-Listener:

- Der VPC Lattice-Dienst muss einen benutzerdefinierten Domainnamen haben. Der benutzerdefinierte Domainname 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

Fügen Sie einen TLS-Listener hinzu

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](#).

Um einen TLS-Listener mithilfe der Konsole hinzuzufügen

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 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. 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.

6. Wählen Sie als Protokoll die Option 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 Neues Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
9. Überprüfen Sie Ihre Konfiguration und wählen Sie dann Hinzufügen.

Um einen TLS-Listener hinzuzufügen, verwenden Sie 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](#)
- [Priorität der Regel](#)
- [Regelaktion](#)
- [Regelbedingungen](#)
- [Hinzufügen einer Regel](#)
- [Aktualisieren Sie eine Regel](#)
- [Löschen einer Regel](#)

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-Antwortcode zurückzugeben.

Example Beispiel für eine feste Antwortaktion für AWS CLI

Sie können eine Aktion angeben, wenn Sie eine Regel erstellen oder aktualisieren. 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. Bei der Methode match wird zwischen Groß- und Kleinschreibung unterschieden. Der Methodename muss exakt übereinstimmen. Platzhalterzeichen werden nicht unterstützt.

Pfadübereinstimmung

Das Routing basiert auf dem Abgleich der Pfadmuster in den Anforderungs-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.

Um eine Listener-Regel mithilfe der Konsole hinzuzufügen

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 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 maximale Größe jeder Zeichenfolge beträgt 200 Zeichen. Beim 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.

Um eine Regel hinzuzufügen, verwenden Sie AWS CLI

Verwenden Sie den Befehl [create-rule](#).

Aktualisieren Sie eine 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.

Um eine Listener-Regel 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 auf der Registerkarte Routing die Option Listener bearbeiten aus.

5. Ändern Sie die Prioritäten, Bedingungen und Aktionen der Regel nach Bedarf.
6. Überprüfen Sie Ihre Aktualisierungen und wählen Sie Änderungen speichern.

Um eine Regel mit dem zu aktualisieren 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.

Um eine Listener-Regel 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 Services aus.
3. Wählen Sie den Namen des Dienstes aus, um seine 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.

Um eine Regel mit dem zu löschen AWS CLI

Verwenden Sie den Befehl [delete-rule](#).

Aktualisieren eines Listeners

Nachdem Sie einen Listener erstellt haben, können Sie die Zielgruppe für die Standardaktion ersetzen. Sie können der Standardaktion auch eine Zielgruppe hinzufügen und den Zielgruppen Gewichtungen zuweisen. Sie können den Listener-Namen, das Listener-Protokoll oder den Listener-Port nicht aktualisieren.

Um einen Listener 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 auf der Registerkarte Routing die Option Listener bearbeiten aus.
5. Für die Standardaktion können Sie die Zielgruppe oder das Gewicht nach Bedarf aktualisieren.
6. Um weitere Zielgruppen hinzuzufügen, wählen Sie Aktion hinzufügen und wählen Sie dann eine Zielgruppe aus und geben Sie deren Gewicht an.
7. Sie können auch Listener-Regeln hinzufügen, bearbeiten oder löschen. Weitere Informationen finden Sie unter [Listener-Regeln](#).
8. Überprüfen Sie Ihre Aktualisierungen und wählen Sie Änderungen speichern.

Um die Standardaktion für einen Listener mit dem zu aktualisieren AWS CLI

Verwenden Sie den Befehl [update-listener](#).

Löschen eines Listeners

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 seine 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 zu löschen, verwenden Sie AWS CLI

Verwenden Sie den Befehl [delete-listener](#).

Teilen Sie Ihre VPC Lattice-Ressourcen

Amazon VPC Lattice ist in AWS Resource Access Manager (AWS RAM) integriert, um die gemeinsame Nutzung von Ressourcen zu ermöglichen. AWS RAM ist ein Service, der es Ihnen ermöglicht, einige VPC-Lattice-Ressourcen mit anderen AWS-Konten oder durch andere zu teilen. AWS Organizations Mit AWS RAM geben Sie Ressourcen in Ihrem Besitz frei, indem Sie eine Ressourcenfreigabe erstellen. Eine Ressourcenfreigabe legt die freizugebenden Ressourcen und die Konsumenten fest, für die sie freigegeben werden sollen. Zu den Verbrauchern können gehören:

- AWS-Konten spezifisch innerhalb oder außerhalb seiner Organisation in AWS Organizations.
- Eine Organisationseinheit innerhalb ihrer 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-Ressourcen](#)
- [VPC Lattice-Ressourcen teilen](#)
- [Beenden Sie die gemeinsame Nutzung von VPC Lattice-Ressourcen](#)
- [Zuständigkeiten und Genehmigungen](#)
- [Kontoübergreifende Ereignisse](#)

Voraussetzungen für die gemeinsame Nutzung von VPC Lattice-Ressourcen

- Um eine Ressource gemeinsam zu nutzen, müssen Sie sie in Ihrem besitzen. AWS-Konto Das bedeutet, dass die Ressource Ihrem Konto zugewiesen oder bereitgestellt werden muss. Sie können eine Ressource, die mit Ihnen geteilt wurde, nicht teilen.
- Um eine Ressource mit Ihrer Organisation oder einer Organisationseinheit gemeinsam zu nutzen AWS Organizations, müssen Sie das Teilen mit aktivieren AWS Organizations. Weitere Informationen finden Sie [AWS Organizations im AWS RAM Benutzerhandbuch unter Aktivieren der gemeinsamen Nutzung von Ressourcen](#).

VPC Lattice-Ressourcen teilen

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

Wenn Sie eine VPC Lattice-Ressource, die Sie besitzen, mit anderen teilen AWS-Konten, ermöglichen Sie diesen Konten, ihre Ressourcen mit Ressourcen in Ihrem Konto zu verknüpfen. Wenn Sie eine Zuordnung für eine gemeinsam genutzte Ressource erstellen, generieren wir einen Amazon-Ressourcennamen (ARN) im Konto des Ressourcenbesitzers und zusätzlich einen ARN in dem Konto, mit dem die Zuordnung erstellt wurde. Auf diese Weise können sowohl der Eigentümer der Ressource 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 Ressource. Andernfalls erhalten Verbraucher eine Einladung, dem Resource Share beizutreten, und erhalten nach Annahme der Einladung Zugriff auf die gemeinsam genutzte Ressource.

Überlegungen

- Sie können zwei Arten von VPC-Lattice-Ressourcen gemeinsam nutzen: Dienstnetzwerke und Dienste.
- Sie können Ihre VPC Lattice-Ressourcen mit jedem teilen. AWS-Konto
- Sie können Ihre VPC Lattice-Ressourcen nicht mit einzelnen IAM-Benutzern und -Rollen teilen.
- VPC Lattice unterstützt vom Kunden verwaltete Berechtigungen sowohl für Servicenetzwerke als auch für Dienste.

Um eine Ressource, die Ihnen gehört, mithilfe der VPC Lattice-Konsole gemeinsam zu nutzen

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

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

Um eine Ressource, die Ihnen gehört, über die AWS RAM Konsole gemeinsam zu nutzen

Gehen Sie wie im AWS RAM Benutzerhandbuch unter [Erstellen einer gemeinsamen Ressource](#) beschrieben vor.

Um eine Ressource, die Sie besitzen, gemeinsam zu nutzen, verwenden Sie den AWS CLI

Verwenden Sie den [associate-resource-share](#)-Befehl.

Beenden Sie die gemeinsame Nutzung von VPC Lattice-Ressourcen

Um die gemeinsame Nutzung einer VPC Lattice-Ressource, die Sie besitzen, zu beenden, müssen Sie sie aus der Ressourcenfreigabe entfernen. Bestehende Verknüpfungen bleiben bestehen, nachdem Sie die gemeinsame Nutzung Ihrer Ressource beendet haben. Neue Verknüpfungen zu einer zuvor gemeinsam genutzten Ressource sind nicht zulässig. Wenn entweder der Ressourcenbesitzer oder der Zuordnungsbesitzer eine Zuordnung löscht, wird sie aus beiden Konten gelöscht. Wenn ein Kontoinhaber eine Ressourcenfreigabe verlassen möchte, muss er den Besitzer der Ressourcenfreigabe bitten, das Konto zu entfernen.

So beenden Sie die gemeinsame Nutzung einer Ressource, 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 oder Service Networks aus.
3. Wählen Sie den Namen der Ressource aus, 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 Ressource, deren Eigentümer Sie sind, über die AWS RAM Konsole zu beenden

Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch unter [Aktualisieren einer gemeinsam genutzten Ressource](#).

Um die gemeinsame Nutzung einer Ressource, deren Eigentümer Sie sind, zu beenden, verwenden Sie 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-Ressourcen.

Besitzer von Ressourcen

- Der Besitzer des Dienstnetzwerks 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 Dienstes kann alle Netzwerkzuordnungen mit dem Dienst beschreiben.
- Der Dienstbesitzer kann einen Dienst von jedem Dienstnetzwerk trennen, mit dem er verknüpft ist.
- Nur das Konto, das eine Zuordnung erstellt hat, kann die Zuordnung zwischen dem Servicenetzwerk und der VPC aktualisieren.

Nutzer von Ressourcen

- Der Verbraucher kann einen Dienst nicht löschen, den er nicht erstellt hat.
- Der Verbraucher kann nur die Dienste trennen, die er einem Servicenetzwerk zugeordnet hat.

- Der Verbraucher und der Netzwerkbesitzer können alle Verbindungen zwischen einem Dienstnetz und einem Dienst beschreiben.
- Der Verbraucher kann keine Dienstinformationen zu einem Dienst abrufen, der ihm nicht gehört.
- Der Verbraucher kann alle Dienstzuordnungen zu einem gemeinsamen Servicenetzwerk beschreiben.
- Der Verbraucher kann einen Dienst 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 die VPCs trennen, die er einem Servicenetzwerk zugeordnet hat.
- Der Nutzer eines gemeinsam genutzten Dienstes kann einen Dienst nicht einem Servicenetzwerk zuordnen, das ihm nicht gehört.
- Der Nutzer eines Shared-Service-Netzwerks kann keine VPC oder einen Service zuordnen, den er nicht besitzt.
- Der Verbraucher kann einen Dienst oder ein Servicenetzwerk beschreiben, das mit ihm gemeinsam genutzt wird.
- Der Verbraucher kann zwei Ressourcen nicht zuordnen, wenn beide mit ihm gemeinsam genutzt werden.

Kontoübergreifende Ereignisse

Wenn Ressourcenbesitzer und -nutzer Aktionen an einer gemeinsam genutzten Ressource ausführen, werden diese Aktionen als kontoübergreifende Ereignisse in aufgezeichnet. AWS CloudTrail

CreateServiceNetworkServiceAssociationBySharee

Wird an den Ressourcenbesitzer gesendet, wenn ein Ressourcennutzer [CreateServiceNetworkServiceAssociation](#) mit einer gemeinsam genutzten Ressource 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 Besitzer der Ressource gesendet, wenn ein Ressourcennutzer [CreateServiceNetworkVpcAssociation](#) über ein Shared Service Network anruft.

DeleteServiceNetworkServiceAssociationByOwner

Wird an den Eigentümer der Zuordnung gesendet, wenn der Ressourcenbesitzer [DeleteServiceNetworkServiceAssociation](#) mit einer gemeinsam genutzten Ressource 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 Besitzer der Ressource gesendet, wenn ein Ressourcennutzer [DeleteServiceNetworkServiceAssociation](#) mit einer gemeinsam genutzten Ressource 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 Besitzer der Assoziation gesendet, wenn der Besitzer der Ressource über ein gemeinsames Servicenetzwerk anruft [DeleteServiceNetworkVpcAssociation](#).

DeleteServiceNetworkVpcAssociationBySharee

Wird an den Besitzer der Ressource gesendet, wenn ein Ressourcennutzer [DeleteServiceNetworkVpcAssociation](#) über ein Shared Service Network anruft.

GetServiceBySharee

Wird an den Ressourcenbesitzer gesendet, wenn ein Ressourcennutzer über einen [GetService](#) gemeinsam genutzten Dienst anruft.

GetServiceNetworkBySharee

Wird an den Ressourcenbesitzer gesendet, wenn ein Ressourcennutzer [GetServiceNetwork](#) über ein Shared Service-Netzwerk anruft.

GetServiceNetworkServiceAssociationBySharee

Wird an den Ressourcenbesitzer gesendet, wenn ein Ressourcennutzer [GetServiceNetworkServiceAssociation](#) mit einer gemeinsam genutzten Ressource 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 Besitzer der Ressource gesendet, wenn ein Ressourcennutzer [GetServiceNetworkVpcAssociation](#) über 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-eea89f4a47cd",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::VpcLattice::ServiceNetworkServiceAssociation",
      "ARN": "arn:aws:vpc-lattice:region:123456789012:servicenetworbserviceassociation/snsa-0d5ea7bc72EXAMPLE"
    }
  ],
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management"
}
```

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 können, die Ihnen helfen, Ihre VPC Lattice-Ressourcen zu überwachen und zu sichern.

Inhalt

- [Zugriff auf VPC Lattice-Dienste verwalten](#)
- [Datenschutz in Amazon VPC Lattice](#)
- [Identitäts- und Zugriffsmanagement für Amazon VPC Lattice](#)
- [Konformitätsvalidierung für Amazon VPC Lattice](#)
- [Greifen Sie über Schnittstellenendpunkte auf Amazon VPC Lattice zu \(\) PrivateLink](#)
- [Resilienz in Amazon VPC Lattice](#)
- [Infrastruktursicherheit in Amazon VPC Lattice](#)

Zugriff auf VPC Lattice-Dienste verwalten

VPC Lattice ist standardmäßig sicher, da Sie explizit angeben müssen, auf welche Dienste und mit welchen VPCs Sie Zugriff gewähren möchten. In Szenarien mit mehreren Konten können Sie Ressourcen über Kontogrenzen [AWS Resource Access Manager](#) hinweg gemeinsam nutzen. VPC Lattice bietet ein Framework, mit dem Sie eine defense-in-depth Strategie auf mehreren Ebenen des Netzwerks implementieren können.

- Erste Ebene — Die Service- und VPC-Verknüpfung mit einem Servicenetzwerk. Wenn eine VPC oder ein bestimmter Dienst nicht mit dem Dienstnetzwerk verknüpft ist, haben Clients in der VPC keinen Zugriff auf den Dienst.
- Zweite Ebene — Optionale Sicherheitsvorkehrungen auf Netzwerkebene für das Servicenetzwerk, z. B. Sicherheitsgruppen und Netzwerk-ACLs. Mit diesen können Sie den Zugriff auf bestimmte Ressourcengruppen in einer VPC statt auf alle Ressourcen 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 feinkörnige Kontrollen fest, die möglicherweise restriktiver sind als die grobkörnige Autorisierung, die auf Dienstnetzwerkebene angewendet wird.

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.

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. 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.

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 unter [Servicenetzwerke in VPC Lattice](#).

Aufgaben

- [Fügen Sie einem Servicenetzwerk eine Authentifizierungsrichtlinie hinzu](#)
- [Ändern Sie den Authentifizierungstyp eines Servicenetzwerks](#)
- [Entfernen Sie eine Authentifizierungsrichtlinie aus einem Servicenetzwerk](#)

Fügen Sie einem Servicenetzwerk 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-identifizier 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-  
identifizier 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-identifizier 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 unter [Dienstleistungen 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 `svc-0123456789abcdef0` zu erstellen.

```
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 Deny sein. 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.

Ressourcenbeispiele für Authentifizierungsrichtlinien

Protokoll	Beispiele
HTTP	<ul style="list-style-type: none"> • "Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/rates" • "Resource": "*/rates" • "Resource": "*/*"
gRPC	<ul style="list-style-type: none"> • "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/*"

Protokoll	Beispiele
	<ul style="list-style-type: none"> • "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
```

Beispielsweise:

```
"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 unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

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 für Authentifizierungsrichtlinien

Bedingungsschlüssel	Beschreibung	Beispiel	Verfügbar für anonyme (nicht authentifizierte) Anrufer?	Verfügbar für gRPC?
<code>vpc-lattice-svcs:Port</code>	Filtert den Zugriff nach dem Service-Port, an den die Anfrage gestellt wird	80	Ja	Ja
<code>vpc-lattice-svcs:RequestMethod</code>	Filtert den Zugriff nach der Methode der Anfrage	GET	Ja	Immer POSTEN
<code>vpc-lattice-svcs:RequestHeader/ <i>header-name</i> : <i>value</i></code>	Filtert den Zugriff nach einem Header-Namen-Wert-Paar in den Anforderungsheadern	content-type: application/json	Ja	Ja
<code>vpc-lattice-svcs:QueryString/ <i>key-name</i> : <i>value</i></code>	Filtert den Zugriff nach den Schlüssel-Wert-Paaren der Abfragezeichenfolge in der Anforderungs-URL	quux: [corge, grault]	Ja	Nein
<code>vpc-lattice-svcs:ServiceNetworkArn</code>	Filtert den Zugriff nach dem ARN des Servicenetzwerks des Dienstes, der die Anfrage empfängt	arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/sn-0123456789abcdef0	Ja	Ja

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

Alle Beispiele verwenden die us-west-2 Region und enthalten fiktive 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"
        }
      }
    }
  ]
}

```

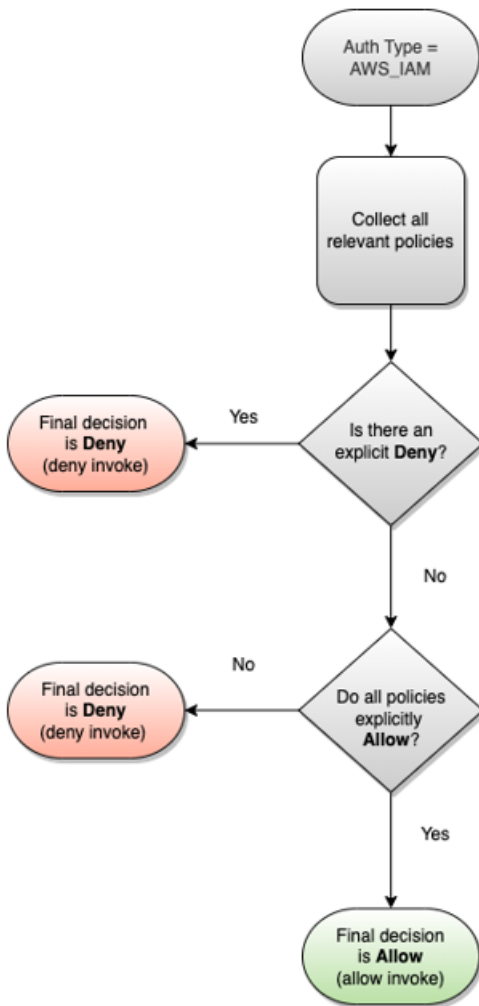
Wie funktioniert die Autorisierung

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 `istNONE`, 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“ `istNONE`, 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 Ressourcen, 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.

Inhalt

- [Liste der verwalteten Präfixe](#)
- [Sicherheitsgruppenregeln](#)
- [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. 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-lattice`
- `com.amazonaws.region.ipv6.vpc-lattice`

Weitere Informationen finden Sie im Abschnitt zur [AWS-verwalteten Präfixliste](#) im Amazon-VPC-Benutzerhandbuch.

Windows-Clients

Die Adressen in den VPC Lattice-Präfixlisten sind verknüpfungsl lokale Adressen. Wenn Sie von einem Windows-Client aus eine Verbindung zu VPC Lattice herstellen, müssen Sie die Konfiguration des Windows-Clients aktualisieren, sodass er die von VPC Lattice verwendeten Link-Local-Adressen an die primäre IP-Adresse des Clients weiterleitet. Im Folgenden finden Sie einen Beispielbefehl, der die Konfiguration des Windows-Clients aktualisiert. Dabei `169.254.171.0` handelt es sich um die von VPC Lattice verwendete Link-Local-Adresse.

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

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.

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

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

Eingehend

Source	Protocol (Protokoll)	Port-Bereich	Kommentar
<i>VPC-CIDR</i>	<i>listener</i>	<i>listener</i>	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.

Ausgehend

Ziel	Protocol (Protokoll)	Port-Bereich	Kommentar
<i>ID der VPC Lattice-Präfixliste</i>	<i>listener</i>	<i>listener</i>	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.

Eingehend

Source	Protocol (Protokoll)	Port-Bereich	Kommentar
<i>ID der VPC Lattice-Präfixliste</i>	<i>target</i>	<i>target</i>	Verkehr von VPC Lattice zu Zielen zulassen
<i>ID der VPC Lattice-Präfixliste</i>	<i>health check</i>	<i>health check</i>	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, vergewissern Sie sich, 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-identifizier sn-0123456789abcdef0 \  
  --vpc-identifizier 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 die IDs der Sicherheitsgruppen an. Diese Sicherheitsgruppen haben Vorrang vor allen zuvor zugewiesenen Sicherheitsgruppen. Definieren Sie mindestens eine Sicherheitsgruppe, wenn Sie die Liste aktualisieren.

```
aws vpc-lattice update-service-network-vpc-association
  --service-network-vpc-association-identifizier 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 mithilfe von 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 benutzerdefinierte 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](#)
- [Netzwerk-ACLs für Ihre Zielsubnetze](#)

Netzwerk-ACLs für Ihre Client-Subnetze

Die Netzwerk-ACLs für Client-Subnetze müssen den Verkehr zwischen Clients und VPC Lattice zulassen. Sie können den IP-Adressbereich, der zugelassen werden soll, aus der [Liste der verwalteten Präfixe](#) für VPC Lattice abrufen.

Eingehend

Source	Protocol (Protokoll)	Port-Bereich	Kommentar
<i>vpc_lattice_cidr_block</i>	TCP	1025-65535	Verkehr von VPC Lattice zu Clients zulassen

Ausgehend

Ziel	Protocol (Protokoll)	Port-Bereich	Kommentar
<i>vpc_lattice_cidr_block</i>	<i>listener</i>	<i>listener</i>	Datenverkehr von Clients zu VPC Lattice zulassen

Netzwerk-ACLs für Ihre Zielsubnetze

Die Netzwerk-ACLs für Zielsubnetze müssen den Datenverkehr zwischen Zielen und VPC Lattice sowohl am Zielport als auch am Health Check-Port zulassen. Sie können den IP-Adressbereich, der zugelassen werden soll, aus der [Liste der verwalteten Präfixe](#) für VPC Lattice abrufen.

Eingehend

Source	Protocol (Protokoll)	Port-Bereich	Kommentar
<i>vpc_lattice_cidr_block</i>	<i>target</i>	<i>target</i>	Verkehr von VPC Lattice zu Zielen zulassen
<i>vpc_lattice_cidr_block</i>	<i>health check</i>	<i>health check</i>	Health Check-Verkehr von VPC Lattice zu Zielen zulassen

Ausgehend

Ziel	Protocol (Protokoll)	Port-Bereich	Kommentar
<code>vpc_lattice_cidr_block</code>	<code>target</code>	1024 - 65535	Datenverkehr von Zielen zu VPC Lattice zulassen
<code>vpc_lattice_cidr_block</code>	<code>health check</code>	1024 - 65535	Zustandsprüfungsverkehr 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 [Signieren von AWS API-Anfragen](#) im IAM-Benutzerhandbuch.

Überlegungen

- VPC Lattice versucht, jede Anfrage zu authentifizieren, die mit Sigv4 oder SigV4a signiert ist. Die Anfrage schlägt ohne Authentifizierung fehl.
- VPC Lattice unterstützt keine Payload-Signierung. Sie müssen einen `x-amz-content-sha256` Header senden, bei dem der Wert auf gesetzt ist. "UNSIGNED-PAYLOAD"

Beispiele

- [Python](#)
- [Java mit Interceptor](#)
- [Java ohne Interceptor](#)
- [Node.js](#)

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
```

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

SIGv4

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

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtS3SigV4Auth(session.get_credentials(), 'vpc-lattice-svcs',
    'us-west-2')
    endpoint = 'https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
    west-2.on.aws/create'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["has_streaming_input"] = True # payload signing is not supported
    signer.add_auth(request)

    prepped = request.prepare()

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

SIGv4A

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



```
if __name__ == '__main__':
    session = boto3.session.Session()
    signer = crt.auth.CrtS3SigV4AsymAuth(session.get_credentials(), 'vpc-lattice-
svcs', 'us-west-2')
    endpoint = 'https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws/create'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["has_streaming_input"] = True # payload signing is not supported
    signer.add_auth(request)

    prepped = request.prepare()

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

Java mit Interceptor

In diesem Beispiel wird [Amazon Request Signing Interceptor für die Signierung](#) von Anfragen verwendet.

```
import com.amazonaws.http.AwsRequestSigningApacheInterceptor;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.auth.signer.Aws4UnsignedPayloadSigner;
import software.amazon.awssdk.regions.Region;

import java.nio.charset.StandardCharsets;

import org.apache.http.client.methods.HttpPost;
import org.apache.http.entity.ByteArrayEntity;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;

public class App {
    public static void main(String[] args) {
        var interceptor = new AwsRequestSigningApacheInterceptor(
            "vpc-lattice-svcs",
            Aws4UnsignedPayloadSigner.create(), // requires HTTPS
            DefaultCredentialsProvider.create(),
            Region.US_WEST_2.id()
        );
        CloseableHttpClient client = HttpClients.custom()
```

```
        .addInterceptorLast(interceptor)
        .build();

    var httpPost = new HttpPost("https://user-02222f67d3a427111.1234abc.vpc-lattice-
svcs.us-west-2.on.aws/create");
    httpPost.setHeader("content-type", "application/json");

    var body = ""
    {
        "name": "Jane Doe",
        "job": "Engineer"
    }
    """;
    httpPost.setEntity(new ByteArrayEntity(body.getBytes(StandardCharsets.UTF_8)));

    try (var response = client.execute(httpPost)) {
        System.out.println(new
String(response.getEntity().getContent().readAllBytes()));
    } catch (Exception e) {
        throw new RuntimeException(e);
    }
}
}
```

Java ohne Interceptor

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 abrufen. Wenn Sie lieber einen bestimmten Anbieter für Anmeldeinformationen verwenden möchten, können Sie einen aus der [AWS SDK for Java 2.x](#) auswählen. Das AWS SDK for Java erlaubt nur unsignierte Payloads über HTTPS. Sie können den Unterzeichner jedoch so erweitern, dass er unsignierte Payloads über HTTP unterstützt.

```
import java.io.ByteArrayInputStream;
import java.io.IOException;
import java.nio.charset.StandardCharsets;
import java.util.HashMap;
import java.util.List;
import java.util.Map;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.auth.signer.Aws4UnsignedPayloadSigner;
```

```
import software.amazon.awssdk.auth.signer.AwsSignerExecutionAttribute;
import software.amazon.awssdk.core.interceptor.ExecutionAttributes;
import software.amazon.awssdk.http.SdkHttpFullRequest;
import software.amazon.awssdk.http.SdkHttpMethod;
import software.amazon.awssdk.regions.Region;

import org.apache.http.client.methods.HttpPost;
import org.apache.http.entity.ByteArrayEntity;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;

public class App {

    public static void main(String[] args) {
        var signer = Aws4UnsignedPayloadSigner.create(); // requires HTTPS

        Map<String, String> headers = new HashMap<>();
        headers.put("content-type", "application/json");
        var body = ""
        {
            "name": "Jane Doe",
            "job": "Engineer"
        }
        """;

        String endpoint = "https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws/create";

        var sdkRequest = SdkHttpFullRequest.builder().method(SdkHttpMethod.POST);

        sdkRequest.host("user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws");
        sdkRequest.protocol("HTTPS");
        sdkRequest.encodedPath("/create");
        sdkRequest.contentStreamProvider(() -> new
ByteArrayInputStream(body.getBytes(StandardCharsets.UTF_8)));

        for (Map.Entry<String, String> header : headers.entrySet()) {
            sdkRequest.putHeader(header.getKey(), header.getValue());
        }

        ExecutionAttributes attributes = ExecutionAttributes.builder()
```

```

        .put(AwsSignerExecutionAttribute.AWS_CREDENTIALS,
DefaultCredentialsProvider.create().resolveCredentials())
        .put(AwsSignerExecutionAttribute.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")

        .put(AwsSignerExecutionAttribute.SIGNING_REGION, Region.US_WEST_2)
        .build();

SdkHttpRequest prepRequest = signer.sign(sdkRequest.build(), attributes);

HttpPost httpPost = new HttpPost(endpoint);
for (Map.Entry<String, List<String>> header : prepRequest.headers().entrySet())
{
    if (header.getKey().equalsIgnoreCase("host")) { continue; }
    for(var value : header.getValue()) {
        httpPost.addHeader(header.getKey(), value);
    }
}

CloseableHttpClient client = HttpClients.custom().build();

httpPost.setEntity(new ByteArrayEntity(body.getBytes(StandardCharsets.UTF_8)));

try (var response = client.execute(httpPost)){
    System.out.println(new
String(response.getEntity().getContent().readAllBytes()));
} catch (IOException e) {
    throw new RuntimeException(e);
}
}
}

```

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 vorhanden ist, verwendet das Beispiel die von angegebene `RegionAWS_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').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: '/',
      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').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: '/',
      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()
  }
)
```

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 administrativen APIs bereit, die zum Erstellen, Lesen/Beschreiben, Aktualisieren, Löschen und Auflisten (CRUDL) von Ressourcen verwendet werden (z. B. und. `CreateService` `UpdateService`). Die Kommunikation mit der Steuerebene von VPC Lattice ist während der Übertragung durch TLS geschützt. Die Datenebene ist die Invoke-API von VPC Lattice, die die Verbindung zwischen Diensten bereitstellt. TLS verschlüsselt auch die Kommunikation mit der Datenebene von VPC Lattice. 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 von Amazon S3 verwalteten Schlüsseln \(SSE-S3\)](#)
- [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 mit einem eindeutigen Schlüssel verschlüsselt. Als zusätzliche Sicherheit verschlüsselt es den Root-Schlüssel selbst mit einem Root-Schlüssel, der regelmäßig rotiert. 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 serverseitige Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) für Ihren S3-Bucket für VPC Lattice-Zugriffsprotokolle aktivieren, verschlüsselt AWS 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 einige zusätzliche Vorteile und Gebühren für die Nutzung dieses Dienstes. Es gibt separate Berechtigungen für die Verwendung eines AWS KMS Schlüssels, 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 des privaten Schlüssels Ihres Zertifikats](#)
- [Verschlüsselungskontext für VPC Lattice](#)
- [Überwachung Ihrer Verschlüsselungsschlüssel für VPC Lattice](#)

Verschlüsselung und Entschlüsselung des privaten Schlüssels Ihres Zertifikats

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 Ihres Zertifikats 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`. Ein Grant ist ein politisches Instrument, das es dem TLS Connection Manager ermöglicht, KMS-Schlüssel für kryptografische Operationen zu verwenden. Die Gewährung ermöglicht es dem Prinzipal des Empfängers (TLS Connection Manager), die angegebenen Grant-Operationen 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 entfernen möchten, empfehlen wir, das Zertifikat mithilfe des `update-service` Befehls 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 zusätzliche Kontextinformationen darüber enthalten, wofür Ihr privater Schlüssel verwendet werden kann. 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.

Um Daten zu entschlüsseln, ist derselbe Verschlüsselungskontext in der Anfrage enthalten. 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.

Das folgende Beispiel zeigt den Verschlüsselungskontext in der Ausgabe eines Vorgangs 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 CloudTrail](#) an 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 unter >> Ereignishistorie>> als Ereignis anzeigen.

CloudTrail **CreateGrant**

Im Folgenden finden Sie ein Beispiel für einen Ereignisdatensatz in der CloudTrail Ereignishistorie 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 werden Sie feststellen, dass der Principal des Empfängers TLS Connection Manager ist und der Verschlüsselungskontext den ARN des VPC-Lattice-Dienstes hat.

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 der AWS CLI , um die Details aller Zuschüsse zu sehen:

```
aws kms list-grants --key-id your-kms-key-id
```

Ihre Ausgabe sollte dem folgenden Beispiel ähneln:

```
{
  "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 werden Sie feststellen, dass der Principal des Empfängers TLS Connection Manager ist und der Verschlüsselungskontext den ARN des VPC-Lattice-Dienstes hat.

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 unter >> Ereignisverlauf >> als Ereignis anzeigen. CloudTrail **Decrypt**

Im Folgenden finden Sie ein Beispiel für einen Ereignisdatensatz in der CloudTrail Ereignishistorie 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-Funktionen, die Sie mit Amazon VPC Lattice verwenden können

IAM-Feature	VPC-Lattice-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja

IAM-Feature	VPC-Lattice-Unterstützung
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 [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

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

Ressourcenbasierte Richtlinien innerhalb von VPC Lattice

Unterstützt ressourcenbasierte Richtlinien	Ja
--	----

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

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 Nutzungsberechtigungen zu erteilen, um die gemeinsame Nutzung von Ressourcen zu ermöglichen. Weitere Informationen finden Sie unter [Teilen Sie Ihre VPC Lattice-Ressourcen](#).

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 `Get` beginnen, 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 ARNs angeben.

Das spezifische Format des Amazon Resource Name (ARN) hängt von der Ressource ab. Wenn Sie einen ARN angeben, ersetzen Sie den *kursiven Text durch* Ihre ressourcenspezifischen Informationen.

- Abonnements für Zugriffsprotokolle:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:accesslogssubscription/access-log-subscription-id"
```

- Zuhörer:

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

- 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
------------------	------

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

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 Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

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

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

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 zu einer Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

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

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 APIs aus aufzurufen. AWS

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.

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](#) im IAM-Benutzerhandbuch.

Einzelheiten zu den von VPC Lattice definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für Amazon VPC Lattice](#) in der Service Authorization Reference.

Inhalt

- [Bewährte Methoden für Richtlinien](#)
- [Für den Vollzugriff sind zusätzliche Berechtigungen erforderlich](#)
- [Beispiele für identitätsbasierte Richtlinien für VPC Lattice](#)

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 [Richtlinienvvalidierung zum 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 [Konfigurieren eines MFA-geschützten API-Zugriffs](#) 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 Vollzugriff 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 es Ihnen, die angegebene verwaltete Richtlinie an die angegebene IAM-Rolle anzuhängen.
- `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

- [VPC-Zuordnungen zu einem Servicenetzwerk verwalten](#)
- [Erstellen Sie Dienstzuordnungen zu einem Servicenetzwerk](#)
- [-Ressourcen Tags hinzufügen](#)
- [Erstellen einer serviceverknüpften Rolle](#)

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"
        }
      }
    }
  ]
}
```

Erstellen Sie Dienstzuordnungen zu einem Servicenetzwerk

Wenn Sie keine Bedingungsschlüssel verwenden, um den Zugriff auf VPC-Lattice-Ressourcen zu steuern, können Sie stattdessen die 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 die ARNs des Dienstes und des Dienstnetzwerks angeben, die mit der API-Aktion verwendet werden können. `CreateServiceNetworkServiceAssociation` Weitere Hinweise zur Angabe der ARN-Werte finden Sie unter [Politische 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"
  ]
}
]
}

```

-Ressourcen Tags hinzufügen

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:*/*"
    }
  ]
}

```

Erstellen einer serviceverknüpften 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.

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"
        }
      }
    }
  ]
}
```

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 [Verwenden von serviceverknüpften Rollen](#) im -IAM-Benutzerhandbuch.

Dienstbezogene Rollenberechtigungen für VPC Lattice

VPC Lattice verwendet die mit dem Dienst verknüpfte Rolle namens `AWSServiceRoleForVpcLattice`

Die `AWSServiceRoleForVpcLattice` dienstverknüpfte Rolle vertraut darauf, dass der folgende Dienst die Rolle übernimmt:

- `vpc-lattice.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie `AWSVpcLatticeServiceRolePolicy` ermöglicht es VPC Lattice, CloudWatch Metriken im Namespace zu veröffentlichen. `AWS/VpcLattice`

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": "cloudwatch:PutMetricData",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "cloudwatch:namespace": "AWS/VpcLattice"
      }
    }
  }
]
```

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 [Serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

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.

Bearbeiten einer serviceverknüpften Rolle für VPC Lattice

Sie können die Beschreibung der Verwendung von `AWSServiceRoleForVpcLatticeIAM` bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften 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 serviceverknüpfte Rolle zu löschen. `AWSServiceRoleForVpcLattice` Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

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 sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [kundenverwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

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

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: `VPC LatticeFullAccess`

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 — Rufen Sie Informationen über EC2-Instances und VPCs ab, um Zielgruppen zu erstellen 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 S3 — Rufen Sie Informationen über S3-Buckets ab, die zum Speichern von Zugriffsprotokollen verwendet werden.

Die Berechtigungen für diese Richtlinie finden Sie unter [VPC LatticeFullAccess](#) in der Referenz für AWS verwaltete 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 Vollzugriff sind zusätzliche Berechtigungen erforderlich](#).

AWS verwaltete Richtlinie: VPC LatticeReadOnlyAccess

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 — Rufen Sie Informationen über EC2-Instances und VPCs ab, um Zielgruppen zu erstellen und Ziele zu 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 S3 — Rufen Sie Informationen zu S3-Buckets für die Zustellung von Zugriffsprotokollen ab.

Die Berechtigungen für diese Richtlinie finden Sie unter [VPC LatticeReadOnlyAccess](#) in der Referenz für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: VPC LatticeServicesInvokeAccess

Diese Richtlinie bietet Zugriff zum Aufrufen der Amazon VPC Lattice-Dienste.

Die Berechtigungen für diese Richtlinie finden Sie unter [VPC LatticeServicesInvokeAccess](#) in der Referenz für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSVpcLatticeServiceRolePolicy

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](#).

Die Berechtigungen für diese Richtlinie finden Sie [AWSVpcLatticeServiceRolePolicy](#) in der Referenz zu 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
VPC LatticeFullAccess	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
VPC LatticeReadOnlyAccess	VPC Lattice fügt eine neue Richtlinie hinzu, um Berechtigungen für	31. März 2023

Änderung	Beschreibung	Datum
	schreibgeschützten Zugriff auf Amazon VPC Lattice und eingeschränkten Zugriff auf andere abhängige Dienste zu gewähren.	
VPC LatticeServicesInvokeAccess	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. <code>AWS/VpcLattice</code> Die <code>AWSVpcLatticeServiceRolePolicy</code> Richtlinie beinhaltet die Erlaubnis, die API-Aktion aufzurufen. CloudWatch PutMetricData Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon VPC Lattice .	5. Dezember 2022
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:

- [Schnellstartanleitungen zu Sicherheit und Compliance](#) — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

 Note

AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der [Referenz für HIPAA-berechtigte Services](#).

- [AWS Compliance-Ressourcen](#) — Diese Sammlung von Arbeitsmapen 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](#)— Auf diese AWS-Service Weise erhalten Sie 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. Eine Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerungsreferenz](#).

- [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 () PrivateLink

Sie können eine private Verbindung zwischen Ihrer VPC und Amazon VPC Lattice herstellen, indem Sie einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellenendpunkte werden von einer Technologie unterstützt [AWS PrivateLink](#), mit der Sie privat auf VPC-Lattice-APIs zugreifen können, ohne dass ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung erforderlich ist. AWS Direct Connect Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit VPC-Lattice-APIs zu kommunizieren.

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](#)
- [Zugriffsprotokolle für Amazon VPC Lattice](#)
- [CloudTrail Protokolle für Amazon VPC Lattice](#)

CloudWatch Metriken für Amazon VPC Lattice

Amazon VPC Lattice sendet Daten zu Ihren Zielgruppen und Services an Amazon und verarbeitet sie zu lesbaren CloudWatch, nahezu in Echtzeit verfügbaren Metriken. Diese Kennzahlen werden 15 Monate lang aufbewahrt, sodass Sie auf historische Informationen zugreifen und sich einen besseren Überblick über die Leistung Ihrer Webanwendung oder Ihres Dienstes verschaffen können. 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

- [CloudWatch Amazon-Metriken anzeigen](#)
- [Kennzahlen für Zielgruppen](#)
- [Servicemetriken](#)

CloudWatch Amazon-Metriken anzeigen

Sie können die CloudWatch Amazon-Metriken für Ihre Zielgruppen und Dienste über die CloudWatch Konsole oder anzeigen AWS CLI.

Um Metriken über die CloudWatch Konsole anzuzeigen

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 Metriken 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 dessen Namen in das Suchfeld ein.

Um Metriken anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den folgenden AWS CLI Befehl [CloudWatch list-metrics](#), um die verfügbaren Metriken aufzulisten:

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

Informationen zu den einzelnen Metriken und ihren Dimensionen finden Sie unter [Kennzahlen für Zielgruppen](#) und [Servicemetriken](#)

Kennzahlen für Zielgruppen

VPC Lattice speichert automatisch Kennzahlen zu Zielgruppen im AWS/VpcLattice [CloudWatch Amazon-Namespace](#). Weitere Informationen zu Zielgruppen finden Sie unter [Zielgruppen in VPC Lattice](#)

Möglicherweise möchten Sie die Zielgruppen überwachen HTTP code und RequestTime Metriken erstellen. Sie können diese Metriken nach Availability Zone (AZ) filtern, um festzustellen, in welcher AZ sich die Zielgruppe befindet.

Metrik	Beschreibung
TotalConnectionCount	<p>Verbindungen insgesamt.</p> <p>Kriterien für die Berichterstattung</p> <ul style="list-style-type: none"> • 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). <p>Häufigkeit der Berichterstattung</p> <ul style="list-style-type: none"> • Einmal pro Minute. <p>Statistiken</p> <ul style="list-style-type: none"> • Die nützlichste Statistik ist Sum. <p>Dimensions (Abmessungen)</p> <ul style="list-style-type: none"> • Name:TargetGroup , Wert: Der Name der Zielgruppe. • Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.
ActiveConnectionCount	<p>Aktive Verbindungen.</p> <p>Kriterien für die Berichterstattung</p> <ul style="list-style-type: none"> • 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). <p>Häufigkeit der Berichterstattung</p> <ul style="list-style-type: none"> • Einmal pro Minute. <p>Statistiken</p>

Metrik	Beschreibung
	<ul style="list-style-type: none"> Die nützlichste Statistik ist Sum. <p>Dimensions (Abmessungen)</p> <ul style="list-style-type: none"> Name:TargetGroup , Wert: Der Name der Zielgruppe. Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.
ConnectionErrorCount	<p>Gesamtzahl der Verbindungsfehler.</p> <p>Kriterien für die Berichterstattung</p> <ul style="list-style-type: none"> 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). <p>Häufigkeit der Berichterstattung</p> <ul style="list-style-type: none"> Einmal pro Minute. <p>Statistiken</p> <ul style="list-style-type: none"> Die nützlichste Statistik ist Sum. <p>Dimensions (Abmessungen)</p> <ul style="list-style-type: none"> Name:TargetGroup , Wert: Der Name der Zielgruppe. Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
HTTP1_ConnectionCount	<p data-bbox="591 226 1179 260">Gesamtzahl der HTTP/1.1-Verbindungen.</p> <p data-bbox="591 306 1057 340">Kriterien für die Berichterstattung</p> <ul data-bbox="591 386 1500 516" style="list-style-type: none">• 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). <p data-bbox="591 592 1037 625">Häufigkeit der Berichterstattung</p> <ul data-bbox="591 672 889 705" style="list-style-type: none">• Einmal pro Minute. <p data-bbox="591 781 740 814">Statistiken</p> <ul data-bbox="591 861 1057 894" style="list-style-type: none">• Die nützlichste Statistik ist Sum. <p data-bbox="591 970 992 1003">Dimensions (Abmessungen)</p> <ul data-bbox="591 1050 1458 1188" style="list-style-type: none">• Name:TargetGroup , Wert: Der Name der Zielgruppe.• Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
HTTP2_ConnectionCount	<p data-bbox="591 226 1154 262">Gesamtzahl der HTTP/2-Verbindungen.</p> <p data-bbox="591 306 1057 342">Kriterien für die Berichterstattung</p> <ul data-bbox="591 386 1474 516" style="list-style-type: none">• 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. <p data-bbox="591 594 1037 630">Häufigkeit der Berichterstattung</p> <ul data-bbox="591 674 889 709" style="list-style-type: none">• Einmal pro Minute. <p data-bbox="591 787 740 823">Statistiken</p> <ul data-bbox="591 867 1057 903" style="list-style-type: none">• Die nützlichste Statistik ist Sum. <p data-bbox="591 980 992 1016">Dimensions (Abmessungen)</p> <ul data-bbox="591 1060 1461 1190" style="list-style-type: none">• Name:TargetGroup , Wert: Der Name der Zielgruppe.• Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
ConnectionTimeoutCount	<p data-bbox="591 226 1398 262">Gesamtzahl der Timeouts bei Verbindungsverbindungen.</p> <p data-bbox="591 306 1057 342">Kriterien für die Berichterstattung</p> <ul data-bbox="591 386 1490 562" style="list-style-type: none">• 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). <p data-bbox="591 640 1037 676">Häufigkeit der Berichterstattung</p> <ul data-bbox="591 720 889 756" style="list-style-type: none">• Einmal pro Minute. <p data-bbox="591 833 740 869">Statistiken</p> <ul data-bbox="591 913 1057 949" style="list-style-type: none">• Die nützlichste Statistik ist Sum. <p data-bbox="591 1026 992 1062">Dimensions (Abmessungen)</p> <ul data-bbox="591 1106 1458 1245" style="list-style-type: none">• Name:TargetGroup , Wert: Der Name der Zielgruppe.• Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
TotalReceivedConnectionBytes	<p data-bbox="591 226 1292 260">Gesamtzahl der empfangenen Verbindungsbytes.</p> <p data-bbox="591 306 1057 340">Kriterien für die Berichterstattung</p> <ul data-bbox="591 386 1507 516" style="list-style-type: none">• 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. <p data-bbox="591 592 1037 625">Häufigkeit der Berichterstattung</p> <ul data-bbox="591 672 889 705" style="list-style-type: none">• Einmal pro Minute. <p data-bbox="591 781 740 814">Statistiken</p> <ul data-bbox="591 861 1057 894" style="list-style-type: none">• Die nützlichste Statistik ist Sum. <p data-bbox="591 970 992 1003">Dimensions (Abmessungen)</p> <ul data-bbox="591 1050 1458 1188" style="list-style-type: none">• Name:TargetGroup , Wert: Der Name der Zielgruppe.• Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
TotalSentConnectionBytes	<p data-bbox="591 226 1263 262">Gesamtzahl der gesendeten Verbindungsbytes.</p> <p data-bbox="591 306 1057 342">Kriterien für die Berichterstattung</p> <ul data-bbox="591 386 1507 516" style="list-style-type: none">• 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. <p data-bbox="591 594 1036 630">Häufigkeit der Berichterstattung</p> <ul data-bbox="591 674 889 709" style="list-style-type: none">• Einmal pro Minute. <p data-bbox="591 787 737 823">Statistiken</p> <ul data-bbox="591 867 1057 903" style="list-style-type: none">• Die nützlichste Statistik ist Sum. <p data-bbox="591 980 992 1016">Dimensions (Abmessungen)</p> <ul data-bbox="591 1060 1458 1190" style="list-style-type: none">• Name:TargetGroup , Wert: Der Name der Zielgruppe.• Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
TotalRequestCount	<p data-bbox="594 226 964 260">Gesamtzahl der Anfragen.</p> <p data-bbox="594 306 1057 340">Kriterien für die Berichterstattung</p> <ul data-bbox="594 386 1500 516" style="list-style-type: none">• 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). <p data-bbox="594 592 1037 625">Häufigkeit der Berichterstattung</p> <ul data-bbox="594 672 889 705" style="list-style-type: none">• Einmal pro Minute. <p data-bbox="594 781 740 814">Statistiken</p> <ul data-bbox="594 861 1057 894" style="list-style-type: none">• Die nützlichste Statistik ist Sum. <p data-bbox="594 970 992 1003">Dimensions (Abmessungen)</p> <ul data-bbox="594 1050 1458 1188" style="list-style-type: none">• Name:TargetGroup , Wert: Der Name der Zielgruppe.• Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
ActiveRequestCount	<p data-bbox="591 226 1073 262">Gesamtzahl der aktiven Anfragen.</p> <p data-bbox="591 306 1057 342">Kriterien für die Berichterstattung</p> <ul data-bbox="591 386 1500 516" style="list-style-type: none"><li data-bbox="591 386 1500 516">• 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). <p data-bbox="591 592 1037 627">Häufigkeit der Berichterstattung</p> <ul data-bbox="591 672 889 707" style="list-style-type: none"><li data-bbox="591 672 889 707">• Einmal pro Minute. <p data-bbox="591 783 740 819">Statistiken</p> <ul data-bbox="591 863 1057 898" style="list-style-type: none"><li data-bbox="591 863 1057 898">• Die nützlichste Statistik ist Sum. <p data-bbox="591 974 992 1010">Dimensions (Abmessungen)</p> <ul data-bbox="591 1054 1458 1184" style="list-style-type: none"><li data-bbox="591 1054 1458 1089">• Name:TargetGroup , Wert: Der Name der Zielgruppe.<li data-bbox="591 1110 1458 1184">• Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
RequestTime	<p data-bbox="591 226 1078 260">Anforderungszeit in Millisekunden.</p> <p data-bbox="591 306 1058 340">Kriterien für die Berichterstattung</p> <ul data-bbox="591 386 1500 516" style="list-style-type: none">• 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). <p data-bbox="591 592 1039 625">Häufigkeit der Berichterstattung</p> <ul data-bbox="591 672 889 705" style="list-style-type: none">• Einmal pro Minute. <p data-bbox="591 781 740 814">Statistiken</p> <ul data-bbox="591 861 1403 945" style="list-style-type: none">• Die nützlichsten Statistiken sind Average und pNN.NN (Perzentile). <p data-bbox="591 1020 993 1054">Dimensions (Abmessungen)</p> <ul data-bbox="591 1100 1458 1243" style="list-style-type: none">• Name:TargetGroup , Wert: Der Name der Zielgruppe.• Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
HTTPCode_2XX_Count, HTTPCode_3XX_Count, HTTPCode_4XX_Count, HTTPCode_5XX_Count	<p data-bbox="591 226 1062 262">Aggregierte HTTP-Antwortcodes.</p> <p data-bbox="591 306 1057 342">Kriterien für die Berichterstattung</p> <ul data-bbox="591 386 1500 516" style="list-style-type: none">• 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). <p data-bbox="591 594 1037 630">Häufigkeit der Berichterstattung</p> <ul data-bbox="591 674 889 709" style="list-style-type: none">• Einmal pro Minute. <p data-bbox="591 787 740 823">Statistiken</p> <ul data-bbox="591 867 1057 903" style="list-style-type: none">• Die nützlichste Statistik ist Sum. <p data-bbox="591 980 992 1016">Dimensions (Abmessungen)</p> <ul data-bbox="591 1060 1459 1190" style="list-style-type: none">• Name:TargetGroup , Wert: Der Name der Zielgruppe.• Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
TLSConnectionError Count	<p data-bbox="591 226 1477 310">Gesamtzahl der TLS-Verbindungsfehler ohne fehlgeschlagene Zertifikatsüberprüfungen.</p> <p data-bbox="591 352 1058 394">Kriterien für die Berichterstattung</p> <ul data-bbox="591 436 1500 567" style="list-style-type: none">• 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). <p data-bbox="591 638 1039 680">Häufigkeit der Berichterstattung</p> <ul data-bbox="591 722 889 764" style="list-style-type: none">• Einmal pro Minute. <p data-bbox="591 835 740 877">Statistiken</p> <ul data-bbox="591 919 1058 961" style="list-style-type: none">• Die nützlichste Statistik ist Sum. <p data-bbox="591 1033 993 1075">Dimensions (Abmessungen)</p> <ul data-bbox="591 1117 1461 1247" style="list-style-type: none">• Name:TargetGroup , Wert: Der Name der Zielgruppe.• Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
TotalTLSConnectionHandshakeCount	<p>Gesamtzahl der erfolgreichen TLS-Verbindungs-Handshakes.</p> <p>Kriterien für die Berichterstattung</p> <ul style="list-style-type: none"> • 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). <p>Häufigkeit der Berichterstattung</p> <ul style="list-style-type: none"> • Einmal pro Minute. <p>Statistiken</p> <ul style="list-style-type: none"> • Die nützlichste Statistik ist Sum. <p>Dimensions (Abmessungen)</p> <ul style="list-style-type: none"> • Name:TargetGroup , Wert: Der Name der Zielgruppe. • Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Servicemetriken

VPC Lattice speichert automatisch Metriken zu Services im AWS/VpcLattice [CloudWatch Amazon-Namespace](#). Weitere Informationen zu Services finden Sie unter [Dienstleistungen in VPC Lattice](#).

Möglicherweise möchten Sie Dienste überwachen HTTP code und RequestTime Metriken erstellen. Sie können diese Metriken nach Availability Zone (AZ) filtern, um festzustellen, in welcher AZ sich der Service befindet.

Metrik	Beschreibung
RequestTimeoutCount	<p data-bbox="592 254 1487 331">Gesamtzahl der Anfragen, bei denen das Timeout beim Warten auf eine Antwort überschritten wurde.</p> <p data-bbox="592 380 1057 415">Kriterien für die Berichterstattung</p> <ul data-bbox="592 464 1500 590" style="list-style-type: none"> • 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). <p data-bbox="592 667 1037 703">Häufigkeit der Berichterstattung</p> <ul data-bbox="592 751 889 787" style="list-style-type: none"> • Einmal pro Minute. <p data-bbox="592 856 740 892">Statistiken</p> <ul data-bbox="592 940 1057 976" style="list-style-type: none"> • Die nützlichste Statistik ist Sum. <p data-bbox="592 1052 992 1087">Dimensions (Abmessungen)</p> <ul data-bbox="592 1136 1458 1262" style="list-style-type: none"> • Name:Service, Wert: Die ID des Dienstes. • Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.
TotalRequestCount	<p data-bbox="592 1318 964 1354">Gesamtzahl der Anfragen.</p> <p data-bbox="592 1402 1057 1438">Kriterien für die Berichterstattung</p> <ul data-bbox="592 1486 1500 1612" style="list-style-type: none"> • 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). <p data-bbox="592 1690 1037 1726">Häufigkeit der Berichterstattung</p> <ul data-bbox="592 1774 889 1810" style="list-style-type: none"> • Einmal pro Minute.

Metrik	Beschreibung
	<p>Statistiken</p> <ul style="list-style-type: none"> Die nützlichste Statistik ist Sum. <p>Dimensions (Abmessungen)</p> <ul style="list-style-type: none"> Name:Service, Wert: Die ID des Dienstes. Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.
RequestTime	<p>Anforderungszeit in Millisekunden.</p> <p>Kriterien für die Berichterstattung</p> <ul style="list-style-type: none"> 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). <p>Häufigkeit der Berichterstattung</p> <ul style="list-style-type: none"> Einmal pro Minute. <p>Statistiken</p> <ul style="list-style-type: none"> Die nützlichsten Statistiken sind Average und pNN.NN (Perzentile). <p>Dimensions (Abmessungen)</p> <ul style="list-style-type: none"> Name:Service, Wert: Die ID des Dienstes. Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Metrik	Beschreibung
HTTPCode_2XX_Count , HTTPCode_3XX_Count , HTTPCode_4XX_Count , HTTPCode_5XX_Count	<p>Aggregierte HTTP-Antwortcodes.</p> <p>Kriterien für die Berichterstattung</p> <ul style="list-style-type: none"> • 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). <p>Häufigkeit der Berichterstattung</p> <ul style="list-style-type: none"> • Einmal pro Minute. <p>Statistiken</p> <ul style="list-style-type: none"> • Die nützlichste Statistik ist Sum. <p>Dimensions (Abmessungen)</p> <ul style="list-style-type: none"> • Name:Service, Wert: Die ID des Dienstes. • Name:AvailabilityZone , Wert: Die AZ, in der sich die Zielgruppe befindet.

Zugriffsprotokolle für Amazon VPC Lattice

Zugriffsprotokolle erfassen detaillierte Informationen zu Ihren VPC Lattice-Diensten. Sie können diese Zugriffsprotokolle verwenden, um Verkehrsmuster zu analysieren und alle Dienste im Netzwerk zu überprüfen.

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

- [Für die Aktivierung von Zugriffsprotokollen sind IAM-Berechtigungen erforderlich](#)
- [Ziele der Zugriffsprotokolle](#)
- [Aktivieren der Zugriffsprotokolle](#)
- [Inhalt des Zugriffsprotokolls](#)
- [Beheben Sie Probleme mit 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": "ManageVPCAccessLogSetup",
      "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
```

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](#)
- [Aktivieren Sie die Zugriffsprotokolle mit dem AWS CLI](#)

Aktivieren Sie die Zugriffsprotokolle mithilfe der Konsole

Sie können während der Erstellung Zugriffsprotokolle für ein Dienstnetzwerk oder für einen Dienst aktivieren. Sie können Zugriffsprotokolle auch aktivieren, nachdem Sie ein Dienstnetzwerk oder einen Dienst 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 Servicenetzwerk oder den Dienst aus.
3. Wählen Sie Aktionen, Protokolleinstellungen bearbeiten aus.
4. Schalten Sie den Schalter Zugriffsprotokolle ein.
5. Fügen Sie wie folgt ein Zustellungsziel 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.	<i>arn:aws:vpc-lattice:region:konto:service-network/id</i>
resolvedUser	Der ARN des Benutzers, wenn die Authentifizierung aktiviert	null ARN „Anonym“ „Unbekannt“

Feld	Beschreibung	Format
	ist und die Authentifizierung abgeschlossen ist.	
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.	<i>TLSv x</i>
userAgent	Der User-Agent-Header.	Zeichenfolge
ServerNameIndication	[Nur HTTPS] Der Wert, der auf dem SSL-Verbindungs-Socket für Server Name Indication (SNI) festgelegt ist.	Zeichenfolge
destinationVpcId	Die Ziel-VPC-ID.	<i>vpc-xxxxxxx</i>
sourceIpPort	Die IP-Adresse und:Port der Quelle.	<i>ip: Port</i>
targetIpPort	Die IP-Adresse und der Port des Ziels.	<i>ip: Anschluss</i>
serviceArn	Der Dienst ARN.	<i>arn:aws:vpc-lattice: region: konto:service/id</i>
sourceVpcId	Die Quell-VPC-ID.	<i>vpc-xxxxxxx</i>
requestPath	Den Pfad der Anfrage.	LatticePath? : <i>Pfad</i>

Feld	Beschreibung	Format
startTime	Die Startzeit der Anfrage.	<i>YYYY - MM - DD T HH:MM: SS Z</i>
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 Beheben Sie Probleme mit 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
<code>grpcResponseCode</code>	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
<code>callerPrincipal</code>	Der authentifizierte Prinzipal.	Zeichenfolge
<code>callerX509SubjectCN</code>	Der Name des Antragstellers (CN).	Zeichenfolge
<code>callerX509IssuerOU</code>	Der Emittent (OU).	Zeichenfolge
<code>callerX509SANNameCN</code>	Die Alternative des Emittenten (Name/CN).	Zeichenfolge
<code>callerX509SANDNS</code>	Der alternative Name des Antragstellers (DNS).	Zeichenfolge
<code>callerX509SANURI</code>	Der alternative Name (URI) des Antragstellers.	Zeichenfolge
<code>sourceVpcArn</code>	Der ARN der VPC, von der die Anfrage stammt.	<i>arn:aws:ec2: region: konto:vpc/id</i>

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
}

```

Beheben Sie Probleme mit Zugriffsprotokollen

Dieser Abschnitt enthält eine Erläuterung der HTTP-Fehlercodes, die Sie möglicherweise in Zugriffsprotokollen sehen.

Fehlercode	Mögliche Ursachen
HTTP 400: Bad Request (Schlechte Anfrage)	<ul style="list-style-type: none"> 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.

Fehlercode	Mögliche Ursachen
HTTP 404: Dienst existiert nicht	Sie versuchen, eine Verbindung zu einem Dienst herzustellen, der nicht existiert oder der nicht im richtigen Dienstnetzwerk registriert ist.
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

AWS CloudTrail ist ein AWS Dienst, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführt wurden. CloudTrail erfasst API-Aufrufe für VPC Lattice als Ereignisse. CloudTrail ist auf Ihrem aktiviert, AWS-Konto wenn Sie es erstellen. Wenn eine Aktivität in VPC Lattice auftritt, wird diese Aktivität zusammen mit anderen AWS Dienstereignissen im CloudTrail Ereignisverlauf als Ereignis aufgezeichnet. Zu den erfassten Aufrufen gehören Aufrufe von der VPC Lattice-Konsole und Codeaufrufen für VPC Lattice-API-Operationen. [Weitere Informationen zu finden Sie im CloudTrail Benutzerhandbuch.AWS CloudTrail](#)

CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden. Ein Trail ist eine CloudTrail Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen S3-Bucket ermöglicht.

Verwenden Sie Zugriffsprotokolle, um zusätzliche Aktionen zu überwachen. Weitere Informationen finden Sie unter [Zugriffsprotokolle](#).

Die Einträge in der VPC Lattice-Protokolldatei verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion,

Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Informationen zu Schlüssel-Wert-Paaren in den Protokollen finden Sie im AWS CloudTrail Benutzerhandbuch unter [CloudTrail Datensatzinhalte](#).

Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag für einen Aufruf der [CreateServiceAPI](#)-Aktion.

```
{
  "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"
}

```

Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag für einen Aufruf der [DeleteServiceAPI](#)-Aktion.

```

{
  "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"
}
```

Kontingente für Amazon VPC Lattice

Ihr AWS-Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jedes AWS-Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Um die Kontingente für VPC Lattice anzuzeigen, öffnen Sie die [Service Quotas-Konsole](#). Wählen Sie im Navigationsbereich VPC Lattice AWS-Services und dann aus.

Um eine Kontingenterhöhung zu beantragen, wenden Sie sich an den - AWS Support oder siehe [Anfordern einer Kontingenterhöhung](#) im Benutzerhandbuch für Service Quotas.

Ihr AWS-Konto verfügt über die folgenden Kontingente im Zusammenhang mit 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.
Listener pro Service	Jede unterstützte Region: 2	Ja	Die maximale Anzahl von Listenern, die Sie für einen Service erstellen können. Für zusätzliche Kapazitäts- und Limiterhöhungen wenden Sie sich an den - AWS Support.
Regeln pro Listener	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 Zuordnung	Jede unterstützte Region: 5	Nein	Die maximale Anzahl von Sicherheitsgruppen, die Sie einer Zuordnung zwischen einer VPC und einem Servicenetzwerk hinzufügen können.
Servicezuordnungen pro Servicenetzwerk	Jede unterstützte Region: 500	Ja	Die maximale Anzahl von Services, die Sie einem einzelnen Servicenetzwerk zuordnen können. Für zusätzliche Kapazitäts- 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 Limiterhöhungen wenden Sie sich an den - AWS Support.
Services pro Region	Jede unterstützte Region: 500	Ja	Die maximale Anzahl von Services pro Region. Für zusätzliche Kapazitäts- 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 Kapazität s- 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 Kapazität s- und Limiterhöhungen wenden Sie sich an den - AWS Support.
VPC-Zuordnungen pro Servicenetzwerk	Jede unterstützte Region: 500	Ja	Die maximale Anzahl von VPCs, die Sie einem einzelnen Servicenetzwerk zuordnen können. Für zusätzliche Kapazität s- und Limiterhöhungen wenden Sie sich an den - AWS Support.

Es gelten auch die folgenden Limits.

Limit	Wert
Bandbreite pro Service und Availability Zone	10 Gbit/s
Maximale Übertragungseinheit (MTU) pro Verbindung	8 500 Byte
Anforderungen pro Sekunde, Service und Availability Zone	10.000

Dokumentenverlauf für das Amazon VPC Lattice- Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für VPC Lattice beschrieben.

Änderung	Beschreibung	Datum
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 gemeinsam genutzte 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-Support	VPC Lattice unterstützt jetzt sowohl IPv4- als auch IPv6-IP-Zielgruppen.	27. März 2023
HTTP2-Protokollversion für Zustandsprüfungen	Integritätsprüfungen werden jetzt unterstützt, wenn die Zielgruppenprotokollversion HTTP2 ist.	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.