Panduan Pengguna

Kisi VPC Amazon

Kisi VPC Amazon: Panduan Pengguna

Table of Contents

Apa itu Amazon VPC Lattice?

Amazon VPC Lattice adalah layanan jaringan aplikasi terkelola penuh yang Anda gunakan untuk menghubungkan, mengamankan, dan memantau layanan untuk aplikasi Anda. Anda dapat menggunakan VPC Lattice dengan satu virtual private cloud (VPC) atau di beberapa VPC dari satu atau beberapa akun.

Aplikasi modern dapat terdiri dari beberapa layanan kecil dan modular, yang sering disebut layanan mikro. Meskipun modernisasi memiliki kelebihan, modernisasi juga dapat memperkenalkan kompleksitas dan tantangan jaringan saat Anda menghubungkan layanan mikro ini. Misalnya, jika pengembang tersebar di tim yang berbeda, mereka mungkin membangun dan menyebarkan layanan mikro di beberapa akun atau VPC.

Dalam VPC Lattice, kami menyebut layanan mikro sebagai layanan. Ini adalah kata-kata yang Anda lihat dalam dokumentasi VPC Lattice.

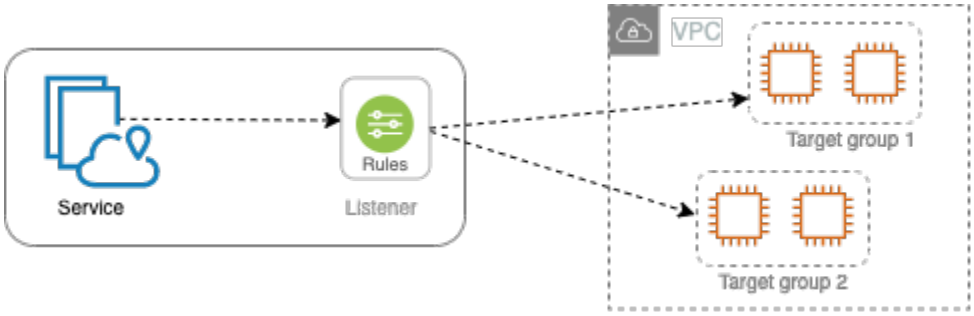
Daftar Isi

Komponen kunci

Untuk menggunakan Amazon VPC Lattice, Anda harus terbiasa dengan komponen utamanya.

Layanan

> Unit perangkat lunak yang dapat digunakan secara independen yang memberikan tugas atau fungsi tertentu. Layanan dapat berjalan pada instans EC2 atau kontainer ECS, atau sebagai fungsi Lambda, dalam akun atau virtual private cloud (VPC). Layanan VPC Lattice memiliki komponen berikut: grup target, pendengar, dan aturan.



Grup target

Kumpulan sumber daya, juga dikenal sebagai target, yang menjalankan aplikasi atau layanan Anda. Target dapat berupa instans EC2, alamat IP, fungsi Lambda, Application Load Balancers, atau Kubernetes Pods. Ini mirip dengan kelompok sasaran yang disediakan oleh Elastic Load Balancing, tetapi mereka tidak dapat dipertukarkan.

Listener

Proses yang memeriksa permintaan koneksi, dan merutekkannya ke target dalam grup target. Anda mengonfigurasi pendengar dengan protokol dan nomor port.

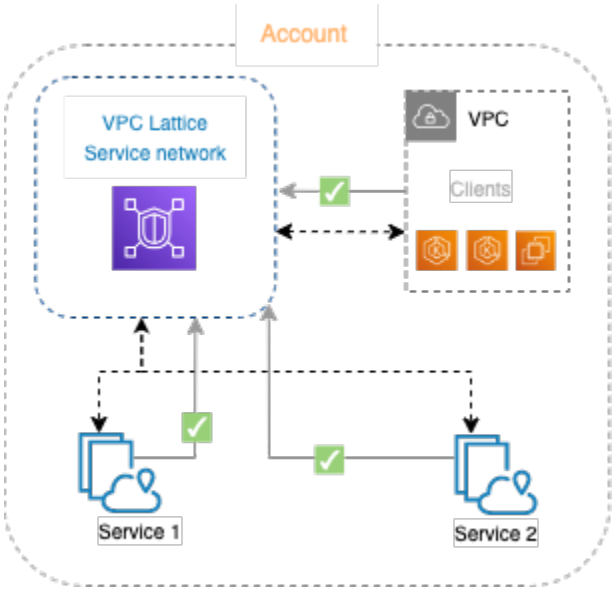
Aturan

Komponen default dari listener yang meneruskan permintaan ke target dalam grup target VPC Lattice. Setiap aturan terdiri dari prioritas, satu atau beberapa tindakan, dan satu atau beberapa syarat. Aturan menentukan cara pendengar merutekan permintaan klien.

Jaringan layanan

Batas logis untuk kumpulan layanan. Klien adalah sumber daya apa pun yang digunakan dalam VPC yang terkait dengan jaringan layanan. Klien dan layanan yang terkait dengan jaringan layanan yang sama dapat berkomunikasi satu sama lain jika mereka berwenang untuk melakukannya.

Pada gambar berikut, klien dapat berkomunikasi dengan kedua layanan, karena VPC dan layanan dikaitkan dengan jaringan layanan yang sama.



Direktori layanan

Registri pusat dari semua layanan VPC Lattice yang Anda miliki atau dibagikan dengan akun Anda melalui AWS Resource Access Manager ().AWS RAM

Kebijakan autentikasi

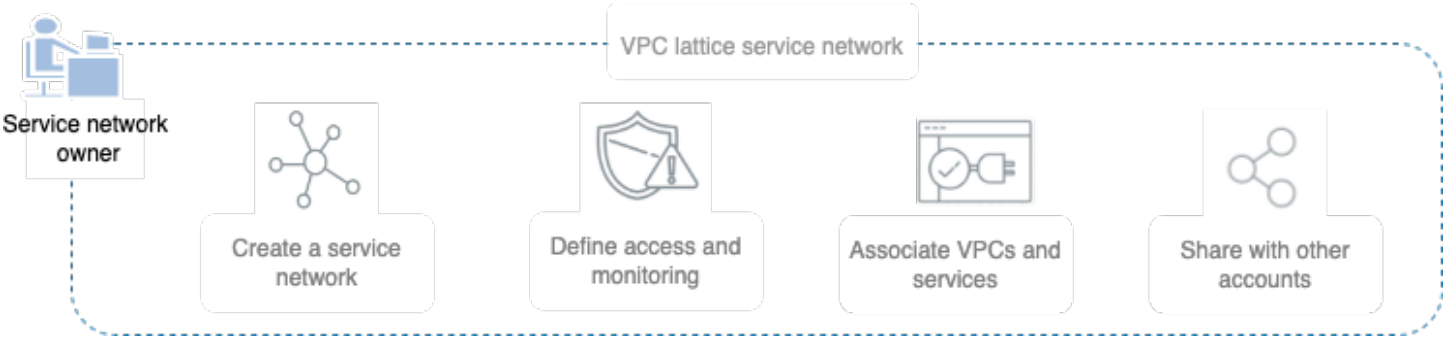
Kebijakan otorisasi berbutir halus yang dapat digunakan untuk menentukan akses ke layanan. Anda dapat melampirkan kebijakan autentikasi terpisah ke layanan individual atau ke jaringan layanan. Misalnya, Anda dapat membuat kebijakan tentang bagaimana layanan pembayaran yang berjalan pada grup penskalaan otomatis instans EC2 harus berinteraksi dengan layanan penagihan yang sedang berjalan. AWS Lambda

Peran dan tanggung jawab

Peran menentukan siapa yang bertanggung jawab atas penyiapan dan aliran informasi dalam Amazon VPC Lattice. Biasanya ada dua peran, pemilik jaringan layanan dan pemilik layanan, dan tanggung jawab mereka dapat tumpang tindih.

Pemilik jaringan layanan — Pemilik jaringan layanan biasanya administrator jaringan atau administrator cloud dalam suatu organisasi. Pemilik jaringan layanan membuat, berbagi, dan menyediakan jaringan layanan. Mereka juga mengelola siapa yang dapat mengakses jaringan layanan atau layanan dalam VPC Lattice. Pemilik jaringan layanan dapat menentukan pengaturan akses berbutir kasar untuk layanan yang terkait dengan jaringan layanan. Kontrol ini digunakan untuk mengelola komunikasi antara klien dan layanan menggunakan kebijakan otentikasi dan otorisasi.

Pemilik jaringan layanan juga dapat mengaitkan layanan dengan jaringan layanan, jika layanan dibagikan dengan akun pemilik jaringan layanan.



Pemilik layanan — Pemilik layanan biasanya adalah pengembang perangkat lunak dalam suatu organisasi. Pemilik layanan membuat layanan dalam VPC Lattice, menentukan aturan perutean, dan juga mengaitkan layanan dengan jaringan layanan. Mereka juga dapat menentukan pengaturan akses berbutir halus, yang dapat membatasi akses hanya ke layanan dan klien yang diautentikasi dan resmi.

Fitur

Berikut ini adalah fitur inti yang disediakan VPC Lattice.

Penemuan Layanan

Semua klien dan layanan dalam VPC yang terkait dengan jaringan layanan dapat berkomunikasi dengan layanan lain dalam jaringan layanan yang sama. DNS mengarahkan client-to-service dan service-to-service lalu lintas melalui titik akhir VPC Lattice. Ketika klien ingin mengirim permintaan ke layanan, ia menggunakan nama DNS layanan. Resolver Route 53 mengirimkan lalu lintas ke VPC Lattice, yang kemudian mengidentifikasi layanan tujuan.

Konektivitas

lient-to-service Konektivitas C dibuat menggunakan bidang data VPC Lattice dalam infrastruktur jaringan. AWS Ketika Anda mengaitkan VPC dengan jaringan layanan, setiap klien dalam VPC dapat terhubung dengan layanan di jaringan layanan, jika mereka memiliki akses yang diperlukan.

Observabilitas

VPC Lattice menghasilkan metrik dan log untuk setiap permintaan dan respons yang melintasi jaringan layanan, untuk membantu Anda memantau dan memecahkan masalah aplikasi. Secara default, VPC Lattice menerbitkan metrik di akun pemilik layanan, dan memberi Anda opsi untuk mengaktifkan logging. Jika klien juga terkait dengan jaringan layanan yang sama, pemilik jaringan layanan menerima log untuk semua layanan yang terkait dengan jaringan layanan. Pemilik layanan menerima log untuk semua klien yang mengajukan permintaan ke layanan mereka.

VPC Lattice bekerja dengan alat berikut untuk membantu Anda memantau dan memecahkan masalah layanan Anda: CloudWatch grup log, aliran pengiriman Firehose, dan bucket S3.

Keamanan

VPC Lattice menyediakan kerangka kerja yang dapat Anda gunakan untuk menerapkan strategi pertahanan di beberapa lapisan jaringan. Lapisan pertama adalah layanan dan asosiasi VPC. Tanpa VPC dan asosiasi layanan, klien tidak dapat mengakses layanan. Lapisan kedua memungkinkan pengguna untuk melampirkan grup keamanan ke asosiasi antara VPC dan jaringan layanan. Lapisan ketiga dan keempat adalah kebijakan autentikasi yang dapat diterapkan secara individual di tingkat jaringan layanan dan tingkat layanan.

Cara kerja VPC Lattice

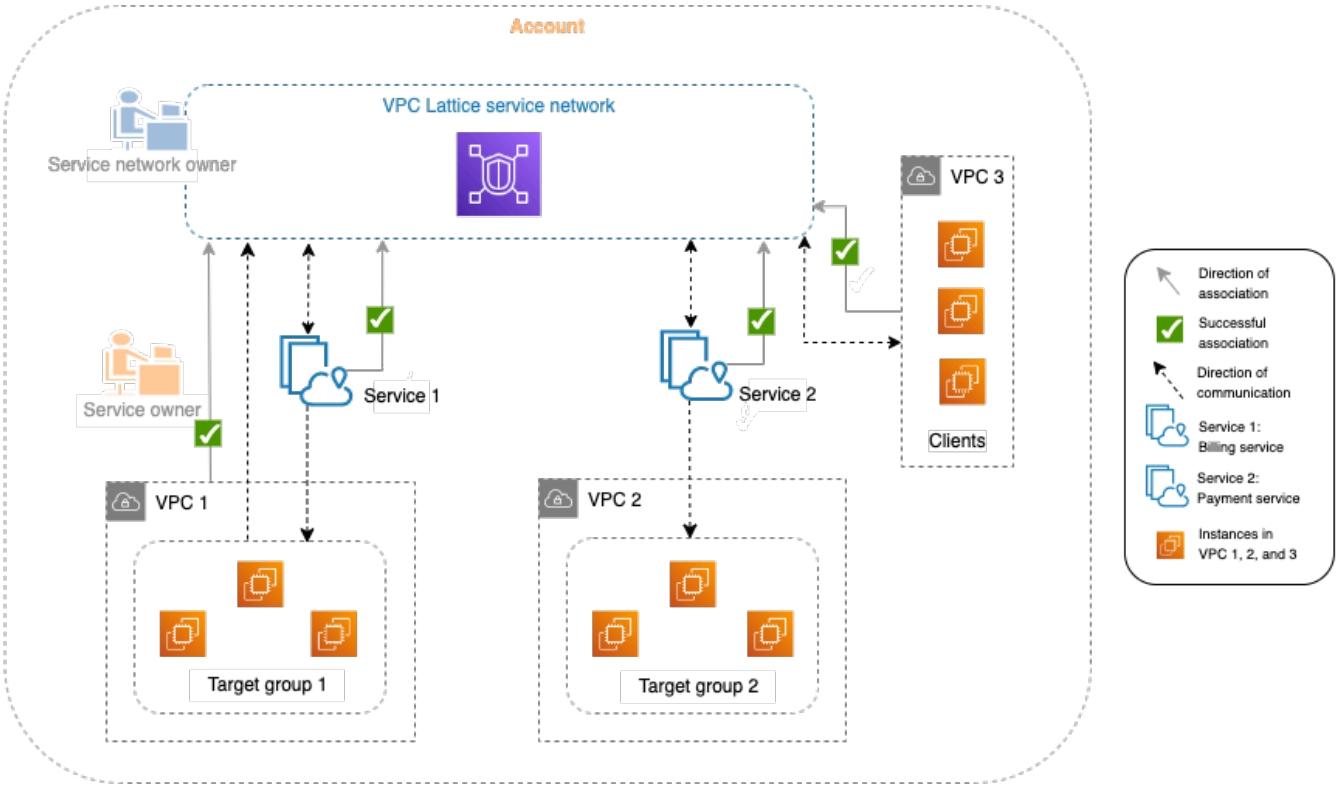
VPC Lattice dirancang untuk membantu Anda menemukan, mengamankan, menghubungkan, dan memantau semua layanan di dalamnya dengan mudah dan efektif. Setiap komponen dalam VPC Lattice berkomunikasi secara searah atau dua arah dalam jaringan layanan berdasarkan hubungannya dengan jaringan layanan dan pengaturan aksesnya. Pengaturan akses terdiri dari kebijakan otentikasi dan otorisasi yang diperlukan untuk komunikasi ini.

Ringkasan berikut menjelaskan komunikasi antar komponen dalam VPC Lattice:

- Layanan yang terkait dengan jaringan layanan dapat menerima permintaan dari klien yang VPC-nya juga terkait dengan jaringan layanan.

- Klien dapat mengirim permintaan ke layanan yang terkait dengan jaringan layanan hanya jika berada di VPC yang terkait dengan jaringan layanan yang sama. Lalu lintas klien yang melintasi koneksi peering VPC atau gateway transit ditolak.
- Klien tidak dapat mengirim permintaan ke klien di VPC lain yang terkait dengan jaringan layanan.
- Target layanan dalam VPC yang terkait dengan jaringan layanan juga klien dan dapat mengirim permintaan ke layanan lain yang terkait dengan jaringan layanan.
- Target layanan di VPC yang tidak terkait dengan jaringan layanan bukanlah klien dan tidak dapat mengirim permintaan ke layanan lain yang terkait dengan jaringan layanan.

Diagram alir berikut menggunakan contoh skenario untuk menjelaskan aliran informasi dan arah komunikasi antara komponen dalam VPC Lattice. Ada dua layanan yang terkait dengan jaringan layanan. Kedua layanan dan ketiga VPC dibuat dalam akun yang sama dengan jaringan layanan. Kedua layanan dikonfigurasi untuk memungkinkan lalu lintas dari jaringan layanan.



Layanan 1 adalah aplikasi penagihan yang berjalan pada sekelompok instance yang terdaftar dengan grup target 1 di VPC 1. Layanan 2 adalah aplikasi pembayaran yang berjalan pada sekelompok instance yang terdaftar dengan grup target 2 di VPC 2. VPC 3 ada di akun yang sama, dan memiliki klien tetapi tidak ada layanan.

Daftar berikut menjelaskan, secara berurutan, alur kerja tipikal tugas untuk VPC Lattice.

1. Buat jaringan layanan

   Pemilik jaringan layanan membuat jaringan layanan.

2. Buat layanan

   Pemilik layanan membuat layanan masing-masing, layanan 1 dan layanan 2. Selama pembuatan, pemilik layanan menambahkan pendengar dan menentukan aturan untuk permintaan perutean ke grup target untuk setiap layanan.

3. Tentukan perutean

   Pemilik layanan membuat grup target untuk setiap layanan (grup target 1 dan grup target 2). Mereka melakukan ini dengan menentukan sumber daya yang ditargetkan di mana layanan dijalankan; misalnya, contoh. Mereka juga menentukan VPC di mana target ini berada.

   Dalam diagram sebelumnya, panah putus-putus yang menunjuk ke kelompok sasaran dari layanan mewakili lalu lintas yang mengalir dari setiap layanan ke kelompok sasaran masing-masing. Panah putus-putus mewakili arah komunikasi antara layanan dan kelompok sasaran.

4. Mengaitkan layanan dengan jaringan layanan

   Pemilik jaringan layanan atau pemilik layanan mengaitkan layanan dengan jaringan layanan. Asosiasi ditampilkan sebagai panah dengan tanda centang yang menunjuk ke jaringan layanan dari layanan. Ketika Anda mengaitkan layanan dengan jaringan layanan, layanan tersebut dapat ditemukan oleh layanan dan klien lain di VPC yang terkait dengan jaringan layanan.

   Panah putus-putus dua arah antara layanan dan jaringan layanan mewakili komunikasi dua arah sebagai hasil dari asosiasi. Panah putus-putus dari jaringan layanan ke layanan mewakili layanan yang menerima permintaan dari klien. Panah putus-putus di arah yang berlawanan, yaitu dari layanan ke jaringan layanan, mewakili layanan yang menanggapi permintaan klien melalui jaringan layanan.

5. Kaitkan VPC dengan jaringan layanan

   Pemilik jaringan layanan mengaitkan VPC 1 dan VPC 3 dengan jaringan layanan. Asosiasi ditampilkan panah dengan tanda centang menunjuk ke jaringan layanan. Dengan asosiasi ini, target dalam VPC ini menjadi klien, dan dapat membuat permintaan ke layanan terkait. Panah putus-putus dua arah antara VPC 3 dan jaringan layanan mewakili komunikasi dua arah antara klien (misalnya, contoh) di VPC 3 dan jaringan layanan sebagai hasil dari asosiasi. Demikian pula, panah putus-putus yang menunjuk dari grup target 1 ke jaringan layanan mewakili klien yang membuat permintaan ke layanan lain yang terkait dengan jaringan layanan.

Perhatikan bahwa VPC 2 tidak memiliki tanda panah atau tanda centang yang mewakili asosiasi. Ini berarti bahwa pemilik jaringan layanan atau pemilik layanan belum mengaitkan VPC 2 dengan jaringan layanan. Ini karena layanan 2, dalam contoh ini, hanya perlu menerima permintaan dan mengirim tanggapan menggunakan permintaan yang sama. Dengan kata lain, target untuk layanan 2 bukan klien dan tidak perlu membuat permintaan ke layanan lain di jaringan layanan.

Mengakses Kisi VPC

Anda dapat membuat, mengakses, dan mengelola VPC Lattice menggunakan salah satu antarmuka berikut:

- AWS Management Console— Menyediakan antarmuka web yang dapat Anda gunakan untuk mengakses VPC Lattice.
- AWS Command Line Interface (AWS CLI) — Menyediakan perintah untuk serangkaian AWS layanan yang luas, termasuk VPC Lattice. AWS CLI Ini didukung di Windows, macOS, dan Linux. Untuk informasi lebih lanjut tentang CLI, lihat. AWS Command Line Interface Untuk informasi selengkapnya tentang API, lihat Referensi API Kisi VPC Amazon.
- VPC Lattice Controller for Kubernetes — Mengelola resource VPC Lattice untuk klaster Kubernetes. Untuk informasi selengkapnya tentang penggunaan VPC Lattice dengan Kubernetes, lihat Panduan Pengguna Gateway API Controller.AWS
- AWS CloudFormation— Membantu Anda memodelkan dan mengatur AWS sumber daya Anda. Untuk informasi selengkapnya, lihat referensi jenis sumber daya Amazon VPC Lattice.

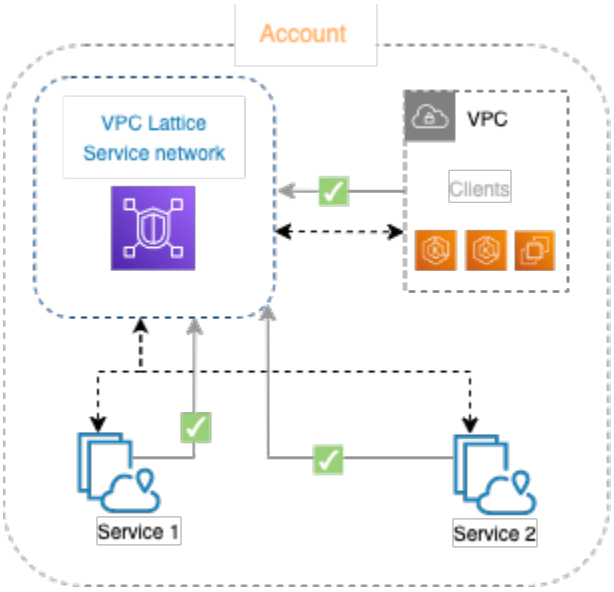
Harga

Dengan VPC Lattice Anda membayar untuk waktu penyediaan layanan, jumlah data yang ditransfer melalui setiap layanan, dan jumlah permintaan. Untuk informasi selengkapnya, lihat Harga Kisi VPC Amazon.

Jaringan layanan di VPC Lattice

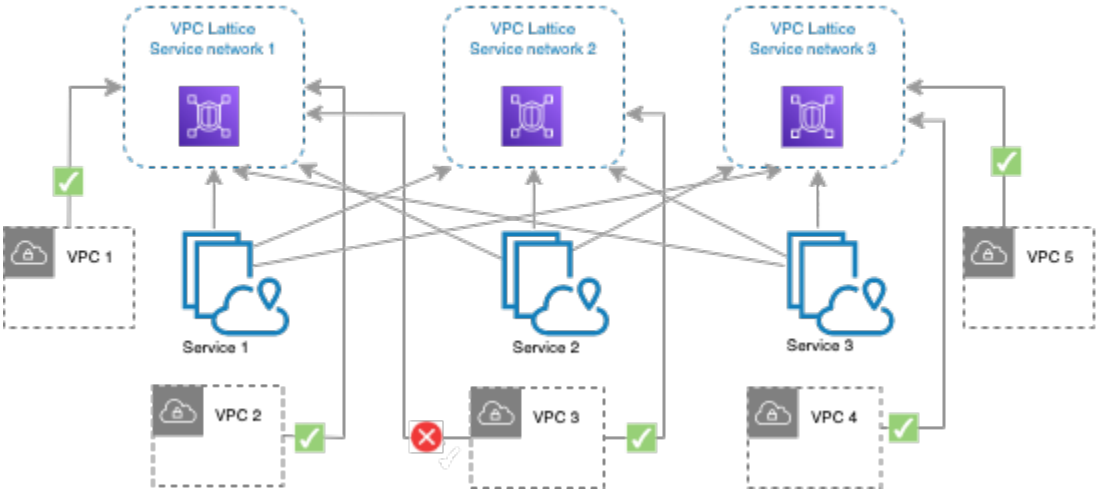
Jaringan layanan adalah batas logis untuk kumpulan layanan. Layanan yang terkait dengan jaringan dapat diotorisasi untuk penemuan, konektivitas, aksesibilitas, dan observabilitas. Untuk membuat permintaan ke layanan di jaringan, layanan atau klien Anda harus dalam VPC yang terkait dengan jaringan layanan.

Diagram berikut menunjukkan komponen kunci dari jaringan layanan tipikal dalam Amazon VPC Lattice. Tanda centang pada panah menunjukkan bahwa layanan dan VPC dikaitkan dengan jaringan layanan. Klien di VPC yang terkait dengan jaringan layanan dapat berkomunikasi dengan kedua layanan melalui jaringan layanan.



Anda dapat mengaitkan satu atau lebih layanan dengan beberapa jaringan layanan. Anda juga dapat mengaitkan beberapa VPC dengan satu jaringan layanan. Namun, setiap VPC dapat dikaitkan dengan hanya satu jaringan layanan.

Dalam diagram berikut, panah mewakili asosiasi antara layanan dan jaringan layanan, serta asosiasi antara VPC dan jaringan layanan. Anda dapat melihat bahwa beberapa layanan terkait dengan beberapa jaringan layanan, dan beberapa VPC terkait ke setiap jaringan layanan. Namun, tanda x merah pada diagram menunjukkan bahwa setiap VPC dapat memiliki tidak lebih dari satu asosiasi ke jaringan layanan.



Untuk informasi selengkapnya, lihat Kuota untuk Amazon VPC Lattice.

Buat jaringan layanan

Gunakan konsol untuk membuat jaringan layanan dan secara opsional mengkonfigurasinya dengan layanan, asosiasi, pengaturan akses, dan log akses.

Untuk membuat jaringan layanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Jaringan layanan.
3. Pilih Buat jaringan layanan.
4. Untuk Pengidentifikasi, masukkan nama, deskripsi opsional, dan tag opsional. Nama harus antara 3 dan 63 karakter. Anda dapat menggunakan huruf kecil, angka, dan tanda hubung. Nama harus dimulai dan diakhiri dengan huruf atau angka. Jangan gunakan tanda hubung berturut-turut. Deskripsi dapat memiliki hingga 256 karakter. Untuk menambahkan tag, pilih Tambahkan tag baru dan tentukan kunci tag dan nilai tag.
5. (Opsional) Untuk mengaitkan layanan, pilih layanan dari asosiasi Layanan, Layanan. Daftar ini mencakup layanan yang ada di akun Anda dan layanan apa pun yang dibagikan dengan Anda dari akun yang berbeda. Jika tidak ada layanan dalam daftar, Anda dapat membuat layanan dengan memilih layanan Create an VPC Lattice.

   Atau, untuk mengaitkan layanan setelah Anda membuat jaringan layanan, lihatthe section called “Kelola asosiasi layanan”.

6. (Opsional) Untuk mengaitkan VPC, pilih Tambahkan asosiasi VPC. Pilih VPC untuk diasosiasikan dari VPC, dan pilih hingga lima grup keamanan dari grup Keamanan. Untuk membuat grup keamanan, pilih Buat grup keamanan baru.

   Atau, untuk mengaitkan VPC setelah Anda membuat jaringan layanan, lihatthe section called "Kelola asosiasi VPC".

7. Untuk akses Jaringan, Anda dapat meninggalkan jenis autentikasi default, Tidak Ada, jika Anda ingin klien di VPC terkait mengakses layanan di jaringan layanan ini. Untuk menerapkan kebijakan autentikasi untuk mengontrol akses ke layanan Anda, pilih AWS IAM dan lakukan salah satu hal berikut untuk kebijakan Auth:
   - Masukkan kebijakan di kolom input. Misalnya kebijakan yang dapat Anda salin dan tempel, pilih Contoh kebijakan.
   - Pilih Terapkan templat kebijakan dan pilih templat Izinkan akses yang diautentikasi dan tidak diautentikasi. Template ini memungkinkan klien dari akun lain untuk mengakses layanan baik dengan menandatangani permintaan (artinya diautentikasi) atau secara anonim (artinya tidak diautentikasi).
   - Pilih Terapkan templat kebijakan dan pilih templat Izinkan hanya akses yang diautentikasi. Template ini memungkinkan klien dari akun lain untuk mengakses layanan hanya dengan menandatangani permintaan (artinya diautentikasi).
8. (Opsional) Untuk mengaktifkan log akses, pilih sakelar sakelar akses log dan tentukan tujuan untuk log akses Anda sebagai berikut:
   - Pilih Grup CloudWatch log dan pilih grup CloudWatch Log. Untuk membuat grup log, pilih Buat grup log masuk CloudWatch.
   - Pilih bucket S3 dan masukkan path bucket S3, termasuk awalan apa pun. Untuk mencari bucket S3 Anda, pilih Browse S3.
   - Pilih aliran pengiriman Kinesis Data Firehose dan pilih aliran pengiriman. Untuk membuat aliran pengiriman, pilih Buat aliran pengiriman di Kinesis.
9. (Opsional) Untuk berbagi jaringan layanan Anda dengan akun lain, pilih pembagian AWS RAM sumber daya dari pembagian Sumber Daya. Untuk membuat pembagian sumber daya, pilih Buat berbagi sumber daya di konsol RAM.
10. Tinjau konfigurasi Anda di bagian Ringkasan, lalu pilih Buat jaringan layanan.

Untuk membuat jaringan layanan menggunakan AWS CLI

Gunakan perintah create-service-network. Perintah ini hanya menciptakan jaringan layanan dasar. Untuk membuat jaringan layanan yang berfungsi penuh, Anda juga harus menggunakan perintah yang membuat asosiasi layanan, asosiasi VPC, dan pengaturan akses.

Mengelola asosiasi untuk jaringan layanan VPC Lattice

Ketika Anda mengaitkan layanan dengan jaringan layanan, ini memungkinkan klien (sumber daya dalam VPC yang terkait dengan jaringan layanan), untuk membuat permintaan ke layanan. Ketika Anda mengaitkan VPC dengan jaringan layanan, itu memungkinkan semua target dalam VPC itu menjadi klien dan berkomunikasi dengan layanan lain di jaringan layanan.

Daftar Isi

Kelola asosiasi layanan

Anda dapat mengaitkan layanan yang berada di akun Anda atau layanan yang dibagikan dengan Anda dari akun yang berbeda. Ini adalah langkah opsional saat membuat jaringan layanan. Namun, jaringan layanan tidak berfungsi penuh sampai Anda mengaitkan layanan. Pemilik layanan dapat mengaitkan layanan mereka ke jaringan layanan jika akun mereka memiliki akses yang diperlukan. Untuk informasi selengkapnya, lihat Cara kerja VPC Lattice.

Ketika Anda menghapus asosiasi layanan, layanan tidak dapat lagi terhubung ke layanan lain di jaringan layanan.

Untuk mengelola asosiasi layanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Jaringan layanan.
3. Pilih nama jaringan layanan untuk membuka halaman detailnya.
4. Pilih tab Asosiasi layanan.
5. Untuk membuat asosiasi, lakukan hal berikut:
    a. Pilih Buat asosiasi.
    b. Pilih layanan dari Layanan. Untuk membuat layanan, pilih Buat layanan Amazon VPC Lattice.

   c. (Opsional) Untuk menambahkan tag, perluas tag asosiasi layanan, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
   d. Pilih Simpan perubahan.
6. Untuk menghapus asosiasi, pilih kotak centang untuk asosiasi, lalu pilih Tindakan, Hapus asosiasi layanan. Saat diminta konfirmasi, masukkan **`confirm`**, lalu pilih Hapus.

Untuk membuat asosiasi layanan menggunakan AWS CLI

Gunakan perintah create-service-network-service-association.

Untuk menghapus asosiasi layanan menggunakan AWS CLI

Gunakan perintah delete-service-network-service-association.

Kelola asosiasi VPC

Klien dapat mengirim permintaan ke layanan yang terkait dengan jaringan layanan hanya jika mereka berada di VPC yang terkait dengan jaringan layanan. Lalu lintas klien yang melintasi koneksi peering VPC atau gateway transit ditolak.

Mengaitkan VPC adalah langkah opsional saat Anda membuat jaringan layanan. Namun, jaringan layanan tidak berfungsi penuh sampai Anda mengaitkan VPC. Pemilik jaringan dapat mengaitkan VPC ke jaringan layanan jika akun mereka memiliki akses yang diperlukan. Untuk informasi selengkapnya, lihat Cara kerja VPC Lattice.

Ketika Anda menghapus asosiasi VPC, klien di VPC tidak dapat lagi terhubung ke layanan di jaringan layanan.

Untuk mengelola asosiasi VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Jaringan layanan.
3. Pilih nama jaringan layanan untuk membuka halaman detailnya.
4. Pilih tab asosiasi VPC.
5. Untuk membuat asosiasi VPC, lakukan hal berikut:
   a. Pilih Buat asosiasi VPC.

   b. Pilih Tambahkan asosiasi VPC.
   c. Pilih VPC dari VPC dan pilih hingga lima grup keamanan dari grup Keamanan. Untuk membuat grup keamanan, pilih Buat grup keamanan baru.
   d. (Opsional) Untuk menambahkan tag, perluas tag asosiasi VPC, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
   e. Pilih Simpan perubahan.
6. Untuk mengedit grup keamanan untuk asosiasi, pilih kotak centang untuk asosiasi, lalu pilih Tindakan, Edit grup keamanan. Tambahkan dan hapus grup keamanan sesuai kebutuhan.
7. Untuk menghapus asosiasi, pilih kotak centang untuk asosiasi, lalu pilih Tindakan, Hapus asosiasi VPC. Saat diminta konfirmasi, masukkan **`confirm`**, lalu pilih Hapus.

Untuk membuat asosiasi VPC menggunakan AWS CLI

Gunakan perintah create-service-network-vpc-association.

Untuk memperbarui grup keamanan untuk asosiasi VPC menggunakan AWS CLI

Gunakan perintah update-service-network-vpc-association.

Untuk menghapus asosiasi VPC menggunakan AWS CLI

Gunakan perintah delete-service-network-vpc-association.

Mengedit setelan akses untuk jaringan layanan VPC Lattice

Pengaturan akses memungkinkan Anda untuk mengkonfigurasi dan mengelola akses klien ke jaringan layanan. Pengaturan akses mencakup jenis autentikasi dan kebijakan autentikasi. Kebijakan autentikasi membantu Anda mengautentikasi dan mengotorisasi lalu lintas yang mengalir ke layanan dalam VPC Lattice.

Anda dapat menerapkan kebijakan autentikasi di tingkat jaringan layanan, tingkat layanan, atau keduanya. Biasanya, kebijakan autentikasi diterapkan oleh pemilik jaringan atau administrator cloud. Mereka dapat menerapkan otorisasi berbutir kursus, misalnya, mengizinkan panggilan yang diautentikasi dari dalam organisasi, atau mengizinkan permintaan GET anonim yang cocok dengan kondisi tertentu. Pada tingkat layanan, pemilik layanan dapat menerapkan kontrol berbutir halus, yang bisa lebih membatasi. Untuk informasi selengkapnya, lihat Kontrol akses ke layanan VPC Lattice menggunakan kebijakan autentikasi.

Untuk menambah atau memperbarui kebijakan akses menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Jaringan layanan.
3. Pilih nama jaringan layanan untuk membuka halaman detailnya.
4. Pilih tab Access untuk memeriksa pengaturan akses saat ini.
5. Untuk memperbarui pengaturan akses, pilih Edit pengaturan akses.
6. Jika Anda ingin klien di VPC terkait mengakses layanan di jaringan layanan ini, pilih None for Auth type.
7. Untuk menerapkan kebijakan sumber daya ke jaringan layanan, pilih AWS IAM untuk jenis Auth dan lakukan kebijakan Auth berikut ini:
   - Masukkan kebijakan di kolom input. Misalnya kebijakan yang dapat Anda salin dan tempel, pilih Contoh kebijakan.
   - Pilih Terapkan templat kebijakan dan pilih templat Izinkan akses yang diautentikasi dan tidak diautentikasi. Template ini memungkinkan klien dari akun lain untuk mengakses layanan baik dengan menandatangani permintaan (artinya diautentikasi) atau secara anonim (artinya tidak diautentikasi).
   - Pilih Terapkan templat kebijakan dan pilih templat Izinkan hanya akses yang diautentikasi. Template ini memungkinkan klien dari akun lain untuk mengakses layanan hanya dengan menandatangani permintaan (artinya diautentikasi).
8. Pilih Simpan perubahan.

Untuk menambah atau memperbarui kebijakan akses menggunakan AWS CLI

Gunakan perintah put-auth-policy.

Mengedit detail pemantauan untuk jaringan layanan VPC Lattice

VPC Lattice menghasilkan metrik dan log untuk setiap permintaan dan respons, membuatnya lebih efisien untuk memantau dan memecahkan masalah aplikasi.

Anda dapat mengaktifkan log akses dan menentukan sumber daya tujuan untuk log Anda. VPC Lattice dapat mengirim log ke sumber daya berikut: Grup CloudWatch log, aliran pengiriman Firehose, dan bucket S3.

Untuk mengaktifkan log akses atau memperbarui tujuan log menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Jaringan layanan.
3. Pilih nama jaringan layanan untuk membuka halaman detailnya.
4. Pilih tab Pemantauan. Periksa log Access untuk melihat apakah log akses diaktifkan.
5. Untuk mengaktifkan atau menonaktifkan log akses, pilih Edit log akses, lalu nyalakan atau nonaktifkan sakelar Access log.
6. Ketika Anda mengaktifkan log akses, Anda harus memilih jenis tujuan pengiriman, dan kemudian membuat atau memilih tujuan untuk log akses. Anda juga dapat mengubah tujuan pengiriman kapan saja. Sebagai contoh:
   - Pilih Grup CloudWatch log dan pilih grup CloudWatch Log. Untuk membuat grup log, pilih Buat grup log masuk CloudWatch.
   - Pilih bucket S3 dan masukkan path bucket S3, termasuk awalan apa pun. Untuk mencari bucket S3 Anda, pilih Browse S3.
   - Pilih aliran pengiriman Kinesis Data Firehose dan pilih aliran pengiriman. Untuk membuat aliran pengiriman, pilih Buat aliran pengiriman di Kinesis.
7. Pilih Simpan perubahan.

Untuk mengaktifkan log akses menggunakan AWS CLI

Gunakan perintah create-access-log-subscription.

Untuk memperbarui tujuan log menggunakan AWS CLI

Gunakan perintah update-access-log-subscription.

Untuk menonaktifkan log akses menggunakan AWS CLI

Gunakan perintah delete-access-log-subscription.

Mengelola tag untuk jaringan layanan VPC Lattice

Tag membantu Anda untuk mengkategorikan jaringan layanan Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan.

Anda dapat menambahkan beberapa tag ke setiap jaringan layanan. Kunci tag harus unik untuk setiap jaringan layanan. Jika Anda menambahkan tag dengan kunci yang sudah dikaitkan dengan

jaringan layanan, itu memperbarui nilai tag tersebut. Anda dapat menggunakan karakter seperti huruf, spasi, angka (dalam UTF-8), dan karakter khusus berikut: + - =. _:/@. Jangan gunakan spasi terkemuka atau paling belakang. Kunci dan nilai tanda peka huruf besar dan kecil.

Untuk menambah atau menghapus tag menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Jaringan layanan.
3. Pilih nama jaringan layanan untuk membuka halaman detailnya.
4. Pilih tab Tanda.
5. Untuk menambahkan tag, pilih Tambahkan tag dan masukkan kunci tag dan nilai tag. Untuk menambahkan tag lain, pilih Tambahkan tag baru. Setelah Anda selesai menambahkan tanda, pilih Simpan perubahan.
6. Untuk menghapus tag, pilih kotak centang untuk tag dan pilih Hapus. Saat diminta konfirmasi, masukkan **`confirm`**, lalu pilih Hapus.

Untuk menambah atau menghapus tag menggunakan AWS CLI

Gunakan perintah tag-resource dan untag-resource.

Hapus jaringan layanan

Sebelum Anda dapat menghapus jaringan layanan, Anda harus terlebih dahulu menghapus semua asosiasi yang mungkin dimiliki jaringan layanan dengan layanan atau VPC apa pun. Saat Anda menghapus jaringan layanan, kami juga menghapus semua sumber daya yang terkait dengan jaringan layanan, seperti kebijakan sumber daya, kebijakan autentikasi, dan langganan log akses.

Untuk menghapus jaringan layanan menggunakan konsol

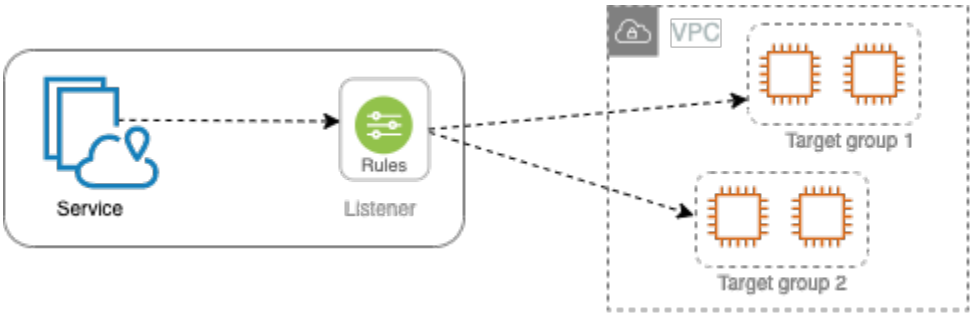
1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Jaringan layanan.
3. Pilih kotak centang untuk jaringan layanan, lalu pilih Tindakan, Hapus jaringan layanan.
4. Saat diminta konfirmasi, masukkan**`confirm`**, lalu pilih Hapus.

Untuk menghapus jaringan layanan menggunakan AWS CLI

Gunakan perintah delete-service-network.

Layanan di VPC Lattice

Layanan dalam VPC Lattice adalah unit perangkat lunak yang dapat digunakan secara independen yang memberikan tugas atau fungsi tertentu. Layanan dapat berjalan pada instance, container, atau sebagai fungsi tanpa server dalam akun atau virtual private cloud (VPC). Layanan memiliki listener yang menggunakan aturan, yang disebut aturan listener, yang dapat Anda konfigurasikan untuk membantu merutekan lalu lintas ke target Anda. Target dapat berupa instans EC2, alamat IP, fungsi Lambda tanpa server, Application Load Balancers, atau Kubernetes Pods. Untuk informasi selengkapnya, lihat Grup sasaran di VPC Lattice. Anda dapat mengaitkan layanan dengan beberapa jaringan layanan. Diagram berikut menunjukkan komponen kunci dari layanan tipikal dalam VPC Lattice.



Anda dapat membuat layanan dengan memberinya nama dan deskripsi. Namun, untuk mengontrol dan memantau lalu lintas ke layanan Anda, penting bagi Anda untuk menyertakan pengaturan akses dan detail pemantauan. Untuk mengirim lalu lintas dari layanan ke target, Anda harus menyiapkan pendengar dan mengonfigurasi aturan. Untuk memungkinkan lalu lintas mengalir dari jaringan layanan ke layanan Anda, Anda harus mengaitkan layanan Anda dengan jaringan layanan.

Ada batas waktu idle dan batas waktu koneksi keseluruhan untuk koneksi ke target. Batas waktu koneksi idle adalah 1 menit, setelah itu kami menutup koneksi. Durasi maksimum adalah 10 menit, setelah itu kami tidak mengizinkan aliran baru melalui koneksi dan kami memulai proses penutupan aliran yang ada.

Tugas

- Langkah 1: Buat layanan VPC Lattice
- Langkah 2: Tentukan perutean
- Langkah 3: Buat asosiasi jaringan
- Langkah 4: Tinjau dan buat
- Mengelola asosiasi untuk layanan VPC Lattice

- Mengedit setelan akses untuk layanan VPC Lattice
- Mengedit detail pemantauan untuk layanan VPC Lattice
- Mengelola tag untuk layanan VPC Lattice
- Konfigurasikan nama domain khusus untuk layanan VPC Lattice Anda
- Bawa Sertifikat Anda Sendiri (BYOC) untuk Kisi VPC
- Hapus layanan

Langkah 1: Buat layanan VPC Lattice

Buat layanan VPC Lattice dasar dengan pengaturan akses dan detail pemantauan. Namun, layanan ini tidak berfungsi penuh sampai Anda menentukan konfigurasi routing dan mengaitkannya dengan jaringan layanan.

Untuk membuat layanan dasar menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih Buat layanan.
4. Untuk Identifier, lakukan hal berikut:

   a. Masukkan nama untuk layanan ini. Nama harus antara 3-63 karakter dan menggunakan huruf kecil, angka, dan tanda hubung. Itu harus dimulai dan diakhiri dengan huruf atau angka. Jangan gunakan tanda hubung ganda.

   b. (Opsional) Masukkan deskripsi untuk jaringan layanan. Anda dapat mengatur atau mengubah deskripsi selama atau setelah pembuatan. Deskripsi dapat memiliki hingga 256 karakter.
5. Untuk menentukan nama domain kustom untuk layanan Anda, pilih Tentukan konfigurasi domain kustom dan masukkan nama domain kustom.

   Untuk pendengar HTTPS, Anda dapat memilih sertifikat yang akan digunakan VPC Lattice untuk melakukan penghentian TLS. Jika Anda tidak memilih sertifikat sekarang, Anda dapat memilihnya saat membuat pendengar HTTPS untuk layanan tersebut.

   Untuk pendengar TCP, Anda harus menentukan nama domain khusus untuk layanan Anda. Jika Anda menentukan sertifikat, itu tidak digunakan. Sebagai gantinya, Anda melakukan penghentian TLS dalam aplikasi Anda.

6. Untuk akses Layanan, pilih Tidak Ada jika Anda ingin klien di VPC yang terkait dengan jaringan layanan untuk mengakses layanan Anda. Untuk menerapkan kebijakan autentikasi untuk mengontrol akses ke layanan, pilih AWS IAM. Untuk menerapkan kebijakan sumber daya ke layanan, lakukan salah satu hal berikut untuk kebijakan Auth:
   - Masukkan kebijakan di kolom input. Misalnya kebijakan yang dapat Anda salin dan tempel, pilih Contoh kebijakan.
   - Pilih Terapkan templat kebijakan dan pilih templat Izinkan akses yang diautentikasi dan tidak diautentikasi. Template ini memungkinkan klien dari akun lain untuk mengakses layanan baik dengan menandatangani permintaan (artinya diautentikasi) atau secara anonim (artinya tidak diautentikasi).
   - Pilih Terapkan templat kebijakan dan pilih templat Izinkan hanya akses yang diautentikasi. Template ini memungkinkan klien dari akun lain untuk mengakses layanan hanya dengan menandatangani permintaan (artinya diautentikasi).
7. (Opsional) Untuk mengaktifkan log akses, aktifkan sakelar sakelar sakelar akses log dan tentukan tujuan untuk log akses Anda sebagai berikut:
   - Pilih Grup CloudWatch log dan pilih grup CloudWatch Log. Untuk membuat grup log, pilih Buat grup log masuk CloudWatch.
   - Pilih bucket S3 dan masukkan path bucket S3, termasuk awalan apa pun. Untuk mencari bucket S3 Anda, pilih Browse S3.
   - Pilih aliran pengiriman Kinesis Data Firehose dan pilih aliran pengiriman. Untuk membuat aliran pengiriman, pilih Buat aliran pengiriman di Kinesis.
8. (Opsional) Untuk membagikan layanan Anda dengan akun lain, pilih pembagian AWS RAM sumber daya dari Pembagian sumber daya. Untuk membuat pembagian sumber daya, pilih Buat berbagi sumber daya di konsol RAM.
9. Untuk meninjau konfigurasi dan membuat layanan, pilih Lewati untuk meninjau dan membuat. Jika tidak, pilih Berikutnya untuk menentukan konfigurasi routing untuk layanan Anda.

Langkah 2: Tentukan perutean

Tentukan konfigurasi perutean Anda menggunakan pendengar sehingga layanan Anda dapat mengirim lalu lintas ke target yang Anda tentukan.

Prasyarat

Sebelum Anda dapat menambahkan listener, Anda harus membuat grup target VPC Lattice. Untuk informasi selengkapnya, lihat the section called “Buat grup target”.

Untuk menentukan perutean untuk layanan Anda menggunakan konsol

1. Pilih Tambahkan pendengar.
2. Untuk nama Listener, Anda dapat memberikan nama pendengar kustom atau menggunakan protokol dan port listener Anda sebagai nama listener. Nama kustom yang Anda tentukan dapat memiliki hingga 63 karakter, dan itu harus unik untuk setiap layanan di akun Anda. Karakter yang valid adalah a-z, 0-9, dan tanda hubung (-). Anda tidak dapat menggunakan tanda hubung sebagai karakter pertama atau terakhir, atau segera setelah tanda hubung lainnya. Anda tidak dapat mengubah nama pendengar setelah Anda membuatnya.
3. Pilih protokol dan kemudian masukkan nomor port.
4. Untuk tindakan Default, pilih grup target VPC Lattice untuk menerima lalu lintas dan pilih bobot yang akan ditetapkan ke grup target ini. Anda dapat menambahkan grup target lain secara opsional untuk tindakan default. Pilih Tambah tindakan dan kemudian pilih grup target lain dan tentukan bobotnya.
5. (Opsional) Untuk menambahkan aturan lain, pilih Tambahkan aturan lalu masukkan nama, prioritas, kondisi, dan tindakan untuk aturan tersebut.

   Anda dapat memberikan setiap aturan nomor prioritas antara 1 dan 100. Listener tidak bisa memiliki beberapa aturan dengan prioritas yang sama. Peraturan dievaluasi dalam urutan prioritas, dari nilai terendah ke nilai tertinggi. Peraturan default dievaluasi terakhir.

   Untuk Kondisi, masukkan pola jalur untuk kondisi pencocokan jalur. Ukuran maksimum setiap string adalah 200 karakter. Perbandingannya tidak peka huruf besar/kecil.
6. (Opsional) Untuk menambahkan tag, perluas tag Listener, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
7. Untuk meninjau konfigurasi dan membuat layanan, pilih Lewati untuk meninjau dan membuat. Jika tidak, pilih Berikutnya untuk mengaitkan layanan Anda ke jaringan layanan.

Langkah 3: Buat asosiasi jaringan

Kaitkan layanan Anda dengan jaringan layanan sehingga klien dapat berkomunikasi dengannya.

Untuk mengaitkan layanan ke jaringan layanan menggunakan konsol

1. Untuk jaringan layanan VPC Lattice, pilih jaringan layanan. Untuk membuat jaringan layanan, pilih Buat jaringan kisi VPC. Anda dapat mengaitkan layanan Anda dengan beberapa jaringan layanan.
2. (Opsional) Untuk menambahkan tag, perluas tag asosiasi jaringan layanan, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
3. Pilih Selanjutnya.

Langkah 4: Tinjau dan buat

Untuk meninjau konfigurasi dan membuat layanan menggunakan konsol

1. Tinjau konfigurasi untuk layanan Anda.
2. Pilih Edit jika Anda perlu mengubah bagian mana pun dari konfigurasi layanan.
3. Setelah selesai meninjau atau mengedit konfigurasi, pilih layanan Create VPC Lattice.
4. Jika Anda menentukan nama domain khusus untuk layanan, Anda harus mengonfigurasi perutean DNS setelah layanan dibuat. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan nama domain khusus”.

Mengelola asosiasi untuk layanan VPC Lattice

Ketika Anda mengaitkan layanan dengan jaringan layanan, ini memungkinkan klien (sumber daya dalam VPC yang terkait dengan jaringan layanan), untuk membuat permintaan ke layanan ini. Anda dapat mengaitkan layanan yang ada di akun Anda atau layanan yang dibagikan dengan Anda dari akun yang berbeda. Langkah ini opsional saat membuat layanan. Namun, setelah pembuatan, layanan tidak dapat berkomunikasi dengan layanan lain sampai Anda mengaitkannya dengan jaringan layanan. Pemilik layanan dapat mengaitkan layanan mereka ke jaringan layanan jika akun mereka memiliki akses yang diperlukan. Untuk informasi selengkapnya, lihat Cara kerja VPC Lattice.

Untuk mengelola asosiasi jaringan layanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih nama layanan untuk membuka halaman detailnya.

4. Pilih tab Asosiasi jaringan layanan.
5. Untuk membuat asosiasi, lakukan hal berikut:
   a. Pilih Buat asosiasi.
   b. Pilih jaringan layanan dari jaringan layanan VPC Lattice. Untuk membuat jaringan layanan, pilih Buat jaringan kisi VPC.
   c. (Opsional) Untuk menambahkan tag, perluas tag asosiasi layanan, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
   d. Pilih Simpan perubahan.
6. Untuk menghapus asosiasi, pilih kotak centang untuk asosiasi, lalu pilih Tindakan, Hapus asosiasi jaringan. Saat diminta konfirmasi, masukkan **`confirm`**, lalu pilih Hapus.

Untuk membuat asosiasi jaringan layanan menggunakan AWS CLI

Gunakan perintah create-service-network-service-association.

Untuk menghapus asosiasi jaringan layanan menggunakan AWS CLI

Gunakan perintah delete-service-network-service-association.

Mengedit setelan akses untuk layanan VPC Lattice

Pengaturan akses memungkinkan Anda mengonfigurasi dan mengelola akses klien ke layanan. Pengaturan akses mencakup jenis autentikasi dan kebijakan autentikasi. Kebijakan autentikasi membantu Anda mengautentikasi dan mengotorisasi lalu lintas yang mengalir ke layanan dalam VPC Lattice.

Anda dapat menerapkan kebijakan autentikasi di tingkat jaringan layanan, tingkat layanan, atau keduanya. Pada tingkat layanan, pemilik layanan dapat menerapkan kontrol berbutir halus, yang bisa lebih membatasi. Biasanya, kebijakan autentikasi diterapkan oleh pemilik jaringan atau administrator cloud. Mereka dapat menerapkan otorisasi berbutir kursus, misalnya, mengizinkan panggilan yang diautentikasi dari dalam organisasi, atau mengizinkan permintaan GET anonim yang cocok dengan kondisi tertentu. Untuk informasi selengkapnya, lihat Kontrol akses ke layanan VPC Lattice menggunakan kebijakan autentikasi.

Untuk menambah atau memperbarui kebijakan akses menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.

2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih nama layanan untuk membuka halaman detailnya.
4. Pilih tab Access untuk memeriksa pengaturan akses saat ini.
5. Untuk memperbarui pengaturan akses, pilih Edit pengaturan akses.
6. Jika Anda ingin klien di VPC di jaringan layanan terkait mengakses layanan Anda, pilih None for Auth type.
7. Untuk menerapkan kebijakan sumber daya untuk mengontrol akses ke layanan, pilih AWS IAM untuk jenis Auth dan lakukan satu hal berikut untuk kebijakan Auth:
   - Masukkan kebijakan di kolom input. Misalnya kebijakan yang dapat Anda salin dan tempel, pilih Contoh kebijakan.
   - Pilih Terapkan templat kebijakan dan pilih templat Izinkan akses yang diautentikasi dan tidak diautentikasi. Template ini memungkinkan klien dari akun lain untuk mengakses layanan baik dengan menandatangani permintaan (artinya diautentikasi) atau secara anonim (artinya tidak diautentikasi).
   - Pilih Terapkan templat kebijakan dan pilih templat Izinkan hanya akses yang diautentikasi. Template ini memungkinkan klien dari akun lain untuk mengakses layanan hanya dengan menandatangani permintaan (artinya diautentikasi).
8. Pilih Simpan perubahan.

Untuk menambah atau memperbarui kebijakan akses menggunakan AWS CLI

Gunakan perintah put-auth-policy.

Mengedit detail pemantauan untuk layanan VPC Lattice

VPC Lattice menghasilkan metrik dan log untuk setiap permintaan dan respons, membuatnya lebih efisien untuk memantau dan memecahkan masalah aplikasi.

Anda dapat mengaktifkan log akses dan menentukan sumber daya tujuan untuk log Anda. VPC Lattice dapat mengirim log ke sumber daya berikut: Grup CloudWatch log, aliran pengiriman Firehose, dan bucket S3.

Untuk mengaktifkan log akses atau memperbarui tujuan log menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.

3. Pilih nama layanan untuk membuka halaman detailnya.
4. Pilih tab Monitoring dan kemudian pilih Log. Periksa log Access untuk melihat apakah log akses diaktifkan.
5. Untuk mengaktifkan atau menonaktifkan log akses, pilih Edit log akses, lalu nyalakan atau nonaktifkan sakelar Access log.
6. Ketika Anda mengaktifkan log akses, Anda harus memilih jenis tujuan pengiriman, dan kemudian membuat atau memilih tujuan untuk log akses. Anda juga dapat mengubah tujuan pengiriman kapan saja. Sebagai contoh:
   - Pilih Grup CloudWatch log dan pilih grup CloudWatch Log. Untuk membuat grup log, pilih Buat grup log masuk CloudWatch.
   - Pilih bucket S3 dan masukkan path bucket S3, termasuk awalan apa pun. Untuk mencari bucket S3 Anda, pilih Browse S3.
   - Pilih aliran pengiriman Kinesis Data Firehose dan pilih aliran pengiriman. Untuk membuat aliran pengiriman, pilih Buat aliran pengiriman di Kinesis.
7. Pilih Simpan perubahan.

Untuk mengaktifkan log akses menggunakan AWS CLI

Gunakan perintah create-access-log-subscription.

Untuk memperbarui tujuan log menggunakan AWS CLI

Gunakan perintah update-access-log-subscription.

Untuk menonaktifkan log akses menggunakan AWS CLI

Gunakan perintah delete-access-log-subscription.

Mengelola tag untuk layanan VPC Lattice

Tag membantu Anda untuk mengkategorikan layanan Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan.

Anda dapat menambahkan beberapa tag ke setiap layanan. Kunci tag harus unik untuk setiap layanan. Jika Anda menambahkan tag dengan kunci yang sudah dikaitkan dengan layanan, itu memperbarui nilai tag tersebut. Anda dapat menggunakan karakter seperti huruf, spasi, angka (dalam UTF-8), dan karakter khusus berikut: + - =. _:/@. Jangan gunakan spasi terkemuka atau paling belakang. Kunci dan nilai tanda peka huruf besar dan kecil.

Untuk menambah atau menghapus tag menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih nama layanan untuk membuka halaman detailnya.
4. Pilih tab Tanda.
5. Untuk menambahkan tag, pilih Tambahkan tag dan masukkan kunci tag dan nilai tag. Untuk menambahkan tag lain, pilih Tambahkan tag baru. Setelah Anda selesai menambahkan tanda, pilih Simpan perubahan.
6. Untuk menghapus tag, pilih kotak centang untuk tag dan pilih Hapus. Saat diminta konfirmasi, masukkan **`confirm`**, lalu pilih Hapus.

Untuk menambah atau menghapus tag menggunakan AWS CLI

Gunakan perintah tag-resource dan untag-resource.

Konfigurasikan nama domain khusus untuk layanan VPC Lattice Anda

Saat Anda membuat layanan baru, VPC Lattice menghasilkan Nama Domain Berkualitas Penuh (FQDN) yang unik untuk layanan dengan sintaks berikut.

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

Namun, nama domain yang disediakan VPC Lattice tidak mudah diingat oleh pengguna Anda. Nama domain khusus adalah URL yang lebih sederhana dan lebih intuitif yang dapat Anda berikan kepada pengguna Anda. Jika Anda lebih suka menggunakan nama domain khusus untuk layanan Anda, seperti `www.parking.example.com` alih-alih nama DNS yang dihasilkan VPC Lattice, Anda dapat mengonfigurasinya saat membuat layanan VPC Lattice. Saat klien membuat permintaan menggunakan nama domain kustom Anda, server DNS menyelesaikannya ke nama domain yang dihasilkan VPC Lattice. Namun, ini hanya terjadi jika Anda memetakan nama domain kustom Anda ke nama domain yang dihasilkan VPC Lattice dengan catatan CNAME untuk merutekan kueri ke layanan Anda. Untuk informasi selengkapnya, lihat Kaitkan nama domain khusus dengan layanan Anda.

Prasyarat

- Anda harus memiliki nama domain terdaftar untuk layanan Anda. Jika Anda belum memiliki nama domain terdaftar, Anda dapat mendaftarkannya melalui Amazon Route 53 atau registrar komersial lainnya.
- Untuk menerima permintaan HTTPS, Anda harus memberikan sertifikat Anda sendiri di AWS Certificate Manager. VPC Lattice tidak mendukung sertifikat default sebagai fallback. Oleh karena itu, jika Anda tidak memberikan sertifikat SSL/TLS yang sesuai dengan nama domain kustom Anda, semua koneksi HTTPS ke nama domain kustom Anda akan gagal. Untuk informasi selengkapnya, lihat Bawa Sertifikat Anda Sendiri (BYOC) untuk Kisi VPC.

Keterbatasan dan pertimbangan

- Anda tidak dapat memiliki lebih dari satu nama domain khusus untuk suatu layanan.
- Anda tidak dapat mengubah nama domain kustom setelah Anda membuat layanan.
- Nama domain khusus harus unik untuk jaringan layanan. Ini berarti bahwa layanan tidak dapat dibuat dengan nama domain kustom yang sudah ada (untuk layanan lain) di jaringan layanan yang sama.

Untuk mengonfigurasi nama domain khusus untuk layanan Anda menggunakan AWS Management Console

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih Buat Layanan. Anda dinavigasi ke Langkah 1: Buat layanan.
4. Di bagian Konfigurasi domain kustom, pilih Tentukan konfigurasi domain kustom.
5. Masukkan nama domain kustom Anda.
6. Untuk melayani permintaan HTTPS, pilih sertifikat SSL/TLS yang cocok dengan nama domain kustom Anda di sertifikat SSL/TLS Kustom. Jika Anda belum memiliki sertifikat, atau tidak ingin menambahkannya sekarang, Anda dapat menambahkan sertifikat saat membuat pendengar HTTPS. Namun, tanpa sertifikat, nama domain kustom Anda tidak akan dapat melayani permintaan HTTPS. Untuk informasi selengkapnya, lihat Menambahkan pendengar HTTPS.
7. Setelah selesai menambahkan semua informasi lain untuk membuat layanan, pilih Buat.

Untuk mengonfigurasi nama domain khusus untuk layanan Anda menggunakan AWS CLI

Gunakan perintah 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
```

Dalam perintah di atas, untuk`--name`, masukkan nama untuk layanan Anda. Untuk`--custom-domain-name`, masukkan nama domain layanan Anda seperti,`parking.example.com`. Untuk `--certificate-arn` masukkan ARN sertifikat Anda di ACM. Sertifikat ARN tersedia di akun Anda di. AWS Certificate Manager

Jika Anda tidak memiliki sertifikat SSL/TLS sendiri di AWS Certificate Manager (ACM), Anda dapat membuat atau mengimpornya sebelum menyiapkan nama domain khusus. Namun, sertifikat hanya diperlukan jika Anda ingin melayani permintaan HTTPS menggunakan nama domain kustom Anda. Untuk informasi selengkapnya, lihat Bawa Sertifikat Anda Sendiri (BYOC) untuk Kisi VPC.

Kaitkan nama domain khusus dengan layanan Anda

Pertama, jika Anda belum melakukannya, daftarkan nama domain khusus Anda. Internet Corporation for Assigned Names and Numbers (ICANN) mengelola nama domain di internet. Anda mendaftarkan nama domain menggunakan pencatat nama domain, organisasi terakreditasi ICANN yang mengelola registri nama domain. Situs web untuk registrar Anda akan memberikan petunjuk terperinci dan informasi harga untuk mendaftarkan nama domain Anda. Untuk informasi selengkapnya, lihat sumber daya berikut:

- Untuk menggunakan Amazon Route 53 untuk mendaftarkan nama domain, lihat Mendaftarkan nama domain menggunakan Route 53 di Panduan Pengembang Amazon Route 53.
- Untuk daftar pendaftar terakreditasi, lihat Direktori Panitera Terakreditasi.

Selanjutnya, gunakan layanan DNS Anda, seperti registrar domain Anda, untuk membuat catatan CNAME untuk merutekan kueri ke layanan Anda. Untuk informasi lebih lanjut, lihat dokumentasi untuk server DNS Anda. Atau, Anda dapat menggunakan Route 53 sebagai layanan DNS Anda.

Jika Anda menggunakan Route 53, Anda harus terlebih dahulu membuat zona yang dihosting, yang berisi informasi tentang cara merutekan lalu lintas di internet untuk domain Anda. Setelah Anda membuat zona yang dihosting pribadi atau publik, buat catatan CNAME sehingga nama domain kustom Anda, misalnya`parking.example.com`, dipetakan ke nama domain yang dibuat secara otomatis VPC Lattice, misalnya,. `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws` Tanpa pemetaan ini, nama domain kustom Anda tidak akan berfungsi di

VPC Lattice. Untuk informasi selengkapnya, lihat Membuat rekaman menggunakan konsol Amazon Route 53 di Panduan Pengembang Amazon Route 53. Selain itu, Anda dapat merujuk ke langkah-langkah di bawah ini untuk membuat zona yang dihosting dan catatan CNAME untuk memetakan nama domain kustom Anda ke titik akhir VPC Lattice.

Untuk membuat zona yang dihosting pribadi atau publik dengan catatan CNAME menggunakan konsol Amazon Route 53

1. Buka konsol Route 53 di https://console.aws.amazon.com/route53/.
2. Di panel navigasi, pilih Zona yang dihosting lalu Buat zona yang dihosting.
3. Untuk nama Domain, pilih nama zona host yang ingin Anda gunakan untuk merutekan lalu lintas ke layanan VPC Lattice Anda. Misalnya, Jika nama domain kustom Anda adalah `parking.example.com` (http://parking.example.com/), maka nama domain untuk zona host Anda adalah `example.com` (http://example.com/), juga dikenal sebagai nama domain apex. Anda kemudian dapat membuat catatan CNAME untuk zona yang dihosting ini untuk merutekan lalu lintas ke layanan VPC Lattice Anda. Catatan: Anda tidak dapat mengubah nama zona yang dihosting setelah membuatnya.
4. Untuk Jenis, pilih Private Hosted Zone atau Public Hosted Zone sesuai kebutuhan.
5. Pilih Wilayah Anda dan pilih ID VPC untuk VPC yang ingin Anda kaitkan dengan zona yang dihosting ini.
6. Tambahkan tag jika perlu, dan pilih Buat zona yang dihosting. Setelah pembuatan, zona yang dihosting Anda terdaftar di bawah Zona yang Dihosting.
7. Untuk membuat catatan CNAME di zona host yang baru saja Anda buat, pilih zona yang dihosting, lalu pilih Buat catatan.
8. Tentukan nilai berikut di bawah Buat catatan:

    a. Untuk nama Rekam, masukkan nama yang ingin Anda gunakan sebagai nama domain kustom Anda. Jika Anda ingin menggunakan `parking.example.com` (http://acme.example.com/) sebagai nama domain khusus Anda, masukkan `parking` *. Ini berarti Anda akan memasukkan nama subdomain `parking` tetapi tanpa nama domain zona yang dihosting `example.com` (http://example.com/).

    b. Untuk jenis Rekam, pilih CNAME.

    c. Tetap Alias dimatikan.

    d. Untuk Nilai, masukkan Kisi VPC yang dihasilkan nama domain untuk layanan Anda (misalnya,). `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-`

`west-2.on.aws` Anda akan menemukan nama domain yang dibuat secara otomatis ini di konsol VPC Lattice di halaman layanan Anda. Jika menggunakan AWS CLI, output dari `list-services` perintah `create-service` or akan mengembalikan nama domain yang dibuat secara otomatis ini.

e. Untuk TTL (detik), terima nilai default 300.

f. Untuk kebijakan Perutean, pilih kebijakan perutean yang berlaku. Untuk informasi selengkapnya, lihat Memilih kebijakan perutean di Panduan Pengembang Amazon Route 53.

9. Pilih Create records (Buat catatan).

   Perubahan umumnya menyebar ke semua server nama Route 53 dalam waktu 60 detik. Ketika propagasi selesai, Anda akan dapat merutekan lalu lintas ke layanan Anda dengan menggunakan nama domain khusus.

Untuk membuat catatan alias di zona yang dihosting menggunakan AWS CLI

1. Dapatkan nama domain yang dihasilkan VPC Lattice untuk layanan Anda (misalnya,`my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`) dan ID zona yang dihosting dengan menjalankan perintah. `get-service`
2. Untuk mengatur alias, gunakan perintah berikut.

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

   Untuk `change-set.json` file tersebut, buat file JSON dengan konten dalam contoh JSON berikut, dan simpan di mesin lokal Anda. Ganti *`file: //~/desktop/Change-set.json pada perintah di atas dengan jalur file JSON`* yang disimpan di mesin lokal Anda. Perhatikan bahwa “Ketik” di JSON berikut dapat berupa tipe catatan A atau AAAA.

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

Bawa Sertifikat Anda Sendiri (BYOC) untuk Kisi VPC

Untuk melayani permintaan HTTPS, Anda harus memiliki sertifikat SSL/TLS Anda sendiri siap di AWS Certificate Manager (ACM) sebelum Anda menyiapkan nama domain kustom. Sertifikat ini harus memiliki Nama Alternatif Subjek (SAN) atau Nama Umum (CN) yang cocok dengan nama domain khusus untuk layanan Anda. Jika SAN hadir, kami memeriksa kecocokan hanya di daftar SAN. Jika SAN tidak ada, kami memeriksa kecocokan di CN.

VPC Lattice melayani permintaan HTTPS menggunakan Server Name Indication (SNI). DNS merutekan permintaan HTTPS ke layanan VPC Lattice Anda berdasarkan nama domain kustom dan sertifikat yang cocok dengan nama domain ini. Untuk meminta sertifikat SSL/TLS untuk nama domain di ACM atau mengimpornya ke ACM, lihat Menerbitkan dan Mengelola Sertifikat dan Mengimpor sertifikat di Panduan Pengguna.AWS Certificate Manager Jika Anda tidak dapat meminta atau mengimpor sertifikat Anda sendiri di ACM, gunakan nama domain dan sertifikat yang dihasilkan oleh VPC Lattice.

VPC Lattice hanya menerima satu sertifikat khusus per layanan. Namun, Anda dapat menggunakan sertifikat khusus untuk beberapa domain kustom. Ini berarti Anda dapat menggunakan sertifikat yang sama untuk semua layanan VPC Lattice yang Anda buat dengan nama domain kustom.

Untuk melihat sertifikat Anda menggunakan konsol ACM, buka Sertifikat, dan pilih ID sertifikat Anda. Anda akan melihat layanan VPC Lattice yang terkait dengan sertifikat tersebut di bawah sumber daya terkait.

Pertimbangan dan batasan

- VPC Lattice memungkinkan pencocokan wildcard yang sedalam satu level di Subject Alternate Name (SAN) atau Common Name (CN) dari sertifikat terkait. Misalnya, jika Anda membuat layanan dengan nama domain khusus `parking.example.com` dan mengaitkan sertifikat Anda sendiri dengan SAN`*.example.com`. Saat permintaan masuk`parking.example.com`, VPC Lattice

mencocokkan SAN dengan nama domain apa pun dengan domain apex. `example.com` Namun, jika Anda memiliki domain khusus `parking.different.example.com` dan sertifikat Anda memiliki SAN`*.example.com`, permintaan gagal.

- VPC Lattice mendukung satu tingkat kecocokan domain wildcard. Ini berarti bahwa wildcard hanya dapat digunakan sebagai subdomain tingkat pertama, dan hanya mengamankan satu tingkat subdomain. Misalnya, jika SAN sertifikat Anda`*.example.com`, maka `parking.*.example.com` tidak didukung.
- VPC Lattice mendukung satu wildcard per nama domain. Ini berarti `*.*.example.com` itu tidak valid. Untuk informasi selengkapnya, lihat Meminta sertifikat publik di Panduan AWS Certificate Manager Pengguna.
- VPC Lattice hanya mendukung sertifikat dengan kunci RSA 2048-bit.
- Sertifikat SSL/TLS di ACM harus berada di Wilayah yang sama dengan layanan VPC Lattice yang Anda kaitkan dengannya.

Mengamankan kunci pribadi sertifikat Anda

Ketika Anda meminta sertifikat SSL/TLS menggunakan ACM, ACM menghasilkan public/private key pair. Saat Anda mengimpor sertifikat, Anda menghasilkan key pair. Kunci publik menjadi bagian dari sertifikat. Untuk menyimpan kunci pribadi dengan aman, ACM membuat kunci lain menggunakan AWS KMS, yang disebut kunci KMS, dengan alias aws/acm. AWS KMS menggunakan kunci ini untuk mengenkripsi kunci pribadi sertifikat Anda. Untuk informasi selengkapnya, lihat Perlindungan data AWS Certificate Manager di Panduan AWS Certificate Manager Pengguna.

VPC Lattice menggunakan AWS TLS Connection Manager, layanan yang hanya dapat diakses AWS layanan, untuk mengamankan dan menggunakan kunci pribadi sertifikat Anda. Saat Anda menggunakan sertifikat ACM untuk membuat layanan VPC Lattice, VPC Lattice mengaitkan sertifikat Anda dengan TLS Connection Manager. AWS Kami melakukan ini dengan membuat hibah AWS KMS terhadap kunci AWS terkelola Anda. Hibah ini memungkinkan TLS Connection Manager digunakan AWS KMS untuk mendekripsi kunci pribadi sertifikat Anda. TLS Connection Manager menggunakan sertifikat dan kunci pribadi yang didekripsi (plaintext) untuk membuat koneksi aman (sesi SSL/TLS) dengan klien layanan VPC Lattice. Ketika sertifikat dipisahkan dari layanan VPC Lattice, hibah dihentikan. Untuk informasi selengkapnya, lihat Hibah di Panduan AWS Key Management Service Pengembang.

Untuk informasi selengkapnya, lihat Enkripsi diam.

Hapus layanan

Untuk menghapus layanan VPC Lattice, Anda harus terlebih dahulu menghapus semua asosiasi yang mungkin dimiliki layanan dengan jaringan layanan apa pun. Jika Anda menghapus layanan, semua sumber daya yang terkait dengan layanan, seperti kebijakan sumber daya, kebijakan autentikasi, pendengar, aturan pendengar, dan langganan log akses, juga akan dihapus.

Untuk menghapus layanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pada halaman Layanan, pilih layanan yang ingin Anda hapus, lalu pilih Tindakan, Hapus layanan.
4. Saat diminta konfirmasi, pilih Hapus.

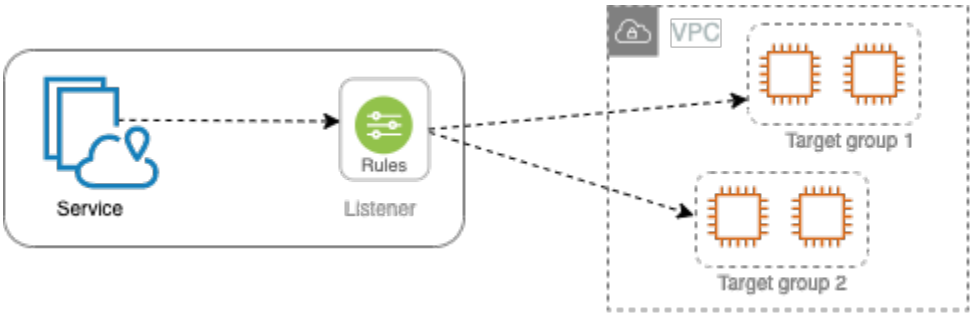
Untuk menghapus layanan menggunakan AWS CLI

Gunakan perintah delete-service.

Grup sasaran di VPC Lattice

Grup target VPC Lattice adalah kumpulan target, atau sumber daya komputasi, yang menjalankan aplikasi atau layanan Anda. Target dapat berupa instans EC2, alamat IP, fungsi Lambda, Application Load Balancers, atau Kubernetes Pods. Anda juga dapat melampirkan layanan yang ada ke grup target Anda. Untuk informasi selengkapnya tentang penggunaan Kubernetes dengan VPC Lattice, lihat Panduan Pengguna Gateway API Controller.AWS

Setiapkelompok target terbiasa merutekan permintaan untuk satu atau lebih target terdaftar. Bila Anda membuat aturan listener, Anda menentukan grup target dan kondisi. Ketika kondisi aturan terpenuhi, lalu lintas diteruskan ke kelompok target yang sesuai. Anda dapat membuat kelompok-kelompok target yang berbeda untuk berbagai jenis permintaan. Misalnya, buat satu grup target untuk permintaan umum dan grup target lainnya untuk permintaan yang menyertakan kondisi aturan tertentu, seperti nilai jalur atau header.



Anda menentukan pengaturan pemeriksaan kesehatan untuk layanan Anda berdasarkan per kelompok target. Setiap kelompok target menggunakan pengaturan pemeriksaan kondisi yang sudah ada, kecuali jika Anda menimpa mereka saat Anda membuat kelompok target atau mengubahnya nanti. Setelah Anda menentukan grup target dalam aturan untuk pendengar, layanan akan terus memantau kesehatan semua target yang terdaftar dengan grup target. Rute layanan meminta ke target terdaftar yang sehat.

Untuk menentukan grup target dalam aturan untuk pendengar layanan, grup target harus berada di akun yang sama dengan layanan.

Kelompok target VPC Lattice mirip dengan kelompok target yang disediakan oleh Elastic Load Balancing, tetapi mereka tidak dapat dipertukarkan.

Daftar Isi

Buat grup target VPC Lattice

Anda mendaftarkan target Anda dengan grup target. Secara default, layanan VPC Lattice mengirimkan permintaan ke target terdaftar menggunakan port dan protokol yang Anda tentukan untuk grup target. Anda dapat mengganti port ini ketika Anda mendaftar setiap target dengan kelompok target.

Untuk merutekan lalu lintas ke target dalam kelompok target, tentukan kelompok target dalam suatu tindakan saat Anda membuat pendengar atau membuat aturan untuk pendengar Anda. Untuk informasi selengkapnya, lihat Aturan pendengar untuk layanan VPC Lattice Anda. Anda dapat menentukan grup target yang sama di beberapa pendengar, tetapi pendengar ini harus milik layanan yang sama. Untuk menggunakan grup target dengan layanan, Anda harus memverifikasi bahwa grup target tidak digunakan oleh pendengar untuk layanan lain.

Anda dapat menambah atau menghapus target dari grup target Anda kapan saja. Untuk informasi selengkapnya, lihat Daftarkan target dengan grup target VPC Lattice. Anda juga dapat mengubah pengaturan pemeriksaan kesehatan untuk grup target Anda. Untuk informasi selengkapnya, lihat Pemeriksaan kesehatan untuk grup target VPC Lattice Anda.

Buat grup target

Anda dapat membuat grup target dan secara opsional mendaftarkan target sebagai berikut.

Untuk membuat grup target menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, di bawah VPC Lattice, pilih Grup target.
3. PilihBuat grup target.
4. Untuk Pilih jenis target, lakukan salah satu hal berikut:
   - Pilih Instans untuk mendaftarkan target berdasarkan ID instans.
   - Pilih alamat IP untuk mendaftarkan target berdasarkan alamat IP.
   - Pilih fungsi Lambda untuk mendaftarkan fungsi Lambda sebagai target.
   - Pilih Application Load Balancer untuk mendaftarkan Application Load Balancer sebagai target.
5. Untuk Name, masukkan nama untuk grup target. Nama ini harus unik untuk akun Anda di setiap AWS Wilayah, dapat memiliki maksimal 32 karakter, harus hanya berisi karakter alfanumerik atau tanda hubung, dan tidak boleh dimulai atau diakhiri dengan tanda hubung.
6. Untuk Protokol dan Port, Anda dapat memodifikasi nilai default sesuai kebutuhan. Protokol defaultnya adalah HTTPS dan port defaultnya adalah 443.

   Jika jenis target adalah fungsi Lambda, Anda tidak dapat menentukan protokol atau port.
7. Untuk jenis alamat IP, pilih IPv4 untuk mendaftarkan target dengan alamat IPv4 atau pilih IPv6 untuk mendaftarkan target dengan alamat IPv6. Anda tidak dapat mengubah pengaturan ini setelah grup target dibuat.

   Opsi ini hanya tersedia jika jenis targetnya adalah alamat IP.
8. UntukVPC, pilih Virtual Private Cloud (VPC).

   Opsi ini tidak tersedia jika jenis target adalah fungsi Lambda.
9. Untuk versi Protokol, ubah nilai default sesuai kebutuhan. Defaultnya adalah HTTP1.

   Opsi ini tidak tersedia jika jenis target adalah fungsi Lambda.
10. Untuk pemeriksaan Kesehatan, ubah pengaturan default sesuai kebutuhan. Untuk informasi selengkapnya, lihat Pemeriksaan kesehatan untuk grup target VPC Lattice Anda.

    Pemeriksaan kesehatan tidak tersedia jika jenis targetnya adalah fungsi Lambda.
11. Untuk versi struktur acara Lambda, pilih versi. Untuk informasi selengkapnya, lihat the section called “Menerima acara dari layanan VPC Lattice”.

Opsi ini hanya tersedia jika jenis target adalah fungsi Lambda

12. (Opsional) Untuk menambahkan tag, memperluas Tag, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
13. Pilih Selanjutnya.
14. Untuk Daftar target, Anda dapat melewati langkah ini atau menambahkan target sebagai berikut:
    - Jika jenis targetnya adalah Instans, pilih instance, masukkan port, lalu pilih Sertakan sebagai tertunda di bawah ini.
    - Jika jenis targetnya adalah alamat IP, lakukan hal berikut:
        a. Untuk Pilih jaringan, simpan VPC yang Anda pilih untuk grup target atau pilih Alamat IP pribadi lainnya.
        b. Untuk Tentukan IP dan tentukan port, masukkan alamat IP dan masukkan port. Port default adalah port grup target.
        c. Pilih Sertakan sebagai tertunda di bawah ini.
    - Jika jenis target adalah fungsi Lambda, pilih fungsi Lambda. Untuk membuat fungsi Lambda, pilih Buat fungsi Lambda baru.
    - Jika jenis target adalah Application Load Balancer, pilih Application Load Balancer. Untuk membuat Application Load Balancer, pilih buat Application Load Balancer.
15. PilihBuat grup target.

Untuk membuat grup target menggunakan AWS CLI

Gunakan create-target-groupperintah untuk membuat grup target dan perintah register-target untuk menambahkan target.

Subnet bersama

Peserta dapat membuat grup target VPC Lattice dalam VPC bersama. Aturan berikut berlaku untuk subnet bersama:

- Semua bagian dari layanan VPC Lattice, seperti pendengar, grup target, dan target, harus dibuat oleh akun yang sama. Mereka dapat dibuat dalam subnet yang dimiliki oleh atau dibagikan dengan pemilik layanan VPC Lattice.
- Target yang terdaftar dengan grup target harus dibuat oleh akun yang sama dengan kelompok sasaran.

- Hanya pemilik VPC yang dapat mengaitkan VPC dengan jaringan layanan. Sumber daya peserta dalam VPC bersama yang terkait dengan jaringan layanan dapat mengirim permintaan ke layanan yang terkait dengan jaringan layanan. Namun, administrator dapat mencegah hal ini dengan menggunakan grup keamanan, ACL jaringan, atau kebijakan autentikasi.

Untuk informasi selengkapnya tentang sumber daya yang dapat dibagikan untuk VPC Lattice, lihat. Bagikan sumber daya VPC Lattice

Daftarkan target dengan grup target VPC Lattice

Layanan Anda berfungsi sebagai titik kontak tunggal untuk klien dan mendistribusikan lalu lintas masuk ke seluruh target terdaftar yang sehat. Anda dapat mendaftarkan setiap target dengan satu atau lebih kelompok target.

Jika permintaan pada aplikasi Anda meningkat, Anda dapat mendaftarkan target tambahan dengan satu atau lebih kelompok sasaran untuk menangani permintaan. Layanan mulai merutekan permintaan ke target yang baru terdaftar segera setelah proses pendaftaran selesai dan target melewati pemeriksaan kesehatan awal.

Jika permintaan pada aplikasi Anda menurun, atau Anda perlu untuk melayani target Anda, Anda dapat membatalkan pendaftaran (deregistrasi) target dari kelompok target Anda. Proses deregisterasi target menghapus itu dari kelompok target Anda, tetapi tidak mempengaruhi target sebaliknya. Layanan berhenti merutekan permintaan ke target segera setelah dideregistrasi. Target memasuki keadaan`DRAINING` hingga permintaan dalam penerbangan telah selesai. Anda dapat mendaftarkan target dengan kelompok target lagi ketika target Anda siap untuk untuk melanjutkan menerima permintaan.

Jenis target grup target Anda menentukan bagaimana Anda mendaftarkan target dengan kelompok target tersebut. Untuk informasi selengkapnya, lihat Tipe target.

Gunakan prosedur konsol berikut untuk mendaftarkan atau membatalkan pendaftaran target. Atau, gunakan perintah register-target dan deregister-target dari. AWS CLI

Daftar Isi

- Mendaftarkan atau membatalkan pendaftaran Application Load Balancer

Register atau target deregister berdasarkan ID instance

Instance target harus berada di virtual private cloud (VPC) yang Anda tentukan untuk grup target. Contoh juga harus dalam keadaan`running` saat Anda mendaftarkannya.

Saat mendaftarkan target berdasarkan ID instans, Anda dapat menggunakan layanan Anda dengan grup Auto Scaling. Setelah Anda melampirkan grup target ke grup Auto Scaling dan grup skala keluar, instance yang diluncurkan grup Auto Scaling secara otomatis terdaftar dengan grup target. Jika Anda memisahkan grup target dari grup Auto Scaling, maka instans tersebut secara otomatis dihapus dari grup target. Untuk informasi selengkapnya, lihat Merutekan lalu lintas ke grup Auto Scaling Anda dengan grup target VPC Lattice di Panduan Pengguna Auto Scaling Amazon EC2.

Untuk mendaftarkan atau membatalkan pendaftaran target berdasarkan ID instans menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, di bawah VPC Lattice, pilih Grup target.
3. Pilih nama grup target untuk menampilkan detailnya.
4. Pilih tabTarget.
5. Untuk mendaftarkan contoh, pilihTarget daftar. Pilih instance, masukkan port instance, lalu pilih Sertakan sebagai tertunda di bawah ini. Setelah selesai menambahkan instance, pilih Daftarkan target.
6. Untuk membatalkan pendaftaran instance, pilih instance, lalu pilih Deregister.

Mendaftar atau membatalkan pendaftaran target berdasarkan alamat IP

Alamat IP target harus dari subnet VPC yang Anda tentukan untuk grup target. Anda tidak dapat mendaftarkan alamat IP layanan lain di VPC yang sama. Anda tidak dapat mendaftarkan titik akhir VPC atau alamat IP yang dapat dirutekan secara publik.

Untuk mendaftarkan atau membatalkan pendaftaran target berdasarkan alamat IP menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.

2. Pada panel navigasi, di bawah VPC Lattice, pilih Grup target.
3. Pilih nama grup target untuk menampilkan detailnya.
4. Pilih tabTarget.
5. Untuk mendaftarkan alamat IP, pilihTarget daftar. Untuk setiap alamat IP, pilih rangkaian, masukkan alamat IP dan port, dan pilihSertakan sebagai tertunda di bawah ini. Setelah selesai menentukan alamat, pilih Daftarkan target.
6. Untuk membatalkan pendaftaran alamat IP, pilih alamat IP, lalu pilihDeregister.

Mendaftar atau membatalkan pendaftaran fungsi Lambda

Anda dapat mendaftarkan satu fungsi Lambda dengan grup target. Jika Anda tidak perlu lagi mengirim lalu lintas ke fungsi Lambda Anda, Anda dapat membatalkan pendaftarannya. Setelah Anda membatalkan pendaftaran fungsi Lambda, permintaan dalam penerbangan gagal dengan galat HTTP 5XX. Lebih baik membuat grup target baru daripada mengganti fungsi Lambda untuk grup target.

Untuk mendaftarkan atau membatalkan pendaftaran fungsi Lambda menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, di bawah VPC Lattice, pilih Grup target.
3. Pilih nama grup target untuk menampilkan detailnya.
4. Pilih tabTarget.
5. Jika tidak ada fungsi Lambda yang terdaftar, pilih Daftarkan target. Pilih fungsi Lambda dan pilih Daftarkan target.
6. Untuk membatalkan pendaftaran fungsi Lambda, pilihDeregister. Saat diminta konfirmasi, masukkan **`confirm`** lalu pilih Deregister.

Mendaftarkan atau membatalkan pendaftaran Application Load Balancer

Anda dapat mendaftarkan Application Load Balancer tunggal dengan masing-masing grup target. Jika Anda tidak perlu lagi mengirim lalu lintas ke penyeimbang beban Anda, Anda dapat membatalkan pendaftarannya. Setelah Anda membatalkan pendaftaran penyeimbang beban, permintaan dalam penerbangan gagal dengan kesalahan HTTP 5XX. Lebih baik membuat grup target baru daripada mengganti Application Load Balancer untuk grup target.

Untuk mendaftarkan atau membatalkan pendaftaran Application Load Balancer menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, di bawah VPC Lattice, pilih Grup target.
3. Pilih nama grup target untuk menampilkan detailnya.
4. Pilih tabTarget.
5. Jika tidak ada Application Load Balancer yang terdaftar, pilih Register target. Pilih Application Load Balancer dan pilih Register target.
6. Untuk membatalkan pendaftaran Application Load Balancer, pilih Deregister. Saat diminta konfirmasi, masukkan **`confirm`** lalu pilih Deregister.

Pemeriksaan kesehatan untuk grup target VPC Lattice Anda

Layanan Anda secara berkala mengirimkan permintaan ke target yang terdaftar untuk menguji statusnya. Uji ini disebut pemeriksaan kondisi.

Setiap rute layanan VPC Lattice hanya meminta target yang sehat. Setiap layanan memeriksa kesehatan setiap target, menggunakan pengaturan pemeriksaan kesehatan untuk kelompok sasaran yang dengannya target terdaftar. Setelah target Anda terdaftar, target itu harus lulus satu pemeriksaan kondisi agar dapat dianggap sehat. Setelah setiap pemeriksaan kesehatan selesai, layanan menutup koneksi yang dibuat untuk pemeriksaan kesehatan.

Keterbatasan dan pertimbangan

- Ketika versi protokol grup target adalah HTTP1, pemeriksaan kesehatan diaktifkan secara default.
- Ketika versi protokol grup target adalah HTTP2, pemeriksaan kesehatan tidak diaktifkan secara default. Namun, Anda dapat mengaktifkan pemeriksaan kesehatan, dan secara manual mengatur versi protokol ke HTTP1 atau HTTP2.
- Pemeriksaan Kesehatan tidak mendukung versi protokol grup target gRPC. Namun, jika Anda mengaktifkan pemeriksaan kesehatan, Anda harus menentukan versi protokol pemeriksaan kesehatan sebagai HTTP1 atau HTTP2.
- Pemeriksaan Kesehatan tidak mendukung kelompok sasaran Lambda.
- Pemeriksaan Kesehatan tidak mendukung kelompok sasaran Application Load Balancer. Namun, Anda dapat mengaktifkan pemeriksaan kesehatan untuk target Application Load Balancer Anda menggunakan Elastic Load Balancing. Untuk informasi selengkapnya, lihat Kesehatan grup target di Panduan Pengguna untuk Penyeimbang Beban Aplikasi.

Pengaturan pemeriksaan kondisi

Anda mengonfigurasi pemeriksaan kondisi untuk target dalam grup target seperti yang dijelaskan dalam tabel berikut. Nama pengaturan yang digunakan dalam tabel adalah nama yang digunakan dalam API. Layanan mengirimkan permintaan pemeriksaan kesehatan ke setiap target yang terdaftar setiap HealthCheckIntervalSecondsdetik, menggunakan port, protokol, dan jalur ping yang ditentukan. Setiap permintaan pemeriksaan kondisi bersifat independen dan hasilnya berlaku selama seluruh interval. Waktu yang dibutuhkan untuk target untuk merespons tidak memengaruhi interval untuk permintaan pemeriksaan kondisi berikutnya. Jika pemeriksaan kesehatan melebihi kegagalan UnhealthyThresholdCountberturut-turut, layanan menghilangkan target dari layanan. Ketika pemeriksaan kesehatan melebihi keberhasilan HealthyThresholdCountberturut-turut, layanan menempatkan target kembali dalam layanan.

Pengaturan	Deskripsi
HealthCheckProtocol	Protokol yang digunakan layanan saat melakukan pemeriksaan kesehatan pada target. Protokol yang mungkin adalah HTTP dan HTTPS. Defaultnya adalah protokol HTTP.
HealthCheckPort	Port yang digunakan layanan saat melakukan pemeriksaan kesehatan pada target. Defaultny a adalah menggunakan port di mana setiap target menerima lalu lintas dari layanan.
HealthCheckPath	Tujuan pemeriksaan kondisi pada target. Jika versi protokol adalah HTTP1 atau HTTP2, tentukan URI (/path yang valid? pertanyaan). Default-nya adalah /.
HealthCheckTimeoutSeconds	Jumlah waktu, dalam detik, selama tidak ada respons dari target berarti pemeriksa an kondisi gagal. Kisarannya adalah 1-120 detik. Defaultnya adalah 5 detik jika tipe targetnya adalah `INSTANCE` atau`IP`. Tentukan 0 untuk mengatur ulang pengaturan ini ke nilai defaultnya.

Pengaturan	Deskripsi
HealthCheckIntervalSeconds	Perkiraan jumlah waktu, dalam hitungan detik, antara pemeriksaan kondisi dari target individu. Rentangnya adalah 5-300 detik. Defaultny a adalah 30 detik jika tipe targetnya adalah `INSTANCE` atau`IP`. Tentukan 0 untuk mengatur ulang pengaturan ini ke nilai defaultnya.
HealthyThresholdCount	Jumlah pemeriksaan kesehatan yang berhasil berturut-turut yang diperlukan sebelum target yang tidak sehat dianggap sehat. Rentangny a adalah 2–10. Defaultnya adalah 5. Tentukan 0 untuk mengatur ulang pengaturan ini ke nilai defaultnya.
UnhealthyThresholdCount	Jumlah pemeriksaan kondisi yang gagal berturut-turut diperlukan sebelum mengangga p target tidak sehat. Rentangnya adalah 2–10. Defaultnya adalah 2. Tentukan 0 untuk mengatur ulang pengaturan ini ke nilai defaultnya.

Pengaturan	Deskripsi
Matcher	Kode yang digunakan saat memeriksa respons yang berhasil dari target. Ini disebut Kode berhasil pada konsol. Jika versi protokol adalah HTTP1 atau HTTP2, nilai yang mungkin adalah dari 200 hingga 499. Anda dapat menentukan beberapa nilai (misalnya, “200,202") atau rentang nilai (misalnya, “200-299"). Nilai default adalah 200. Versi protokol pemeriksaan kesehatan untuk gRPC saat ini tidak didukung. Namun, jika versi protokol grup target Anda adalah gRPC, Anda dapat menentukan versi protokol HTTP1 atau HTTP2 dalam konfigurasi pemeriksaan kesehatan Anda.

Periksa kondisi target Anda

Anda dapat memeriksa status kondisi target yang terdaftar dengan kelompok target Anda.

Untuk memeriksa kesehatan target Anda menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, di bawah VPC Lattice, pilih Grup target.
3. Pilih nama grup target untuk menampilkan detailnya.
4. Pada tab Target, kolom Status Kesehatan menunjukkan status setiap target. Jika status adalah nilai selain`Healthy`, kolom Detail status Kesehatan berisi informasi lebih lanjut.

Untuk memeriksa kesehatan target Anda menggunakan AWS CLI

Gunakan perintah daftar-target. Keluaran dari perintah ini berisi status kondisi target. Jika status adalah nilai selain `Healthy`, output juga termasuk kode alasan.

Untuk menerima pemberitahuan email tentang target yang tidak sehat

Gunakan CloudWatch alarm untuk memulai fungsi Lambda untuk mengirim detail tentang target yang tidak sehat.

Ubah pengaturan pemeriksaan kesehatan

Anda dapat mengubah pengaturan pemeriksaan kondisi untuk grup target kapan saja.

Untuk mengubah pengaturan pemeriksaan kesehatan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, di bawah VPC Lattice, pilih Grup target.
3. Pilih nama grup target untuk menampilkan detailnya.
4. Pada tab Pemeriksaan Kesehatan, di bagian Pengaturan pemeriksaan Kesehatan, pilih Edit.
5. Ubah pengaturan pemeriksaan kesehatan sesuai kebutuhan.
6. Pilih Simpan perubahan.

Untuk mengubah pengaturan pemeriksaan kesehatan menggunakan AWS CLI

Gunakan perintah update-target-group.

Konfigurasi perutean

Secara default, layanan merutekan permintaan ke targetnya menggunakan protokol dan nomor port yang Anda tentukan saat Anda membuat grup target. Atau, Anda dapat mengganti port yang digunakan untuk merutekan lalu lintas ke target saat Anda mendaftarkannya dengan grup target.

Kelompok target mendukung protokol dan port berikut ini:

- Protokol: HTTP, HTTPS, TCP
- Port: 1-65535

Jika grup target dikonfigurasi dengan protokol HTTPS atau menggunakan pemeriksaan kesehatan HTTPS, koneksi TLS ke target menggunakan kebijakan keamanan dari pendengar. VPC Lattice membuat koneksi TLS dengan target menggunakan sertifikat yang Anda instal pada target. VPC Lattice tidak memvalidasi sertifikat ini. Oleh karena itu, Anda dapat menggunakan sertifikat ditandatangani sendiri atau sertifikat yang telah kedaluwarsa. Lalu lintas antara VPC Lattice dan

target diautentikasi pada tingkat paket, sehingga tidak berisiko man-in-the-middle serangan atau spoofing bahkan jika sertifikat pada target tidak valid.

Grup target TCP hanya didukung dengan pendengar TLS.

Algoritma perutean

Secara default, algoritma routing round robin digunakan untuk merutekan permintaan ke target yang sehat.

Ketika layanan VPC Lattice menerima permintaan, ia menggunakan proses berikut:

1. Mengevaluasi aturan pendengar dalam rangka prioritas untuk menentukan aturan yang diterapkan.
2. Memilih target dari kelompok target untuk tindakan aturan, menggunakan algoritma round robin default. Routing dilakukan secara mandiri untuk setiap grup target, bahkan ketika target telah terdaftar dengan beberapa kelompok target.

Jika kelompok sasaran hanya berisi target yang tidak sehat, permintaan diarahkan ke semua target, terlepas dari status kesehatan mereka. Ini berarti bahwa jika semua target gagal pemeriksaan kesehatan pada saat yang sama, layanan VPC Lattice gagal dibuka. Efek dari fail-open adalah untuk memungkinkan lalu lintas ke semua target, terlepas dari status kesehatan mereka, berdasarkan algoritma round robin.

Tipe target

Bila Anda membuat grup target, Anda menentukan jenis targetnya, yang menentukan jenis target yang Anda tentukan saat mendaftarkan target dengan grup target ini. Setelah Anda membuat grup target, Anda tidak dapat mengubah jenis targetnya.

Status yang mungkin muncul adalah sebagai berikut:

`INSTANCE`

Target ditentukan oleh contoh ID.

`IP`

Targetnya adalah alamat IP.

`LAMBDA`

Targetnya adalah fungsi Lambda.

`ALB`

Targetnya adalah Application Load Balancer.

Pertimbangan

- Ketika jenis targetnya`IP`, Anda harus menentukan alamat IP dari subnet VPC untuk grup target. Jika Anda perlu mendaftarkan alamat IP dari luar VPC ini, buat kelompok target tipe `ALB` dan daftarkan alamat IP dengan Application Load Balancer.
- Ketika jenis targetnya`IP`, Anda tidak dapat mendaftarkan titik akhir VPC atau alamat IP yang dapat dirutekan secara publik.
- Ketika jenis targetnya`LAMBDA`, Anda dapat mendaftarkan satu fungsi Lambda. Ketika layanan menerima permintaan untuk fungsi Lambda, ia memanggil fungsi Lambda. Jika Anda ingin mendaftarkan beberapa fungsi lambda ke layanan, Anda perlu menggunakan beberapa grup target.
- Ketika jenis targetnya adalah`ALB`, Anda dapat mendaftarkan Application Load Balancer internal tunggal sebagai target hingga dua VPC Lattice Services. Untuk melakukan ini, daftarkan Application Load Balancer dengan dua kelompok target terpisah, yang digunakan oleh dua layanan VPC Lattice yang berbeda. Selain itu, Application Load Balancer yang ditargetkan harus memiliki setidaknya satu pendengar yang portnya cocok dengan port grup target.
- Untuk mendaftarkan tugas ECS sebagai target, gunakan jenis `ALB` target dan daftarkan Application Load Balancer untuk layanan Amazon ECS Anda. Untuk informasi lebih lanjut, lihat Penyeimbang beban layanan di Panduan Developer Layanan Amazon Elastic Container.
- Untuk mendaftarkan pod EKS sebagai target, gunakan AWS Gateway API Controller, yang mendapatkan alamat IP dari layanan Kubernetes.
- Jika protokol grup target adalah TCP, satu-satunya jenis target yang didukung adalah `INSTANCE` dan`IP`.

Jenis alamat IP

Saat Anda membuat grup target dengan tipe target`IP`, Anda dapat menentukan jenis alamat IP untuk grup target. Ini menentukan jenis alamat apa yang digunakan penyeimbang beban untuk mengirim

permintaan dan pemeriksaan kesehatan ke target. Nilai yang mungkin adalah `IPv4` dan `IPv6`. Default-nya adalah `IPV4`.

Pertimbangan

- Jika Anda membuat grup target dengan jenis alamat IP`IPv6`, VPC yang Anda tentukan untuk grup target harus memiliki rentang alamat IPv6.
- Alamat IP yang Anda daftarkan dengan grup target harus sesuai dengan jenis alamat IP dari grup target. Misalnya, Anda tidak dapat mendaftarkan alamat IPv6 dengan grup target jika jenis alamat IP-nya. `IPv4`
- Alamat IP yang Anda daftarkan dengan grup target harus berada dalam kisaran alamat IP VPC yang Anda tentukan untuk grup target.

Target HTTP di VPC Lattice

Permintaan HTTP dan respons HTTP menggunakan bidang header untuk mengirim informasi tentang pesan HTTP. Header HTTP ditambahkan secara otomatis. Bidang header adalah pasangan nama-nilai yang dipisahkan titik dua yang dipisahkan oleh carriage return (CR) dan line feed (LF). Satu set standar bidang header HTTP didefinisikan dalam RFC 2616, Header Pesan. Ada juga header HTTP non-standar yang tersedia secara otomatis ditambahkan dan digunakan secara luas oleh aplikasi. Misalnya, ada header HTTP non-standar dengan awalan. `x-forwarded`

x-forwardedheader

Amazon VPC Lattice menambahkan header berikut: `x-forwarded`

`x-forwarded-for`

Alamat IP sumber.

`x-forwarded-for-port`

Port tujuan.

`x-forwarded-for-proto`

Protokol koneksi (`http`|`https`).

Header identitas pemanggil

Amazon VPC Lattice menambahkan header identitas pemanggil berikut:

`x-amzn-lattice-identity`

Informasi identitas. Bidang berikut hadir jika AWS otentikasi berhasil.

- `Principal`— Prinsipal yang diautentikasi.
- `PrincipalOrgID`— ID organisasi untuk prinsipal yang diautentikasi.
- `SessionName`— Nama sesi yang diautentikasi.

Bidang berikut hadir jika kredensyal Peran Di Mana Saja digunakan dan otentikasi berhasil.

- `X509Issuer/OU`— Penerbit (OU).
- `X509SAN/DNS`— Nama alternatif subjek (DNS).
- `X509SAN/NameCN`— Nama alternatif penerbit (nama/CN).
- `X509SAN/URI`— Nama alternatif subjek (URI).
- `X509Subject/CN`Nama subjek (CN).

`x-amzn-lattice-network`

VPC. Formatnya adalah sebagai berikut.

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

`x-amzn-lattice-target`

Target. Formatnya adalah sebagai berikut.

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

Untuk informasi tentang ARN sumber daya untuk Kisi VPC, lihat Jenis sumber daya yang ditentukan oleh Amazon VPC Lattice.

Lambda berfungsi sebagai target di VPC Lattice

Anda dapat mendaftarkan fungsi Lambda sebagai target dengan grup target VPC Lattice, dan mengonfigurasi aturan listener untuk meneruskan permintaan ke grup target untuk fungsi Lambda

Anda. Ketika layanan meneruskan permintaan ke grup target dengan fungsi Lambda sebagai target, layanan akan memanggil fungsi Lambda Anda dan meneruskan konten permintaan ke fungsi Lambda, dalam format JSON. Untuk informasi selengkapnya, lihat Menggunakan AWS Lambda dengan Amazon VPC Lattice di Panduan Pengembang.AWS Lambda

Batasan

- Fungsi Lambda dan kelompok target harus dalam akun dan di wilayah yang sama.
- Ukuran maksimum badan permintaan yang dapat Anda kirim ke fungsi Lambda adalah 6 MB.
- Ukuran maksimum respons JSON yang dapat dikirim oleh fungsi Lambda adalah 6 MB.
- Protokol harus HTTP atau HTTPS.

Siapkan fungsi Lambda

Rekomendasi berikut berlaku jika Anda menggunakan fungsi Lambda Anda dengan layanan VPC Lattice.

Izin untuk mengaktifkan fungsi Lambda

Saat Anda membuat grup target dan mendaftarkan fungsi Lambda menggunakan AWS Management Console atau, AWS CLI VPC Lattice menambahkan izin yang diperlukan ke kebijakan fungsi Lambda Anda atas nama Anda.

Anda juga dapat menambahkan izin sendiri menggunakan panggilan API berikut:

```
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
```

Versioning fungsi Lambda

Anda dapat mendaftarkan satu fungsi Lambda per kelompok target. Untuk memastikan bahwa Anda dapat mengubah fungsi Lambda Anda dan bahwa layanan VPC Lattice selalu memanggil versi fungsi Lambda saat ini, buat alias fungsi dan sertakan alias dalam fungsi ARN saat Anda mendaftarkan fungsi Lambda dengan layanan VPC Lattice. Untuk informasi selengkapnya, lihat Versi fungsi Lambda dan Membuat alias untuk fungsi Lambda di Panduan Pengembang.AWS Lambda

Buat grup target untuk fungsi Lambda

Buat grup target, yang digunakan dalam routing permintaan. Jika konten permintaan cocok dengan aturan listener dengan tindakan untuk meneruskannya ke grup target ini, layanan VPC Lattice akan memanggil fungsi Lambda terdaftar.

Untuk membuat grup target dan mendaftarkan fungsi Lambda menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, di bawah VPC Lattice, pilih Grup target.
3. PilihBuat grup target.
4. UntukPilih jenis targetPilihFungsi Lambda.
5. Untuk Name, masukkan nama untuk grup target.
6. Untuk versi struktur acara Lambda, pilih versi. Untuk informasi selengkapnya, lihat the section called “Menerima acara dari layanan VPC Lattice”.
7. (Opsional) Untuk menambahkan tag, memperluas Tag, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
8. Pilih Selanjutnya.
9. UntukFungsi LambdaLakukan salah satu langkah berikut:
   - Pilih fungsi Lambda yang ada.
   - Buat fungsi Lambda baru dan pilih.
   - Daftarkan fungsi Lambda nanti.
10. PilihBuat grup target.

Untuk membuat grup target dan mendaftarkan fungsi Lambda menggunakan AWS CLI

Gunakan perintah create-target-groupdan daftar-target.

Menerima acara dari layanan VPC Lattice

Layanan VPC Lattice mendukung pemanggilan Lambda untuk permintaan melalui HTTP dan HTTPS. Layanan mengirimkan acara dalam format JSON, dan menambahkan `X-Forwarded-For` header ke setiap permintaan.

Enkode Base64

Layanan Base64 mengkodekan badan jika `content-encoding` header ada dan jenis konten bukan salah satu dari yang berikut:

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

Jika`content-encoding`header tidak hadir, encoding Base64 tergantung pada jenis konten. Untuk jenis konten di atas, layanan mengirimkan badan apa adanya, tanpa pengkodean Base64.

Format struktur acara

Saat membuat atau memperbarui jenis grup target`LAMBDA`, Anda dapat menentukan versi struktur acara yang diterima fungsi Lambda Anda. Versi yang mungkin adalah `V1` dan`V2`.

Example Contoh acara: 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`

Tubuh permintaan. Hadir hanya jika protokolnya HTTP, HTTPS, atau gRPC.

`headers`

Header HTTP dari permintaan. Hadir hanya jika protokolnya HTTP, HTTPS, atau gRPC.

`identity`

Informasi identitas. Berikut ini adalah bidang yang mungkin.

- `principal`— Prinsipal yang diautentikasi. Hadir hanya jika AWS otentikasi berhasil.
- `principalOrgID`— ID organisasi untuk prinsipal yang diautentikasi. Hadir hanya jika AWS otentikasi berhasil.
- `sessionName`— Nama sesi yang diautentikasi. Hadir hanya jika AWS otentikasi berhasil.
- `sourceVpcArn`— ARN dari VPC tempat permintaan berasal. Hadir hanya jika sumber VPC dapat diidentifikasi.
- `type`— Nilainya adalah `AWS_IAM` jika kebijakan autentikasi digunakan dan AWS otentikasi berhasil.

Jika kredensyal Roles Anywhere digunakan dan otentikasi berhasil, berikut ini adalah bidang yang memungkinkan.

- `x509IssuerOu`— Penerbit (OU).
- `x509SanDns`— Nama alternatif subjek (DNS).
- `x509SanNameCn`— Nama alternatif penerbit (nama/CN).

- `x509SanUri`— Nama alternatif subjek (URI).
- `x509SubjectCn`Nama subjek (CN).

`isBase64Encoded`

Menunjukkan apakah tubuh dikodekan base64. Hadir hanya jika protokolnya HTTP, HTTPS, atau gRPC dan badan permintaan belum berupa string.

`method`

Metode HTTP permintaan. Hadir hanya jika protokolnya HTTP, HTTPS, atau gRPC.

`path`

Jalur permintaan. Hadir hanya jika protokolnya HTTP, HTTPS, atau gRPC.

`queryStringParameters`

Parameter string kueri HTTP. Hadir hanya jika protokolnya HTTP, HTTPS, atau gRPC.

`serviceArn`

ARN dari layanan yang menerima permintaan.

`serviceNetworkArn`

ARN dari jaringan layanan yang memberikan permintaan.

`targetGroupArn`

ARN dari kelompok sasaran yang menerima permintaan.

`timeEpoch`

Waktu, dalam mikrodetik.

Example Contoh acara: 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
```

```
}
```

Menanggapi layanan VPC Lattice

Respon dari fungsi Lambda Anda harus mencakup status encoding Base64, kode status, dan header. Anda bisa menghilangkan bagian tubuhnya.

Untuk memasukkan konten biner dalam tubuh respon, Anda harus mengkodekan Base64 konten dan mengatur`isBase64Encodedketrue`. Layanan menerjemahkan konten untuk mengambil konten biner dan mengirimkannya ke klien di badan respons HTTP.

Layanan VPC Lattice tidak menghormati hop-by-hop header, seperti atau. `Connection` `Transfer-Encoding` Anda dapat menghilangkan `Content-Length` header karena layanan menghitungnya sebelum mengirim tanggapan ke klien.

Berikut ini adalah contoh respon dari fungsi Lambda:

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

Header nilai ganda

Secara default, VPC Lattice mendukung permintaan dari klien atau tanggapan dari fungsi Lambda yang berisi header dengan beberapa nilai atau berisi header yang sama beberapa kali. VPC Lattice juga mendukung parameter kueri dengan beberapa nilai untuk kunci yang sama.

Untuk header permintaan, jika beberapa parameter memiliki nama yang sama, VPC Lattice akan meneruskan kedua nilai ke target. Berikut ini adalah contoh di mana `header 1` adalah nama dari dua header terpisah:

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

Kemudian VPC Lattice mengirimkan kedua nilai ke target:

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

Untuk string kueri, jika beberapa parameter berbagi nama yang sama, nilai terakhir menang. Ini berarti bahwa parameter `_not_ coalesced` menjadi satu nilai jika mereka berbagi nama kunci yang sama.

Berikut ini adalah contoh di mana `foo` dan `bar` merupakan nilai parameter dengan nama yang sama,`QS1`:

```
http://www.example.com?&QS1=foo&QS1=bar
```

Kemudian VPC Lattice mengirimkan nilai terakhir ke target:

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

Deregristrasi fungsi Lambda

Jika Anda tidak perlu lagi mengirim lalu lintas ke fungsi Lambda Anda, Anda dapat membatalkan pendaftarannya. Setelah Anda membatalkan pendaftaran fungsi Lambda, permintaan dalam penerbangan gagal dengan galat HTTP 5XX.

Untuk mengganti fungsi Lambda, kami sarankan Anda membuat grup target baru, mendaftarkan fungsi baru dengan kelompok target baru, dan memperbarui aturan pendengar untuk menggunakan kelompok target baru bukan yang sudah ada.

Untuk membatalkan pendaftaran fungsi Lambda menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, di bawah VPC Lattice, pilih Grup target.
3. Pilih nama grup target untuk menampilkan detailnya.
4. Pada tab Target, pilihDeregister.
5. Saat diminta konfirmasi, masukkan **`confirm`** lalu pilih Deregister.

Untuk membatalkan pendaftaran fungsi Lambda menggunakan AWS CLI

Gunakan perintah Target deregister.

Aplikasi Load Balancer sebagai target di VPC Lattice

Anda dapat membuat grup target VPC Lattice, mendaftarkan Application Load Balancer internal tunggal sebagai target, dan mengonfigurasi layanan VPC Lattice Anda untuk meneruskan lalu lintas ke grup target ini. Dalam skenario ini, Application Load Balancer mengambil alih keputusan routing segera setelah lalu lintas mencapainya. Konfigurasi ini memungkinkan Anda untuk menggunakan fitur routing berbasis permintaan lapisan 7 dari Application Load Balancer dalam kombinasi dengan fitur yang didukung VPC Lattice, seperti autentikasi dan otorisasi IAM, dan konektivitas di seluruh VPC dan akun.

Batasan

- Anda dapat mendaftarkan Application Load Balancer internal tunggal sebagai target dalam jenis grup target VPC Lattice. `ALB`
- Anda dapat mendaftarkan Application Load Balancer sebagai target hingga dua grup target VPC Lattice, yang digunakan oleh dua layanan VPC Lattice yang berbeda.
- VPC Lattice tidak menyediakan pemeriksaan kesehatan untuk kelompok target `ALB` tipe. Namun, Anda dapat mengonfigurasi pemeriksaan kesehatan secara independen di level load balancer untuk target di Elastic Load Balancing. Untuk informasi selengkapnya, lihat Pemeriksaan Kesehatan untuk grup target Anda di Panduan Pengguna untuk Penyeimbang Beban Aplikasi

Prasyarat

Buat Application Load Balancer untuk mendaftar sebagai target dengan grup target VPC Lattice Anda. Penyeimbang beban harus memenuhi kriteria berikut:

- Skema penyeimbang beban adalah Internal.
- Application Load Balancer harus berada dalam akun yang sama dengan grup target VPC Lattice, dan harus dalam status Aktif.
- Application Load Balancer harus berada dalam VPC yang sama dengan grup target VPC Lattice.
- Anda dapat menggunakan pendengar HTTPS pada Application Load Balancer untuk mengakhiri TLS, tetapi hanya jika layanan VPC Lattice menggunakan sertifikat SSL/TLS yang sama dengan penyeimbang beban.
- Untuk mempertahankan IP klien dari layanan VPC Lattice di header `X-Forwarded-For` permintaan, Anda harus mengatur atribut untuk Application Load Balancer ke. `routing.http.xff_header_processing.mode` `Preserve` Jika nilainya`Preserve`,

penyeimbang beban mempertahankan `X-Forwarded-For` header dalam permintaan HTTP, dan mengirimkannya ke target tanpa perubahan apa pun. Untuk informasi selengkapnya, lihat X-Forwarded-For di Panduan Pengguna untuk Penyeimbang Beban Aplikasi.

Untuk informasi selengkapnya, lihat Membuat Application Load Balancer di Panduan Pengguna untuk Application Load Balancers.

Langkah 1: Buat grup target tipe ALB

Gunakan prosedur berikut untuk membuat grup target. Perhatikan bahwa VPC Lattice tidak mendukung pemeriksaan kesehatan untuk kelompok sasaran ALB. Namun, Anda dapat mengonfigurasi pemeriksaan kesehatan untuk grup target untuk Application Load Balancer Anda. Untuk informasi selengkapnya, lihat Kesehatan grup target di Panduan Pengguna untuk Penyeimbang Beban Aplikasi.

Untuk membuat grup target

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, di bawah VPC Lattice, pilih Grup target.
3. PilihBuat grup target.
4. Pada halaman Tentukan detail grup target, di bawah konfigurasi Dasar, pilih Application Load Balancer sebagai tipe target.
5. Untuk Name, masukkan nama untuk grup target.
6. Untuk Protokol, pilih **`HTTP`** atau **`HTTPS`**. Protokol grup target harus sesuai dengan protokol pendengar untuk Application Load Balancer internal Anda.
7. Untuk Port, tentukan port untuk grup target Anda. Port ini harus cocok dengan port listener untuk Application Load Balancer internal Anda. Anda dapat menambahkan port listener pada Application Load Balancer internal agar sesuai dengan port grup target yang Anda tentukan di sini.
8. Untuk VPC, pilih virtual private cloud (VPC) yang sama dengan yang Anda pilih saat membuat Application Load Balancer internal. Ini harus menjadi VPC yang berisi sumber daya VPC Lattice Anda.
9. Untuk versi Protokol, pilih versi protokol yang didukung Application Load Balancer Anda.
10. (Opsional) Tambahkan tag yang diperlukan.
11. Pilih Selanjutnya.

Langkah 2: Daftarkan Application Load Balancer sebagai target

Anda dapat mendaftarkan penyeimbang beban sebagai target sekarang atau nanti.

Mendaftarkan Application Load Balancer sebagai target

1. Pilih Daftar sekarang.
2. Untuk Application Load Balancer, pilih Application Load Balancer internal Anda.
3. Untuk Port, pertahankan default atau tentukan port yang berbeda sesuai kebutuhan. Port ini harus cocok dengan port listener yang ada di Application Load Balancer Anda. Jika Anda melanjutkan tanpa port yang cocok, lalu lintas tidak akan mencapai Application Load Balancer Anda.
4. PilihBuat grup target.

Versi protokol

Secara default, layanan mengirim permintaan ke target menggunakan HTTP/1.1. Anda dapat menggunakan versi protokol untuk mengirim permintaan ke target menggunakan HTTP/2 atau gRPC.

Tabel berikut merangkum hasil untuk kombinasi protokol permintaan dan versi protokol kelompok target.

Protokol permintaan	Versi protokol	Hasil
HTTP/1.1	HTTP/1.1	Sukses
HTTP/2	HTTP/1.1	Sukses
gRPC	HTTP/1.1	Kesalahan
HTTP/1.1	HTTP/2	Kesalahan
HTTP/2	HTTP/2	Sukses
gRPC	HTTP/2	Sukses jika target mendukung gRPC
HTTP/1.1	gRPC	Kesalahan

Protokol permintaan	Versi protokol	Hasil
HTTP/2	gRPC	Sukses jika permintaan POST
gRPC	gRPC	Sukses

Pertimbangan untuk versi protokol gRPC

- Satu-satunya protokol pendengar yang didukung adalah HTTPS.
- Jenis-jenis target yang didukung hanya `INSTANCE` dan `IP`.
- Layanan mem-parsing permintaan gRPC dan merutekan panggilan gRPC ke grup target yang sesuai berdasarkan paket, layanan, dan metode.
- Anda tidak dapat menggunakan fungsi Lambda sebagai target.

Pertimbangan untuk versi protokol HTTP/2

- Satu-satunya protokol pendengar yang didukung adalah HTTPS. Anda dapat memilih HTTP atau HTTPS untuk protokol grup target.
- Satu-satunya aturan pendengar yang didukung adalah respons maju dan tetap.
- Jenis-jenis target yang didukung hanya `INSTANCE` dan `IP`.
- Layanan ini mendukung streaming dari klien. Layanan ini tidak mendukung streaming ke target.

Tag untuk grup target VPC Lattice Anda

Tag membantu Anda mengategorikan grup target Auto dengan berbagai cara, misalnya, berdasarkan tujuan, pemilik, atau lingkungan.

Anda dapat menambahkan beberapa tag ke setiap grup Auto Scaling. Tombol tag harus unik untuk setiap kelompok target. Jika Anda menambahkan tag dengan kunci yang sudah terkait dengan grup target, maka akan memperbarui nilai tag tersebut.

Setelah selesai dengan tag, Anda dapat menghapusnya.

Pembatasan

- Jumlah maksimum tanda per sumber daya—50

- Panjang kunci maksimum – 127 karakter Unicode
- Panjang nilai maksimum—255 karakter Unicode
- Kunci dan nilai tag peka huruf besar/kecil. Karakter yang diizinkan adalah huruf, spasi, dan angka yang dapat diwakili dalam UTF-8, ditambah karakter khusus berikut: + - = . _:/@. Jangan gunakan spasi terkemuka atau paling belakang.
- Jangan gunakan `aws:` awalan dalam nama atau nilai tag Anda karena itu dicadangkan untuk AWS digunakan. Anda tidak dapat mengedit atau menghapus nama atau nilai tag dengan awalan ini. Tag dengan awalan ini tidak dihitung terhadap tag Anda per batas sumber daya.

Untuk memperbarui tag untuk grup target menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Grup target.
3. Pilih nama grup target untuk membuka halaman detailnya.
4. Pilih tab Tanda.
5. Untuk menambahkan tag, pilih Tambahkan tag dan masukkan kunci tag dan nilai tag. Untuk menambahkan tag lain, pilih Tambahkan tag baru. Setelah Anda selesai menambahkan tanda, pilih Simpan perubahan.
6. Untuk menghapus tag, pilih kotak centang untuk tag dan pilih Hapus. Saat diminta konfirmasi, masukkan **`confirm`**, lalu pilih Hapus.

Untuk memperbarui tag untuk grup target menggunakan AWS CLI

Gunakan perintah tag-resource dan untag-resource.

Menghapus grup target VPC Lattice

Anda dapat menghapus kelompok target jika tidak direferensikan oleh tindakan lanjut dari aturan pendengar. Menghapus kelompok target tidak mempengaruhi target terdaftar dengan kelompok target. Jika Anda tidak lagi membutuhkan instance EC2 terdaftar, Anda dapat menghentikan atau menghapusnya.

Untuk menghapus grup target menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.

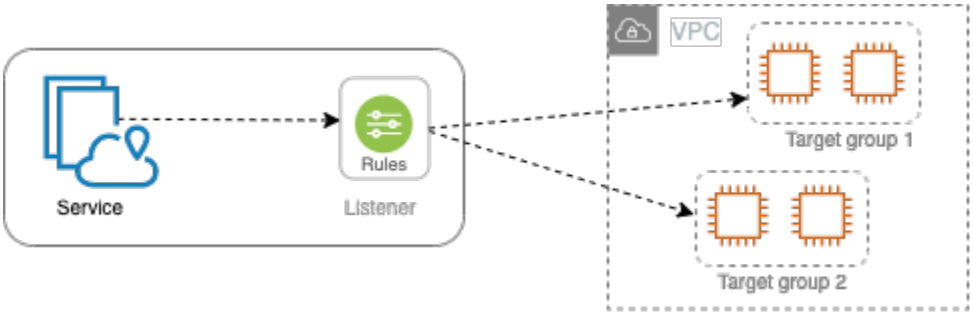
2. Pada panel navigasi, pilih Grup sasaran.
3. Pilih kotak centang untuk grup target dan kemudian pilih Tindakan, Hapus.
4. Saat diminta konfirmasi, masukkan **`confirm`**, lalu pilih Hapus.

Untuk menghapus grup target menggunakan AWS CLI

Gunakan perintah delete-target-group.

Pendengar untuk layanan VPC Lattice Anda

Sebelum Anda mulai menggunakan layanan VPC Lattice Anda, Anda harus menambahkan pendengar. Listener adalah proses yang memeriksa permintaan koneksi, menggunakan protokol dan port yang Anda konfigurasikan. Aturan yang Anda tetapkan untuk pendengar menentukan cara layanan merutekan permintaan ke target terdaftarnya.



Daftar Isi

Konfigurasi listener

Listener mendukung protokol dan port berikut ini:

- Protokol: HTTP, HTTPS, TLS
- Port: 1-65535

Jika protokol pendengar adalah HTTPS, VPC Lattice akan menyediakan dan mengelola sertifikat TLS yang terkait dengan VPC Lattice yang dihasilkan FQDN. VPC Lattice mendukung TLS pada

HTTP/1.1 dan HTTP/2. Saat Anda mengonfigurasi layanan dengan pendengar HTTPS, VPC Lattice akan secara otomatis menentukan protokol HTTP menggunakan Application-Layer Protocol Negotiation (ALPN). Jika ALPN tidak ada, VPC Lattice default ke HTTP/1.1. Untuk informasi selengkapnya, lihat Pendengar HTTPS.

VPC Lattice dapat mendengarkan HTTP, HTTPS, HTTP/1.1, dan HTTP/2 dan berkomunikasi dengan target di salah satu protokol dan versi ini. Kami tidak mengharuskan pendengar dan protokol grup target cocok. VPC Lattice mengelola seluruh proses upgrade dan downgrade antara protokol dan versi. Untuk informasi selengkapnya, lihat Versi protokol.

Anda dapat membuat pendengar TLS untuk memastikan bahwa aplikasi Anda mendekripsi lalu lintas terenkripsi, bukan VPC Lattice. Untuk informasi selengkapnya, lihat Pendengar TLS.

VPC Lattice tidak mendukung. WebSockets

Buat pendengar

Anda dapat membuat pendengar untuk layanan VPC Lattice Anda. Saat membuat listener, Anda harus menentukan nama, tindakan default, dan protokol. Pendengar dilengkapi dengan aturan default. Anda juga dapat membuat aturan tambahan untuk pendengar Anda.

Untuk membuat listener menggunakan konsol

- the section called “Menambahkan listener HTTP ”
- the section called “Menambahkan pendengar HTTPS”
- the section called “Tambahkan pendengar TLS”
- the section called “Tambahkan peraturan”

Untuk membuat pendengar menggunakan AWS CLI

Gunakan perintah create-listener dan create-rule.

Pendengar HTTP untuk layanan VPC Lattice

Listener adalah proses memeriksa permintaan koneksi. Anda dapat menentukan listener saat membuat layanan VPC Lattice Anda. Anda dapat menambahkan pendengar ke layanan Anda kapan saja.

Informasi di halaman ini membantu Anda membuat pendengar HTTP untuk layanan Anda. Untuk informasi tentang membuat pendengar yang menggunakan protokol lain, lihat dan. Pendengar HTTPS Pendengar TLS

Prasyarat

- Untuk menambahkan tindakan penerusan ke aturan pendengar default, Anda harus menentukan grup target VPC Lattice yang tersedia. Untuk informasi selengkapnya, lihat Buat grup target VPC Lattice.
- Anda dapat menentukan grup target yang sama di beberapa pendengar, tetapi pendengar ini harus milik layanan yang sama. Untuk menggunakan grup target dengan layanan VPC Lattice, Anda harus memverifikasi bahwa grup tersebut tidak digunakan oleh pendengar untuk layanan VPC Lattice lainnya.

Menambahkan listener HTTP

Anda dapat menambahkan pendengar dan aturan ke layanan Anda kapan saja. Anda mengonfigurasi listener dengan protokol dan port untuk koneksi dari klien ke layanan, dan grup target VPC Lattice untuk aturan pendengar default. Untuk informasi selengkapnya, lihat Konfigurasi listener.

Untuk menambahkan listener HTTP menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih nama layanan untuk membuka halaman detailnya.
4. Pada tab Routing, pilih Add listener.
5. Untuk nama Listener, Anda dapat memberikan nama pendengar kustom, atau menggunakan protokol dan port listener Anda sebagai nama listener. Nama kustom yang Anda tentukan dapat memiliki hingga 63 karakter, dan itu harus unik untuk setiap layanan di akun Anda. Karakter yang valid adalah a-z, 0-9, dan tanda hubung (-). Anda tidak dapat menggunakan tanda hubung sebagai karakter pertama atau terakhir, atau segera setelah tanda hubung lainnya. Anda tidak dapat mengubah nama setelah Anda membuatnya.
6. Untuk Protokol: port, pilih HTTP dan masukkan nomor port.
7. Untuk tindakan Default, pilih grup target VPC Lattice untuk menerima lalu lintas dan pilih bobot yang akan ditetapkan ke grup target ini. Bobot yang Anda tetapkan ke grup sasaran menetapkan prioritasnya untuk menerima lalu lintas. Misalnya, jika dua kelompok sasaran memiliki bobot

yang sama, masing-masing kelompok sasaran menerima setengah dari lalu lintas. Jika Anda telah menentukan hanya satu kelompok target, maka 100 persen dari lalu lintas dikirim ke satu kelompok target.

Anda dapat menambahkan grup target lain secara opsional untuk tindakan default. Pilih Tambah tindakan dan kemudian pilih grup target dan tentukan bobotnya.

8. (Opsional) Untuk menambahkan aturan lain, pilih Tambahkan aturan lalu masukkan nama, prioritas, kondisi, dan tindakan untuk aturan tersebut.

   Anda dapat memberikan setiap aturan nomor prioritas antara 1 dan 100. Listener tidak bisa memiliki beberapa aturan dengan prioritas yang sama. Peraturan dievaluasi dalam urutan prioritas, dari nilai terendah ke nilai tertinggi. Peraturan default dievaluasi terakhir. Untuk informasi selengkapnya, lihat Aturan pendengar.
9. (Opsional) Untuk menambahkan tag, perluas tag Listener, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
10. Tinjau konfigurasi Anda, lalu pilih Tambah.

Untuk menambahkan pendengar HTTP menggunakan AWS CLI

Gunakan perintah create-listener untuk membuat listener dengan aturan default, dan perintah create-rule untuk membuat aturan listener tambahan.

Pendengar HTTPS untuk layanan VPC Lattice

Listener adalah proses memeriksa permintaan koneksi. Anda menentukan pendengar ketika Anda membuat layanan Anda. Anda dapat menambahkan pendengar ke layanan Anda di VPC Lattice kapan saja.

Anda dapat membuat pendengar HTTPS, yang menggunakan TLS versi 1.2 untuk menghentikan koneksi HTTPS dengan VPC Lattice secara langsung. VPC Lattice akan menyediakan dan mengelola sertifikat TLS yang terkait dengan VPC Lattice generated Fully Qualified Domain Name (FQDN). VPC Lattice mendukung TLS pada HTTP/1.1 dan HTTP/2. Saat Anda mengonfigurasi layanan dengan pendengar HTTPS, VPC Lattice akan secara otomatis menentukan protokol HTTP melalui Application-Layer Protocol Negotiation (ALPN). Jika ALPN tidak ada, VPC Lattice default ke HTTP/1.1.

VPC Lattice menggunakan arsitektur multi-tenancy, yang berarti dapat meng-host beberapa layanan pada titik akhir yang sama. VPC Lattice menggunakan TLS dengan Server Name Indication (SNI) untuk setiap permintaan klien.

VPC Lattice dapat mendengarkan HTTP, HTTPS, HTTP/1.1, dan HTTP/2 dan berkomunikasi dengan target di salah satu protokol dan versi ini. Konfigurasi pendengar dan grup target ini tidak perlu dicocokkan. VPC Lattice mengelola seluruh proses upgrade dan downgrade antara protokol dan versi. Untuk informasi selengkapnya, lihat Versi protokol.

Untuk memastikan bahwa aplikasi Anda mendekripsi lalu lintas, buat pendengar TLS sebagai gantinya. Dengan passthrough TLS, VPC Lattice tidak mengakhiri TLS. Untuk informasi selengkapnya, lihat Pendengar TLS.

Daftar Isi

Kebijakan keamanan

VPC Lattice menggunakan kebijakan keamanan yang merupakan kombinasi dari protokol TLSv1.2 dan daftar cipher SSL/TLS. Protokol menetapkan koneksi aman antara klien dan server dan membantu memastikan bahwa semua data yang dilewatkan antara klien dan layanan Anda di VPC Lattice bersifat pribadi. Sandi adalah algoritme enkripsi yang menggunakan kunci enkripsi untuk membuat pesan kode. Protokol menggunakan beberapa cipher untuk mengenkripsi data. Selama proses negosiasi koneksi, klien dan VPC Lattice menyajikan daftar sandi dan protokol yang masing-masing mereka dukung, dalam urutan preferensi. Secara default, sandi pertama pada daftar server yang cocok salah satu sandi klien dipilih untuk sambungan aman.

VPC Lattice menggunakan protokol TLSv1.2 dan cipher SSL/TLS berikut dalam urutan preferensi ini:

- `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`

Kebijakan ALPN

Application-Layer Protocol Negotiation (ALPN) adalah ekstensi TLS yang dikirim pada pesan halo jabat tangan TLS awal. ALPN memungkinkan lapisan aplikasi untuk menegosiasikan protokol mana yang harus digunakan melalui koneksi aman, seperti HTTP/1 dan HTTP/2.

Ketika klien memulai koneksi ALPN, layanan VPC Lattice membandingkan daftar preferensi ALPN klien dengan kebijakan ALPN-nya. Jika klien mendukung protokol dari kebijakan ALPN, layanan VPC Lattice menetapkan koneksi berdasarkan daftar preferensi kebijakan ALPN. Jika tidak, layanan tidak menggunakan ALPN.

VPC Lattice mendukung kebijakan ALPN berikut:

`HTTP2Preferred`

Lebih suka HTTP/2 daripada HTTP/1.1. Daftar preferensi ALPN adalah h2, http/1.1.

Menambahkan pendengar HTTPS

Anda mengonfigurasi listener dengan protokol dan port untuk koneksi dari klien ke layanan, dan grup target untuk aturan pendengar default. Untuk informasi selengkapnya, lihat Konfigurasi listener.

Prasyarat

- Untuk menambahkan tindakan penerusan ke aturan pendengar default, Anda harus menentukan grup target VPC Lattice yang tersedia. Untuk informasi selengkapnya, lihat Buat grup target VPC Lattice.
- Anda dapat menentukan grup target yang sama di beberapa pendengar, tetapi pendengar ini harus termasuk dalam layanan VPC Lattice yang sama. Untuk menggunakan grup target dengan layanan VPC Lattice, Anda harus memverifikasi bahwa grup tersebut tidak digunakan oleh pendengar untuk layanan VPC Lattice lainnya.
- Anda dapat menggunakan sertifikat yang disediakan oleh VPC Lattice atau mengimpor sertifikat Anda sendiri ke. AWS Certificate Manager Untuk informasi selengkapnya, lihat the section called “BYOC”.

Untuk menambahkan listener HTTPS menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih nama layanan untuk membuka halaman detailnya.
4. Pada tab Routing, pilih Add listener.
5. Untuk nama Listener, Anda dapat memberikan nama pendengar kustom atau menggunakan protokol dan port listener Anda sebagai nama listener. Nama kustom yang Anda tentukan dapat memiliki hingga 63 karakter, dan itu harus unik untuk setiap layanan di akun Anda. Karakter yang valid adalah a-z, 0-9, dan tanda hubung (-). Anda tidak dapat menggunakan tanda hubung sebagai karakter pertama atau terakhir, atau segera setelah tanda hubung lainnya. Anda tidak dapat mengubah nama pendengar setelah Anda membuatnya.
6. Untuk Protokol: port, pilih HTTPS dan masukkan nomor port.
7. Untuk tindakan Default, pilih grup target VPC Lattice untuk menerima lalu lintas dan pilih bobot yang akan ditetapkan ke grup target ini. Bobot yang Anda tetapkan ke grup sasaran menetapkan prioritasnya untuk menerima lalu lintas. Misalnya, jika dua kelompok sasaran memiliki bobot yang sama, masing-masing kelompok sasaran menerima setengah dari lalu lintas. Jika Anda telah menentukan hanya satu kelompok target, maka 100 persen dari lalu lintas dikirim ke satu kelompok target.

   Anda dapat menambahkan grup target lain secara opsional untuk tindakan default. Pilih Tambah tindakan dan kemudian pilih grup target dan tentukan bobotnya.
8. (Opsional) Untuk menambahkan aturan lain, pilih Tambahkan aturan lalu masukkan nama, prioritas, kondisi, dan tindakan untuk aturan tersebut.

   Anda dapat memberikan setiap aturan nomor prioritas antara 1 dan 100. Listener tidak bisa memiliki beberapa aturan dengan prioritas yang sama. Peraturan dievaluasi dalam urutan prioritas, dari nilai terendah ke nilai tertinggi. Peraturan default dievaluasi terakhir. Untuk informasi selengkapnya, lihat Aturan pendengar.
9. (Opsional) Untuk menambahkan tag, perluas tag Listener, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
10. Untuk pengaturan sertifikat pendengar HTTPS, jika Anda tidak menentukan nama domain kustom saat membuat layanan, VPC Lattice secara otomatis menghasilkan sertifikat TLS untuk mengamankan lalu lintas yang mengalir melalui pendengar.

Jika Anda membuat layanan dengan nama domain kustom, tetapi tidak menentukan sertifikat yang cocok, Anda dapat melakukannya sekarang dengan memilih sertifikat dari sertifikat SSL/TLS Kustom. Jika tidak, sertifikat yang Anda tentukan saat Anda membuat layanan sudah dipilih.

11. Tinjau konfigurasi Anda, lalu pilih Tambah.

Untuk menambahkan pendengar HTTPS menggunakan AWS CLI

Gunakan perintah create-listener untuk membuat listener dengan aturan default, dan perintah create-rule untuk membuat aturan listener tambahan.

Pendengar TLS untuk layanan VPC Lattice

Listener adalah proses memeriksa permintaan koneksi. Anda dapat menentukan listener saat membuat layanan VPC Lattice Anda. Anda dapat menambahkan pendengar ke layanan Anda kapan saja.

Anda dapat membuat pendengar TLS sehingga VPC Lattice meneruskan lalu lintas terenkripsi ke aplikasi Anda tanpa mendekripsi.

Jika Anda lebih suka VPC Lattice mendekripsi lalu lintas terenkripsi dan mengirimkan lalu lintas yang tidak terenkripsi ke aplikasi Anda, buatlah pendengar HTTPS sebagai gantinya. Untuk informasi selengkapnya, lihat Pendengar HTTPS.

Pertimbangan

Pertimbangan berikut berlaku untuk pendengar TLS:

- Layanan VPC Lattice harus memiliki nama domain khusus. Nama domain kustom layanan digunakan sebagai pencocokan Service Name Indication (SNI). Jika Anda menentukan sertifikat saat Anda membuat layanan, itu tidak digunakan.
- Satu-satunya aturan yang diizinkan untuk pendengar TLS adalah aturan default.
- Tindakan default untuk pendengar TLS harus berupa tindakan penerusan ke grup target TCP.
- Secara default, pemeriksaan kesehatan dinonaktifkan untuk grup target TCP. Jika Anda mengaktifkan pemeriksaan kesehatan untuk grup target TCP, Anda harus menentukan protokol dan versi protokol.

- Pendengar TLS merutekan permintaan menggunakan bidang SNI dari pesan client-hello. Anda dapat menggunakan wildcard dan sertifikat SAN pada target Anda jika kondisi pencocokan sama persis dengan client-hello.
- Karena semua lalu lintas tetap dienkripsi dari klien ke target, VPC Lattice tidak dapat membaca header HTTP dan tidak dapat menyisipkan atau menghapus header HTTP. Oleh karena itu, dengan pendengar TLS, ada batasan berikut:
  - Durasi koneksi dibatasi hingga 10 menit
  - Kebijakan autentikasi terbatas pada prinsipal anonim
  - Target Lambda tidak didukung

Tambahkan pendengar TLS

Anda mengonfigurasi listener dengan protokol dan port untuk koneksi dari klien ke layanan, dan grup target untuk aturan pendengar default. Untuk informasi selengkapnya, lihat Konfigurasi listener.

Untuk menambahkan pendengar TLS menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih nama layanan untuk membuka halaman detailnya.
4. Pada tab Routing, pilih Add listener.
5. Untuk nama Listener, Anda dapat memberikan nama pendengar kustom atau menggunakan protokol dan port listener Anda sebagai nama listener. Nama kustom yang Anda tentukan dapat memiliki hingga 63 karakter, dan itu harus unik untuk setiap layanan di akun Anda. Karakter yang valid adalah a-z, 0-9, dan tanda hubung (-). Anda tidak dapat menggunakan tanda hubung sebagai karakter pertama atau terakhir, atau segera setelah tanda hubung lainnya. Anda tidak dapat mengubah nama pendengar setelah Anda membuatnya.
6. Untuk Protokol, pilih TLS. Untuk Port, masukkan nomor port.
7. Untuk Forward to target group, pilih grup target VPC Lattice yang menggunakan protokol TCP untuk menerima lalu lintas, dan pilih bobot yang akan ditetapkan ke grup target ini. Anda dapat menambahkan grup target lain secara opsional. Pilih Tambahkan grup target dan kemudian pilih grup target dan masukkan bobotnya.
8. (Opsional) Untuk menambahkan tag, perluas tag Listener, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
9. Tinjau konfigurasi Anda, lalu pilih Tambah.

Untuk menambahkan pendengar TLS menggunakan AWS CLI

Gunakan perintah create-listener untuk membuat listener dengan aturan default. Tentukan protokol TLS_PASSTHOUGH.

Aturan pendengar untuk layanan VPC Lattice Anda

Setiap pendengar memiliki aturan default dan aturan tambahan yang dapat Anda tentukan. Setiap peraturan terdiri dari prioritas, satu tindakan atau lebih, dan satu syarat atau lebih. Anda dapat menambahkan atau mengedit peraturan kapan saja.

Daftar Isi

Peraturan default

Bila Anda membuat listener, Anda menentukan tindakan untuk peraturan default. Peraturan default tidak dapat memiliki syarat. Jika tidak ada syarat untuk peraturan listener yang terpenuhi, maka tindakan untuk peraturan default akan dilakukan.

Prioritas peraturan

Setiap peraturan memiliki prioritas. Peraturan dievaluasi dalam urutan prioritas, dari nilai terendah ke nilai tertinggi. Peraturan default dievaluasi terakhir. Anda dapat mengubah prioritas aturan non-default kapan saja. Anda tidak dapat mengubah prioritas peraturan default.

Tindakan aturan

Pendengar untuk layanan VPC Lattice mendukung tindakan maju dan tindakan respons tetap.

Tindakan ke depan

Anda dapat menggunakan `forward` tindakan untuk merutekan permintaan ke satu atau beberapa grup target VPC Lattice. Jika Anda menentukan beberapa kelompok target untuk tindakan `forward`, Anda harus menentukan bobot untuk setiap grup target. Bobot setiap grup target adalah nilai dari 0 hingga 999. Permintaan yang sesuai dengan peraturan listener dengan kelompok target tertimbang didistribusikan ke grup target ini berdasarkan bobot mereka. Misalnya, jika Anda menentukan dua grup target, masing-masing dengan bobot 10, setiap grup target menerima setengah dari permintaan. Jika Anda menentukan dua grup target, satu dengan bobot 10 dan lainnya dengan bobot 20, grup target dengan bobot 20 menerima permintaan dua kali lebih banyak dari grup target lainnya.

Tindakan respons tetap

Anda dapat menggunakan `fixed-response` untuk menjatuhkan permintaan klien dan mengembalikan respons HTTP khusus. Anda dapat menggunakan tindakan ini untuk mengembalikan kode respons 404.

Example Contoh tindakan respons tetap untuk AWS CLI

Anda dapat menentukan tindakan saat membuat atau memperbarui aturan. Tindakan berikut mengirimkan respons tetap dengan kode status yang ditentukan.

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

Syarat peraturan

Setiap syarat peraturan memiliki jenis dan konfigurasi informasi. Bila syarat untuk suatu peraturan terpenuhi, maka tindakannya dilakukan.

Berikut ini adalah kriteria pencocokan yang didukung untuk aturan:

Pertandingan header

Routing didasarkan pada header HTTP untuk setiap permintaan. Anda dapat menggunakan syarat header HTTP untuk mengonfigurasi aturan yang merutekan permintaan berdasarkan header HTTP untuk permintaan tersebut. Anda dapat menentukan nama-nama bidang header HTTP standar atau kustom. Nama header dan evaluasi kecocokan tidak peka huruf besar/

kecil. Anda dapat mengubah pengaturan ini dengan mengaktifkan sensitivitas huruf besar/kecil. Karakter wildcard tidak didukung dalam nama header. Awalan, tepat, dan berisi pencocokan didukung pada pencocokan header.

Metode pencocokan

Routing didasarkan pada metode permintaan HTTP dari setiap permintaan.

Anda dapat menggunakan syarat metode permintaan HTTP untuk mengonfigurasi aturan yang merutekan permintaan berdasarkan metode permintaan HTTP dari permintaan tersebut. Anda dapat menentukan metode HTTP standar atau kustom. Metode pencocokan peka huruf besar/kecil. Nama metode harus sama persis. Karakter wildcard tidak didukung.

Pertandingan jalur

Perutean didasarkan pada pencocokan pola jalur di URL permintaan.

Anda dapat menggunakan kondisi jalur untuk menentukan aturan yang merutekan permintaan berdasarkan URL dalam permintaan. Karakter wildcard tidak didukung. Awalan dan pencocokan tepat di jalur didukung.

Tambahkan peraturan

Anda dapat menambahkan aturan pendengar kapan saja.

Untuk menambahkan aturan listener menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih nama layanan untuk membuka halaman detailnya.
4. Pada tab Routing, pilih Edit listener.
5. Perluas aturan Listener dan pilih Tambahkan aturan.
6. Untuk nama Aturan, masukkan nama untuk aturan.
7. Untuk Prioritas, masukkan prioritas antara 1 dan 100. Peraturan dievaluasi dalam urutan prioritas, dari nilai terendah ke nilai tertinggi. Peraturan default dievaluasi terakhir.
8. Untuk Kondisi, masukkan pola jalur untuk kondisi pencocokan jalur. Ukuran maksimum setiap string adalah 200 karakter. Perbandingannya tidak peka huruf besar/kecil. Karakter wildcard tidak didukung.

Untuk menambahkan kondisi aturan kecocokan header atau kecocokan metode, gunakan AWS CLI atau AWS SDK.

9. Untuk Tindakan, pilih grup target VPC Lattice.
10. Pilih Simpan perubahan.

Untuk menambahkan aturan menggunakan AWS CLI

Gunakan perintah create-rule.

Perbarui aturan

Anda dapat memperbarui aturan pendengar kapan saja. Anda dapat memodifikasi prioritas, kondisi, kelompok target, dan bobot masing-masing kelompok target. Anda tidak dapat mengubah nama aturan.

Untuk memperbarui aturan listener menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih nama layanan untuk membuka halaman detailnya.
4. Pada tab Routing, pilih Edit listener.
5. Ubah prioritas aturan, kondisi, dan tindakan sesuai kebutuhan.
6. Tinjau pembaruan Anda dan pilih Simpan perubahan.

Untuk memperbarui aturan menggunakan AWS CLI

Gunakan perintah update-rule.

Menghapus peraturan

Anda dapat menghapus aturan non-default untuk pendengar kapan saja. Anda tidak dapat menghapus peraturan default untuk listener. Saat Anda menghapus pendengar, semua aturannya akan dihapus.

Untuk menghapus aturan listener menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.

2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih nama layanan untuk membuka halaman detailnya.
4. Pada tab Routing, pilih Edit listener.
5. Temukan aturannya dan pilih Hapus.
6. Pilih Simpan perubahan.

Untuk menghapus aturan menggunakan AWS CLI

Gunakan perintah hapus-peraturan.

Memperbarui pendengar

Setelah membuat listener, Anda dapat mengganti grup target untuk tindakan default. Anda juga dapat menambahkan grup target ke tindakan default dan menetapkan bobot ke grup target. Anda tidak dapat memperbarui nama listener, protokol listener, atau port listener.

Untuk memperbarui listener menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih nama layanan untuk membuka halaman detailnya.
4. Pada tab Routing, pilih Edit listener.
5. Untuk tindakan Default, Anda dapat memperbarui grup target atau bobot sesuai kebutuhan.
6. Untuk menambahkan grup target tambahan, pilih Tambah tindakan lalu pilih grup target dan tentukan bobotnya.
7. Anda juga dapat menambahkan, mengedit, atau menghapus aturan listener. Untuk informasi selengkapnya, lihat Aturan pendengar.
8. Tinjau pembaruan Anda, dan pilih Simpan perubahan.

Untuk memperbarui tindakan default untuk pendengar menggunakan AWS CLI

Gunakan perintah update-listener.

Menghapus listener

Anda dapat menghapus listener kapan saja. Saat Anda menghapus pendengar, semua aturannya akan dihapus secara otomatis.

Untuk menghapus listener menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Layanan.
3. Pilih nama layanan untuk membuka halaman detailnya.
4. Pada tab Routing, pilih Hapus pendengar.
5. Saat diminta konfirmasi, masukkan **`confirm`**, lalu pilih Hapus.

Untuk menghapus pendengar menggunakan AWS CLI

Gunakan perintah hapus-listener.

Bagikan sumber daya VPC Lattice

Amazon VPC Lattice terintegrasi dengan AWS Resource Access Manager (AWS RAM) untuk mengaktifkan berbagi sumber daya. AWS RAMadalah layanan yang memungkinkan Anda berbagi beberapa sumber daya VPC Lattice dengan yang lain Akun AWS atau melalui. AWS Organizations Dengan, AWS RAMAnda dapat berbagi sumber daya yang Anda miliki dengan membuat berbagi sumber daya. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan dibagikan. Konsumen dapat mencakup:

- Khusus Akun AWS di dalam atau di luar organisasinya diAWS Organizations.
- Unit organisasi di dalam organisasinya diAWS Organizations.
- Seluruh organisasi di AWS Organizations

Untuk informasi selengkapnya tentang AWS RAM, lihat AWS RAMPanduan Pengguna .

Daftar Isi

Prasyarat untuk berbagi sumber daya VPC Lattice

- Untuk berbagi sumber daya, Anda harus memilikinya di AndaAkun AWS. Ini berarti bahwa sumber daya harus dialokasikan atau disediakan di akun Anda. Anda tidak dapat berbagi sumber daya yang telah dibagikan dengan Anda.
- Untuk berbagi sumber daya dengan organisasi Anda atau unit organisasi diAWS Organizations, Anda harus mengaktifkan berbagi denganAWS Organizations. Untuk informasi selengkapnya, lihat Mengaktifkan berbagi sumber daya AWS Organizations di dalam Panduan AWS RAM Pengguna.

Bagikan sumber daya VPC Lattice

Untuk berbagi sumber daya, mulailah dengan membuat pembagian sumber daya menggunakanAWS Resource Access Manager. Pembagian sumber daya menentukan sumber daya untuk dibagikan, konsumen dengan siapa mereka dibagikan, dan tindakan apa yang dapat dilakukan oleh kepala sekolah.

Saat membagikan sumber daya VPC Lattice yang Anda miliki dengan orang lainAkun AWS, Anda mengaktifkan akun tersebut untuk mengaitkan sumber daya mereka dengan sumber daya di akun Anda. Saat Anda membuat asosiasi terhadap sumber daya bersama, kami membuat Amazon Resource Name (ARN) di akun pemilik sumber daya dan ditambah ARN di akun yang membuat asosiasi. Dengan cara ini, baik pemilik sumber daya maupun akun yang membuat asosiasi dapat menghapus asosiasi.

Jika Anda adalah bagian dari organisasi AWS Organizations dan berbagi dalam organisasi Anda diaktifkan, konsumen di organisasi Anda secara otomatis diberikan akses ke sumber daya bersama. Jika tidak, konsumen menerima undangan untuk bergabung dengan pembagian sumber daya dan diberikan akses ke sumber daya bersama setelah menerima undangan.

Pertimbangan-pertimbangan

- Anda dapat berbagi dua jenis sumber daya VPC Lattice: jaringan layanan dan layanan.
- Anda dapat membagikan sumber daya VPC Lattice Anda dengan sumber daya apa pun. Akun AWS
- Anda tidak dapat membagikan sumber daya VPC Lattice Anda dengan masing-masing pengguna dan peran IAM.
- VPC Lattice mendukung izin terkelola pelanggan untuk jaringan layanan dan layanan.

Untuk berbagi sumber daya yang Anda miliki menggunakan konsol VPC Lattice

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah Kisi VPC, pilih Jaringan Layanan atau Layanan.
3. Pilih nama sumber daya untuk membuka halaman detailnya, lalu pilih Bagikan layanan atau Bagikan jaringan layanan dari tab Berbagi.
4. Pilih pembagian AWS RAM sumber daya dari pembagian Sumber Daya. Untuk membuat pembagian sumber daya, pilih Buat berbagi sumber daya di konsol RAM.

5. Pilih Bagikan layanan atau Bagikan jaringan layanan.

Untuk berbagi sumber daya yang Anda miliki menggunakan AWS RAM konsol

Gunakan prosedur yang dijelaskan dalam Buat berbagi sumber daya di Panduan AWS RAM Pengguna.

Untuk berbagi sumber daya yang Anda miliki menggunakan AWS CLI

Gunakan perintah associate-resource-share.

Berhenti berbagi sumber daya VPC Lattice

Untuk berhenti berbagi sumber daya VPC Lattice yang Anda miliki, Anda harus menghapusnya dari pembagian sumber daya. Asosiasi yang ada tetap ada setelah Anda berhenti membagikan sumber daya Anda. Asosiasi baru ke sumber daya yang dibagikan sebelumnya tidak diizinkan. Ketika pemilik sumber daya atau pemilik asosiasi menghapus asosiasi, itu dihapus dari kedua akun. Jika pemilik akun ingin meninggalkan pembagian sumber daya, mereka harus meminta pemilik pembagian sumber daya untuk menghapus akun.

Untuk berhenti berbagi sumber daya yang Anda miliki menggunakan konsol VPC Lattice

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah Kisi VPC, pilih Jaringan Layanan atau Layanan.
3. Pilih nama sumber daya untuk membuka halaman detailnya.
4. Pada tab Berbagi, pilih kotak centang untuk berbagi sumber daya dan kemudian pilih Hapus.

Untuk berhenti berbagi sumber daya yang Anda miliki menggunakan AWS RAM konsol

Lihat Memperbarui bagian sumber daya di Panduan AWS RAM Pengguna.

Untuk berhenti berbagi sumber daya yang Anda miliki menggunakan AWS CLI

Gunakan perintah disassociate-resource-share.

Tanggung jawab dan izin

Tanggung jawab dan izin berikut berlaku saat menggunakan sumber daya VPC Lattice bersama.

Pemilik sumber daya

- Pemilik jaringan layanan tidak dapat memodifikasi layanan yang dibuat oleh konsumen.
- Pemilik jaringan layanan tidak dapat menghapus layanan yang dibuat oleh konsumen.
- Pemilik jaringan layanan dapat menggambarkan semua asosiasi layanan untuk jaringan layanan.
- Pemilik jaringan layanan dapat memisahkan layanan apa pun yang terkait dengan jaringan layanan, terlepas dari siapa yang membuat asosiasi.
- Pemilik jaringan layanan dapat menggambarkan semua asosiasi VPC untuk jaringan layanan.
- Pemilik jaringan layanan dapat memisahkan VPC apa pun yang dikaitkan konsumen dengan jaringan layanan.
- Pemilik layanan dapat menggambarkan semua asosiasi jaringan dengan layanan.
- Pemilik layanan dapat memisahkan layanan dari jaringan layanan apa pun yang terkait dengannya.
- Hanya akun yang membuat asosiasi yang dapat memperbarui hubungan antara jaringan layanan dan VPC.

Konsumen sumber daya

- Konsumen tidak dapat menghapus layanan yang tidak mereka buat.
- Konsumen hanya dapat memisahkan layanan yang mereka kaitkan dengan jaringan layanan.
- Konsumen dan pemilik jaringan dapat menggambarkan semua asosiasi antara jaringan layanan dan layanan.
- Konsumen tidak dapat mengambil informasi layanan dari layanan yang tidak mereka miliki.
- Konsumen dapat menggambarkan semua asosiasi layanan dengan jaringan layanan bersama.
- Konsumen dapat mengaitkan layanan dengan jaringan layanan bersama.
- Konsumen dapat melihat semua asosiasi VPC dengan jaringan layanan bersama.
- Konsumen dapat mengaitkan VPC dengan jaringan layanan bersama.
- Konsumen hanya dapat memisahkan VPC yang mereka kaitkan dengan jaringan layanan.
- Konsumen layanan bersama tidak dapat mengaitkan layanan dengan jaringan layanan yang tidak mereka miliki.
- Konsumen jaringan layanan bersama tidak dapat mengaitkan VPC atau layanan yang tidak mereka miliki.
- Konsumen dapat menggambarkan layanan atau jaringan layanan yang dibagikan dengan mereka.

- Konsumen tidak dapat mengaitkan dua sumber daya jika keduanya dibagikan dengan mereka.

Acara lintas akun

Ketika pemilik sumber daya dan konsumen melakukan tindakan pada sumber daya bersama, tindakan tersebut dicatat sebagai peristiwa lintas akun. AWS CloudTrail

`CreateServiceNetworkServiceAssociationBySharee`

Dikirim ke pemilik sumber daya saat konsumen sumber daya memanggil CreateServiceNetworkServiceAssociationdengan sumber daya bersama. Jika penelepon memiliki layanan, acara dikirim ke pemilik jaringan layanan. Jika penelepon memiliki jaringan layanan, acara dikirim ke pemilik layanan.

`CreateServiceNetworkVpcAssociationBySharee`

Dikirim ke pemilik sumber daya saat konsumen sumber daya memanggil CreateServiceNetworkVpcAssociationdengan jaringan layanan bersama.

`DeleteServiceNetworkServiceAssociationByOwner`

Dikirim ke pemilik asosiasi saat pemilik sumber daya memanggil DeleteServiceNetworkServiceAssociationdengan sumber daya bersama. Jika penelepon memiliki layanan, acara dikirim ke pemilik asosiasi jaringan layanan. Jika penelepon memiliki jaringan layanan, acara dikirim ke pemilik asosiasi layanan.

`DeleteServiceNetworkServiceAssociationBySharee`

Dikirim ke pemilik sumber daya saat konsumen sumber daya memanggil DeleteServiceNetworkServiceAssociationdengan sumber daya bersama. Jika penelepon memiliki layanan, acara dikirim ke pemilik jaringan layanan. Jika penelepon memiliki jaringan layanan, acara dikirim ke pemilik layanan.

`DeleteServiceNetworkVpcAssociationByOwner`

Dikirim ke pemilik asosiasi saat pemilik sumber daya memanggil DeleteServiceNetworkVpcAssociationdengan jaringan layanan bersama.

`DeleteServiceNetworkVpcAssociationBySharee`

Dikirim ke pemilik sumber daya saat konsumen sumber daya memanggil DeleteServiceNetworkVpcAssociationdengan jaringan layanan bersama.

`GetServiceBySharee`

Dikirim ke pemilik sumber daya saat konsumen sumber daya memanggil GetServicedengan layanan bersama.

`GetServiceNetworkBySharee`

Dikirim ke pemilik sumber daya saat konsumen sumber daya memanggil GetServiceNetworkdengan jaringan layanan bersama.

`GetServiceNetworkServiceAssociationBySharee`

Dikirim ke pemilik sumber daya saat konsumen sumber daya memanggil GetServiceNetworkServiceAssociationdengan sumber daya bersama. Jika penelepon memiliki layanan, acara dikirim ke pemilik jaringan layanan. Jika penelepon memiliki jaringan layanan, acara dikirim ke pemilik layanan.

`GetServiceNetworkVpcAssociationBySharee`

Dikirim ke pemilik sumber daya saat konsumen sumber daya memanggil GetServiceNetworkVpcAssociationdengan jaringan layanan bersama.

Berikut ini adalah contoh entri untuk `CreateServiceNetworkServiceAssociationBySharee` acara tersebut.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-04-27T17:12:46Z",
    "eventSource": "vpc-lattice.amazonaws.com",
    "eventName": "CreateServiceNetworkServiceAssociationBySharee",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "vpc-lattice.amazonaws.com",
    "userAgent": "ec2.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "callerAccountId": "111122223333"
    },
    "requestID": "ddabb0a7-70c6-4f70-a6c9-00cbe8a6a18b",
    "eventID": "bd03cdca-7edd-4d50-b9c9-eaa89f4a47cd",
```

```
    "readOnly": false,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::VpcLattice::ServiceNetworkServiceAssociation",
            "ARN": "arn:aws:vpc-
lattice:region:123456789012:servicenetworkserviceassociation/snsa-0d5ea7bc72EXAMPLE"
        }
    ],
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Keamanan di Amazon VPC Lattice

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon VPC Lattice, lihat AWS Layanan dalam Lingkup menurut Program Kepatuhan dalam Lingkup oleh Program Kepatuhan.
- Keamanan di cloud — Anda bertanggung jawab untuk menjaga kontrol atas konten Anda yang di-host di infrastruktur ini. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan VPC Lattice. Topik berikut menunjukkan cara mengonfigurasi Kisi VPC untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya VPC Lattice Anda.

Daftar Isi

Mengelola akses ke layanan VPC Lattice

VPC Lattice aman secara default karena Anda harus eksplisit tentang layanan mana yang menyediakan akses ke dan dengan VPC mana. Untuk skenario multi-akun, Anda dapat menggunakan AWS Resource Access Manageruntuk berbagi sumber daya di seluruh batas akun. VPC Lattice menyediakan kerangka kerja yang memungkinkan Anda menerapkan defense-in-depth strategi di beberapa lapisan jaringan.

- Lapisan pertama — Layanan dan asosiasi VPC dengan jaringan layanan. Jika VPC atau layanan tertentu tidak terkait dengan jaringan layanan, klien di VPC tidak memiliki akses ke layanan.
- Lapisan kedua — Perlindungan keamanan tingkat jaringan opsional untuk jaringan layanan, seperti grup keamanan dan ACL jaringan. Dengan menggunakan ini, Anda dapat mengizinkan akses ke grup sumber daya tertentu dalam VPC alih-alih semua sumber daya di VPC.
- Lapisan ketiga - Kebijakan autentikasi VPC Lattice opsional. Anda dapat menerapkan kebijakan autentikasi ke jaringan layanan dan layanan individual. Biasanya, kebijakan autentikasi pada jaringan layanan dioperasikan oleh administrator jaringan atau cloud, dan mereka menerapkan otorisasi kasar. Misalnya, hanya mengizinkan permintaan yang diautentikasi dari organisasi tertentu di AWS Organizations. Untuk kebijakan autentikasi di tingkat layanan, biasanya pemilik layanan menetapkan kontrol berbutir halus, yang mungkin lebih ketat daripada otorisasi kasar yang diterapkan di tingkat jaringan layanan.

Metode kontrol akses

- Kebijakan autentikasi
- Grup keamanan
- ACL jaringan

Kontrol akses ke layanan VPC Lattice menggunakan kebijakan autentikasi

Kebijakan autentikasi VPC Lattice adalah dokumen kebijakan IAM yang Anda lampirkan ke jaringan layanan atau layanan untuk mengontrol apakah prinsipal tertentu memiliki akses ke grup layanan atau layanan tertentu. Anda dapat melampirkan satu kebijakan autentikasi ke setiap jaringan layanan atau layanan yang ingin Anda kendalikan aksesnya.

Kebijakan autentikasi berbeda dari kebijakan berbasis identitas IAM. Kebijakan berbasis identitas IAM dilampirkan ke pengguna, grup, atau peran IAM dan menentukan tindakan apa yang dapat

dilakukan identitas tersebut pada sumber daya mana. Kebijakan autentikasi dilampirkan ke layanan dan jaringan layanan. Agar otorisasi berhasil, kebijakan autentikasi dan kebijakan berbasis identitas harus memiliki pernyataan izin eksplisit. Untuk informasi selengkapnya, lihat Cara kerja otorisasi.

Anda dapat menggunakan AWS CLI dan konsol untuk melihat, menambah, memperbarui, atau menghapus kebijakan autentikasi pada layanan dan jaringan layanan. Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wilayah AWS konfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter `--region` bersama perintah tersebut.

Daftar Isi

Untuk memulai kebijakan autentikasi, ikuti prosedur untuk membuat kebijakan autentikasi yang berlaku untuk jaringan layanan. Untuk izin yang lebih ketat yang tidak ingin diterapkan ke layanan lain, Anda dapat secara opsional menetapkan kebijakan autentikasi pada layanan individual.

Mengelola akses ke jaringan layanan dengan kebijakan autentikasi

AWS CLI Tugas berikut menunjukkan cara mengelola akses ke jaringan layanan menggunakan kebijakan autentikasi. Untuk petunjuk yang menggunakan konsol, lihatJaringan layanan di VPC Lattice.

Tugas

- Menambahkan kebijakan autentikasi ke jaringan layanan
- Mengubah jenis autentikasi jaringan layanan
- Menghapus kebijakan autentikasi dari jaringan layanan

Menambahkan kebijakan autentikasi ke jaringan layanan

Ikuti langkah-langkah di bagian ini untuk menggunakan AWS CLI to:

- Aktifkan kontrol akses pada jaringan layanan menggunakan IAM.
- Tambahkan kebijakan autentikasi ke jaringan layanan. Jika Anda tidak menambahkan kebijakan autentikasi, semua lalu lintas akan mendapatkan kesalahan akses ditolak.

Untuk mengaktifkan kontrol akses dan menambahkan kebijakan autentikasi ke jaringan layanan baru

1. Untuk mengaktifkan kontrol akses pada jaringan layanan sehingga dapat menggunakan kebijakan autentikasi, gunakan create-service-network perintah dengan `--auth-type` opsi dan nilai`AWS_IAM`.

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

   Jika berhasil, perintah mengembalikan output yang serupa dengan berikut.

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

2. Gunakan put-auth-policy perintah, tentukan ID jaringan layanan tempat Anda ingin menambahkan kebijakan autentikasi dan kebijakan autentikasi yang ingin Anda tambahkan.

   Misalnya, gunakan perintah berikut untuk membuat kebijakan autentikasi untuk jaringan layanan dengan ID *sn-0123456789abcdef0*.

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

   Gunakan JSON untuk membuat definisi kebijakan. Untuk informasi selengkapnya, lihat Elemen umum dalam kebijakan autentikasi.

   Jika berhasil, perintah ini mengembalikan output yang serupa dengan yang berikut ini.

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

```
}
```

Untuk mengaktifkan kontrol akses dan menambahkan kebijakan autentikasi ke jaringan layanan yang ada

1. Untuk mengaktifkan kontrol akses pada jaringan layanan sehingga dapat menggunakan kebijakan autentikasi, gunakan update-service-network perintah dengan `--auth-type` opsi dan nilai`AWS_IAM`.

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

   Jika berhasil, perintah mengembalikan output yang serupa dengan berikut.

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

2. Gunakan put-auth-policy perintah, tentukan ID jaringan layanan tempat Anda ingin menambahkan kebijakan autentikasi dan kebijakan autentikasi yang ingin Anda tambahkan.

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

   Gunakan JSON untuk membuat definisi kebijakan. Untuk informasi selengkapnya, lihat Elemen umum dalam kebijakan autentikasi.

   Jika berhasil, perintah ini mengembalikan output yang serupa dengan yang berikut ini.

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

Mengubah jenis autentikasi jaringan layanan

Untuk menonaktifkan kebijakan autentikasi untuk jaringan layanan

Gunakan update-service-network perintah dengan `--auth-type` opsi dan nilai`NONE`.

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

Jika Anda perlu mengaktifkan kebijakan autentikasi lagi nanti, jalankan perintah ini dengan `AWS_IAM` ditentukan untuk `--auth-type` opsi.

Menghapus kebijakan autentikasi dari jaringan layanan

Untuk menghapus kebijakan autentikasi dari jaringan layanan

Gunakan perintah delete-auth-policy.

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

Permintaan gagal jika Anda menghapus kebijakan autentikasi sebelum mengubah jenis autentikasi jaringan layanan menjadi. `NONE`

Mengelola akses ke layanan dengan kebijakan autentikasi

AWS CLI Tugas berikut menunjukkan cara mengelola akses ke layanan menggunakan kebijakan autentikasi. Untuk petunjuk yang menggunakan konsol, lihatLayanan di VPC Lattice.

Tugas

- Menambahkan kebijakan autentikasi ke layanan
- Mengubah jenis autentikasi layanan
- Menghapus kebijakan autentikasi dari layanan

Menambahkan kebijakan autentikasi ke layanan

Ikuti langkah-langkah ini untuk menggunakan AWS CLI untuk:

- Aktifkan kontrol akses pada layanan menggunakan IAM.

- Tambahkan kebijakan autentikasi ke layanan. Jika Anda tidak menambahkan kebijakan autentikasi, semua lalu lintas akan mendapatkan kesalahan akses ditolak.

Untuk mengaktifkan kontrol akses dan menambahkan kebijakan autentikasi ke layanan baru

1. Untuk mengaktifkan kontrol akses pada layanan sehingga dapat menggunakan kebijakan autentikasi, gunakan create-service perintah dengan `--auth-type` opsi dan nilai`AWS_IAM`.

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

   Jika berhasil, perintah mengembalikan output yang serupa dengan berikut.

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

2. Gunakan put-auth-policy perintah, tentukan ID layanan tempat Anda ingin menambahkan kebijakan autentikasi dan kebijakan autentikasi yang ingin Anda tambahkan.

   Misalnya, gunakan perintah berikut untuk membuat kebijakan autentikasi untuk layanan dengan ID *svc-0123456789abcdef0*.

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

   Gunakan JSON untuk membuat definisi kebijakan. Untuk informasi selengkapnya, lihat Elemen umum dalam kebijakan autentikasi.

   Jika berhasil, perintah ini mengembalikan output yang serupa dengan yang berikut ini.

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

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

Untuk mengaktifkan kontrol akses dan menambahkan kebijakan autentikasi ke layanan yang ada

1. Untuk mengaktifkan kontrol akses pada layanan sehingga dapat menggunakan kebijakan autentikasi, gunakan update-service perintah dengan `--auth-type` opsi dan nilai`AWS_IAM`.

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

   Jika berhasil, perintah mengembalikan output yang serupa dengan berikut.

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

2. Gunakan put-auth-policy perintah, tentukan ID layanan tempat Anda ingin menambahkan kebijakan autentikasi dan kebijakan autentikasi yang ingin Anda tambahkan.

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

   Gunakan JSON untuk membuat definisi kebijakan. Untuk informasi selengkapnya, lihat Elemen umum dalam kebijakan autentikasi.

   Jika berhasil, perintah ini mengembalikan output yang serupa dengan yang berikut ini.

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

Mengubah jenis autentikasi layanan

Untuk menonaktifkan kebijakan autentikasi untuk layanan

Gunakan update-service perintah dengan `--auth-type` opsi dan nilai`NONE`.

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

Jika Anda perlu mengaktifkan kebijakan autentikasi lagi nanti, jalankan perintah ini dengan `AWS_IAM` ditentukan untuk `--auth-type` opsi.

Menghapus kebijakan autentikasi dari layanan

Untuk menghapus kebijakan autentikasi dari layanan

Gunakan perintah delete-auth-policy.

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

Permintaan gagal jika Anda menghapus kebijakan autentikasi sebelum mengubah jenis autentikasi layanan menjadi. `NONE`

Jika Anda mengaktifkan kebijakan autentikasi yang memerlukan permintaan terautentikasi ke layanan, permintaan apa pun ke layanan tersebut harus berisi tanda tangan permintaan yang valid yang dihitung menggunakan Sigv4 (SigV4). Untuk informasi selengkapnya, lihat Permintaan yang diautentikasi SiGv4 untuk Amazon VPC Lattice.

Elemen umum dalam kebijakan autentikasi

Kebijakan autentikasi VPC Lattice ditentukan menggunakan sintaks yang sama dengan kebijakan IAM. Untuk informasi selengkapnya, lihat Kebijakan berbasis identitas dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Kebijakan autentikasi berisi elemen-elemen berikut:

- Kepala Sekolah — Orang atau aplikasi yang diizinkan mengakses tindakan dan sumber daya dalam pernyataan. Dalam kebijakan autentikasi, prinsipal adalah entitas IAM yang merupakan penerima izin ini. Prinsipal diautentikasi sebagai entitas IAM untuk membuat permintaan ke sumber daya tertentu, atau kelompok sumber daya seperti dalam kasus layanan dalam jaringan layanan.

  Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau layanan. AWS Untuk informasi selengkapnya, lihat elemen kebijakan AWS JSON: Principal dalam Panduan Pengguna IAM.

- Efek — Efek ketika prinsipal yang ditentukan meminta tindakan spesifik. Ini bisa salah satu `Allow` atau`Deny`. Secara default, ketika Anda mengaktifkan kontrol akses pada layanan atau jaringan layanan menggunakan IAM, prinsipal tidak memiliki izin untuk membuat permintaan ke jaringan layanan atau layanan.
- Tindakan — Tindakan API spesifik yang Anda berikan atau tolak izinnya. VPC Lattice mendukung tindakan yang menggunakan awalan. `vpc-lattice-svcs` Untuk informasi selengkapnya, lihat Tindakan yang ditentukan oleh Amazon VPC Lattice Services di Referensi Otorisasi Layanan.
- Sumber Daya — Layanan yang dipengaruhi oleh tindakan.
- Kondisi - Kondisi bersifat opsional. Anda dapat menggunakannya untuk mengontrol kapan kebijakan Anda berlaku. Untuk informasi selengkapnya, lihat Kunci kondisi untuk Layanan Kisi VPC Amazon di Referensi Otorisasi Layanan.

Saat Anda membuat dan mengelola kebijakan autentikasi, Anda mungkin ingin menggunakan IAM Policy Generator.

Persyaratan

Kebijakan di JSON tidak boleh berisi baris baru atau baris kosong.

Format sumber daya untuk kebijakan autentikasi

Anda dapat membatasi akses ke sumber daya tertentu dengan membuat kebijakan autentikasi yang menggunakan skema yang cocok dengan `<serviceARN>/<path>` pola dan kode `Resource` elemen seperti yang ditunjukkan pada contoh berikut.

Contoh sumber daya untuk kebijakan autentikasi

Protokol	Contoh
HTTP	• `"Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/rates"` • `"Resource": "*/rates"` • `"Resource": "*/*"`
gRPC	• `"Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:ser`

Protokol	Contoh
	vice/svc-0123456789abcdef0/ api.parking/GetRates" • "Resource": "arn:aws:vpc-latti ce:us-west-2:1234567890:ser vice/svc-0123456789abcdef0/ api.parking/*" • "Resource": "arn:aws:vpc-latti ce:us-west-2:1234567890:ser vice/svc-0123456789abcdef0/*"

Gunakan format sumber daya Amazon Resource Name (ARN) berikut untuk: `<serviceARN>`

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

Sebagai contoh:

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

Kunci kondisi yang dapat digunakan dalam kebijakan autentikasi

Akses dapat dikontrol lebih lanjut oleh kunci kondisi dalam elemen Kondisi kebijakan autentikasi. Kunci kondisi ini hadir untuk evaluasi tergantung pada protokol dan apakah permintaan ditandatangani dengan Signature Version 4 (SigV4) atau anonim. Kunci kondisi peka huruf besar/kecil.

AWS menyediakan kunci kondisi global yang dapat Anda gunakan untuk mengontrol akses, seperti `aws:PrincipalOrgID` dan`aws:SourceIp`. Untuk melihat daftar kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Kisah berikut mencantumkan kunci kondisi VPC Lattice. Untuk informasi selengkapnya, lihat Kunci kondisi untuk Layanan Kisi VPC Amazon di Referensi Otorisasi Layanan.

Kunci kondisi untuk kebijakan autentikasi

Kunci syarat	Deskripsi	Contoh	Tersedia untuk penelepon anonim (tidak diautentikasi)?	Tersedia untuk gRPC?
`vpc-lattice-svcs:Port`	Memfilter akses oleh port layanan permintaan dibuat	80	Ya	Ya
`vpc-lattice-svcs:RequestMethod`	Memfilter akses dengan metode permintaan	GET	Ya	Selalu POST
`vpc-lattice-svcs:RequestHeader/` *`header-name`* `:` *`value`*	Memfilter akses dengan pasangan nama-nilai header di header permintaan	content-type: application/json	Ya	Ya
`vpc-lattice-svcs:RequestQueryString/` *`key-name`*`:` *`value`*	Memfilter akses dengan pasangan nilai kunci string kueri di URL permintaan	quux: [corge, grault]	Ya	Tidak
`vpc-lattice-svcs:ServiceNetworkArn`	Memfilter akses oleh ARN dari jaringan layanan layanan yang menerima permintaan	arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/sn-0123456789abcdef0	Ya	Ya

Kunci syarat	Deskripsi	Contoh	Tersedia untuk penelepon anonim (tidak diautentikasi)?	Tersedia untuk gRPC?
`vpc-lattice-svcs:ServiceArn`	Memfilter akses oleh ARN dari layanan yang menerima permintaan	arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0	Ya	Ya
`vpc-lattice-svcs:SourceVpc`	Memfilter akses oleh VPC permintaan dibuat dari	vpc-1a2b3c4d	Ya	Ya
`vpc-lattice-svcs:SourceVpcOwnerAccount`	Memfilter akses oleh akun pemilik VPC permintaan dibuat dari	123456789012	Ya	Ya

Prinsipal anonim (tidak diautentikasi)

Prinsipal anonim adalah penelepon yang tidak menandatangani AWS permintaan mereka dengan Signature Version 4 (SigV4), dan berada dalam VPC yang terhubung ke jaringan layanan. Prinsipal anonim dapat membuat permintaan yang tidak diautentikasi ke layanan di jaringan layanan jika kebijakan autentikasi mengizinkannya.

Contoh kebijakan autentikasi

Berikut ini adalah contoh kebijakan autentikasi yang mengharuskan permintaan dibuat oleh prinsipal yang diautentikasi.

Semua contoh menggunakan `us-west-2` Wilayah dan berisi ID akun fiktif.

Contoh 1: Batasi akses ke layanan oleh organisasi tertentu AWS

Contoh kebijakan autentikasi berikut memberikan izin untuk setiap permintaan yang diautentikasi untuk mengakses layanan apa pun di jaringan layanan tempat kebijakan tersebut berlaku. Namun, permintaan harus berasal dari kepala sekolah yang termasuk dalam AWS organisasi yang ditentukan dalam kondisi.

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

Contoh 2: Batasi akses ke layanan dengan peran IAM tertentu

Contoh kebijakan autentikasi berikut memberikan izin untuk setiap permintaan yang diautentikasi yang menggunakan peran IAM `rates-client` untuk membuat permintaan HTTP GET pada layanan yang ditentukan dalam elemen. `Resource` Sumber daya dalam `Resource` elemen sama dengan layanan yang dilampirkan kebijakan tersebut.

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

Contoh 3: Batasi akses ke layanan oleh prinsipal yang diautentikasi di VPC tertentu

Contoh kebijakan autentikasi berikut hanya mengizinkan permintaan yang diautentikasi dari prinsipal di VPC yang ID VPC-nya. *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"
            }
         }
      }
   ]
}
```

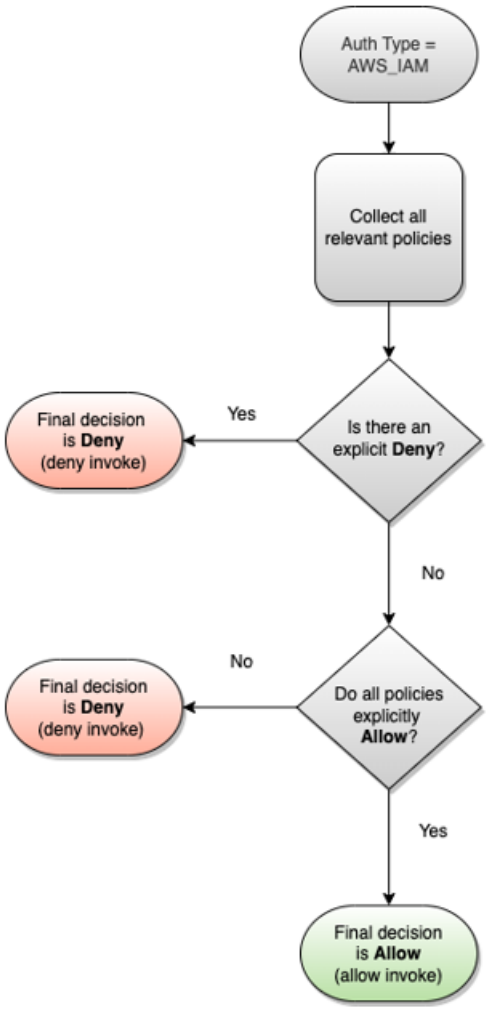
Cara kerja otorisasi

Ketika layanan VPC Lattice menerima permintaan, kode AWS penegakan akan mengevaluasi semua kebijakan izin yang relevan secara bersamaan untuk menentukan apakah akan mengotorisasi atau menolak permintaan tersebut. Ini mengevaluasi semua kebijakan berbasis identitas IAM dan kebijakan autentikasi yang berlaku dalam konteks permintaan selama otorisasi. Secara default, semua permintaan ditolak secara implisit saat jenis autentikasi. `AWS_IAM` Izin eksplisit dari semua kebijakan yang relevan akan mengesampingkan default.

Otorisasi meliputi:

- Mengumpulkan semua kebijakan dan kebijakan autentikasi berbasis identitas IAM yang relevan.
- Mengevaluasi serangkaian kebijakan yang dihasilkan:
  - Memverifikasi bahwa pemohon (seperti pengguna atau peran IAM) memiliki izin untuk melakukan operasi dari akun tempat pemohon berada. Jika tidak ada pernyataan izin eksplisit, AWS tidak mengotorisasi permintaan.
  - Memverifikasi bahwa permintaan diizinkan oleh kebijakan autentikasi untuk jaringan layanan. Jika kebijakan autentikasi diaktifkan, tetapi tidak ada pernyataan izin eksplisit, AWS tidak mengotorisasi permintaan. Jika ada pernyataan allow eksplisit, atau tipe autentikasi`NONE`, kode akan berlanjut.
  - Memverifikasi bahwa permintaan diizinkan oleh kebijakan autentikasi untuk layanan. Jika kebijakan autentikasi diaktifkan, tetapi tidak ada pernyataan izin eksplisit, AWS tidak mengotorisasi permintaan. Jika ada pernyataan allow eksplisit, atau tipe autentikasi**`NONE`**, maka kode penegakan mengembalikan keputusan akhir Izinkan.
  - Penolakan secara tegas dalam kebijakan apa pun akan mengesampingkan izin apa pun.

Diagram menunjukkan alur kerja otorisasi. Ketika permintaan dibuat, kebijakan yang relevan mengizinkan atau menolak akses permintaan ke layanan tertentu.



Kontrol lalu lintas di VPC Lattice menggunakan grup keamanan

AWS Kelompok keamanan bertindak sebagai firewall virtual, mengendalikan lalu lintas jaringan ke dan dari sumber daya yang terkait dengannya. Dengan VPC Lattice, Anda dapat membuat grup keamanan dan menetapkannya ke asosiasi VPC yang menautkan VPC ke jaringan layanan untuk menegakkan perlindungan keamanan tingkat jaringan tambahan untuk jaringan layanan Anda.

Daftar Isi

Daftar awalan terkelola

VPC Lattice menyediakan daftar awalan terkelola yang menyertakan alamat IP yang digunakan untuk merutekan lalu lintas melalui jaringan VPC Lattice. Anda dapat mereferensikan daftar awalan terkelola VPC Lattice dalam aturan grup keamanan Anda. Hal ini memungkinkan lalu lintas mengalir dari klien, melalui jaringan layanan VPC Lattice, dan ke target layanan VPC Lattice.

Misalnya, Anda memiliki instans EC2 yang terdaftar sebagai target di Wilayah Barat AS (Oregon) (`us-west-2`). Anda dapat menambahkan aturan ke grup keamanan instans yang mengizinkan akses HTTPS masuk dari daftar awalan terkelola VPC Lattice, sehingga lalu lintas VPC Lattice di Wilayah ini dapat mencapai instance. Jika Anda menghapus semua aturan masuk lainnya dari grup keamanan, Anda dapat mencegah lalu lintas apa pun selain lalu lintas VPC Lattice mencapai instans.

Nama-nama daftar awalan terkelola untuk VPC Lattice adalah sebagai berikut:

- com.amazonaws.*wilayah*.*vpc-kisi*
- com.amazonaws.*wilayah*.*ipv6.vpc-kisi*

Untuk informasi selengkapnya, lihat daftar awalan AWS-terkelola di Panduan Pengguna Amazon VPC.

Klien Windows

Alamat dalam daftar awalan VPC Lattice adalah alamat link-local. Jika Anda terhubung ke VPC Lattice dari klien Windows, Anda harus memperbarui konfigurasi klien Windows sehingga meneruskan alamat link-lokal yang digunakan oleh VPC Lattice ke alamat IP utama untuk klien. Berikut ini adalah contoh perintah yang memperbarui konfigurasi klien Windows, di mana alamat link-lokal yang 169.254.171.0 digunakan oleh VPC Lattice.

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

Aturan-aturan grup keamanan

Menggunakan VPC Lattice dengan atau tanpa grup keamanan tidak akan memengaruhi konfigurasi grup keamanan VPC Anda yang ada. Namun, Anda dapat menambahkan grup keamanan Anda sendiri kapan saja.

Pertimbangan utama

- Aturan grup keamanan untuk klien mengontrol lalu lintas keluar ke VPC Lattice.

- Aturan grup keamanan untuk target mengontrol lalu lintas masuk dari Kisi VPC ke target, termasuk lalu lintas pemeriksaan kesehatan.
- Aturan grup keamanan untuk hubungan antara jaringan layanan dan kontrol VPC yang klien dapat mengakses jaringan layanan VPC Lattice.

Aturan masuk yang direkomendasikan untuk jaringan layanan dan asosiasi VPC

Agar lalu lintas mengalir dari VPC klien ke layanan yang terkait dengan jaringan layanan, Anda harus membuat aturan masuk untuk port pendengar dan protokol pendengar untuk layanan.

Jalur masuk

Sumber	Protokol	Rentang port	Komentar
VPC CIDR	*listener*	*listener*	Izinkan lalu lintas dari klien ke VPC Lattice

Aturan keluar yang disarankan untuk lalu lintas yang mengalir dari instance klien ke VPC Lattice

Secara default, grup keamanan mengizinkan semua lalu lintas ke luar. Namun, jika Anda memiliki aturan keluar khusus, Anda harus mengizinkan lalu lintas keluar ke awalan VPC Lattice untuk port dan protokol pendengar sehingga instance klien dapat terhubung ke semua layanan yang terkait dengan jaringan layanan VPC Lattice. Anda dapat mengizinkan lalu lintas ini dengan mereferensikan ID daftar awalan untuk VPC Lattice.

Jalur keluar

Tujuan	Protokol	Rentang port	Komentar
ID dari daftar awalan VPC Lattice	*listener*	*listener*	Izinkan lalu lintas dari klien ke VPC Lattice

Aturan masuk yang direkomendasikan untuk lalu lintas yang mengalir dari VPC Lattice ke instance target

Anda tidak dapat menggunakan grup keamanan klien sebagai sumber untuk grup keamanan target Anda, karena lalu lintas mengalir dari VPC Lattice. Anda dapat mereferensikan ID daftar awalan untuk VPC Lattice.

Jalur masuk

Sumber	Protokol	Rentang port	Komentar
ID dari daftar awalan VPC Lattice	*target*	*target*	Izinkan lalu lintas dari VPC Lattice ke target
ID dari daftar awalan VPC Lattice	*health check*	*health check*	Izinkan lalu lintas pemeriksaan kesehatan dari VPC Lattice ke target

Mengelola grup keamanan untuk asosiasi VPC

Anda dapat menggunakan AWS CLI untuk melihat, menambah, atau memperbarui grup keamanan di VPC ke asosiasi jaringan layanan. Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wilayah AWS konfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter `--region` bersama perintah tersebut.

Sebelum Anda mulai, konfirmasikan bahwa Anda telah membuat grup keamanan di VPC yang sama dengan VPC yang ingin Anda tambahkan ke jaringan layanan. Untuk informasi selengkapnya, lihat Mengontrol lalu lintas ke sumber daya Anda menggunakan grup keamanan di Panduan Pengguna Amazon VPC

Untuk menambahkan grup keamanan saat Anda membuat asosiasi VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Jaringan layanan.
3. Pilih nama jaringan layanan untuk membuka halaman detailnya.
4. Pada tab asosiasi VPC, pilih Buat asosiasi VPC lalu pilih Tambahkan asosiasi VPC.
5. Pilih VPC dan hingga lima grup keamanan.
6. Pilih Simpan perubahan.

Untuk menambah atau memperbarui grup keamanan untuk asosiasi VPC yang ada menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah VPC Lattice, pilih Jaringan layanan.
3. Pilih nama jaringan layanan untuk membuka halaman detailnya.
4. Pada tab Asosiasi VPC, pilih kotak centang untuk asosiasi, lalu pilih Tindakan, Edit grup keamanan.
5. Tambahkan dan hapus grup keamanan sesuai kebutuhan.
6. Pilih Simpan perubahan.

Untuk menambahkan grup keamanan saat Anda membuat asosiasi VPC menggunakan AWS CLI

Gunakan perintah create-service-network-vpc-association, tentukan ID VPC untuk asosiasi VPC dan ID grup keamanan yang akan ditambahkan.

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

Jika berhasil, perintah mengembalikan output yang serupa dengan berikut.

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

Untuk menambah atau memperbarui grup keamanan untuk asosiasi VPC yang ada menggunakan AWS CLI

Gunakan perintah update-service-network-vpc-association, tentukan ID jaringan layanan dan ID grup keamanan. Grup keamanan ini mengesampingkan grup keamanan yang sebelumnya terkait. Tentukan setidaknya satu grup keamanan saat memperbarui daftar.

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

> **Warning**
>
> Anda tidak dapat menghapus semua grup keamanan. Sebagai gantinya, Anda harus terlebih dahulu menghapus asosiasi VPC, dan kemudian membuat ulang asosiasi VPC tanpa grup keamanan apa pun. Berhati-hatilah saat menghapus asosiasi VPC. Ini mencegah lalu lintas mencapai layanan yang ada di jaringan layanan itu.

Kontrol lalu lintas ke VPC Lattice menggunakan ACL jaringan

Daftar kontrol akses jaringan (ACL) memungkinkan atau menolak lalu lintas masuk atau keluar tertentu di tingkat subnet. ACL jaringan default memungkinkan semua lalu lintas masuk dan keluar. Anda dapat membuat ACL jaringan khusus untuk subnet Anda untuk memberikan lapisan keamanan tambahan. Untuk informasi selengkapnya, lihat ACL Jaringan di Panduan Pengguna Amazon VPC.

Daftar Isi

ACL jaringan untuk subnet klien Anda

ACL jaringan untuk subnet klien harus memungkinkan lalu lintas antara klien dan VPC Lattice. Anda bisa mendapatkan rentang alamat IP untuk mengizinkan dari daftar awalan terkelola untuk VPC Lattice.

Jalur masuk

Sumber	Protokol	Rentang port	Komentar
vpc_lattice_cidr_block	TCP	1025-65535	Izinkan lalu lintas dari VPC Lattice ke klien

Jalur keluar

Tujuan	Protokol	Rentang port	Komentar
vpc_lattice_cidr_block	*listener*	*listener*	Izinkan lalu lintas dari klien ke VPC Lattice

ACL jaringan untuk subnet target Anda

ACL jaringan untuk subnet target harus memungkinkan lalu lintas antara target dan Kisi VPC pada port target dan port pemeriksaan kesehatan. Anda bisa mendapatkan rentang alamat IP untuk mengizinkan dari daftar awalan terkelola untuk VPC Lattice.

Jalur masuk

Sumber	Protokol	Rentang port	Komentar
vpc_lattice_cidr_block	*target*	*target*	Izinkan lalu lintas dari VPC Lattice ke target
vpc_lattice_cidr_block	*health check*	*health check*	Izinkan lalu lintas pemeriksaan kesehatan dari VPC Lattice ke target

Jalur keluar

Tujuan	Protokol	Rentang port	Komentar
vpc_lattice_cidr_block	*target*	1024-65535	Izinkan lalu lintas dari target ke VPC Lattice
vpc_lattice_cidr_block	*health check*	1024-65535	Izinkan lalu lintas pemeriksaan kesehatan dari target ke VPC Lattice

Permintaan yang diautentikasi SiGv4 untuk Amazon VPC Lattice

VPC Lattice menggunakan Signature Version 4 (SigV4) atau Signature Version 4A (SigV4a) untuk otentikasi klien. Untuk informasi selengkapnya, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Pertimbangan

- VPC Lattice mencoba mengautentikasi permintaan apa pun yang ditandatangani dengan SigV4 atau Sigv4a. Permintaan gagal tanpa otentikasi.
- VPC Lattice tidak mendukung penandatanganan payload. Anda harus mengirim `x-amz-content-sha256` header dengan nilai yang disetel ke`"UNSIGNED-PAYLOAD"`.

Contoh

- Python
- Java dengan pencegat
- Java tanpa pencegat
- Node.js

Python

Contoh ini mengirimkan permintaan yang ditandatangani melalui koneksi aman ke layanan yang terdaftar di jaringan. Jika Anda lebih suka menggunakan permintaan, paket botocore menyederhanakan proses otentikasi, tetapi tidak sepenuhnya diperlukan. Untuk informasi selengkapnya, lihat Kredensyal dalam dokumentasi Boto3.

Untuk menginstal `botocore` dan `awscrt` paket, gunakan perintah berikut. Untuk informasi lebih lanjut, lihat AWS CRT Python.

```
pip install botocore awscrt
```

Dalam contoh berikut, ganti nilai placeholder dengan nilai Anda sendiri.

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 = botocore.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 dengan pencegat

Contoh ini menggunakan Amazon Request Signing Interceptor untuk menangani penandatanganan permintaan.

```
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.addHeader("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 tanpa pencegat

Contoh ini menunjukkan bagaimana Anda dapat melakukan penandatanganan permintaan dengan menggunakan pencegat khusus. Ini menggunakan kelas penyedia kredensyal default dari AWS SDK for Java 2.x, yang mendapatkan kredensyal yang benar untuk Anda. Jika Anda lebih suka menggunakan penyedia kredensi tertentu, Anda dapat memilih salah satu dari. AWS SDK for Java 2.x Hanya AWS SDK for Java memungkinkan muatan yang tidak ditandatangani melalui HTTPS. Namun, Anda dapat memperpanjang penandatangan untuk mendukung muatan yang tidak ditandatangani melalui HTTP.

```
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();

        SdkHttpFullRequest 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

Contoh ini menggunakan binding NodeJS aws-crt untuk mengirim permintaan yang ditandatangani menggunakan HTTPS.

Untuk menginstal `aws-crt` paket, gunakan perintah berikut.

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

Jika variabel `AWS_REGION` lingkungan ada, contoh menggunakan Region ditentukan oleh`AWS_REGION`. Wilayah default adalah`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()
  }
)
```

Perlindungan data di Amazon VPC Lattice

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon VPC Lattice. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda harus bertanggung jawab untuk memelihara kendali terhadap konten yang di-hosting pada infrastruktur ini. Konten ini meliputi konfigurasi keamanan dan tugas-tugas pengelolaan untuk berbagai layanan AWS layanan yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Enkripsi bergerak

VPC Lattice adalah layanan yang dikelola sepenuhnya yang terdiri dari bidang kontrol dan pesawat data. Setiap pesawat melayani tujuan yang berbeda dalam layanan. Bidang kontrol menyediakan API administratif yang digunakan untuk membuat, membaca/mendeskripsikan, memperbarui, menghapus, dan mencantumkan sumber daya (CRUDL) (misalnya, dan. `CreateService` `UpdateService` Komunikasi ke pesawat kontrol VPC Lattice dilindungi dalam perjalanan oleh TLS. Bidang data adalah API Invoke VPC Lattice yang menyediakan interkoneksi antar layanan. TLS juga mengenkripsi komunikasi ke bidang data VPC Lattice. Suite cipher dan versi protokol menggunakan default yang disediakan oleh VPC Lattice dan tidak dapat dikonfigurasi. Untuk informasi selengkapnya, lihat Pendengar HTTPS untuk layanan VPC Lattice.

Enkripsi diam

Secara default, enkripsi data saat istirahat membantu mengurangi overhead operasional dan kompleksitas yang terlibat dalam melindungi data sensitif. Pada saat yang sama, ini memungkinkan Anda untuk membangun aplikasi aman yang memenuhi kepatuhan enkripsi yang ketat dan persyaratan peraturan.

Daftar Isi

Enkripsi di sisi server dengan kunci terkelola Amazon S3 (SSE-S3)

Saat Anda menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3), setiap objek dienkripsi dengan kunci unik. Sebagai perlindungan tambahan, ia mengenkripsi kunci itu sendiri dengan kunci root yang diputar secara teratur. Enkripsi sisi server Amazon S3 menggunakan salah satu cipher blok terkuat yang tersedia, 256-bit Advanced Encryption Standard (AES-256) GCM, untuk mengenkripsi data Anda. Untuk objek yang dienkripsi sebelum AES-GCM, AES-CBC masih didukung untuk mendekripsi objek tersebut. Untuk informasi selengkapnya, lihat Menggunakan enkripsi sisi server dengan kunci enkripsi terkelola Amazon S3 (SSE-S3).

Jika Anda mengaktifkan enkripsi sisi server dengan kunci enkripsi terkelola Amazon S3 (SSE-S3) untuk bucket S3 untuk log akses VPC Lattice, AWS secara otomatis mengenkripsi setiap file log akses sebelum disimpan di bucket S3 Anda. Untuk informasi selengkapnya, lihat Log yang dikirim ke Amazon S3 di CloudWatch Panduan Pengguna Amazon.

Enkripsi sisi server dengan AWS KMS kunci yang disimpan di (SSE-KMS) AWS KMS

Enkripsi sisi server dengan AWS KMS kunci (SSE-KMS) mirip dengan SSE-S3, tetapi dengan beberapa manfaat dan biaya tambahan untuk menggunakan layanan ini. Ada izin terpisah untuk penggunaan AWS KMS kunci yang memberikan perlindungan tambahan terhadap akses tidak sah objek Anda di Amazon S3. SSE-KMS juga memberi Anda jejak audit yang menunjukkan kapan AWS KMS kunci Anda digunakan dan oleh siapa. Untuk informasi selengkapnya, lihat Menggunakan enkripsi sisi server dengan AWS Key Management Service (SSE-KMS).

Daftar Isi

- Memantau kunci enkripsi Anda untuk VPC Lattice

Enkripsi dan dekripsi kunci pribadi sertifikat Anda

Sertifikat ACM dan kunci pribadi Anda dienkripsi dengan kunci KMS AWS terkelola yang memiliki alias aws/acm. Anda dapat melihat ID kunci dengan alias ini di AWS KMS konsol di bawah kunci AWS terkelola.

VPC Lattice tidak langsung mengakses sumber daya ACM Anda. Ini menggunakan AWS TLS Connection Manager untuk mengamankan dan mengakses kunci pribadi sertifikat Anda. Saat Anda menggunakan sertifikat ACM untuk membuat layanan VPC Lattice, VPC Lattice mengaitkan sertifikat Anda dengan TLS Connection Manager. AWS Ini dilakukan dengan membuat hibah AWS KMS terhadap Kunci AWS Terkelola Anda dengan awalan aws/acm. Hibah adalah instrumen kebijakan yang memungkinkan TLS Connection Manager untuk menggunakan kunci KMS dalam operasi kriptografi. Hibah ini memungkinkan prinsipal penerima hibah (TLS Connection Manager) untuk memanggil operasi hibah yang ditentukan pada kunci KMS untuk mendekripsi kunci pribadi sertifikat Anda. TLS Connection Manager kemudian menggunakan sertifikat dan kunci pribadi yang didekripsi (plaintext) untuk membuat koneksi aman (sesi SSL/TLS) dengan klien layanan VPC Lattice. Ketika sertifikat dipisahkan dari layanan VPC Lattice, hibah dihentikan.

Jika Anda ingin menghapus akses ke kunci KMS, kami sarankan Anda mengganti atau menghapus sertifikat dari layanan menggunakan AWS Management Console atau dengan `update-service` perintah menggunakan. AWS CLI

Konteks enkripsi untuk VPC Lattice

Konteks enkripsi adalah kumpulan opsional pasangan kunci-nilai yang berisi informasi kontekstual tambahan tentang apa yang mungkin digunakan untuk kunci pribadi Anda. AWS KMS mengikat konteks enkripsi ke data terenkripsi dan menggunakannya sebagai data otentikasi tambahan untuk mendukung enkripsi yang diautentikasi.

Ketika kunci TLS Anda digunakan dengan VPC Lattice dan TLS Connection manager, nama layanan VPC Lattice Anda disertakan dalam konteks enkripsi yang digunakan untuk mengenkripsi kunci Anda saat istirahat. Anda dapat memverifikasi layanan VPC Lattice yang digunakan untuk sertifikat dan kunci pribadi Anda, dengan melihat konteks enkripsi di CloudTrail log Anda seperti yang ditunjukkan di bagian berikutnya, atau dengan melihat tab Sumber Daya Terkait di konsol ACM.

Untuk mendekripsi data, konteks enkripsi yang sama disertakan dalam permintaan. VPC Lattice menggunakan konteks enkripsi yang sama di semua operasi kriptografi AWS KMS, di mana kuncinya

adalah `aws:vpc-lattice:arn` dan nilainya adalah Nama Sumber Daya Amazon (ARN) dari layanan VPC Lattice.

Contoh berikut menunjukkan konteks enkripsi dalam output operasi seperti`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"
}
```

Memantau kunci enkripsi Anda untuk VPC Lattice

Bila Anda menggunakan kunci AWS terkelola dengan layanan VPC Lattice, Anda dapat menggunakannya AWS CloudTrailuntuk melacak permintaan yang dikirimkan oleh VPC Lattice. AWS KMS

CreateGrant

Ketika Anda menambahkan sertifikat ACM Anda ke layanan VPC Lattice, `CreateGrant` permintaan dikirim atas nama Anda untuk TLS Connection Manager untuk dapat mendekripsi kunci pribadi yang terkait dengan sertifikat ACM Anda

Anda dapat melihat `CreateGrant` operasi sebagai acara di CloudTrail >> Riwayat **`CreateGrant`** acara>>.

Berikut ini adalah contoh catatan peristiwa dalam riwayat CloudTrail acara untuk `CreateGrant` operasi:

```
{
    "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"
}
```

Anda akan melihat dalam `CreateGrant` contoh di atas bahwa prinsipal penerima hibah adalah TLS Connection Manager, dan konteks enkripsi memiliki layanan VPC Lattice ARN.

ListGrants

Anda dapat menggunakan ID kunci KMS dan ID akun Anda untuk memanggil `ListGrants` API. Ini memberi Anda daftar semua hibah untuk kunci KMS yang ditentukan. Untuk informasi lebih lanjut, lihat ListGrants.

Gunakan `ListGrants` perintah berikut di AWS CLI untuk melihat rincian semua hibah:

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

Output Anda akan terlihat mirip dengan contoh ini:

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

Anda akan melihat dalam `ListGrants` contoh di atas bahwa prinsipal penerima hibah adalah TLS Connection Manager, dan konteks enkripsi memiliki layanan VPC Lattice ARN.

Dekripsi

VPC Lattice menggunakan TLS Connection Manager untuk memanggil `Decrypt` operasi untuk mendekripsi kunci pribadi Anda untuk melayani koneksi TLS di layanan VPC Lattice Anda. Anda dapat melihat `Decrypt` operasi sebagai acara di CloudTrail >> Riwayat acara >> **`Decrypt`**.

Berikut ini adalah contoh catatan peristiwa dalam riwayat CloudTrail acara untuk `Decrypt` operasi:

```
{
    "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"
}
```

Manajemen identitas dan akses untuk Amazon VPC Lattice

Bagian berikut menjelaskan bagaimana Anda dapat menggunakan AWS Identity and Access Management (IAM) untuk membantu mengamankan sumber daya VPC Lattice Anda, dengan mengontrol siapa yang dapat melakukan tindakan VPC Lattice API.

Topik

Bagaimana Amazon VPC Lattice bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke VPC Lattice, pelajari fitur IAM apa saja yang tersedia untuk digunakan dengan VPC Lattice.

Fitur IAM yang dapat Anda gunakan dengan Amazon VPC Lattice

Fitur IAM	Dukungan VPC Lattice
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Ya
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk tampilan tingkat tinggi tentang cara kerja Kisi VPC dan layanan AWS lainnya dengan sebagian besar fitur IAM, AWS lihat layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk VPC Lattice

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya

tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya dalam VPC Lattice

Mendukung kebijakan berbasis sumber daya	Ya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya.

VPC Lattice mendukung kebijakan auth, kebijakan berbasis sumber daya yang memungkinkan Anda mengontrol akses ke layanan di jaringan layanan Anda. Untuk informasi selengkapnya, lihat Kontrol akses ke layanan VPC Lattice menggunakan kebijakan autentikasi.

VPC Lattice juga mendukung kebijakan izin berbasis sumber daya untuk integrasi dengan. AWS Resource Access Manager Anda dapat menggunakan kebijakan berbasis sumber daya ini untuk memberikan izin penggunaan ke AWS akun atau organisasi lain guna mengaktifkan berbagi sumber daya. Untuk informasi selengkapnya, lihat Bagikan sumber daya VPC Lattice.

Tindakan kebijakan untuk VPC Lattice

Mendukung tindakan kebijakan	Ya

Dalam pernyataan kebijakan IAM, Anda dapat menentukan tindakan API apa pun dari layanan apa pun yang mendukung IAM. Untuk VPC Lattice, gunakan awalan berikut dengan nama aksi API:. `vpc-lattice:` Misalnya:`vpc-lattice:CreateService`,`vpc-lattice:CreateTargetGroup`, dan`vpc-lattice:PutAuthPolicy`.

Untuk menentukan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma, sebagai berikut:

```
"Action": [ "vpc-lattice:action1", "vpc-lattice:action2" ]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard. Misalnya, Anda dapat menentukan semua tindakan yang namanya dimulai dengan kata`Get`, sebagai berikut:

```
"Action": "vpc-lattice:Get*"
```

Untuk daftar lengkap tindakan VPC Lattice API, lihat Tindakan yang ditentukan oleh Amazon VPC Lattice dalam Referensi Otorisasi Layanan.

Sumber daya kebijakan untuk VPC Lattice

Mendukung sumber daya kebijakan	Ya

Dalam pernyataan kebijakan IAM, `Resource` elemen menentukan objek atau objek yang dicakup oleh pernyataan tersebut. Untuk VPC Lattice, setiap pernyataan kebijakan IAM berlaku untuk sumber daya yang Anda tentukan menggunakan ARN mereka.

Format Amazon Resource Name (ARN) tertentu bergantung pada sumber daya. Saat Anda memberikan ARN, ganti teks yang *dicetak miring* dengan informasi spesifik sumber daya Anda.

- Akses langganan log:

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

- Pendengar:

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

- Aturan:

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

- Layanan:

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

- Jaringan layanan:

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

- Asosiasi layanan jaringan layanan:

```
"Resource": "arn:aws:vpc-lattice:region:account-
id:servicenetworkserviceassociation/service-network-service-association-id"
```

- Asosiasi VPC jaringan layanan:

```
"Resource": "arn:aws:vpc-lattice:region:account-
id:servicenetworkvpcassociation/service-network-vpc-association-id"
```

- Kelompok sasaran:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:targetgroup/target-group-id"
```

Kunci kondisi kebijakan untuk VPC Lattice

Mendukung kunci kondisi kebijakan khusus layanan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi

AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Kisi VPC, lihat Kunci kondisi untuk Amazon VPC Lattice di Referensi Otorisasi Layanan.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk informasi tentang kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Daftar kontrol akses (ACL) di VPC Lattice

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Kontrol akses berbasis atribut (ABAC) dengan VPC Lattice

Mendukung ABAC (tanda dalam kebijakan)	Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tag milik prinsipal cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensyal sementara dengan VPC Lattice

Mendukung penggunaan kredensial sementara	Ya

Beberapa AWS layanan tidak berfungsi saat Anda masuk menggunakan kredensyal sementara. Untuk informasi tambahan, termasuk yang AWS layanan bekerja dengan kredensyal sementara, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensyal sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensyal sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensyal sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Peran layanan untuk VPC Lattice

Mendukung peran layanan	Tidak

Peran layanan adalah sebuah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke AWS layanan dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas VPC Lattice. Edit peran layanan hanya jika VPC Lattice memberikan panduan untuk melakukannya.

Peran terkait layanan untuk VPC Lattice

Mendukung peran terkait layanan	Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. AWS layanan Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk informasi tentang membuat atau mengelola peran terkait layanan VPC Lattice, lihat. Menggunakan peran terkait layanan untuk Amazon VPC Lattice

Izin API Amazon VPC Lattice

Anda harus memberikan izin identitas IAM (seperti pengguna atau peran) untuk memanggil tindakan VPC Lattice API yang mereka butuhkan, seperti yang dijelaskan dalam. Tindakan kebijakan untuk VPC Lattice Selain itu, untuk beberapa tindakan VPC Lattice, Anda harus memberikan izin identitas IAM untuk memanggil tindakan tertentu dari API lain. AWS

Izin yang diperlukan untuk API

Saat memanggil tindakan berikut dari API, Anda harus memberikan izin kepada pengguna IAM untuk memanggil tindakan yang ditentukan.

`CreateServiceNetworkVpcAssociation`

- `vpc-lattice:CreateServiceNetworkVpcAssociation`

- `ec2:DescribeVpcs`
- `ec2:DescribeSecurityGroups`(Hanya diperlukan ketika kelompok keamanan disediakan)

`UpdateServiceNetworkVpcAssociation`

- `vpc-lattice:UpdateServiceNetworkVpcAssociation`
- `ec2:DescribeSecurityGroups`(Hanya diperlukan ketika kelompok keamanan disediakan)

`CreateTargetGroup`

- `vpc-lattice:CreateTargetGroup`
- `ec2:DescribeVpcs`

`RegisterTargets`

- `vpc-lattice:RegisterTargets`
- `ec2:DescribeInstances`(Hanya `INSTANCE` diperlukan kapan tipe grup target)
- `ec2:DescribeVpcs`(Hanya diperlukan ketika `INSTANCE` atau `IP` tipe grup target)
- `ec2:DescribeSubnets`(Hanya diperlukan ketika `INSTANCE` atau `IP` tipe grup target)
- `lambda:GetFunction`(Hanya `LAMBDA` diperlukan kapan tipe grup target)
- `lambda:AddPermission`(Hanya diperlukan jika grup target belum memiliki izin untuk menjalankan fungsi Lambda yang ditentukan)

`DeregisterTargets`

- `vpc-lattice:DeregisterTargets`

`CreateAccessLogSubscription`

- `vpc-lattice:CreateAccessLogSubscription`
- `logs:GetLogDelivery`
- `logs:CreateLogDelivery`

`DeleteAccessLogSubscription`

- `vpc-lattice:DeleteAccessLogSubscription`
- `logs:DeleteLogDelivery`

`UpdateAccessLogSubscription`

- `vpc-lattice:UpdateAccessLogSubscription`
- `logs:UpdateLogDelivery`

Kebijakan berbasis identitas untuk Amazon VPC Lattice

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya VPC Lattice. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Kisi VPC, termasuk format ARN untuk setiap jenis sumber daya, lihat Kunci Tindakan, Sumber Daya, dan Kondisi untuk Kisi VPC Amazon di Referensi Otorisasi Layanan.

Daftar Isi

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya VPC Lattice di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya

dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.

- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik AWS layanan, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan dalam IAM dalam Panduan Pengguna IAM.

Izin tambahan yang diperlukan untuk akses penuh

Untuk menggunakan AWS layanan lain yang terintegrasi dengan VPC Lattice dan seluruh rangkaian fitur VPC Lattice, Anda harus memiliki izin tambahan tertentu. Izin ini tidak termasuk dalam kebijakan `VPCLatticeFullAccess` terkelola karena risiko eskalasi hak istimewa wakil yang membingungkan.

Anda harus melampirkan kebijakan berikut ke peran Anda dan menggunakannya bersama dengan kebijakan `VPCLatticeFullAccess` terkelola.

```
{
```

```
    "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*"
        }
    ]
```

```
}
```

Kebijakan ini memberikan izin tambahan berikut:

- `iam:AttachRolePolicy`: Memungkinkan Anda melampirkan kebijakan terkelola yang ditentukan ke peran IAM yang ditentukan.
- `iam:PutRolePolicy`: Memungkinkan Anda menambahkan atau memperbarui dokumen kebijakan sebaris yang disematkan dalam peran IAM yang ditentukan.
- `s3:PutBucketPolicy`: Memungkinkan Anda menerapkan kebijakan bucket ke bucket Amazon S3.
- `firehose:TagDeliveryStream`: Memungkinkan Anda menambahkan atau memperbarui tag untuk aliran pengiriman Firehose.

Contoh kebijakan berbasis identitas untuk VPC Lattice

Topik

- Mengelola asosiasi VPC ke jaringan layanan
- Buat asosiasi layanan ke jaringan layanan
- Menambahkan tanda ke sumber daya
- Buat peran tertaut layanan

Mengelola asosiasi VPC ke jaringan layanan

Contoh berikut menunjukkan kebijakan yang memberi pengguna kebijakan ini izin untuk membuat, memperbarui, dan menghapus asosiasi VPC ke jaringan layanan, tetapi hanya untuk VPC dan jaringan layanan yang ditentukan dalam kondisi tersebut. Untuk informasi selengkapnya tentang menentukan kunci kondisi, lihatKunci kondisi kebijakan untuk 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"
            }
         }
      }
   ]
}
```

Buat asosiasi layanan ke jaringan layanan

Jika Anda tidak menggunakan tombol kondisi untuk mengontrol akses ke sumber daya VPC Lattice, Anda dapat menentukan ARN sumber daya dalam `Resource` elemen untuk mengontrol akses sebagai gantinya.

Contoh berikut menunjukkan kebijakan yang membatasi asosiasi layanan ke jaringan layanan yang dapat dibuat oleh pengguna dengan kebijakan ini dengan menentukan ARN jaringan layanan dan layanan yang dapat digunakan dengan tindakan API. `CreateServiceNetworkServiceAssociation` Untuk informasi selengkapnya tentang menentukan nilai ARN, lihat. Sumber daya kebijakan untuk 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"
         ]
```

```
      }
   ]
}
```

Menambahkan tanda ke sumber daya

Contoh berikut menunjukkan kebijakan yang memberi pengguna izin kebijakan ini untuk membuat tag pada resource VPC Lattice.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:TagResource"
         ],
         "Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:*/*"
      }
   ]
}
```

Buat peran tertaut layanan

VPC Lattice memerlukan izin untuk membuat peran terkait layanan saat pertama kali setiap pengguna di Anda membuat sumber daya VPC Lattice. Akun AWS Jika peran terkait layanan belum ada, VPC Lattice membuatnya di akun Anda. Peran terkait layanan memberikan izin ke VPC Lattice sehingga dapat memanggil orang lain atas nama Anda. AWS layanan

Agar pembuatan peran otomatis berhasil, pengguna harus memiliki izin untuk tindakan `iam:CreateServiceLinkedRole` nyata.

```
"Action": "iam:CreateServiceLinkedRole"
```

Contoh berikut menunjukkan kebijakan yang memberi pengguna izin kebijakan ini untuk membuat peran terkait layanan untuk VPC Lattice.

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

Menggunakan peran terkait layanan untuk Amazon VPC Lattice

Amazon VPC Lattice menggunakan peran terkait layanan untuk izin yang diperlukan untuk memanggil orang lain atas nama Anda. AWS layanan Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan dalam Panduan Pengguna IAM.

Izin peran terkait layanan untuk VPC Lattice

VPC Lattice menggunakan peran terkait layanan bernama. AWSServiceRoleForVpcLattice

Peran AWSServiceRoleForVpcLatticeterkait layanan mempercayai layanan berikut untuk mengambil peran:

- `vpc-lattice.amazonaws.com`

Kebijakan izin peran bernama `AWSVpcLatticeServiceRolePolicy` memungkinkan VPC Lattice CloudWatch mempublikasikan metrik di namespace. `AWS/VpcLattice`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "cloudwatch:namespace": "AWS/VpcLattice"
                }
            }
        }
    ]
}
```

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran terkait layanan untuk VPC Lattice

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat resource VPC Lattice di AWS Management Console, the, atau API AWS CLI AWS , VPC Lattice membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran tertaut layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat resource VPC Lattice, VPC Lattice membuat peran yang ditautkan layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk VPC Lattice

Anda dapat mengedit deskripsi AWSServiceRoleForVpcLatticemenggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran tertaut layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk VPC Lattice

Jika Anda tidak perlu lagi menggunakan Amazon VPC Lattice, kami sarankan Anda menghapus. AWSServiceRoleForVpcLattice

Anda dapat menghapus peran terkait layanan ini hanya setelah Anda menghapus semua sumber daya VPC Lattice di situs Anda. Akun AWS

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForVpcLatticeterkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

Setelah Anda menghapus peran terkait layanan, VPC Lattice akan membuat peran tersebut lagi saat Anda membuat resource VPC Lattice di. Akun AWS

Wilayah yang Didukung untuk peran terkait layanan VPC Lattice

VPC Lattice mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia.

AWS kebijakan terkelola untuk Amazon VPC Lattice

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru AWS layanan diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: VPC LatticeFullAccess

Kebijakan ini menyediakan akses penuh ke Amazon VPC Lattice dan akses terbatas ke layanan dependen lainnya. Ini termasuk izin untuk melakukan hal berikut:

- ACM — Ambil sertifikat SSL/TLS ARN untuk nama domain kustom.
- CloudWatch — Lihat log akses dan data pemantauan.
- CloudWatch Log - Mengatur dan mengirim log akses ke CloudWatch Log.
- Amazon EC2 — Ambil informasi tentang instans EC2 dan VPC untuk membuat grup target dan mendaftarkan target.
- Elastic Load Balancing — Ambil informasi tentang Application Load Balancer untuk mendaftarkannya sebagai target.
- Firehose — Mengambil informasi tentang aliran pengiriman yang digunakan untuk menyimpan log akses.
- Lambda — Ambil informasi tentang fungsi Lambda untuk mendaftarkannya sebagai target.

- Amazon S3 - Ambil informasi tentang bucket S3 yang digunakan untuk menyimpan log akses.

Untuk melihat izin kebijakan ini, lihat LatticeFullAccessVPC di Referensi Kebijakan AWS Terkelola.

Untuk menggunakan AWS layanan lain yang terintegrasi dengan VPC Lattice dan seluruh rangkaian fitur VPC Lattice, Anda harus memiliki izin tambahan tertentu. Izin ini tidak termasuk dalam kebijakan `VPCLatticeFullAccess` terkelola karena risiko eskalasi hak istimewa wakil yang membingungkan. Untuk informasi selengkapnya, lihat Izin tambahan yang diperlukan untuk akses penuh.

AWS kebijakan terkelola: VPC LatticeReadOnlyAccess

Kebijakan ini menyediakan akses hanya-baca ke Amazon VPC Lattice dan akses terbatas ke layanan dependen lainnya. Ini termasuk izin untuk melakukan hal berikut:

- ACM — Ambil sertifikat SSL/TLS ARN untuk nama domain kustom.
- CloudWatch — Lihat log akses dan data pemantauan.
- CloudWatch Log - Lihat informasi pengiriman log untuk langganan log akses.
- Amazon EC2 — Ambil informasi tentang instans EC2 dan VPC untuk membuat grup target dan mendaftarkan target.
- Elastic Load Balancing — Mengambil informasi tentang Application Load Balancer.
- Firehose — Ambil informasi tentang aliran pengiriman untuk pengiriman log akses.
- Lambda - Lihat informasi tentang fungsi Lambda.
- Amazon S3 - Ambil informasi tentang bucket S3 untuk pengiriman log akses.

Untuk melihat izin kebijakan ini, lihat LatticeReadOnlyAccessVPC di Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: VPC LatticeServicesInvokeAccess

Kebijakan ini menyediakan akses untuk memanggil layanan Amazon VPC Lattice.

Untuk melihat izin kebijakan ini, lihat LatticeServicesInvokeAccessVPC di Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AWSVpcLatticeServiceRolePolicy

Kebijakan ini dilampirkan ke peran terkait layanan yang diberi nama AWSServiceRoleForVpcLatticeuntuk mengizinkan VPC Lattice melakukan tindakan atas nama Anda.

Anda tidak dapat melampirkan kebijakan ini ke entitas IAM Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Amazon VPC Lattice.

Untuk melihat izin kebijakan ini, lihat AWSVpcLatticeServiceRolePolicydi Referensi Kebijakan AWS Terkelola.

VPC Lattice memperbarui kebijakan terkelola AWS

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk VPC Lattice sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS untuk Panduan Pengguna VPC Lattice.

Perubahan	Deskripsi	Tanggal
VPC LatticeFullAccess	VPC Lattice menambahkan kebijakan baru untuk memberikan izin akses penuh ke Amazon VPC Lattice dan akses terbatas ke layanan dependen lainnya.	31 Maret 2023
VPC LatticeReadOnlyAccess	VPC Lattice menambahkan kebijakan baru untuk memberikan izin akses hanya-baca ke Amazon VPC Lattice dan akses terbatas ke layanan dependen lainnya.	31 Maret 2023
VPC LatticeServicesInvokeAccess	VPC Lattice menambahkan kebijakan baru untuk memberikan akses ke layanan Amazon VPC Lattice.	31 Maret 2023
AWSVpcLatticeServiceRolePolicy	VPC Lattice menambahkan izin ke peran terkait layananny a untuk memungkinkan VPC Lattice mempublikasikan metrik di namespace. CloudWatch `AWS/VpcLattice` `AWSVpcLatticeServiceRolePolicy` Kebijakan ini mencakup izin untuk memanggil tindakan	Desember 5, 2022

Perubahan	Deskripsi	Tanggal
	CloudWatch PutMetricDataAPI. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Amazon VPC Lattice.	
VPC Lattice mulai melacak perubahan	VPC Lattice mulai melacak perubahan untuk kebijakan terkelola nya AWS .	Desember 5, 2022

Validasi kepatuhan untuk Amazon VPC Lattice

Auditor pihak ketiga menilai keamanan dan kepatuhan Amazon VPC Lattice sebagai bagian dari beberapa AWS program kepatuhan.

Untuk mempelajari apakah an AWS layanan berada dalam lingkup program kepatuhan tertentu, lihat AWS layanan di Lingkup oleh Program Kepatuhan AWS layanan dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan AWS layanan ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

> **Note**
>
> Tidak semua memenuhi AWS layanan syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan AWS layanan dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini AWS layanan memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini AWS layanan mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni AWS layanan membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Akses Amazon VPC Lattice menggunakan titik akhir antarmuka () PrivateLink

Anda dapat membuat koneksi pribadi antara VPC dan Amazon VPC Lattice dengan membuat antarmuka VPC endpoint. Endpoint antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda mengakses VPC Lattice API secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan VPC Lattice API.

Setiap titik akhir antarmuka diwakili oleh satu atau lebih antarmuka jaringan di subnet Anda.

Pertimbangan untuk titik akhir VPC antarmuka

Sebelum Anda menyiapkan titik akhir VPC antarmuka untuk VPC Lattice, pastikan Anda meninjau Akses melalui Panduan. AWS layanan AWS PrivateLinkAWS PrivateLink

VPC Lattice mendukung panggilan ke semua tindakan API-nya dari VPC Anda.

Membuat antarmuka VPC endpoint untuk VPC Lattice

Anda dapat membuat titik akhir VPC untuk layanan VPC Lattice menggunakan konsol VPC Amazon atau (). AWS Command Line Interface AWS CLIUntuk informasi selengkapnya, lihat Membuat titik akhir VPC antarmuka di Panduan.AWS PrivateLink

Buat titik akhir VPC untuk VPC Lattice menggunakan nama layanan berikut:

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

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API ke VPC Lattice menggunakan nama DNS default untuk Wilayah, misalnya,. `vpc-lattice.us-east-1.amazonaws.com`

Ketahanan di Amazon VPC Lattice

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones.

Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan.

Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan infrastruktur di Amazon VPC Lattice

Sebagai layanan terkelola, Amazon VPC Lattice dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat

Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses VPC Lattice melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Memantau Amazon VPC Lattice

Gunakan fitur di bagian ini untuk memantau jaringan layanan Amazon VPC Lattice, layanan, grup target, dan koneksi VPC.

Konten

CloudWatch metrik untuk Amazon VPC Lattice

Amazon VPC Lattice mengirimkan data yang terkait dengan grup target dan layanan Anda ke Amazon CloudWatch, dan memprosesnya menjadi metrik hampir real-time yang dapat dibaca. Metrik ini disimpan selama 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang kinerja aplikasi atau layanan web Anda. Anda juga dapat mengatur alarm yang mengawasi ambang batas tertentu dan mengirim pemberitahuan atau mengambil tindakan ketika ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Amazon VPC Lattice menggunakan peran terkait layanan di AWS akun Anda untuk mengirim metrik ke Amazon. CloudWatch Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Amazon VPC Lattice.

Daftar Isi

Lihat CloudWatch metrik Amazon

Anda dapat melihat CloudWatch metrik Amazon untuk grup dan layanan target menggunakan CloudWatch konsol atau AWS CLI.

Untuk melihat metrik menggunakan konsol CloudWatch

1. Buka CloudWatch konsol Amazon di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Metrik.
3. Pilih `AWS/VpcLattice` namespace.
4. (Opsional) Untuk melihat metrik di semua dimensi, masukkan namanya di kolom pencarian.
5. (Opsional) Untuk memfilter metrik berdasarkan dimensi, pilih salah satu hal berikut:
   - Untuk hanya menampilkan metrik yang dilaporkan untuk grup target Anda, pilih Grup target. Untuk melihat metrik untuk satu grup target, masukkan namanya di kolom pencarian.
   - Untuk hanya menampilkan metrik yang dilaporkan untuk layanan Anda, pilih Layanan. Untuk melihat metrik untuk satu layanan, masukkan namanya di bidang pencarian.

Untuk melihat metrik menggunakan AWS CLI

Gunakan AWS CLI perintah CloudWatch daftar-metrik berikut untuk membuat daftar metrik yang tersedia:

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

Untuk informasi tentang masing-masing metrik dan dimensinya, lihat Metrik kelompok sasaran danMetrik Layanan.

Metrik kelompok sasaran

VPC Lattice secara otomatis menyimpan metrik yang terkait dengan grup target di namespace Amazon. `AWS/VpcLattice` CloudWatch Untuk informasi selengkapnya tentang kelompok sasaran, lihatGrup sasaran di VPC Lattice.

Anda mungkin ingin memantau `HTTP code` dan `RequestTime` metrik untuk grup target. Anda dapat memfilter metrik ini berdasarkan Availability Zone (AZ) untuk menentukan AZ mana grup target berada.

Metrik	Deskripsi
`TotalConnectionCount`	Total koneksi. Kriteria pelaporan

Metrik	Deskripsi
	• Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`ActiveConnectionCount`	Koneksi aktif. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`ConnectionErrorCount`	Kegagalan koneksi total. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`HTTP1_ConnectionCount`	Total koneksi HTTP/1.1. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`HTTP2_ConnectionCount`	Total koneksi HTTP/2. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`ConnectionTimeoutCount`	Total koneksi menghubungkan batas waktu. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`TotalReceivedConnectionBytes`	Total byte koneksi yang diterima. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`TotalSentConnectionBytes`	Total byte koneksi yang dikirim. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`TotalRequestCount`	Total permintaan. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`ActiveRequestCount`	Total permintaan aktif. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`RequestTime`	Minta waktu dalam milidetik. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah `Average` dan `pNN.NN` (persentil). Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`HTTPCode_2XX_Count`, `HTTPCode_3XX_Count`, `HTTPCode_4XX_Count`, `HTTPCode_5XX_Count`	Kode respons HTTP agregat. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`TLSConnectionErrorCount`	Total kesalahan koneksi TLS tidak termasuk verifikasi sertifikat yang gagal. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`TotalTLSConnection HandshakeCount`	Total jabat tangan koneksi TLS yang berhasil. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`TargetGroup` , Nilai: Nama kelompok sasaran. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik Layanan

VPC Lattice secara otomatis menyimpan metrik yang terkait dengan layanan di namespace Amazon. `AWS/VpcLattice` CloudWatch Untuk informasi selengkapnya tentang layanan, lihatLayanan di VPC Lattice.

Anda mungkin ingin memantau `HTTP code` dan `RequestTime` metrik untuk layanan. Anda dapat memfilter metrik ini berdasarkan Availability Zone (AZ) untuk menentukan AZ mana layanan tersebut berada.

Metrik	Deskripsi
`RequestTimeoutCount`	Total permintaan yang waktunya habis menunggu respons.

Metrik	Deskripsi
	Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`Service`, Nilai: ID layanan. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`TotalRequestCount`	Total permintaan. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`Service`, Nilai: ID layanan. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`RequestTime`	Minta waktu dalam milidetik. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah `Average` dan `pNN.NN` (persentil). Dimensi • Nama:`Service`, Nilai: ID layanan. • Nama:`AvailabilityZone` , Nilai: AZ tempat grup target berada.

Metrik	Deskripsi
`HTTPCode_2XX_Count`, `HTTPCode_3XX_Count`, `HTTPCode_4XX_Count`, `HTTPCode_5XX_Count`	Kode respons HTTP agregat. Kriteria pelaporan • Selalu dilaporkan (apakah itu nilai nol atau bukan nol) sejak sumber daya menerima lalu lintas. Frekuensi pelaporan • Sekali semenit. Statistik • Statistik yang paling berguna adalah`Sum`. Dimensi • Nama:`Service`, Nilai: ID layanan. • Nama:`AvailabilityZone`, Nilai: AZ tempat grup target berada.

Akses log untuk Amazon VPC Lattice

Log akses menangkap informasi terperinci tentang layanan VPC Lattice Anda. Anda dapat menggunakan log akses ini untuk menganalisis pola lalu lintas dan mengaudit semua layanan di jaringan.

Log akses bersifat opsional dan dinonaktifkan secara default. Setelah Anda mengaktifkan log akses, Anda dapat menonaktifkannya kapan saja.

Harga

Biaya berlaku ketika log akses dipublikasikan. Log yang diterbitkan AWS secara native atas nama Anda disebut vended logs. Untuk informasi selengkapnya tentang harga untuk log penjual, lihat CloudWatch Harga Amazon, pilih Log, dan lihat harga di bawah Log Penjual.

Daftar Isi

Izin IAM diperlukan untuk mengaktifkan log akses

Untuk mengaktifkan log akses dan mengirim log ke tujuan mereka, Anda harus memiliki tindakan berikut dalam kebijakan yang dilampirkan pada pengguna, grup, atau peran IAM yang Anda gunakan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Sid": "ManageVPCLatticeAccessLogSetup",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:GetLogDelivery",
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "vpc-lattice:CreateAccessLogSubscription",
                "vpc-lattice:GetAccessLogSubscription",
                "vpc-lattice:UpdateAccessLogSubscription",
                "vpc-lattice:DeleteAccessLogSubscription",
                "vpc-lattice:ListAccessLogSubscriptions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Untuk informasi selengkapnya, lihat Menambahkan dan menghapus izin identitas IAM di AWS Identity and Access Management Panduan Pengguna.

Setelah memperbarui kebijakan yang dilampirkan ke pengguna, grup, atau peran IAM yang Anda gunakan, buka. Aktifkan log akses

Akses tujuan log

Anda dapat mengirim log akses ke tujuan berikut.

CloudWatch Log Amazon

- VPC Lattice biasanya mengirimkan log ke CloudWatch Log dalam waktu 2 menit. Namun, perlu diingat bahwa waktu pengiriman log yang sebenarnya adalah upaya terbaik dan mungkin ada latensi tambahan.
- Kebijakan sumber daya dibuat secara otomatis dan ditambahkan ke grup CloudWatch log jika grup log tidak memiliki izin tertentu. Untuk informasi selengkapnya, lihat Log yang dikirim ke CloudWatch Log di Panduan CloudWatch Pengguna Amazon.
- Anda dapat menemukan log akses yang dikirim ke CloudWatch bawah Grup Log di CloudWatch konsol. Untuk informasi selengkapnya, lihat Melihat data log yang dikirim ke CloudWatch Log di Panduan CloudWatch Pengguna Amazon.

Amazon S3

- VPC Lattice biasanya mengirimkan log ke Amazon S3 dalam waktu 6 menit. Namun, perlu diingat bahwa waktu pengiriman log yang sebenarnya adalah upaya terbaik dan mungkin ada latensi tambahan.
- Kebijakan bucket akan dibuat secara otomatis dan ditambahkan ke bucket Amazon S3 Anda jika bucket tidak memiliki izin tertentu. Untuk informasi selengkapnya, lihat Log yang dikirim ke Amazon S3 di CloudWatchPanduan Pengguna Amazon.
- Akses log yang dikirim ke Amazon S3 menggunakan konvensi penamaan berikut:

```
[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 biasanya mengirimkan log ke Firehose dalam waktu 2 menit. Namun, perlu diingat bahwa waktu pengiriman log yang sebenarnya adalah upaya terbaik dan mungkin ada latensi tambahan.
- Peran terkait layanan dibuat secara otomatis yang memberikan izin VPC Lattice untuk mengirim log akses ke. Amazon Data Firehose Agar pembuatan peran otomatis berhasil, pengguna harus memiliki izin untuk tindakan `iam:CreateServiceLinkedRole` nyata. Untuk informasi selengkapnya, lihat Log yang dikirimkan Amazon Data Firehose di Panduan CloudWatch Pengguna Amazon.
- Untuk informasi selengkapnya tentang melihat log yang dikirimkan Amazon Data Firehose, lihat Memantau Aliran Data Amazon Kinesis Amazon Data Firehose di Panduan Pengembang.

Aktifkan log akses

Selesaikan prosedur berikut untuk mengonfigurasi log akses untuk menangkap dan mengirimkan log akses ke tujuan yang Anda pilih.

Daftar Isi

Aktifkan log akses menggunakan konsol

Anda dapat mengaktifkan log akses untuk jaringan layanan atau untuk layanan selama pembuatan. Anda juga dapat mengaktifkan log akses setelah Anda membuat jaringan layanan atau layanan, seperti yang dijelaskan dalam prosedur berikut.

Untuk membuat layanan dasar menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pilih jaringan layanan atau layanan.
3. Pilih Tindakan, Edit pengaturan log.
4. Aktifkan sakelar sakelar Access logs.
5. Tambahkan tujuan pengiriman untuk log akses Anda sebagai berikut:

- Pilih Grup CloudWatch log dan pilih grup log. Untuk membuat grup log, pilih Buat grup log masuk CloudWatch.
- Pilih bucket S3 dan masukkan path bucket S3, termasuk awalan apa pun. Untuk mencari bucket S3 Anda, pilih Browse S3.
- Pilih aliran pengiriman Kinesis Data Firehose dan pilih aliran pengiriman. Untuk membuat aliran pengiriman, pilih Buat aliran pengiriman di Kinesis.

6. Pilih Simpan perubahan.

Aktifkan log akses menggunakan AWS CLI

Gunakan perintah CLI create-access-log-subscriptionuntuk mengaktifkan log akses untuk jaringan layanan atau layanan.

Akses isi log

Tabel berikut menjelaskan bidang entri log akses.

Bidang	Deskripsi	format
`hostHeader`	Header otoritas permintaan.	string
`sslCipher`	Nama OpenSSL untuk set cipher yang digunakan untuk membangun koneksi TLS klien.	string
`serviceNetworkArn`	Jaringan layanan ARN.	*`arn:aws:vpc-lattice: wilayah: akun:servicenetwork/ id`*
`resolvedUser`	ARN pengguna saat otentikasi diaktifkan dan otentikasi dilakukan.	null | ARN | “Anonim” | “Tidak diketahui”
`authDeniedReason`	Alasan bahwa akses ditolak ketika otentikasi diaktifkan.	null | “Layanan” | “Jaringan” | “Identitas”
`requestMethod`	Header metode permintaan.	string

Bidang	Deskripsi	format
`targetGroupArn`	Grup host target tempat host target berada.	string
`tlsVersion`	Versi TLS.	*TlSV x*
`userAgent`	Header user-agent.	string
`ServerNameIndication`	[Hanya HTTPS] Nilai yang ditetapkan pada soket koneksi ssl untuk Indikasi Nama Server (SNI).	string
`destinationVpcId`	ID VPC tujuan.	*vpc- xxxxxxxx*
`sourceIpPort`	Alamat IP dan:port sumber.	*ip*: *port*
`targetIpPort`	Alamat IP dan port target.	*ip*: *port*
`serviceArn`	Layanan ARN.	*arn:aws:vpc-lattice: wilayah: akun:layanan/id*
`sourceVpcId`	ID VPC sumber.	*vpc- xxxxxxxx*
`requestPath`	Jalur permintaan.	LatticePath? : *jalur*
`startTime`	Waktu mulai permintaan.	*YYYY - MM - DD T HH: MM: SS Z*
`protocol`	Protokol. Saat ini HTTP/1.1 atau HTTP/2.	string
`responseCode`	Kode respons HTTP. Hanya kode respons untuk header akhir yang dicatat. Untuk informasi selengkapnya, lihat Memecahkan masalah log akses.	integer

Bidang	Deskripsi	format
`bytesReceived`	Body dan header byte diterima.	integer
`bytesSent`	Body dan header byte dikirim.	integer
`duration`	Total durasi dalam milidetik permintaan dari waktu mulai hingga byte terakhir keluar.	integer
`requestToTargetDuration`	Total durasi dalam milidetik permintaan dari waktu mulai hingga byte terakhir yang dikirim ke target.	integer
`responseFromTargetDuration`	Total durasi dalam milidetik permintaan dari byte pertama yang dibaca dari host target ke byte terakhir yang dikirim ke klien.	integer
`grpcResponseCode`	Kode respons gRPC. Untuk informasi selengkapnya, lihat Kode status dan penggunaannya di gRPC. Bidang ini dicatat hanya jika layanan mendukung gRPC.	integer
`callerPrincipal`	Prinsipal yang diautentikasi.	string
`callerX509SubjectCN`	Nama subjek (CN).	string
`callerX509IssuerOU`	Penerbit (OU).	string
`callerX509SANNameCN`	Alternatif penerbit (Nama/CN).	string
`callerX509SANDNS`	Nama alternatif subjek (DNS).	string

Bidang	Deskripsi	format
`callerX509SANURI`	Nama alternatif subjek (URI).	string
`sourceVpcArn`	ARN dari VPC tempat permintaan berasal.	*`arn:aws:ec2: wilayah: akun:vpc/ id`*

Contoh

Berikut ini adalah contoh entri log.

```
{
    "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
}
```

Memecahkan masalah log akses

Bagian ini berisi penjelasan tentang kode kesalahan HTTP yang mungkin Anda lihat di log akses.

Kode kesalahan	Kemungkinan penyebab
HTTP 400: Permintaan Buruk	• Klien mengirim permintaan cacat yang tidak memenuhi spesifikasi HTTP. • Header permintaan melebihi 60K untuk seluruh header permintaan atau lebih dari 100 header. • Klien menutup koneksi sebelum mengirim badan permintaan lengkap.
HTTP 403: Terlarang	Otentikasi telah dikonfigurasi untuk layanan, tetapi permintaan yang masuk tidak diautentikasi atau diotorisasi.
HTTP 404: Layanan Tidak Ada	Anda mencoba untuk terhubung ke layanan yang tidak ada atau tidak terdaftar ke jaringan layanan yang tepat.
HTTP 500: Kesalahan Server Internal	VPC Lattice telah mengalami kesalahan, seperti kegagalan untuk terhubung ke target.
HTTP 502: Gerbang Buruk	VPC Lattice mengalami kesalahan.

CloudTrail log untuk Amazon VPC Lattice

AWS CloudTrail adalah AWS layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan. CloudTrail menangkap panggilan API untuk VPC Lattice sebagai peristiwa. CloudTrail diaktifkan pada Anda Akun AWS saat Anda membuatnya. Ketika aktivitas terjadi di VPC Lattice, aktivitas tersebut dicatat sebagai CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Panggilan yang diambil termasuk panggilan dari konsol VPC Lattice dan panggilan kode ke operasi VPC Lattice API. Untuk informasi selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan

dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu. Trail adalah CloudTrail konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket S3 yang Anda tentukan.

Untuk memantau tindakan tambahan, gunakan log akses. Untuk informasi selengkapnya, lihat Log akses.

Memahami entri file log VPC Lattice

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Untuk informasi terkait pasangan nilai kunci di log, lihat CloudTrail merekam konten di AWS CloudTrail Panduan Pengguna.

Berikut ini adalah contoh entri log untuk panggilan ke tindakan CreateServiceAPI.

```
{
  "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"
}
```

Berikut ini adalah contoh entri log untuk panggilan ke tindakan DeleteServiceAPI.

```
{
  "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"
}
```

Kuota untuk Amazon VPC Lattice

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk masing-masing. AWS layananKecuali dinyatakan sebaliknya, setiap kuota unik untuk suatu Wilayah. Anda dapat meminta penambahan untuk beberapa kuota, sementara kuota lainnya tidak dapat ditambah.

Untuk melihat kuota untuk VPC Lattice, buka konsol Service Quotas. Di panel navigasi, pilih AWS layanandan pilih VPC Lattice.

Untuk meminta peningkatan kuota, hubungi AWS Support, atau lihat Meminta Peningkatan Kuota dalam Panduan Pengguna Service Quotas.

Anda Akun AWS memiliki kuota berikut yang terkait dengan VPC Lattice.

Nama	Default	Dapat disesuan	Deskripsi
Ukuran kebijakan autentikasi	Setiap Wilayah yang didukung: 10 Kilobyte	Tidak	Ukuran maksimum file JSON dalam kebijakan Auth.
Pendengar per layanan	Setiap Wilayah yang didukung: 2	Ya	Jumlah maksimum pendengar yang dapat Anda buat untuk suatu layanan. Untuk peningkatan kapasitas dan batas tambahan, hubungi AWS Support.
Aturan per pendengar	Setiap Wilayah yang didukung: 5	Ya	Jumlah maksimum aturan yang dapat Anda tentukan untuk pendengar layanan Anda. Untuk peningkatan kapasitas dan batas tambahan, hubungi AWS Support.

Nama	Default	Dapat disesuaian	Deskripsi
Kelompok keamanan per asosiasi	Setiap Wilayah yang didukung: 5	Tidak	Jumlah maksimum grup keamanan yang dapat Anda tambahkan ke asosiasi antara VPC dan jaringan layanan.
Asosiasi layanan per jaringan layanan	Setiap Wilayah yang didukung: 500	Ya	Jumlah maksimum layanan yang dapat Anda kaitkan dengan satu jaringan layanan. Untuk peningkatan kapasitas dan batas tambahan, hubungi AWS Support.
Jaringan layanan per wilayah	Setiap Wilayah yang didukung: 10	Ya	Jumlah maksimum jaringan layanan per wilayah. Untuk peningkatan kapasitas dan batas tambahan, hubungi AWS Support.
Layanan per wilayah	Setiap Wilayah yang didukung: 500	Ya	Jumlah maksimum layanan per wilayah. Untuk peningkatan kapasitas dan batas tambahan, hubungi AWS Support.

Nama	Default	Dapat disesuaian	Deskripsi
Kelompok sasaran per wilayah	Setiap Wilayah yang didukung: 500	Ya	Jumlah maksimum kelompok sasaran per wilayah. Untuk peningkatan kapasitas dan batas tambahan, hubungi AWS Support.
Grup target per layanan	Setiap Wilayah yang didukung: 5	Ya	Jumlah maksimum kelompok sasaran yang dapat Anda kaitkan dengan layanan. Untuk peningkatan kapasitas dan batas tambahan, hubungi AWS Support.
Target per kelompok sasaran	Setiap Wilayah yang didukung: 1.000	Ya	Jumlah maksimum target yang dapat Anda kaitkan dengan satu kelompok target. Untuk peningkatan kapasitas dan batas tambahan, hubungi AWS Support.
Asosiasi VPC per jaringan layanan	Setiap Wilayah yang didukung: 500	Ya	Jumlah maksimum VPC yang dapat Anda kaitkan dengan satu jaringan layanan. Untuk peningkatan kapasitas dan batas tambahan, hubungi AWS Support.

Batasan berikut juga berlaku.

Kuota	Nilai
Bandwidth per layanan per Availability Zone	10 Gbps
Unit transmisi maksimum (MTU) per koneksi	8500 byte
Permintaan per detik per layanan per Availability Zone	10.000

Riwayat dokumen untuk Panduan Pengguna Amazon VPC Lattice

Tabel berikut menjelaskan rilis dokumentasi untuk VPC Lattice.

Perubahan	Deskripsi	Tanggal
Passthrough TLS	VPC Lattice sekarang mendukung passthrough TLS, yang memungkinkan Anda melakukan penghenti an TLS di aplikasi Anda untuk otentikasi. end-to-end	14 Mei 2024
Versi struktur acara Lambda	VPC Lattice sekarang mendukung versi baru dari struktur acara Lambda.	7 September 2023
Support untuk VPC bersama	Peserta dapat membuat grup target VPC Lattice dalam VPC bersama.	5 Juli 2023
Rilis Ketersediaan Umum	Rilis Panduan Pengguna Kisi VPC untuk Ketersediaan Umum (GA)	31 Maret 2023
VPC Lattice sekarang melaporkan perubahan pada kebijakan yang dikelola AWS	Perubahan pada kebijakan terkelola dilaporkan dalam "kebijakan AWS terkelola untuk Kisi VPC” di bagian “Keamanan”.	29 Maret 2023
Support untuk tipe target Application Load Balancer	VPC Lattice sekarang mendukung pembuatan grup target tipe Application Load Balancer.	29 Maret 2023

Support untuk semua jenis instans	VPC Lattice sekarang mendukung semua jenis instance.	Maret 27, 2023
Dukungan IPv6	VPC Lattice sekarang mendukung kelompok target IPv4 dan IPv6 IP.	Maret 27, 2023
Versi protokol HTTP2 untuk pemeriksaan kesehatan	Pemeriksaan kesehatan sekarang didukung ketika versi protokol grup target adalah HTTP2.	Maret 27, 2023
Tindakan respons tetap untuk aturan pendengar	Pendengar untuk layanan VPC Lattice sekarang mendukung tindakan respons tetap selain tindakan penerusan.	Maret 27, 2023
Support untuk nama domain kustom	Anda sekarang dapat mengonfigurasi nama domain khusus untuk layanan VPC Lattice Anda	14 Februari 2023
Support untuk BYOC (Bring Your Own Certificate)	VPC Lattice mendukung penggunaan sertifikat SSL/TLS Anda sendiri di ACM untuk nama domain khusus.	14 Februari 2023
VPC Lattice sekarang melaporkan daftar terbaru dari jenis instans yang tidak didukung	Tiga instance tambahan telah ditambahkan ke daftar instans yang tidak didukung.	26 Januari 2023

VPC Lattice sekarang melaporkan perubahan pada kebijakan yang dikelola AWS	Mulai 5 Desember 2022, perubahan kebijakan terkelola dilaporkan dalam topik "kebijakan AWS terkelola untuk Kisi VPC” di bagian “Keamanan”. Perubahan pertama yang tercantum adalah penambahan izin yang diperlukan untuk CloudWatch pemantauan.	Desember 5, 2022
Rilis awal	Rilis awal Panduan Pengguna VPC Lattice	Desember 5, 2022

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.