AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

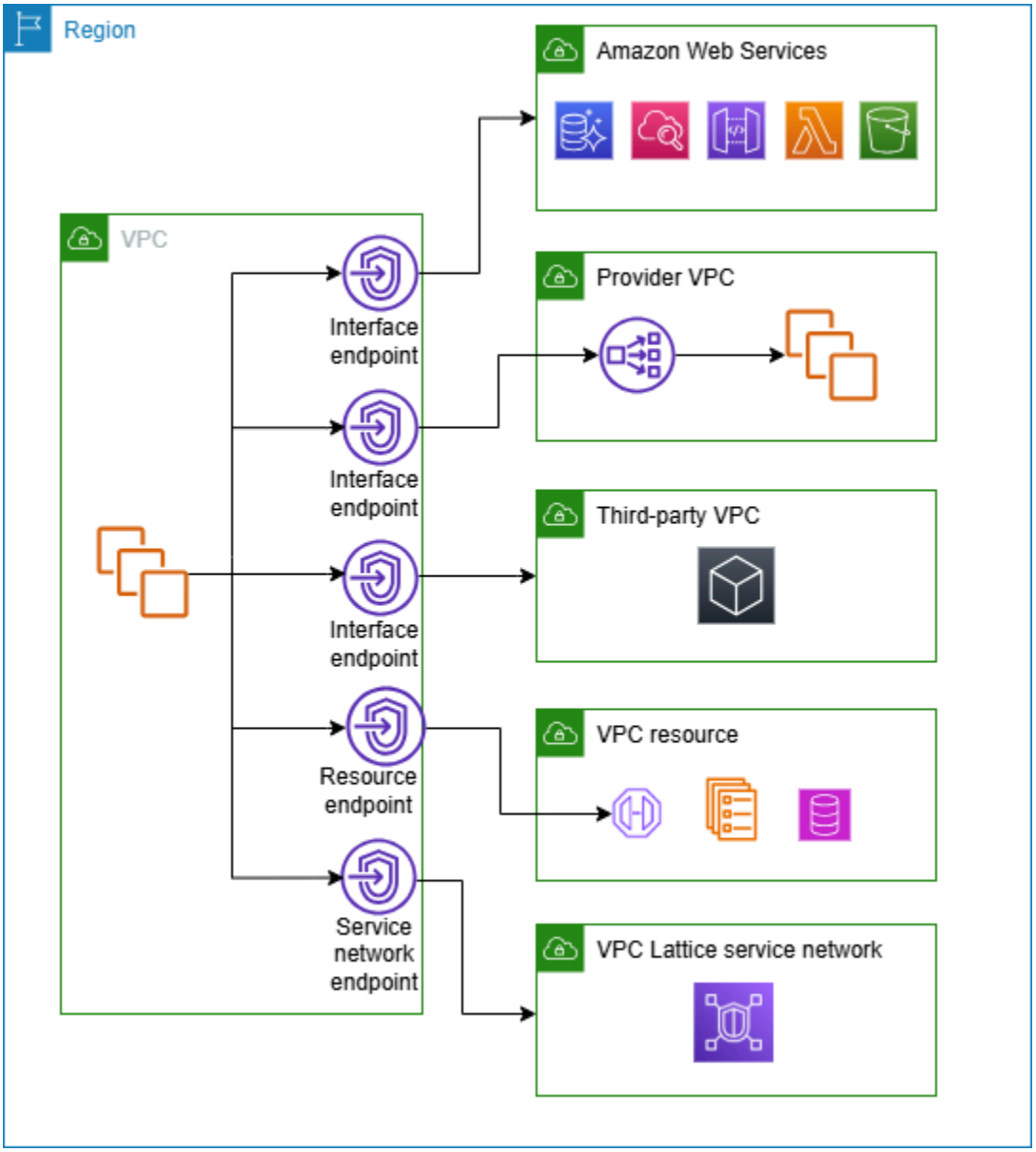
Apa itu AWS PrivateLink?

AWS PrivateLink adalah teknologi yang sangat tersedia dan dapat diskalakan yang dapat Anda gunakan untuk menghubungkan VPC Anda secara pribadi ke layanan dan sumber daya seolah-olah mereka ada di VPC Anda. Anda tidak perlu menggunakan gateway internet, perangkat NAT, alamat IP publik, Direct Connect koneksi, atau AWS Site-to-Site VPN koneksi untuk memungkinkan komunikasi dengan layanan atau sumber daya dari subnet pribadi Anda. Oleh karena itu, Anda mengontrol titik akhir API tertentu, situs, layanan, dan sumber daya yang dapat dijangkau dari VPC Anda.

Kasus penggunaan

Anda dapat membuat titik akhir VPC untuk menghubungkan klien di VPC Anda ke layanan dan sumber daya yang terintegrasi dengannya. AWS PrivateLink Anda dapat membuat layanan endpoint VPC Anda sendiri dan membuatnya tersedia untuk pelanggan lain. AWS Untuk informasi selengkapnya, lihat the section called “Konsep”.

Dalam diagram berikut, VPC di sebelah kiri memiliki beberapa instans Amazon EC2 dalam subnet pribadi dan lima titik akhir VPC - tiga titik akhir VPC antarmuka, titik akhir VPC sumber daya, dan titik akhir VPC jaringan layanan. Titik akhir VPC antarmuka pertama terhubung ke layanan. AWS Titik akhir VPC antarmuka kedua terhubung ke layanan yang dihosting oleh AWS akun lain (layanan titik akhir VPC). Endpoint VPC antarmuka ketiga terhubung ke layanan mitra AWS Marketplace. Titik akhir VPC sumber daya terhubung ke database. Titik akhir VPC jaringan layanan terhubung ke jaringan layanan.



Pelajari selengkapnya

- Konsep
- Akses Layanan AWS
- Akses produk SaaS
- Akses peralatan virtual
- Bagikan layanan Anda

Bekerja dengan titik akhir VPC

Anda dapat membuat, mengakses, dan mengelola titik akhir VPC menggunakan salah satu dari berikut ini:

- Konsol Manajemen AWSMenyediakan antarmuka web yang dapat Anda gunakan untuk mengakses AWS PrivateLink sumber daya Anda. Buka konsol Amazon VPC dan pilih layanan Endpoint atau Endpoint.
- AWS Command Line Interface (AWS CLI) — Menyediakan perintah untuk serangkaian luas Layanan AWS, termasuk AWS PrivateLink. Untuk informasi selengkapnya tentang perintah AWS PrivateLink, lihat ec2 di Referensi AWS CLI Perintah.
- CloudFormation- Buat template yang menggambarkan AWS sumber daya Anda. Anda menggunakan templat untuk menyediakan dan mengelola sumber daya ini sebagai satu unit. Untuk informasi selengkapnya, lihat AWS PrivateLink sumber daya berikut:
  - AWS: :EC2: :VPCendPoint
  - AWS: :EC2:: VPCEndpointConnectionNotification
  - AWS: :EC2:: VPCEndpointService
  - AWS: :EC2:: VPCEndpointServicePermissions
  - AWS::ElasticLoadBalancingV2:: LoadBalancer
- AWS SDK — Menyediakan API khusus bahasa. SDK menangani banyak detail koneksi, seperti menghitung tanda tangan, menangani percobaan ulang permintaan, dan menangani kesalahan. Untuk informasi lebih lanjut, lihat Alat untuk Membangun di AWS.
- Kueri API — Menyediakan tindakan API tingkat rendah yang Anda hubungi menggunakan permintaan HTTPS. Menggunakan Query API adalah cara paling langsung untuk mengakses Amazon VPC. Namun, aplikasi Anda harus menangani detail tingkat rendah seperti membuat hash untuk menandatangani permintaan dan menangani kesalahan. Untuk informasi selengkapnya, lihat AWS PrivateLink tindakan di Referensi API Amazon EC2.

Harga

Untuk informasi tentang harga titik akhir VPC, lihat Harga.AWS PrivateLink

AWS PrivateLink konsep

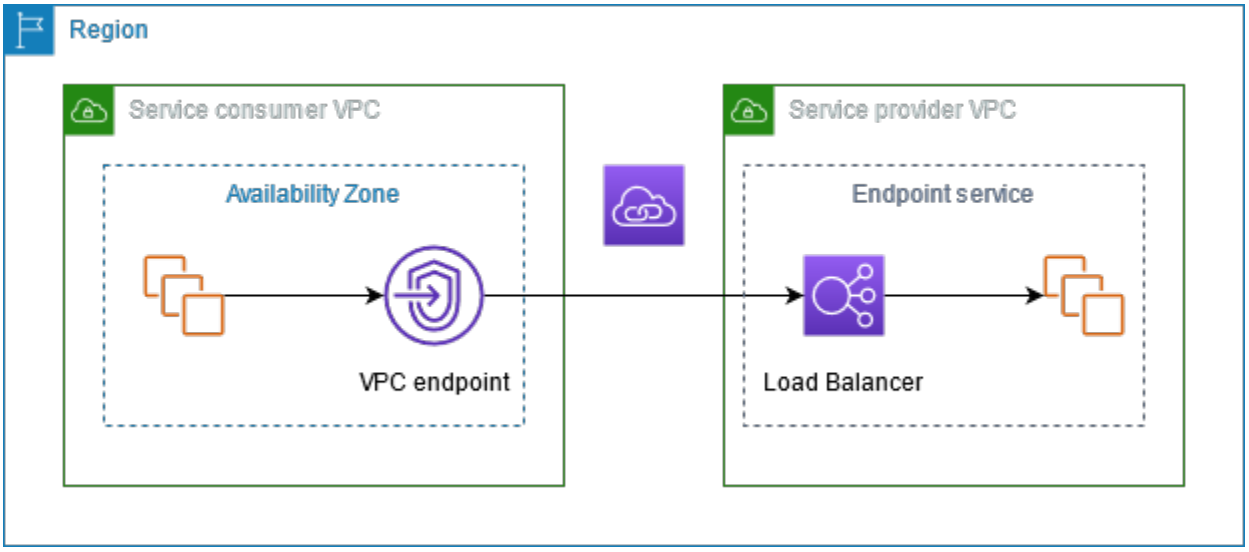
Anda dapat menggunakan Amazon VPC untuk mendefinisikan virtual private cloud (VPC), yang merupakan jaringan virtual yang terisolasi secara logis. Anda dapat mengizinkan klien di VPC Anda untuk terhubung ke tujuan di luar VPC itu. Misalnya, tambahkan gateway internet ke VPC untuk mengizinkan akses ke internet, atau tambahkan koneksi VPN untuk memungkinkan akses ke jaringan lokal Anda. Atau, gunakan AWS PrivateLink untuk memungkinkan klien di VPC Anda terhubung ke layanan dan sumber daya di VPC lain menggunakan alamat IP pribadi, seolah-olah layanan dan sumber daya tersebut di-host langsung di VPC Anda.

Berikut ini adalah konsep penting untuk dipahami saat Anda mulai menggunakan AWS PrivateLink.

Daftar Isi

Diagram arsitektur

Diagram berikut memberikan gambaran tingkat tinggi tentang cara AWS PrivateLink kerja. Konsumen membuat titik akhir VPC untuk terhubung ke layanan endpoint dan sumber daya yang di-host oleh penyedia.



Penyedia

Memahami konsep yang terkait dengan penyedia.

Penyedia layanan

Pemilik layanan adalah penyedia layanan. Penyedia layanan termasuk AWS, AWS Mitra, dan lainnya Akun AWS. Penyedia layanan dapat meng-host layanan mereka menggunakan AWS sumber daya, seperti instans EC2, atau menggunakan server lokal.

Penyedia sumber daya

Pemilik sumber daya, misalnya database atau instans Amazon EC2, adalah penyedia sumber daya. Penyedia sumber daya mencakup AWS layanan, AWS Mitra, dan AWS akun lainnya. Penyedia sumber daya dapat meng-host sumber daya mereka di VPC atau lokal.

Konsep

- Layanan titik akhir
- Nama layanan
- Status layanan
- Konfigurasi sumber daya
- Gateway sumber daya

Layanan titik akhir

Penyedia layanan membuat layanan endpoint untuk membuat layanan mereka tersedia di suatu Wilayah. Penyedia layanan harus menentukan penyeimbang beban saat membuat layanan endpoint. Penyeimbang beban menerima permintaan dari konsumen layanan dan mengarahkan mereka ke layanan Anda.

Secara default, layanan endpoint Anda tidak tersedia untuk konsumen layanan. Anda harus menambahkan izin yang memungkinkan AWS prinsipal tertentu untuk terhubung ke layanan endpoint Anda.

Nama layanan

Setiap layanan endpoint diidentifikasi dengan nama layanan. Konsumen layanan harus menentukan nama layanan saat membuat titik akhir VPC. Konsumen layanan dapat menanyakan nama layanan

untuk Layanan AWS. Penyedia layanan harus membagikan nama layanan mereka dengan konsumen layanan.

Status layanan

Berikut ini adalah status yang mungkin untuk layanan endpoint:

- Tertunda - Layanan endpoint sedang dibuat.
- Tersedia - Layanan endpoint tersedia.
- Gagal - Layanan endpoint tidak dapat dibuat.
- Menghapus - Penyedia layanan menghapus layanan titik akhir dan penghapusan sedang berlangsung.
- Dihapus - Layanan titik akhir dihapus.

Konfigurasi sumber daya

Penyedia sumber daya membuat konfigurasi sumber daya untuk berbagi sumber daya. Konfigurasi sumber daya adalah objek logis yang mewakili sumber daya tunggal seperti database, atau sekelompok sumber daya. Sumber daya dapat berupa alamat IP, target nama domain, atau database Amazon Relational Database Service (Amazon RDS).

Saat berbagi dengan akun lain, penyedia sumber daya harus membagikan sumber daya melalui pembagian sumber daya AWS Resource Access Manager(AWS RAM) untuk memungkinkan AWS prinsipal tertentu di akun lain terhubung ke sumber daya melalui titik akhir VPC sumber daya.

Konfigurasi sumber daya dapat dikaitkan dengan jaringan layanan yang terhubung oleh prinsipal melalui titik akhir VPC jaringan layanan.

Gateway sumber daya

Gateway sumber daya adalah titik masuknya ke VPC dari mana sumber daya dibagikan. Penyedia membuat gateway sumber daya untuk berbagi sumber daya dari VPC.

Konsumen layanan atau sumber daya

Pengguna layanan atau sumber daya adalah konsumen. Konsumen dapat mengakses layanan endpoint dan sumber daya dari VPC mereka atau dari lokal.

Konsep

- Titik akhir VPC
- Antarmuka jaringan titik akhir
- Kebijakan titik akhir
- Status titik akhir

Titik akhir VPC

Konsumen membuat titik akhir VPC untuk menghubungkan VPC mereka ke layanan atau sumber daya titik akhir. Konsumen harus menentukan layanan titik akhir, sumber daya, atau jaringan layanan saat membuat titik akhir VPC. Ada beberapa jenis titik akhir VPC. Anda harus membuat jenis titik akhir VPC yang Anda butuhkan.

- `Interface`- Buat titik akhir antarmuka untuk mengirim lalu lintas TCP atau UDP ke layanan endpoint. Lalu lintas yang ditujukan untuk layanan titik akhir diselesaikan menggunakan DNS.
- `GatewayLoadBalancer`- Buat titik akhir Load Balancer Gateway untuk mengirim lalu lintas ke armada peralatan virtual menggunakan alamat IP pribadi. Anda merutekan lalu lintas dari VPC ke titik akhir Load Balancer Gateway menggunakan tabel rute. Load Balancer Gateway mendistribusikan lalu lintas ke peralatan virtual dan dapat menskalakan sesuai permintaan.
- `Resource`- Buat titik akhir sumber daya untuk mengakses sumber daya yang dibagikan dengan Anda dan berada di VPC lain. Titik akhir sumber daya memungkinkan Anda mengakses sumber daya secara pribadi dan aman seperti database, instans Amazon EC2, titik akhir aplikasi, target nama domain, atau alamat IP yang mungkin ada di subnet pribadi di VPC lain atau di lingkungan di lokasi. Titik akhir sumber daya tidak memerlukan penyeimbang beban, dan memungkinkan Anda mengakses sumber daya secara langsung.
- `Service network`- Buat titik akhir jaringan layanan untuk mengakses jaringan layanan yang Anda buat atau bagikan dengan Anda. Anda dapat menggunakan endpoint jaringan layanan tunggal untuk mengakses beberapa sumber daya dan layanan secara pribadi dan aman yang terkait dengan jaringan layanan.

Ada jenis lain dari titik akhir VPC`Gateway`, yang menciptakan titik akhir gateway untuk mengirim lalu lintas ke Amazon S3 atau DynamoDB. Titik akhir Gateway tidak digunakan AWS PrivateLink, tidak seperti jenis titik akhir VPC lainnya. Untuk informasi selengkapnya, lihat the section called “Titik akhir Gateway”.

Antarmuka jaringan titik akhir

Antarmuka jaringan endpoint adalah antarmuka jaringan yang dikelola pemohon yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan ke layanan endpoint, sumber daya, atau jaringan layanan. Untuk setiap subnet yang Anda tentukan saat Anda membuat titik akhir VPC, kami membuat antarmuka jaringan titik akhir di subnet.

Jika titik akhir VPC mendukung IPv4, antarmuka jaringan titik akhir memiliki alamat IPv4. Jika titik akhir VPC mendukung IPv6, antarmuka jaringan titik akhir memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Saat Anda mendeskripsikan antarmuka jaringan titik akhir dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Kebijakan titik akhir

Kebijakan titik akhir VPC adalah kebijakan sumber daya IAM yang Anda lampirkan ke titik akhir VPC. Ini menentukan prinsip mana yang dapat menggunakan titik akhir VPC untuk mengakses layanan titik akhir. Kebijakan titik akhir VPC default memungkinkan semua tindakan oleh semua prinsipal pada semua sumber daya melalui titik akhir VPC.

Status titik akhir

Saat Anda membuat titik akhir VPC antarmuka, layanan titik akhir menerima permintaan koneksi. Penyedia layanan dapat menerima atau menolak permintaan tersebut. Jika penyedia layanan menerima permintaan, konsumen layanan dapat menggunakan titik akhir VPC setelah memasuki status Tersedia.

Berikut ini adalah status yang mungkin untuk titik akhir VPC:

- PendingAcceptance - Permintaan koneksi tertunda. Ini adalah status awal jika permintaan diterima secara manual.
- Tertunda - Penyedia layanan menerima permintaan koneksi. Ini adalah status awal jika permintaan diterima secara otomatis. Titik akhir VPC kembali ke status ini jika konsumen layanan memodifikasi titik akhir VPC.
- Tersedia - Titik akhir VPC tersedia untuk digunakan.
- Ditolak - Penyedia layanan menolak permintaan koneksi. Penyedia layanan juga dapat menolak koneksi setelah tersedia untuk digunakan.
- Kedaluwarsa - Permintaan koneksi kedaluwarsa.

- Gagal - Titik akhir VPC tidak dapat dibuat tersedia.
- Menghapus - Konsumen layanan menghapus titik akhir VPC dan penghapusan sedang berlangsung.
- Dihapus - Titik akhir VPC dihapus.

AWS PrivateLink API mengembalikan status yang mungkin menggunakan kasus unta.

AWS PrivateLink koneksi

Lalu lintas dari VPC Anda dikirim ke layanan atau sumber daya titik akhir menggunakan koneksi antara titik akhir VPC dan layanan atau sumber daya titik akhir. Lalu lintas antara titik akhir VPC dan layanan titik akhir atau sumber daya tetap berada dalam AWS jaringan, tanpa melintasi internet publik.

Penyedia layanan menambahkan izin sehingga konsumen layanan dapat mengakses layanan endpoint. Konsumen layanan memulai koneksi dan penyedia layanan menerima atau menolak permintaan koneksi. Pemilik sumber daya atau pemilik jaringan layanan berbagi konfigurasi sumber daya atau jaringan layanan dengan konsumen AWS Resource Access Manager sehingga konsumen dapat mengakses sumber daya atau jaringan layanan.

Dengan titik akhir VPC antarmuka, konsumen dapat menggunakan kebijakan titik akhir untuk mengontrol prinsipal IAM mana yang dapat menggunakan titik akhir VPC untuk mengakses layanan atau sumber daya titik akhir.

Zona host pribadi

Zona yang dihosting adalah wadah untuk catatan DNS yang menentukan cara merutekan lalu lintas untuk domain atau subdomain. Dengan zona yang dihosting publik, catatan menentukan cara merutekan lalu lintas di internet. Dengan zona host pribadi, catatan menentukan cara merutekan lalu lintas di VPC Anda.

Anda dapat mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas domain ke titik akhir VPC. Untuk informasi selengkapnya, lihat Merutekan lalu lintas ke titik akhir VPC menggunakan nama domain Anda.

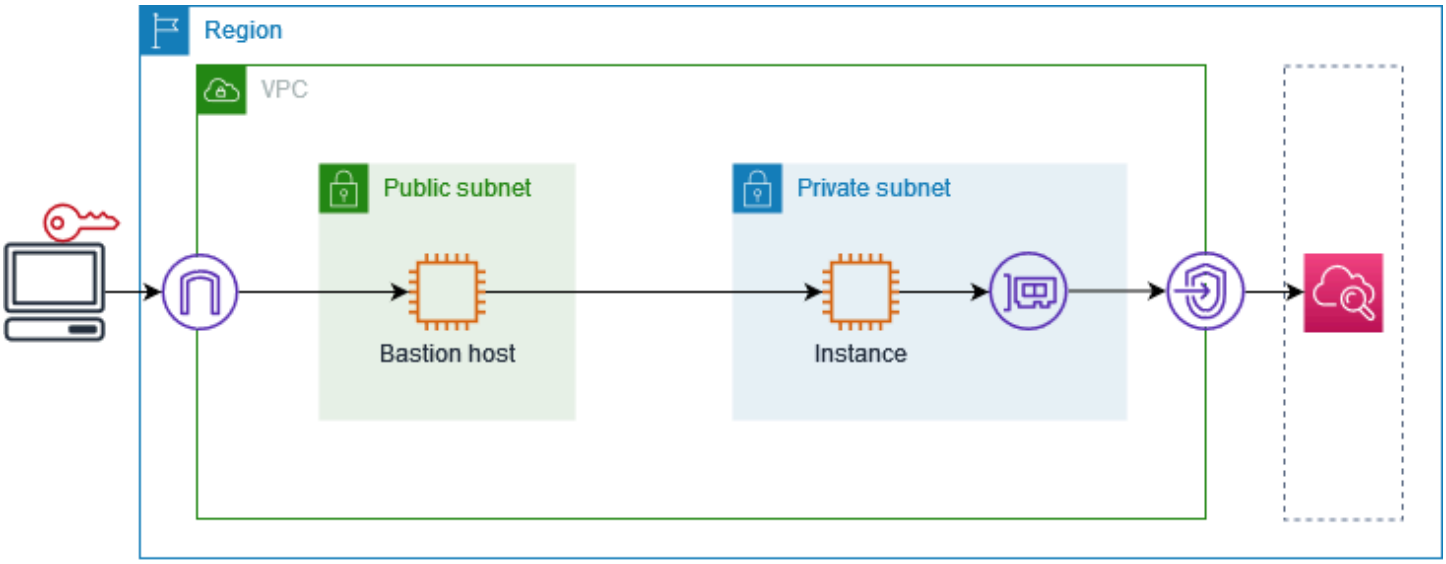
Anda dapat menggunakan Route 53 untuk mengonfigurasi DNS split-horizon, di mana Anda menggunakan nama domain yang sama untuk situs web publik dan layanan endpoint yang didukung oleh. AWS PrivateLink Permintaan DNS untuk nama host publik dari VPC konsumen diselesaikan

ke alamat IP pribadi dari antarmuka jaringan titik akhir, tetapi permintaan dari luar VPC terus diselesaikan ke titik akhir publik. Untuk informasi selengkapnya, lihat Mekanisme DNS untuk Lalu Lintas Perutean dan Mengaktifkan Failover untuk Penerapan. AWS PrivateLink

Memulai dengan AWS PrivateLink

Tutorial ini menunjukkan cara mengirim permintaan dari instans EC2 di subnet pribadi ke Amazon menggunakan. CloudWatch AWS PrivateLink

Diagram berikut memberikan gambaran umum tentang skenario ini. Untuk terhubung dari komputer Anda ke instance di subnet pribadi, pertama-tama Anda akan terhubung ke host bastion di subnet publik. Baik host bastion dan instance harus menggunakan key pair yang sama. Karena `.pem` file untuk kunci pribadi ada di komputer Anda, bukan host bastion, Anda akan menggunakan penerusan kunci SSH. Kemudian, Anda dapat terhubung ke instance dari host bastion tanpa menentukan `.pem` file dalam perintah. ssh Setelah Anda menyiapkan titik akhir VPC CloudWatch, lalu lintas dari instance yang ditakdirkan akan diselesaikan ke antarmuka jaringan titik akhir dan kemudian dikirim ke menggunakan CloudWatch titik akhir VPC. CloudWatch



Untuk tujuan pengujian, Anda dapat menggunakan Availability Zone tunggal. Dalam produksi, kami menyarankan Anda menggunakan setidaknya dua Availability Zone untuk latensi rendah dan ketersediaan tinggi.

Tugas

- Langkah 1: Buat VPC dengan subnet
- Langkah 2: Luncurkan instance
- Langkah 3: Uji CloudWatch akses
- Langkah 4: Buat titik akhir VPC untuk mengakses CloudWatch

Langkah 1: Buat VPC dengan subnet

Gunakan prosedur berikut untuk membuat VPC dengan subnet publik dan subnet pribadi.

Untuk membuat VPC

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pilih Buat VPC.
3. Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.
4. Untuk Pembuatan otomatis tanda nama, masukkan nama untuk VPC.
5. Untuk mengkonfigurasi subnet, lakukan hal berikut:
    a. Untuk Jumlah Availability Zone, pilih 1 atau 2, tergantung kebutuhan Anda.
    b. Untuk Jumlah subnet publik, pastikan Anda memiliki satu subnet publik per Availability Zone.
    c. Untuk Jumlah subnet pribadi, pastikan Anda memiliki satu subnet pribadi per Availability Zone.
6. Pilih Buat VPC.

Langkah 2: Luncurkan instance

Menggunakan VPC yang Anda buat pada langkah sebelumnya, luncurkan host bastion di subnet publik dan instance di subnet pribadi.

Prasyarat

- Buat key pair menggunakan format.pem. Anda harus memilih key pair ini saat meluncurkan host bastion dan instance-nya.
- Buat grup keamanan untuk host bastion yang memungkinkan lalu lintas SSH masuk dari blok CIDR untuk komputer Anda.
- Buat grup keamanan untuk instance yang memungkinkan lalu lintas SSH masuk dari grup keamanan untuk host bastion.
- Buat profil instans IAM dan lampirkan CloudWatchReadOnlyAccesskebijakan.

Untuk meluncurkan host benteng

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Luncurkan instans.
3. Untuk Nama, masukkan nama untuk host benteng Anda.
4. Pertahankan gambar default dan tipe instance.
5. Untuk Key pair, pilih key pair Anda.
6. Untuk pengaturan Jaringan, lakukan hal berikut:
    a. Untuk VPC, pilih VPC Anda.
    b. Untuk Subnet, pilih subnet publik.
    c. Untuk IP Auto-assign publik, pilih Aktifkan.
    d. Untuk Firewall, pilih Pilih grup keamanan yang ada dan kemudian pilih grup keamanan untuk host bastion.
7. Pilih Luncurkan instans.

Untuk meluncurkan instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Luncurkan instans.
3. Untuk Nama, masukkan nama untuk instance Anda.
4. Pertahankan gambar default dan tipe instance.
5. Untuk Key pair, pilih key pair Anda.
6. Untuk pengaturan Jaringan, lakukan hal berikut:
    a. Untuk VPC, pilih VPC Anda.
    b. Untuk Subnet, pilih subnet pribadi.
    c. Untuk IP Auto-assign publik, pilih Nonaktifkan.
    d. Untuk Firewall, pilih Pilih grup keamanan yang ada dan kemudian pilih grup keamanan untuk instance.
7. Perluas Detail lanjutan. Untuk profil instans IAM, pilih profil instans IAM Anda.
8. Pilih Luncurkan instans.

Langkah 3: Uji CloudWatch akses

Gunakan prosedur berikut untuk mengonfirmasi bahwa instans tidak dapat mengakses CloudWatch. Anda akan melakukannya menggunakan AWS CLI perintah read-only untuk. CloudWatch

Untuk menguji CloudWatch akses

1. Dari komputer Anda, tambahkan key pair ke agen SSH menggunakan perintah berikut, di mana *key.pem* nama file.pem Anda.

   ```
   ssh-add ./key.pem
   ```

   Jika Anda menerima kesalahan bahwa izin untuk key pair Anda terlalu terbuka, jalankan perintah berikut, lalu coba lagi perintah sebelumnya.

   ```
   chmod 400 ./key.pem
   ```

2. Connect ke host bastion dari komputer Anda. Anda harus menentukan `-A` opsi, nama pengguna instance (misalnya,`ec2-user`), dan alamat IP publik dari host bastion.

   ```
   ssh -A ec2-user@bastion-public-ip-address
   ```

3. Connect ke instance dari host bastion. Anda harus menentukan nama pengguna instance (misalnya,`ec2-user`) dan alamat IP pribadi dari instance tersebut.

   ```
   ssh ec2-user@instance-private-ip-address
   ```

4. Jalankan perintah CloudWatch list-metrics pada instance sebagai berikut. Untuk `--region` opsi, tentukan Wilayah tempat Anda membuat VPC.

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

5. Setelah beberapa menit, perintah habis. Ini menunjukkan bahwa Anda tidak dapat mengakses CloudWatch dari instance dengan konfigurasi VPC saat ini.

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

6. Tetap terhubung dengan instans Anda. Setelah Anda membuat titik akhir VPC, Anda akan mencoba perintah ini list-metrics lagi.

Langkah 4: Buat titik akhir VPC untuk mengakses CloudWatch

Gunakan prosedur berikut untuk membuat titik akhir VPC yang terhubung ke. CloudWatch

Prasyarat

Buat grup keamanan untuk titik akhir VPC yang memungkinkan lalu lintas ke. CloudWatch Misalnya, tambahkan aturan yang memungkinkan lalu lintas HTTPS dari blok CIDR VPC.

Untuk membuat titik akhir VPC untuk CloudWatch

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk tag Nama, masukkan nama untuk titik akhir.
5. Untuk Kategori layanan, pilih Layanan AWS.
6. Untuk Layanan, pilih com.amazonaws. ***region***.pemantauan.
7. Untuk VPC, pilih VPC Anda.
8. Untuk Subnet, pilih Availability Zone dan kemudian pilih subnet pribadi.
9. Untuk grup Keamanan, pilih grup keamanan untuk titik akhir VPC.
10. Untuk Kebijakan, pilih Akses penuh untuk mengizinkan semua operasi oleh semua prinsipal di semua sumber daya melalui titik akhir VPC.
11. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
12. Pilih Buat titik akhir. Status awal adalah Tertunda. Sebelum Anda pergi ke langkah berikutnya, tunggu sampai statusnya Tersedia. Hal ini dapat menghabiskan waktu beberapa menit.

Langkah 5: Uji titik akhir VPC

Verifikasi bahwa titik akhir VPC mengirimkan permintaan dari instans Anda ke. CloudWatch

Untuk menguji titik akhir VPC

Jalankan perintah berikut di instans Anda. Untuk `--region` opsi, tentukan Wilayah tempat Anda membuat titik akhir VPC.

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

Jika Anda mendapatkan respons, bahkan respons dengan hasil kosong, maka Anda terhubung untuk CloudWatch menggunakan AWS PrivateLink.

Jika Anda mendapatkan `UnauthorizedOperation` kesalahan, pastikan instans memiliki peran IAM yang memungkinkan akses ke CloudWatch.

Jika waktu permintaan habis, verifikasi hal berikut:

- Grup keamanan untuk titik akhir memungkinkan lalu lintas ke CloudWatch.
- `--region`Opsi menentukan Wilayah di mana Anda membuat titik akhir VPC.

Langkah 6: Bersihkan

Jika Anda tidak lagi membutuhkan host bastion dan instance yang Anda buat untuk tutorial ini, Anda dapat menghentikannya.

Untuk mengakhirkan instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih kedua instance pengujian dan pilih status Instance, Terminate instance.
4. Saat diminta konfirmasi, pilih Akhiri.

Jika Anda tidak lagi membutuhkan titik akhir VPC, Anda dapat menghapusnya.

Untuk menghapus titik akhir VPC

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir VPC.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta konfirmasi, masukkan **`delete`**, lalu pilih Hapus.

Akses Layanan AWS melalui AWS PrivateLink

Anda mengakses Layanan AWS menggunakan titik akhir. Endpoint layanan default adalah antarmuka publik, jadi Anda harus menambahkan gateway internet ke VPC Anda sehingga lalu lintas dapat diperoleh dari VPC ke VPC. Layanan AWS Jika konfigurasi ini tidak sesuai dengan persyaratan keamanan jaringan Anda, Anda dapat menggunakan AWS PrivateLink untuk menghubungkan VPC Anda Layanan AWS seolah-olah mereka berada di VPC Anda, tanpa menggunakan gateway internet.

Anda dapat mengakses secara pribadi Layanan AWS yang terintegrasi dengan AWS PrivateLink menggunakan titik akhir VPC. Anda dapat membangun dan mengelola semua lapisan tumpukan aplikasi Anda tanpa menggunakan gateway internet.

Harga

Anda ditagih untuk setiap jam bahwa titik akhir VPC antarmuka Anda disediakan di setiap Availability Zone. Anda juga ditagih per GB data yang diproses. Untuk informasi selengkapnya, silakan lihat AWS PrivateLink Harga.

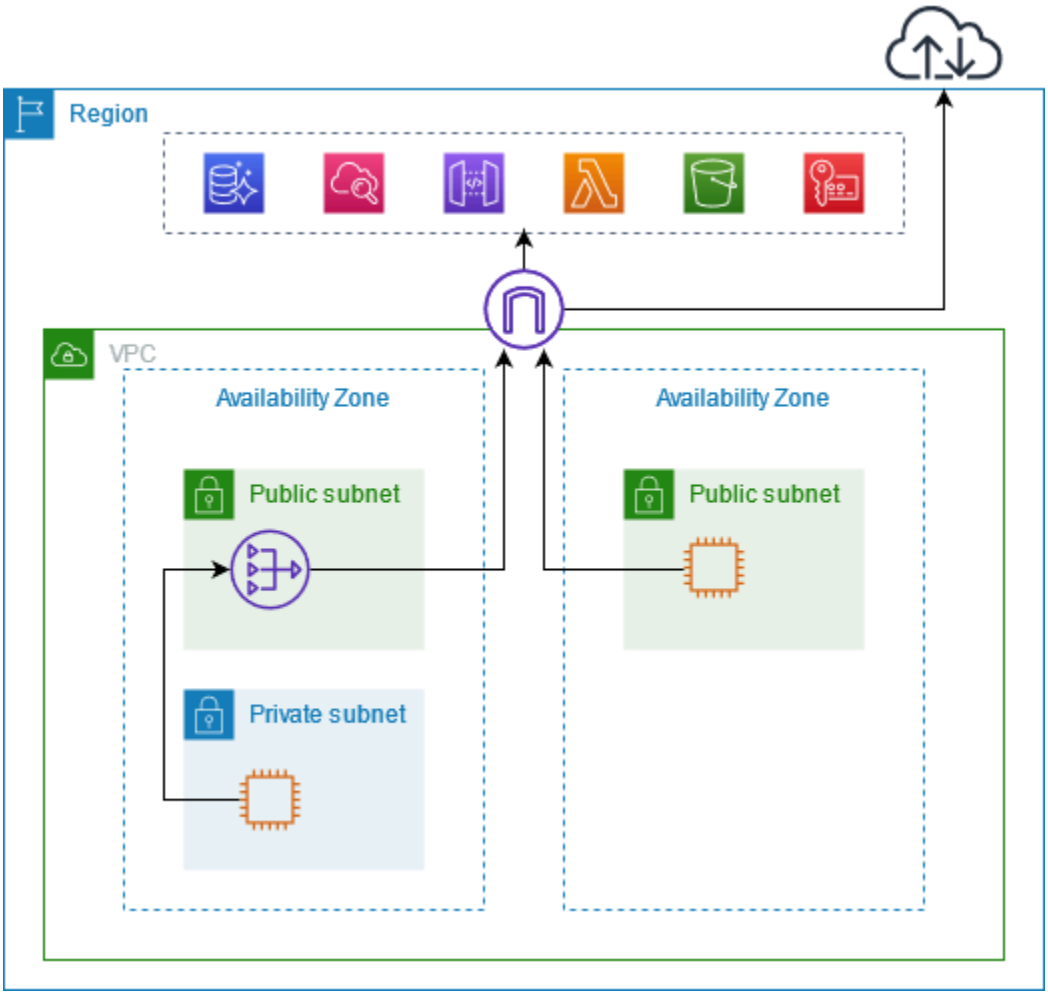
Daftar Isi

Ikhtisar

Anda dapat mengakses Layanan AWS melalui titik akhir layanan publik mereka atau terhubung ke Layanan AWS penggunaan AWS PrivateLink yang didukung. Ikhtisar ini membandingkan metode ini.

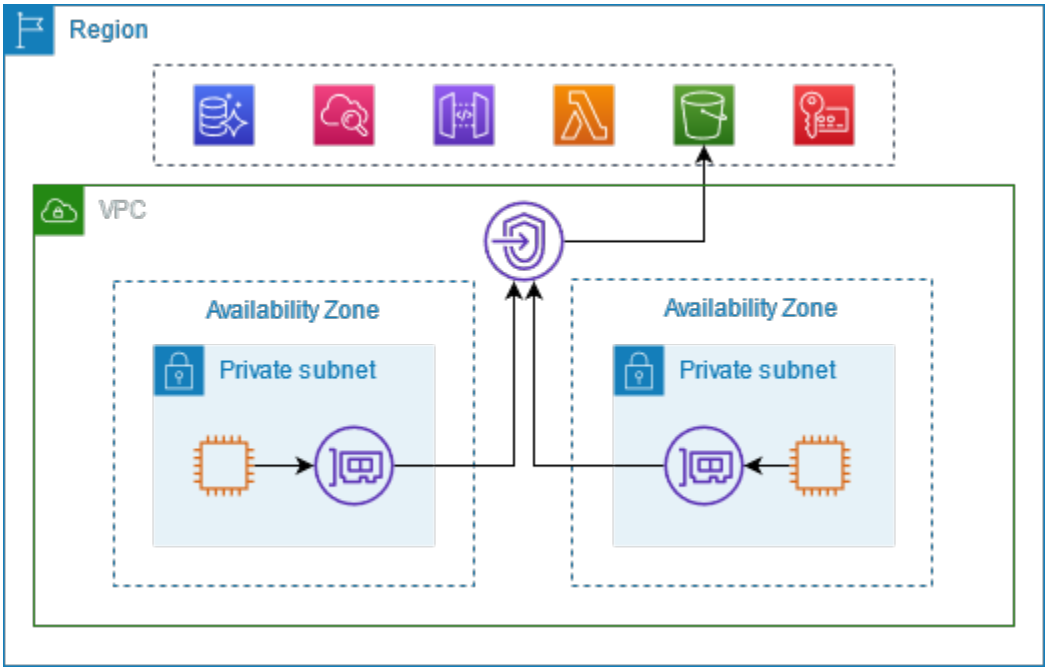
Akses melalui titik akhir layanan publik

Diagram berikut menunjukkan bagaimana instance mengakses Layanan AWS melalui endpoint layanan publik. Lalu lintas ke instance Layanan AWS dari sebuah subnet publik dialihkan ke gateway internet untuk VPC dan kemudian ke. Layanan AWS Lalu lintas ke Layanan AWS dari instance di subnet pribadi dirutekan ke gateway NAT, lalu ke gateway internet untuk VPC, dan kemudian ke. Layanan AWS Sementara lalu lintas ini melintasi gateway internet, ia tidak meninggalkan jaringan. AWS



Connect melalui AWS PrivateLink

Diagram berikut menunjukkan bagaimana instance mengakses Layanan AWS melalui AWS PrivateLink. Pertama, Anda membuat antarmuka VPC endpoint, yang menetapkan koneksi antara subnet di VPC Anda dan menggunakan antarmuka jaringan. Layanan AWS Lalu lintas yang Layanan AWS ditujukan untuk diselesaikan ke alamat IP pribadi dari antarmuka jaringan endpoint menggunakan DNS, dan kemudian dikirim ke Layanan AWS menggunakan koneksi antara titik akhir VPC dan. Layanan AWS



Layanan AWS menerima permintaan koneksi secara otomatis. Layanan tidak dapat memulai permintaan ke sumber daya melalui titik akhir VPC.

Nama host DNS

Sebagian besar Layanan AWS menawarkan titik akhir Regional publik, yang memiliki sintaks berikut.

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

Misalnya, titik akhir publik untuk Amazon CloudWatch di us-east-2 adalah sebagai berikut.

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

Dengan AWS PrivateLink, Anda mengirim lalu lintas ke layanan menggunakan titik akhir pribadi. Saat Anda membuat titik akhir VPC antarmuka, kami membuat nama DNS Regional dan zona yang dapat Anda gunakan untuk berkomunikasi dengan VPC Anda. Layanan AWS

Nama DNS Regional untuk titik akhir VPC antarmuka Anda memiliki sintaks berikut:

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

Nama DNS zonal memiliki sintaks berikut:

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

Saat Anda membuat antarmuka VPC endpoint untuk sebuah Layanan AWS, Anda dapat mengaktifkan DNS pribadi. Dengan DNS pribadi, Anda dapat terus membuat permintaan ke layanan menggunakan nama DNS untuk titik akhir publiknya, sambil memanfaatkan konektivitas pribadi melalui titik akhir VPC antarmuka. Untuk informasi selengkapnya, lihat the section called “Resolusi DNS”.

Perintah deskripsi-vpc-endpoints berikut menampilkan entri DNS untuk titik akhir antarmuka.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-id vpce-099deb00b40f00e22 --query
 VpcEndpoints[*].DnsEntries
```

Berikut ini adalah contoh output untuk titik akhir antarmuka untuk Amazon CloudWatch dengan nama DNS pribadi diaktifkan. Entri pertama adalah titik akhir Regional pribadi. Tiga entri berikutnya adalah titik akhir zona pribadi. Entri terakhir berasal dari zona host pribadi tersembunyi, yang menyelesaikan permintaan ke titik akhir publik ke alamat IP pribadi dari antarmuka jaringan titik akhir.

```
[
    [
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2c.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2a.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
```

```
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2b.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "monitoring.us-east-2.amazonaws.com",
            "HostedZoneId": "Z06320943MMOWYG6MAVL9"
        }
    ]
]
```

Resolusi DNS

Catatan DNS yang kami buat untuk titik akhir VPC antarmuka Anda bersifat publik. Oleh karena itu, nama-nama DNS ini dapat diselesaikan secara publik. Namun, permintaan DNS dari luar VPC masih mengembalikan alamat IP pribadi dari antarmuka jaringan titik akhir, sehingga alamat IP ini tidak dapat digunakan untuk mengakses layanan titik akhir kecuali Anda memiliki akses ke VPC.

DNS privat

Jika Anda mengaktifkan DNS pribadi untuk titik akhir VPC antarmuka Anda, dan VPC Anda mengaktifkan nama host DNS dan resolusi DNS, kami membuat zona host pribadi yang tersembunyi dan dikelola untuk Anda. AWS Zona yang dihosting berisi kumpulan catatan untuk nama DNS default untuk layanan yang menyelesaikannya ke alamat IP pribadi antarmuka jaringan titik akhir di VPC Anda. Oleh karena itu, jika Anda memiliki aplikasi yang ada yang mengirim permintaan ke Layanan AWS menggunakan titik akhir Regional publik, permintaan tersebut sekarang melalui antarmuka jaringan titik akhir, tanpa mengharuskan Anda membuat perubahan apa pun pada aplikasi tersebut.

Kami menyarankan Anda mengaktifkan nama DNS pribadi untuk titik akhir VPC Anda. Layanan AWS Ini memastikan bahwa permintaan yang menggunakan titik akhir layanan publik, seperti permintaan yang dibuat melalui AWS SDK, diselesaikan ke titik akhir VPC Anda.

Amazon menyediakan server DNS untuk VPC Anda, yang disebut Resolver Route 53. Resolver Route 53 secara otomatis menyelesaikan nama domain VPC lokal dan merekam di zona host pribadi. Namun, Anda tidak dapat menggunakan Resolver Route 53 dari luar VPC Anda. Jika ingin mengakses titik akhir VPC dari jaringan lokal, Anda dapat menggunakan titik akhir Route 53 Resolver

dan aturan Resolver. Untuk informasi selengkapnya, lihat Mengintegrasikan AWS Transit Gateway dengan AWS PrivateLink dan Amazon Route 53 Resolver.

Subnet dan Availability Zone

Anda dapat mengonfigurasi titik akhir VPC Anda dengan satu subnet per Availability Zone. Kami membuat antarmuka jaringan endpoint untuk titik akhir VPC di subnet Anda. Kami menetapkan alamat IP ke setiap antarmuka jaringan titik akhir dari subnetnya, berdasarkan jenis alamat IP dari titik akhir VPC. Alamat IP dari antarmuka jaringan endpoint tidak akan berubah selama masa pakai titik akhir VPC-nya.

Dalam lingkungan produksi, untuk ketersediaan dan ketahanan yang tinggi, kami merekomendasikan hal berikut:

- Konfigurasikan setidaknya dua Availability Zone per titik akhir VPC dan terapkan AWS sumber daya Anda yang harus mengakses Layanan AWS di Availability Zone ini.
- Konfigurasikan nama DNS pribadi untuk titik akhir VPC.
- Akses Layanan AWS dengan menggunakan nama DNS Regional, juga dikenal sebagai titik akhir publik.

Diagram berikut menunjukkan titik akhir VPC untuk Amazon CloudWatch dengan antarmuka jaringan titik akhir dalam satu Availability Zone. Ketika sumber daya apa pun di subnet apa pun di VPC mengakses CloudWatch Amazon menggunakan titik akhir publiknya, kami menyelesaikan lalu lintas ke alamat IP antarmuka jaringan titik akhir. Ini termasuk lalu lintas dari subnet di Availability Zone lainnya. Namun, jika Availability Zone 1 terganggu, sumber daya di Availability Zone 2 kehilangan akses ke Amazon CloudWatch.

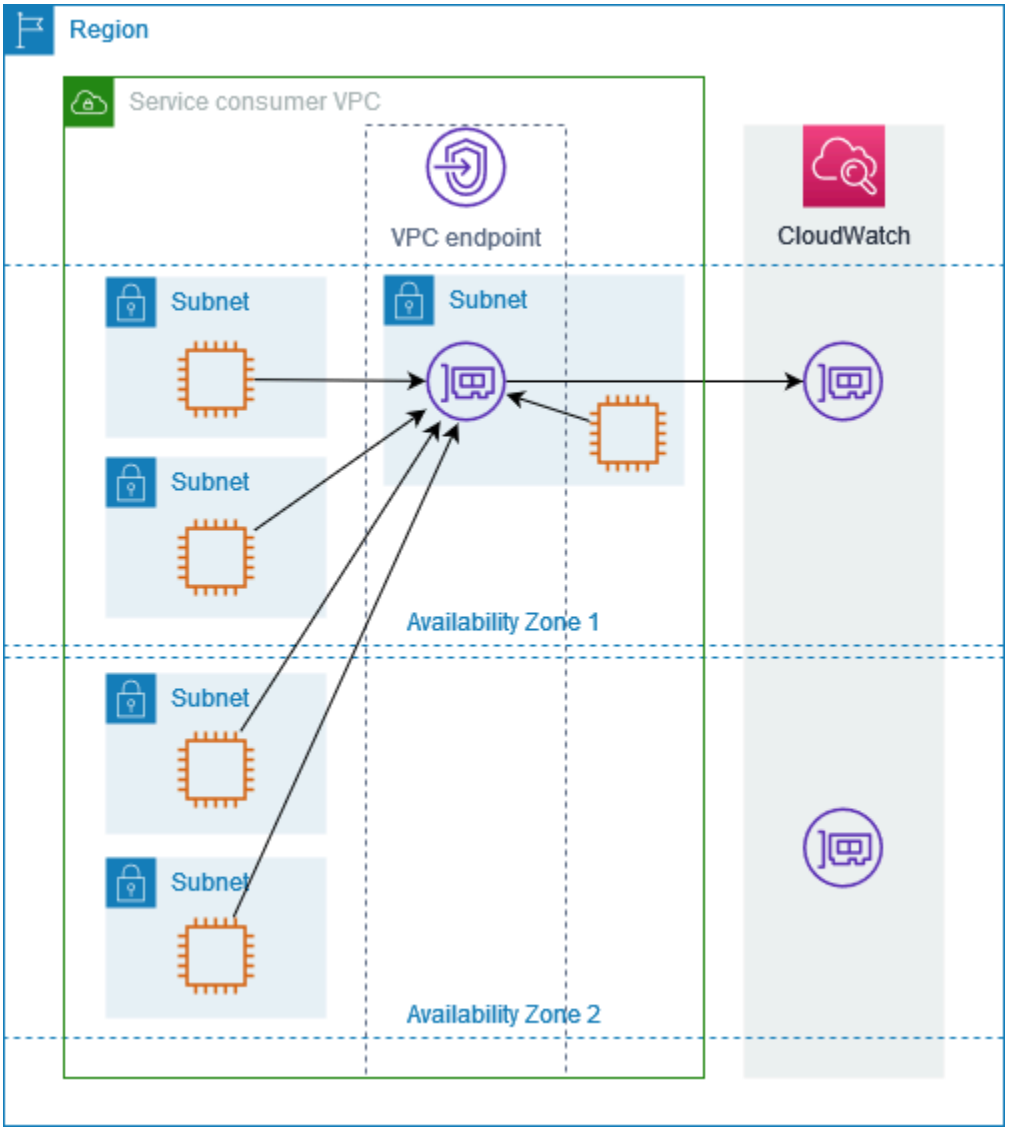
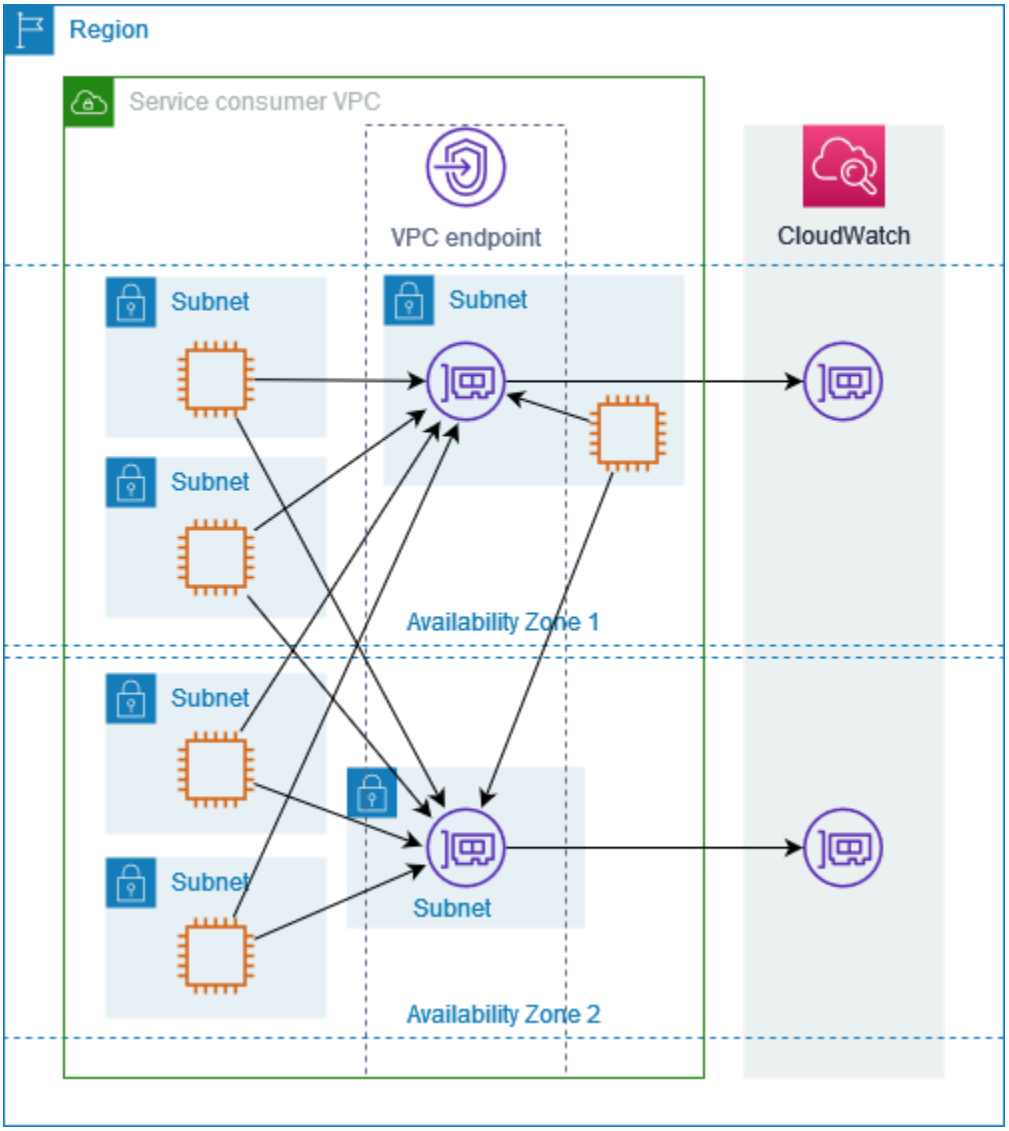
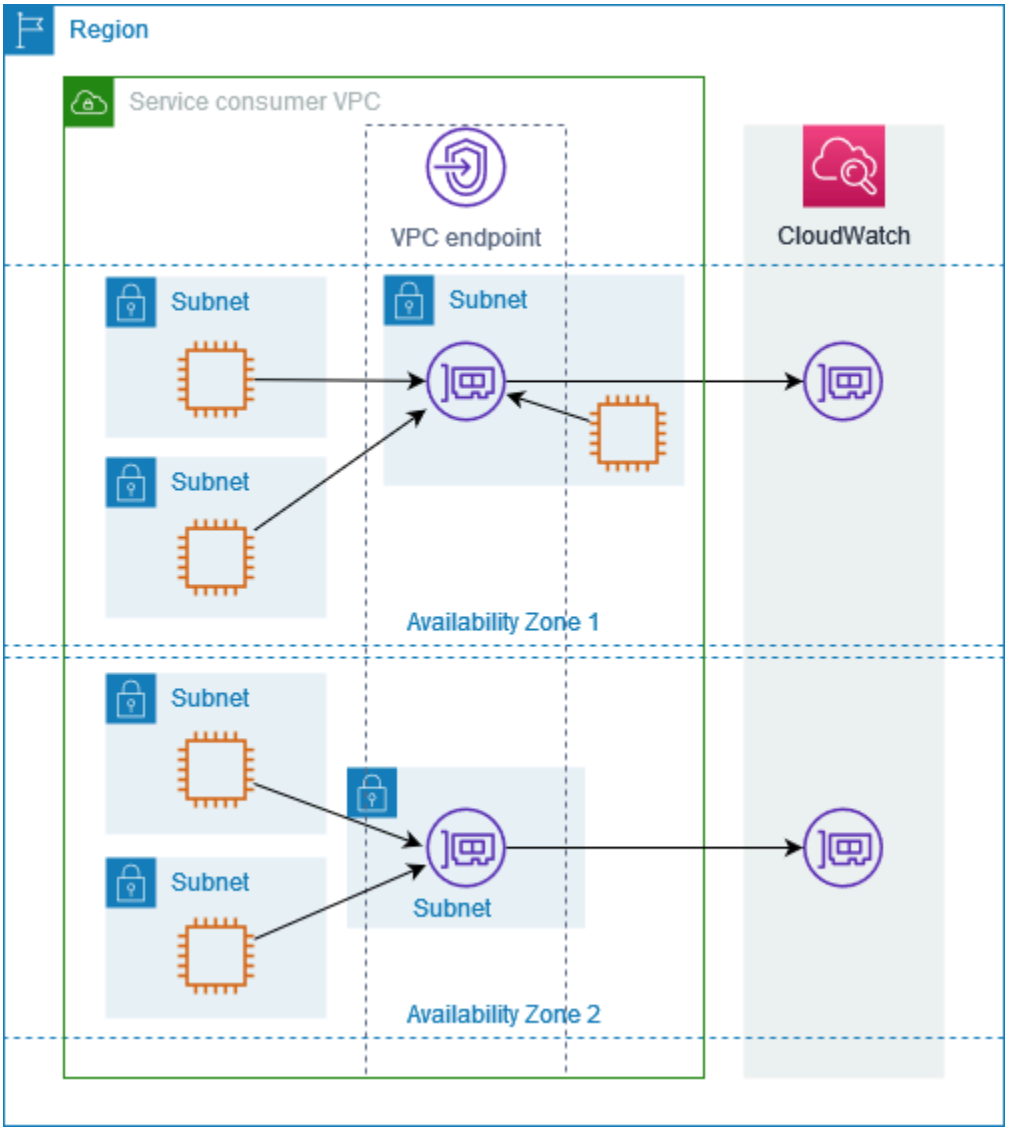


Diagram berikut menunjukkan titik akhir VPC untuk Amazon CloudWatch dengan antarmuka jaringan titik akhir di dua Availability Zones. Ketika sumber daya apa pun di subnet apa pun di VPC mengakses CloudWatch Amazon dengan menggunakan titik akhir publiknya, kami memilih antarmuka jaringan titik akhir yang sehat, menggunakan algoritma round robin untuk bergantian di antara mereka. Kami kemudian menyelesaikan lalu lintas ke alamat IP dari antarmuka jaringan titik akhir yang dipilih.



Jika lebih baik untuk kasus penggunaan Anda, Anda dapat mengirim lalu lintas dari sumber daya Anda ke Layanan AWS dengan menggunakan antarmuka jaringan titik akhir di Availability Zone yang sama. Untuk melakukannya, gunakan titik akhir zona pribadi atau alamat IP dari antarmuka jaringan titik akhir.



Jenis alamat IP

Layanan AWS dapat mendukung IPv6 melalui titik akhir pribadi mereka bahkan jika mereka tidak mendukung IPv6 melalui titik akhir publik mereka. Titik akhir yang mendukung IPv6 dapat merespons kueri DNS dengan catatan AAAA.

Persyaratan untuk mengaktifkan IPv6 untuk titik akhir antarmuka

- Layanan AWS Harus membuat titik akhir layanannya tersedia melalui IPv6. Untuk informasi selengkapnya, lihat the section called “Lihat dukungan IPv6”.
- Jenis alamat IP dari titik akhir antarmuka harus kompatibel dengan subnet untuk titik akhir antarmuka, seperti yang dijelaskan di sini:

- IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4.
- IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6.
- Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan endpoint Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6.

Jika antarmuka VPC endpoint mendukung IPv4, antarmuka jaringan endpoint memiliki alamat IPv4. Jika antarmuka VPC endpoint mendukung IPv6, antarmuka jaringan endpoint memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Jika Anda mendeskripsikan antarmuka jaringan endpoint dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Jenis IP catatan DNS

Bergantung pada jenis alamat IP Anda, saat Anda memanggil titik akhir VPC, AWS layanan dapat mengembalikan catatan A, catatan AAAA, atau catatan A dan AAAA. Anda dapat menyesuaikan jenis rekaman yang dikembalikan AWS layanan Anda dengan memodifikasi jenis IP rekaman DNS. Tabel berikut menunjukkan jenis IP rekaman DNS yang didukung dan jenis rekaman yang dikembalikan:

Jenis IP catatan DNS	Jenis catatan yang dikembalikan
IPv4	A
IPv6	AAAA
Tumpukan ganda	A dan AAAA

Secara default, jenis catatan DNS sama dengan jenis alamat IP. Anda dapat memilih jenis IP rekaman DNS yang berbeda, tetapi Anda harus menggunakan jenis alamat IP yang kompatibel untuk layanan titik akhir. Tabel berikut menunjukkan jenis IP rekaman DNS yang didukung untuk setiap jenis alamat IP untuk titik akhir antarmuka:

Jenis alamat IP	Jenis IP rekaman DNS yang didukung
IPv4	IPv4

Jenis alamat IP	Jenis IP rekaman DNS yang didukung
IPv6	IPv6
Tumpukan ganda	Dualstack*, IPv4, IPv6, ditentukan layanan

* Merupakan tipe IP catatan DNS default.

Jenis IP catatan DNS yang ditentukan layanan mengembalikan catatan DNS berdasarkan titik akhir layanan yang Anda panggil. Jika Anda menggunakan jenis IP rekaman DNS yang ditentukan layanan, pastikan layanan Anda dapat menangani panggilan variabel dari titik akhir layanan. Untuk melihat catatan DNS yang didukung oleh titik akhir antarmuka Anda, lihat nama DNS untuk titik akhir VPC Anda di, atau gunakan. Konsol Manajemen AWSDescribeVpcEndpoints

Perilaku tipe IP rekaman DNS berbeda untuk titik akhir gateway. Untuk informasi selengkapnya, lihat Jenis IP rekaman DNS untuk titik akhir gateway.

Layanan AWS yang terintegrasi dengan AWS PrivateLink

Berikut ini Layanan AWS terintegrasi dengan AWS PrivateLink. Anda dapat membuat titik akhir VPC untuk terhubung ke layanan ini secara pribadi, seolah-olah mereka berjalan di VPC Anda sendiri.

Pilih tautan di Layanan AWSkolom untuk melihat dokumentasi layanan yang terintegrasi dengannya AWS PrivateLink. Kolom Nama layanan berisi nama layanan yang Anda tentukan saat Anda membuat titik akhir VPC antarmuka, atau ini menunjukkan bahwa layanan mengelola titik akhir.

Layanan AWS	Nama layanan
AWS Account Management	com.amazonaws. *region*.akun
Amazon API Gateway	com.amazonaws. *region*.eksekusi api
	com.amazonaws. *region*.apigateway
AWS AppConfig	com.amazonaws. *region*.appconfig
	com.amazonaws. *region*.appconfig-fips
	com.amazonaws. *region*.appconfigdata

Layanan AWS	Nama layanan
	com.amazonaws. *region*.appconfigdata-fips
AWS App Mesh	com.amazonaws. *region*.appmesh
	com.amazonaws. *region*.appmesh-utusan-manajemen
AWS Pelari Aplikasi	com.amazonaws. *region*.apprunner
AWS Layanan Pelari Aplikasi	com.amazonaws. *region*.apprunner.requests
Penskalaan Otomatis Aplikasi	com.amazonaws. *region*.application-autoscaling
AWS Application Discovery Service	com.amazonaws. *region*.penemuan
	com.amazonaws. *region*.arsenal-penemuan
AWS Layanan Migrasi Aplikasi	com.amazonaws. *region*.mgn
WorkSpaces Aplikasi Amazon	com.amazonaws. *region*.appstream.api
	com.amazonaws. *region*.appstream.streaming
AWS AppSync	com.amazonaws. *region*.appsync-api
Amazon Athena	com.amazonaws. *region*.athena
AWS Audit Manager	com.amazonaws. *region*.auditmanager
Amazon Aurora	com.amazonaws. *region*.rds
	com.amazonaws. *region*.rds-fips
Amazon Aurora DSQL	com.amazonaws. *region*.dsql
AWS Auto Scaling	com.amazonaws. *region*.rencana penskalaan otomatis
AWS Pertukaran Data B2B	com.amazonaws. *region*.b2bi
AWS Backup	com.amazonaws. *region*.cadangan

Layanan AWS	Nama layanan
	com.amazonaws. *region*.backup-gateway
AWS Batch	com.amazonaws. *region*.batch
Amazon Bedrock	com.amazonaws. *region*.batuan dasar
	com.amazonaws. *region*.bedrock-agen
	com.amazonaws. *region*.bedrock-agent-runtime
	com.amazonaws. *region*.bedrock-data-otomatisasi
	com.amazonaws. *region*.bedrock-data-otomasi-fips
	com.amazonaws. *region*.bedrock-data-automation-runtime
	com.amazonaws. *region*.bedrock-data-automation-runtime-fips
	com.amazonaws. *region*.bedrock-runtime
Amazon Bedrock AgentCore	com.amazonaws. *region*.bedrock-agen-kontrol
	com.amazonaws. *region*.bedrock-agentcore
AWS Manajemen Penagihan dan Biaya	com.amazonaws. *region*.penagihan
	com.amazonaws. *region*.lebih bebas
	com.amazonaws. *region*.pajak
AWS Billing Conductor	com.amazonaws. *region*.billingkonduktor
Amazon Braket	com.amazonaws. *region*.braket
AWS Certificate Manager	com.amazonaws. *region*.acm
	com.amazonaws. *region*.acm-fips

Layanan AWS	Nama layanan
AWS Kamar Bersih	com.amazonaws. *region*.kamar bersih
	com.amazonaws. *region*.cleanrooms-fips
AWS Kamar Bersih ML	com.amazonaws. *region*.cleanrooms-ml
AWS Cloud Control API	com.amazonaws. *region*.cloudcontrolapi
	com.amazonaws. *region*.cloudcontrolapi-fips
Amazon Cloud Directory	com.amazonaws. *region*.clouddirectory
AWS CloudFormation	com.amazonaws. *region*.cloudformasi
	com.amazonaws. *region*.cloudformation-fips
Amazon CloudFront	com.amazonaws.cloudfront
AWS CloudHSM	com.amazonaws. *region*.cloudhsmv2
AWS Cloud Map	com.amazonaws. *region*.servicediscovery
	com.amazonaws. *region*.servicediscovery-fips
	com.amazonaws. *region*.data-servicediscovery
	com.amazonaws. *region*.data-servicediscovery-fips
AWS CloudTrail	com.amazonaws. *region*.cloudtrail
AWS Awan WAN	com.amazonaws. *region*.networkmanager
Amazon CloudWatch	com.amazonaws. *region*.aplikasi-sinyal
	com.amazonaws. *region*.applicationinsights
	com.amazonaws. *region*.internetmonitor
	com.amazonaws. *region*.internetmonitor-fips

Layanan AWS	Nama layanan
	com.amazonaws. *region*.pemantauan
	com.amazonaws. *region*.networkflowmonitor
	com.amazonaws. *region*.networkflowmonitorreport
	com.amazonaws. *region*.networkmonitor
	com.amazonaws. *region*.observabilityadmin
	com.amazonaws. *region*.rum
	com.amazonaws. *region*.rum-dataplane
	com.amazonaws. *region*.sintetis
	com.amazonaws. *region*.synthetics-fips
	com.amazonaws. *region*.oam
CloudWatch Log Amazon	com.amazonaws. *region*.log
AWS CodeArtifact	com.amazonaws. *region*.codeartifact.api
	com.amazonaws. *region*.codeartifact.repositori
AWS CodeBuild	com.amazonaws. *region*.codebuild
	com.amazonaws. *region*.codebuild-fips
AWS CodeCommit	com.amazonaws. *region*.codecommit
	com.amazonaws. *region*.codecommit-fips
	com.amazonaws. *region*.git-codecommit
	com.amazonaws. *region*.git-codecommit-fips
AWS CodeConnections	com.amazonaws. *region*.codeconnections.api

Layanan AWS	Nama layanan
	com.amazonaws. *region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws. *region*.codedeploy
	com.amazonaws. *region*.codedeploy-perintah-aman
	com.amazonaws. *region*.codedeploy-fips
Amazon CodeGuru Profiler	com.amazonaws. *region*.codeguru-profiler
CodeGuru Peninjau Amazon	com.amazonaws. *region*.codeguru-pengulas
AWS CodePipeline	com.amazonaws. *region*.codepipeline
Amazon Comprehend	com.amazonaws. *region*.comprehend
Amazon Comprehend Medical	com.amazonaws. *region*.comprehendmedis
AWS Compute Optimizer	com.amazonaws. *region*.pengoptimal komputasi
AWS Config	com.amazonaws. *region*.config
	com.amazonaws. *region*.config-fips
Connect Pelanggan	com.amazonaws. *region*.app-integrasi
	com.amazonaws. *region*.kasus
	com.amazonaws. *region*.menghubungkan
	com.amazonaws. *region*.connect-fips
	com.amazonaws. *region*.connect-kampanye
	com.amazonaws. *region*.profil
	com.amazonaws. *region*.voiceid
	com.amazonaws. *region*.kebijaksanaan

Layanan AWS	Nama layanan
AWS Connector Service	com.amazonaws. *region*.awskonektor
AWS Katalog Kontrol	com.amazonaws. *region*.controlcatalog
AWS Cost Explorer	com.amazonaws. *region*.ce
Hub Optimisasi Biaya AWS	com.amazonaws. *region*.cost-optimization-hub
AWS Control Tower	com.amazonaws. *region*.menara pengontrol
	com.amazonaws. *region*.controltower-fips
AWS Data Exchange	com.amazonaws. *region*.pertukaran data
Ekspor Data AWS	aws.api. *region*.bcm-data-ekspor
	com.amazonaws. *region*.bcm-harga-kalkulator
Amazon Data Firehose	com.amazonaws. *region*.kinesis-firehose
Amazon Data Lifecycle Manager	com.amazonaws. *region*.dlm
	com.amazonaws. *region*.dlm-fips
AWS Database Migration Service	com.amazonaws. *region*.dms
	com.amazonaws. *region*.dms-fips
AWS DataSync	com.amazonaws. *region*.datasync
Amazon DataZone	com.amazonaws. *region*.datazone
	com.amazonaws. *region*.datazone-fips
AWS Deadline Cloud	com.amazonaws. *region*.deadline.management
	com.amazonaws. *region*.deadline.scheduling
Amazon Detective	com.amazonaws. *region*.detektif

Layanan AWS	Nama layanan
	com.amazonaws. *region*.detektif-fips
DevOpsGuru Amazon	com.amazonaws. *region*.devops-guru
AWS Direct Connect	com.amazonaws. *region*.directconnect
	com.amazonaws. *region*.directconnect-fips
AWS Directory Service	com.amazonaws. *region*.ds
	com.amazonaws. *region*.ds-data
	com.amazonaws. *region*.ds-data-fips
Amazon DocumentDB	com.amazonaws. *region*.rds
Amazon DynamoDB	com.amazonaws. *region*.dynamodb
	com.amazonaws. *region*.dynamodb-fips
	com.amazonaws. *region*.dynamodb-stream
API langsung Amazon EBS	com.amazonaws. *region*.ebs
	com.amazonaws. *region*.ebs-fips
Amazon EC2	com.amazonaws. *region*.ec2
	com.amazonaws. *region*.ec2-fips
Amazon EC2 Auto Scaling	com.amazonaws. *region*.penskalaan otomatis
	com.amazonaws. *region*.autoscaling-fips
EC2 Image Builder	com.amazonaws. *region*.imagebuilder
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr

Layanan AWS	Nama layanan
Amazon ECS	com.amazonaws. *region*.ecs
	com.amazonaws. *region*.ecs-agen
	com.amazonaws. *region*.ecs-telemetri
Amazon EKS	com.amazonaws. *region*.eks
	com.amazonaws. *region*.eks-auth
	com.amazonaws. *region*.eks-fips
	com.amazonaws. *region*.eks-proxy
AWS Elastic Beanstalk	com.amazonaws. *region*.elasticbeanstalk
	com.amazonaws. *region*.elasticbeanstalk-kesehatan
AWS Elastic Disaster Recovery	com.amazonaws. *region*.drs
Sistem File Elastis Amazon	com.amazonaws. *region*.elasticfilesystem
	com.amazonaws. *region*.elasticfilesystem-fips
Elastic Load Balancing	com.amazonaws. *region*.elasticloadbalancing
Layanan VMware Amazon Elastic	com.amazonaws. *region*.evs
	com.amazonaws. *region*.evs-fips
Amazon ElastiCache	com.amazonaws. *region*.elasticache
	com.amazonaws. *region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws. *region*.mediaconnect
AWS Elemental MediaConvert	com.amazonaws. *region*.mediaconvert
	com.amazonaws. *region*.mediaconvert-fips

Layanan AWS	Nama layanan
Amazon EMR	com.amazonaws. *region*.elasticmapreduce
	com.amazonaws. *region*.elasticmapreduce-fips
Amazon EMR di EKS	com.amazonaws. *region*.emr-kontainer
Amazon EMR Tanpa Server	com.amazonaws. *region*.emr-tanpa server
	com.amazonaws. *region*.emr-serverless-services.livy
	com.amazonaws. *region*.emr-serverless.dasbor
Amazon EMR WAL	com.amazonaws. *region*.emrwal.prod
AWS Pesan Pengguna Akhir Sosial	com.amazonaws. *region*.pesan sosial
	com.amazonaws. *region*.fips pesan-sosial
Resolusi Entitas AWS	com.amazonaws. *region*.entityresolution
	com.amazonaws. *region*.entityresolusi-fips
Amazon EventBridge	com.amazonaws. *region*.acara
	com.amazonaws. *region*.acara-fips
	com.amazonaws. *region*.pipa
	com.amazonaws. *region*.pipa-data
	com.amazonaws. *region*.pipes-fips
	com.amazonaws. *region*.skema
EventBridge Penjadwal Amazon	com.amazonaws. *region*.penjadwal
AWS Fault Injection Service	com.amazonaws. *region*.fis
	com.amazonaws. *region*.fis-fips

Layanan AWS	Nama layanan
Amazon FinSpace	com.amazonaws. *region*.finspace
	com.amazonaws. *region*.finspace-api
AWS Firewall Manager	com.amazonaws. *region*.fms
	com.amazonaws. *region*.fms-fips
Amazon Forecast	com.amazonaws. *region*.perkiraan
	com.amazonaws. *region*.forecastquery
	com.amazonaws. *region*.forecast-fips
	com.amazonaws. *region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws. *region*.detektor penipuan
Amazon FSx	com.amazonaws. *region*.fsx
	com.amazonaws. *region*.fsx-fips
GameLift Peladen Amazon	com.amazonaws. *region*.gamelift
GameLift Aliran Amazon	com.amazonaws. *region*.gameliftstream
AWS Global Networks for Transit Gateways	com.amazonaws. *region*.networkmanager
AWS Glue	com.amazonaws. *region*.lem
	com.amazonaws. *region*.glue.dasbor
AWS Glue DataBrew	com.amazonaws. *region*.databrew
	com.amazonaws. *region*.databrew-fips
Amazon Managed Grafana	com.amazonaws. *region*.grafana
	com.amazonaws. *region*.grafana-ruang kerja

Layanan AWS	Nama layanan
AWS Ground Station	com.amazonaws. *region*.groundstation
	com.amazonaws. *region*.groundstation-fips
Amazon GuardDuty	com.amazonaws. *region*.guardduty
	com.amazonaws. *region*.guardduty-data
	com.amazonaws. *region*.guardduty-data-fips
	com.amazonaws. *region*.guardduty-fips
AWS HealthImaging	com.amazonaws. *region*.dicom-medis-pencitraan
	com.amazonaws. *region*.pencitraan medis
	com.amazonaws. *region*.runtime-medis-pencitraan
AWS HealthLake	com.amazonaws. *region*.healthlake
AWS HealthOmics	com.amazonaws. *region*.analytics-omics
	com.amazonaws. *region*.analytics-omics-fips
	com.amazonaws. *region*.control-penyimpanan-omics
	com.amazonaws. *region*.control-storage-omics-fips
	com.amazonaws. *region*.penyimpanan-omics
	com.amazonaws. *region*.tags-omics
	com.amazonaws. *region*.tags-omics-fips
	com.amazonaws. *region*.workflows-omics
	com.amazonaws. *region*.workflows-omics-fips
AWS Identity and Access Management (IAM)	com.amazonaws.iam

Layanan AWS	Nama layanan
Penganalisis Akses IAM	com.amazonaws. *region*.akses-penganalisis
	com.amazonaws. *region*.access-analyzer-fips
Pusat Identitas IAM	com.amazonaws. *region*.identitystore
IAM Roles Anywhere	com.amazonaws. *region*.rolesdi mana saja
	com.amazonaws. *region*.rolesanywhere-fips
Amazon Inspector	com.amazonaws. *region*.inspektor2
	com.amazonaws. *region*.inspector2-fips
	com.amazonaws. *region*.inspektor-pemindaian
	com.amazonaws. *region*.inspector-scan-fips
Amazon Interactive Video Service	com.amazonaws. *region*.ivs.berkontribusi
AWS IoT Core	com.amazonaws. *region*.iot.api
	com.amazonaws. *region*.iot-fips.api
	com.amazonaws. *region*.iot.data
	com.amazonaws. *region*.iot.credentials
AWS IoT Device Management terowongan aman	com.amazonaws. *region*.iot.tunneling.api
	com.amazonaws. *region*.iot-fips.tunneling.api
	com.amazonaws. *region*.iot.tunneling.data
	com.amazonaws. *region*.iot-fips.tunneling.data
AWS IoT Core Device Advisor	com.amazonaws. *region*.deviceadvisor.iot
Integrasi terkelola untuk AWS IoT Device Management	com.amazonaws. *region*.iotmanagedintegrations.api

Layanan AWS	Nama layanan
	com.amazonaws. *region*.iotmanagedintegrations-fips.api
AWS IoT Core for LoRaWAN	com.amazonaws. *region*.iotwireless.api
	com.amazonaws. *region*.lorawan.cangkir
	com.amazonaws. *region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws. *region*.iotfleetwise
AWS IoT Greengrass	com.amazonaws. *region*.greengrass
AWS IoT RoboRunner	com.amazonaws. *region*.iotroborunner
AWS IoT SiteWise	com.amazonaws. *region*.iotsitewise.api
	com.amazonaws. *region*.iotsitewise.data
AWS IoT TwinMaker	com.amazonaws. *region*.iottwinmaker.api
	com.amazonaws. *region*.iottwinmaker.data
Amazon Kendra	com.amazonaws. *region*.kendra
	aws.api. *region*peringkat.kendra
AWS Key Management Service	com.amazonaws. *region*.kms
	com.amazonaws. *region*.kms-fips
Amazon Keyspaces (untuk Apache Cassandra)	com.amazonaws. *region*.cassandra
	com.amazonaws. *region*.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws. *region*.kinesis-stream
	com.amazonaws. *region*.kinesis-streams-fips
AWS Lake Formation	com.amazonaws. *region*.lakeformasi

Layanan AWS	Nama layanan
AWS Lambda	com.amazonaws. *region*.lambda
AWS Launch Wizard	com.amazonaws. *region*.launchwizard
Amazon Lex	com.amazonaws. *region*.model-v2-lex
	com.amazonaws. *region*.runtime-v2-lex
AWS License Manager	com.amazonaws. *region*.license-manajer
	com.amazonaws. *region*.license-manager-fips
	com.amazonaws. *region*.license-manager-linux-langganan
	com.amazonaws. *region*.license-manager-linux-subscriptions-fips
	com.amazonaws. *region*.license-manager-user-subscriptions
	com.amazonaws. *region*.license-manager-user-subscriptions-fips
Amazon Lightsail	com.amazonaws. *region*.lightsail
Amazon Location Service	com.amazonaws. *region*.geo.maps
	com.amazonaws. *region*.geo.places
	com.amazonaws. *region*.geo.routes
	com.amazonaws. *region*.geo.geofencing
	com.amazonaws. *region*.geo.tracking
	com.amazonaws. *region*.geo.metadata
Amazon Lookout for Equipment	com.amazonaws. *region*.lookoutequipment

Layanan AWS	Nama layanan
Amazon Lookout for Vision	com.amazonaws. *region*.lookoutvision
Amazon Macie	com.amazonaws. *region*.macie2
	com.amazonaws. *region*.macie2-fips
AWS Mainframe Modernization	com.amazonaws. *region*.apptest
	com.amazonaws. *region*.m2
Amazon Managed Blockchain	com.amazonaws. *region*.managedblockchain-query
	com.amazonaws. *region*.managedblockchain.bitcoin.mainnet
	com.amazonaws. *region*.managedblockchain.bitcoin.testnet
AWS Perjanjian Marketplace	com.amazonaws. *region*.perjanjian-pasar
AWS Penemuan Marketplace	com.amazonaws. *region*.penemuan-pasar
AWS Marketplace Metering Service	com.amazonaws. *region*.metering-pasar
Layanan Terkelola Amazon untuk Prometheus	com.amazonaws. *region*.aps
	com.amazonaws. *region*.aps-ruang kerja
Amazon Managed Streaming for Apache Kafka (MSK)	com.amazonaws. *region*.kafka
	com.amazonaws. *region*.kafka-fips
Alur Kerja Terkelola Amazon untuk Apache Airflow	com.amazonaws. *region*.airflow.api
	com.amazonaws. *region*.airflow.api-fips
	com.amazonaws. *region*.airflow.env
	com.amazonaws. *region*.airflow.env-fips

Layanan AWS	Nama layanan
	com.amazonaws. *region*.airflow.ops
Amazon Route 53	com.amazonaws.route53
Amazon Route 53 Global Resolver	aws.api.us-east-2.route53globalresolver
	aws.api.us-east-2.route53globalresolver-fips
Konsol Manajemen AWS	com.amazonaws. *region*.konsol
	com.amazonaws. *region*.masuk
Amazon MemoryDB	com.amazonaws. *region*.memori-db
	com.amazonaws. *region*.memorydb-fips
Orkestrator AWS Migration Hub	com.amazonaws. *region*.migrationhub-orkestrator
AWS Migration Hub Refactor Spaces	com.amazonaws. *region*.refactor-spasi
Rekomendasi Strategi Migrasi Hub	com.amazonaws. *region*.migrationhub-strategi
Amazon MQ	com.amazonaws. *region*.mq
	com.amazonaws. *region*.mq-fips
Analisis Amazon Neptunus	com.amazonaws. *region*.neptunus grafik
	com.amazonaws. *region*.neptunus-grafik-data
	com.amazonaws. *region*.neptunus-graf-fips
AWS Network Firewall	com.amazonaws. *region*.jaringan-firewall
	com.amazonaws. *region*.network-firewall-fips
OpenSearch Layanan Amazon	Titik akhir ini dikelola layanan
OpenSearch Tertelan Amazon	com.amazonaws. *region*.osis

Layanan AWS	Nama layanan
AWS Organizations	com.amazonaws. *region*.organisasi
	com.amazonaws. *region*.organisasi-fips
AWS Outposts	com.amazonaws. *region*.pos terdepan
AWS Panorama	com.amazonaws. *region*.panorama
AWS Kriptografi Pembayaran	com.amazonaws. *region*.pembayaran-cryptography.control plane
	com.amazonaws. *region*.pembayaran-cryptography.data plane
AWS PCS	com.amazonaws. *region*.pcs
	com.amazonaws. *region*.pcs-fips
Amazon Personalisasi	com.amazonaws. *region*.personalisasi
	com.amazonaws. *region*.personalisasi-acara
	com.amazonaws. *region*.personalisasi-runtime
Amazon Pinpoint	com.amazonaws. *region*.tepat
	com.amazonaws. *region*.pinpoint-sms-suara-v2
Amazon Polly	com.amazonaws. *region*.polly
	com.amazonaws. *region*.polly-fips
Daftar Harga AWS	com.amazonaws. *region*.pricing.api
AWS Private Certificate Authority	com.amazonaws. *region*.acm-pca
	com.amazonaws. *region*.acm-pca-fips
	com.amazonaws. *region*.pca-konektor-iklan

Layanan AWS	Nama layanan
	com.amazonaws. *region*.pca-konektor-scep
AWS Proton	com.amazonaws. *region*.proton
Amazon Q Bisnis	aws.api. *region*.qbisnis
Amazon Q Developer	com.amazonaws. *region*.codewhisperer
	com.amazonaws. *region*.q
	com.amazonaws. *region*.qapps
Langganan Pengguna Amazon Q	com.amazonaws. *region*.service.user-langganan
Quick	com.amazonaws. *region*.situs web quicksight-
Amazon RDS	com.amazonaws. *region*.rds
	com.amazonaws. *region*.rds-fips
API Data Amazon RDS	com.amazonaws. *region*.rds-data
Wawasan Performa Amazon RDS	com.amazonaws. *region*.pi
	com.amazonaws. *region*.pi-fips
AWS Re: Post Pribadi	com.amazonaws. *region*.repostspace
Tempat Sampah Daur Ulang	com.amazonaws. *region*.rbin
	com.amazonaws. *region*.rbin-fips
Amazon Redshift	com.amazonaws. *region*.pergeseran merah
	com.amazonaws. *region*.redshift-fips
	com.amazonaws. *region*.redshift-tanpa server
	com.amazonaws. *region*.redshift-serverless-fips

Layanan AWS	Nama layanan
API Data Pergeseran Merah Amazon	com.amazonaws. *region*.redshift-data
	com.amazonaws. *region*.redshift-data-fips
Amazon Rekognition	com.amazonaws. *region*.rekognisi
	com.amazonaws. *region*.rekognition-fips
	com.amazonaws. *region*.streaming-rekognisi
	com.amazonaws. *region*.streaming-rekognition-fips
AWS Resource Access Manager	com.amazonaws. *region*.ram
	com.amazonaws. *region*.ram-fips
Penjelajah Sumber Daya AWS	com.amazonaws. *region*.sumber daya-penjelajah-2
	com.amazonaws. *region*.resource-explorer-2-fips
AWS Resource Groups	com.amazonaws. *region*.resource-group
	com.amazonaws. *region*.resource-groups-fips
AWS Resource Groups Tagging API	com.amazonaws. *region*.penandaan
Amazon S3	com.amazonaws. *region*.s3
	com.amazonaws. *region*.s3tabel
Titik Akses Amazon S3 Multi-Region	com.amazonaws.s3-global.accesspoint
Amazon S3 on Outposts	com.amazonaws. *region*.s3-pos terdepan
Amazon SageMaker AI	aws.sagemaker. *region*.eksperimen
	aws.sagemaker. *region*.buku catatan
	aws.sagemaker. *region*.partner-aplikasi

Layanan AWS	Nama layanan
	aws.sagemaker. *region*.studio
	com.amazonaws. *region*.sagemaker-data-asisten-ilmu-
	com.amazonaws. *region*.sagemaker.api
	com.amazonaws. *region*.sagemaker.api-fips
	com.amazonaws. *region*.sagemaker.featurestore-run time
	com.amazonaws. *region*.sagemaker.featurestore-run time-fips
	com.amazonaws. *region*.sagemaker.metrics
	com.amazonaws. *region*.sagemaker.runtime
	com.amazonaws. *region*.sagemaker.runtime-fips
Savings Plans	com.amazonaws.savingsplans
AWS Secrets Manager	com.amazonaws. *region*.secretsmanager
AWS Agen Keamanan	com.amazonaws. *region*.securityagent
AWS Security Hub CSPM	com.amazonaws. *region*.securityhub
	com.amazonaws. *region*.securityhub-fips
Amazon Security Lake	com.amazonaws. *region*.securitylake
	com.amazonaws. *region*.securitylake-fips
AWS Security Token Service	com.amazonaws. *region*.sts
	com.amazonaws. *region*.sts-fips

Layanan AWS	Nama layanan
AWS Serverless Application Repository	com.amazonaws. *region*.serverlessrepo
Service Catalog	com.amazonaws. *region*.servicecatalog
	com.amazonaws. *region*.servicecatalog-appregistry
Service Quotas	com.amazonaws. *region*.servicequotas
Amazon SES	com.amazonaws. *region*.email-smtp
	com.amazonaws. *region*.mail-manajer
	com.amazonaws. *region*.mail-manager-fips
	com.amazonaws. *region*.mail-manager-smtp.auth.fips
	com.amazonaws. *region*.mail-manager-smtp.open.fips
AWS Snowball Edge Device Management	com.amazonaws. *region*.manajemen perangkat salju
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
	com.amazonaws. *region*.sqs-fips
Amazon SWF	com.amazonaws. *region*.swf
	com.amazonaws. *region*.swf-fips
AWS Step Functions	com.amazonaws. *region*.negara
	com.amazonaws. *region*.sync-status
AWS Storage Gateway	com.amazonaws. *region*.storagegateway
Rantai Pasokan AWS	com.amazonaws. *region*.scn

Layanan AWS	Nama layanan
AWS Systems Manager	com.amazonaws. *region*.ec2pesan
	com.amazonaws. *region*.ssm
	com.amazonaws. *region*.ssm-kontak
	com.amazonaws. *region*.ssm-insiden
	com.amazonaws. *region*.ssm-insiden-fips
	com.amazonaws. *region*.ssm-pengaturan cepat
	com.amazonaws. *region*.ssmmessages
Manajer Sistem AWS untuk SAP	com.amazonaws. *region*.ssm-sap
	com.amazonaws. *region*.ssm-sap-fips
AWS Pembangun Jaringan Telco	com.amazonaws. *region*.tnb
Amazon Texttract	com.amazonaws. *region*.textract
	com.amazonaws. *region*.textract-fips
Amazon Timestream	com.amazonaws. *region*.timestream.ingest- *cell*
	com.amazonaws. *region*.timestream.query- *cell*
Amazon Timestream untuk InfluxDB	com.amazonaws. *region*.timestream-influxdb
	com.amazonaws. *region*.timestream-influxdb-fips
Amazon Transcribe	com.amazonaws. *region*.transkripsikan
	com.amazonaws. *region*.transcribe-fips
	com.amazonaws. *region*.transcribestreaming
com.amazonaws. *region*.transcribestreaming-fips	

Layanan AWS	Nama layanan
Amazon Transcribe Medis	com.amazonaws. *region*.transkripsikan
	com.amazonaws. *region*.transcribestreaming
AWS Transfer for SFTP	com.amazonaws. *region*.transfer
	com.amazonaws. *region*.transfer.server
AWS Transform	com.amazonaws. *region*.mengubah
AWS Transform kustom	com.amazonaws. *region*.transform-kustom
Amazon Translate	com.amazonaws. *region*.terjemahkan
AWS Trusted Advisor	com.amazonaws. *region*.trustedadvisor
Notifikasi Pengguna AWS	com.amazonaws. *region*.notifikasi
	com.amazonaws. *region*.notifikasi-kontak
Izin Terverifikasi Amazon	com.amazonaws. *region*.verifiedpermissions
	com.amazonaws. *region*.verifiedpermissions-fips
Kisi VPC Amazon	com.amazonaws. *region*.vpc-kisi
AWS WAFV2	com.amazonaws. *region*.wafv2
	com.amazonaws. *region*.wafv2-fips
AWS Well-Architected Tool	com.amazonaws. *region*.wellarchitected
Amazon WorkMail	com.amazonaws. *region*.workmail
	com.amazonaws. *region*.workmailmessageflow
Amazon WorkSpaces	com.amazonaws. *region*.ruang kerja
Browser WorkSpaces Aman Amazon	com.amazonaws. *region*.workspace-web

Layanan AWS	Nama layanan
	com.amazonaws. *region*.workspaces-web-fips
WorkSpaces streaming	com.amazonaws. *region*.dataran tinggi
Klien WorkSpaces Tipis Amazon	com.amazonaws. *region*.thinclient.api
aws.api. *region*.s3file	
aws.api. *region*.s3file-fips	
AWS X-Ray	com.amazonaws. *region*.xray
Layanan Dikelola Amazon untuk Apache Flink	com.amazonaws. *region*.kinesisanalytics
	com.amazonaws. *region*.kinesisanalytics-fips

Lihat Layanan AWS nama yang tersedia

Anda dapat menggunakan perintah describe-vpc-endpoint-services untuk melihat nama layanan yang mendukung titik akhir VPC.

Contoh berikut menampilkan Layanan AWS yang mendukung titik akhir antarmuka di Wilayah tertentu. `--query`Opsi membatasi output ke nama layanan.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query ServiceNames
```

Berikut ini adalah output contoh. Output lengkap tidak ditampilkan.

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

```
    . . .
     "com.amazonaws.us-east-1.xray"
]
```

Melihat informasi tentang layanan

Setelah Anda memiliki nama layanan, Anda dapat menggunakan perintah describe-vpc-endpoint-services untuk melihat informasi rinci tentang setiap layanan endpoint.

Contoh berikut menampilkan informasi tentang titik akhir CloudWatch antarmuka Amazon di Wilayah yang ditentukan.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.monitoring" \
  --region us-east-1
```

Berikut ini adalah contoh output. `VpcEndpointPolicySupported`menunjukkan apakah kebijakan titik akhir didukung. `SupportedIpAddressTypes`menunjukkan jenis alamat IP mana yang didukung.

```
{
    "ServiceDetails": [
        {
            "ServiceName": "com.amazonaws.us-east-1.monitoring",
            "ServiceId": "vpce-svc-0fc975f3e7e5beba4",
            "ServiceType": [
                {
                    "ServiceType": "Interface"
                }
            ],
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
                "us-east-1c",
                "us-east-1d",
                "us-east-1e",
                "us-east-1f"
            ],
            "Owner": "amazon",
            "BaseEndpointDnsNames": [
                "monitoring.us-east-1.vpce.amazonaws.com"
            ],
```

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

Lihat dukungan kebijakan titik akhir

Untuk memverifikasi apakah layanan mendukung kebijakan titik akhir, panggil perintah describe-vpc-endpoint-services dan periksa nilainya. `VpcEndpointPolicySupported` Nilai yang mungkin adalah `true` dan `false`.

Contoh berikut memeriksa apakah layanan yang ditentukan mendukung kebijakan titik akhir di Wilayah tertentu. `--query`Opsi membatasi output ke nilai`VpcEndpointPolicySupported`.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.s3" \
  --region us-east-1 \
  --query ServiceDetails[*].VpcEndpointPolicySupported \
```

```
  --output text
```

Berikut ini adalah output contoh.

```
True
```

Contoh berikut mencantumkan kebijakan Layanan AWS yang mendukung titik akhir di Wilayah yang ditentukan. `--query`Opsi membatasi output ke nama layanan. Untuk menjalankan perintah ini menggunakan prompt perintah Windows, hapus tanda kutip tunggal di sekitar string kueri, dan ubah karakter kelanjutan baris dari\ ke ^.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`true`].ServiceName'
```

Berikut ini adalah output contoh. Output lengkap tidak ditampilkan.

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

Contoh berikut mencantumkan kebijakan Layanan AWS yang tidak mendukung endpoint di Wilayah tertentu. `--query`Opsi membatasi output ke nama layanan. Untuk menjalankan perintah ini menggunakan prompt perintah Windows, hapus tanda kutip tunggal di sekitar string kueri, dan ubah karakter kelanjutan baris dari\ ke ^.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`false`].ServiceName'
```

Berikut ini adalah output contoh. Output lengkap tidak ditampilkan.

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

Lihat dukungan IPv6

Untuk melihat dukungan IPv6 untuk AWS layanan, lihat AWS layanan yang mendukung IPv6. Anda juga dapat menggunakan perintah describe-vpc-endpoint-services berikut untuk melihat yang dapat Anda akses melalui IPv6 di Wilayah Layanan AWS yang ditentukan. `--query`Opsi membatasi output ke nama layanan.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=supported-ip-address-types,Values=ipv6 Name=owner,Values=amazon
 Name=service-type,Values=Interface \
  --region us-east-1 \
  --query ServiceNames
```

Berikut ini adalah output contoh. Output lengkap tidak ditampilkan.

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

Cross-region diaktifkan Layanan AWS

Berikut ini Layanan AWS terintegrasi dengan lintas Wilayah AWS PrivateLink. Anda dapat membuat titik akhir antarmuka untuk terhubung ke layanan ini di AWS Wilayah lain, secara pribadi, seolah-olah mereka berjalan di VPC Anda sendiri.

Pilih tautan di Layanan AWSkolom untuk melihat dokumentasi layanan. Kolom Nama layanan berisi nama layanan yang Anda tentukan saat Anda membuat titik akhir antarmuka.

Layanan AWS	Nama layanan
Amazon S3	com.amazonaws. *region*.s3
AWS Identity and Access Management (IAM)	com.amazonaws.iam
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
AWS Key Management Service	com.amazonaws. *region*.kms
	com.amazonaws. *region*.kms-fips
Amazon ECS	com.amazonaws. *region*.ecs
AWS Lambda	com.amazonaws. *region*.lambda
Amazon Data Firehose	com.amazonaws. *region*.kinesis-firehose
Layanan Dikelola Amazon untuk Apache Flink	com.amazonaws. *region*.kinesisanalytics
	com.amazonaws. *region*.kinesisanalytics-fips
Amazon Route 53	com.amazonaws.route53

Lihat Layanan AWS nama yang tersedia

Anda dapat menggunakan perintah describe-vpc-endpoint-services untuk melihat layanan yang diaktifkan lintas Wilayah.

Contoh berikut menampilkan Layanan AWS bahwa pengguna di `us-east-1` Wilayah dapat mengakses melalui titik akhir antarmuka, ke Wilayah layanan (`us-west-2`) yang ditentukan. `--query`Opsi membatasi output ke nama layanan.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --service-region us-west-2 \
  --query ServiceNames
```

Berikut ini adalah output contoh. Output lengkap tidak ditampilkan.

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

> **Note**
>
> Anda harus menggunakan DNS regional. DNS Zonal tidak didukung saat mengakses Layanan AWS di Wilayah lain. Untuk informasi selengkapnya, lihat Melihat dan memperbarui atribut DNS di Panduan Pengguna Amazon VPC.

Izin dan Pertimbangan

- Secara default, entitas IAM tidak memiliki izin untuk mengakses Layanan AWS di Wilayah lain. Untuk memberikan izin yang diperlukan untuk akses lintas Wilayah, administrator IAM dapat membuat kebijakan IAM yang mengizinkan tindakan khusus izin. `vpce:AllowMultiRegion`
- Pastikan Kebijakan Kontrol Layanan (SCP) Anda tidak menolak tindakan hanya `vpce:AllowMultiRegion` izin. Untuk menggunakan AWS PrivateLink fitur konektivitas lintas wilayah, kebijakan identitas dan SCP Anda harus mengizinkan tindakan ini.
- Untuk mengontrol Wilayah yang dapat ditentukan oleh entitas IAM sebagai Wilayah layanan saat membuat titik akhir VPC, gunakan `ec2:VpceServiceRegion` kunci kondisi.

- Konsumen layanan harus memilih masuk ke Wilayah keikutsertaan sebelum memilihnya sebagai Wilayah layanan untuk titik akhir. Jika memungkinkan, kami menyarankan agar konsumen layanan mengakses layanan menggunakan konektivitas intra-wilayah, bukan konektivitas lintas wilayah. Intra-Region konektivitas memberikan latensi yang lebih rendah dan biaya yang lebih rendah.
- Anda dapat menggunakan kunci kondisi `aws:SourceVpcArn` global baru IAM untuk mengamankan Wilayah mana, Akun AWS dan VPC sumber daya Anda dapat diakses. Kunci ini membantu mengimplementasikan residensi data dan kontrol akses berbasis wilayah.
- Untuk ketersediaan tinggi, buat titik akhir antarmuka berkemampuan lintas Wilayah di setidaknya dua Availability Zone. Dalam hal ini, penyedia dan konsumen tidak diharuskan menggunakan Availability Zone yang sama.
- Dengan akses lintas Wilayah, AWS PrivateLink mengelola failover antara Availability Zone di Wilayah layanan dan konsumen. Itu tidak mengelola failover di seluruh Wilayah.
- Akses Lintas Wilayah tidak didukung untuk Availability Zone berikut: `use1-az3usw1-az2,apne1-az3,,apne2-az2`, dan`apne2-az4`.
- Anda dapat menggunakan AWS Fault Injection Service untuk mensimulasikan peristiwa regional dan memodelkan skenario kegagalan untuk titik akhir antarmuka yang diaktifkan di dalam wilayah dan lintas wilayah. Untuk mempelajari lebih lanjut, lihat AWS FIS dokumentasi.

Buat titik akhir antarmuka ke Layanan AWS Wilayah lain

Untuk membuat titik akhir antarmuka menggunakan Konsol, lihat bagian Buat titik akhir VPC.

Di CLI, Anda dapat menggunakan perintah create-vpc-endpoint untuk membuat titik akhir VPC ke Region yang berbeda. Layanan AWS Contoh berikut membuat titik akhir antarmuka ke Amazon S3 dari `us-west-2` VPC di. `us-east-1`

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

Akses Layanan AWS menggunakan titik akhir VPC antarmuka

Anda dapat membuat titik akhir VPC antarmuka untuk terhubung ke layanan yang didukung oleh AWS PrivateLink, termasuk banyak. Layanan AWS Untuk ikhtisar, lihat the section called “Konsep” danAkses Layanan AWS.

Untuk setiap subnet yang Anda tentukan dari VPC Anda, kami membuat antarmuka jaringan endpoint di subnet dan menetapkannya alamat IP pribadi dari rentang alamat subnet. Antarmuka jaringan endpoint adalah antarmuka jaringan yang dikelola pemohon; Anda dapat melihatnya di Anda Akun AWS, tetapi Anda tidak dapat mengelolanya sendiri.

Anda ditagih untuk penggunaan per jam dan biaya pemrosesan data. Untuk informasi selengkapnya, lihat Harga titik akhir antarmuka.

Daftar Isi

Prasyarat

- Menyebarkan sumber daya yang akan mengakses Layanan AWS di VPC Anda.
- Untuk menggunakan DNS pribadi, Anda harus mengaktifkan nama host DNS dan resolusi DNS untuk VPC Anda. Untuk informasi selengkapnya, lihat Melihat dan memperbarui atribut DNS di Panduan Pengguna Amazon VPC.
- Untuk mengaktifkan IPv6 untuk titik akhir antarmuka, Layanan AWS harus mendukung akses melalui IPv6. Untuk informasi selengkapnya, lihat the section called “Jenis alamat IP”.
- Buat grup keamanan untuk antarmuka jaringan titik akhir yang memungkinkan lalu lintas yang diharapkan dari sumber daya di VPC Anda. Misalnya, untuk memastikan bahwa AWS CLI dapat mengirim permintaan HTTPS ke Layanan AWS, grup keamanan harus mengizinkan lalu lintas HTTPS masuk.
- Jika sumber daya Anda berada dalam subnet dengan ACL jaringan, verifikasi bahwa ACL jaringan memungkinkan lalu lintas antara sumber daya di VPC Anda dan antarmuka jaringan titik akhir.
- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat AWS PrivateLink kuota.

Buat VPC endpoint

Gunakan prosedur berikut untuk membuat titik akhir VPC antarmuka yang terhubung ke file. Layanan AWS

Untuk membuat titik akhir antarmuka untuk sebuah Layanan AWS

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Jenis, pilih AWS layanan.
5. (Opsional) Jika membuat titik akhir ke Wilayah lain, pilih kotak centang Aktifkan lintas Wilayah dan kemudian pilih wilayah layanan dari drop-down. Layanan AWS
6. Untuk nama Layanan, pilih layanan. Untuk informasi selengkapnya, lihat the section called “Layanan yang terintegrasi”.
7. Untuk VPC, pilih VPC dari mana Anda akan mengakses file. Layanan AWS
8. Jika, pada Langkah 5, Anda memilih nama layanan untuk Amazon S3, dan jika Anda ingin mengonfigurasi dukungan DNS pribadi, pilih Pengaturan tambahan, Aktifkan nama DNS. Ketika Anda membuat pilihan ini, itu juga secara otomatis memilih Aktifkan DNS pribadi hanya untuk titik akhir masuk. Anda dapat mengonfigurasi DNS pribadi dengan titik akhir Resolver masuk hanya untuk titik akhir antarmuka untuk Amazon S3. Jika Anda tidak memiliki titik akhir gateway untuk Amazon S3 dan Anda memilih Aktifkan DNS pribadi hanya untuk titik akhir masuk, Anda akan menerima kesalahan saat mencoba langkah terakhir dalam prosedur ini.

   Jika, pada Langkah 5, Anda memilih nama layanan untuk layanan apa pun selain Amazon S3, Pengaturan tambahan, Aktifkan nama DNS sudah dipilih. Kami menyarankan agar Anda tetap default. Ini memastikan bahwa permintaan yang menggunakan titik akhir layanan publik, seperti permintaan yang dibuat melalui AWS SDK, diselesaikan ke titik akhir VPC Anda.
9. Untuk Subnet, pilih subnet untuk membuat antarmuka jaringan titik akhir. Anda dapat memilih satu subnet per Availability Zone. Anda tidak dapat memilih beberapa subnet dari Availability Zone yang sama. Untuk informasi selengkapnya, lihat the section called “Subnet dan Availability Zone”.

   Secara default, kami memilih alamat IP dari rentang alamat IP subnet dan menetapkannya ke antarmuka jaringan titik akhir. Untuk memilih alamat IP sendiri, pilih Tentukan alamat IP. Perhatikan bahwa empat alamat IP pertama dan alamat IP terakhir di blok CIDR subnet

dicadangkan untuk penggunaan internal, sehingga Anda tidak dapat menentukannya untuk antarmuka jaringan titik akhir Anda.

10. Untuk jenis alamat IP, pilih dari opsi berikut:

    - IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan layanan menerima permintaan IPv4.
    - IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6 dan layanan menerima permintaan IPv6.
    - Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan endpoint. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6 dan layanan menerima permintaan IPv4 dan IPv6.

11. Untuk grup Keamanan, pilih grup keamanan untuk diasosiasikan dengan antarmuka jaringan titik akhir. Secara default, kami mengaitkan grup keamanan default untuk VPC.
12. Untuk Kebijakan, untuk mengizinkan semua operasi oleh semua prinsipal pada semua sumber daya melalui titik akhir antarmuka, pilih Akses penuh. Untuk membatasi akses, pilih Kustom dan masukkan kebijakan. Opsi ini hanya tersedia jika layanan mendukung kebijakan titik akhir VPC. Untuk informasi selengkapnya, lihat Kebijakan titik akhir.
13. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
14. Pilih Buat titik akhir.

Untuk membuat titik akhir antarmuka menggunakan baris perintah

- buat-vpc-titik akhir ()AWS CLI
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Subnet bersama

Anda tidak dapat membuat, mendeskripsikan, memodifikasi, atau menghapus titik akhir VPC di subnet yang dibagikan dengan Anda. Titik akhir VPC yang dikelola oleh AWS layanan (titik akhir VPC yang dikelola layanan) dapat dibuat oleh layanan di subnet bersama.

ICMP

Endpoint antarmuka tidak menanggapi ping permintaan. Anda dapat menggunakan nmap perintah nc atau sebagai gantinya.

Konfigurasikan titik akhir antarmuka

Setelah Anda membuat antarmuka VPC endpoint, Anda dapat memperbarui konfigurasinya.

Tugas

- Menambah atau menghapus subnet
- Grup keamanan asosiasi
- Edit kebijakan titik akhir VPC
- Aktifkan nama DNS pribadi
- Kelola tanda

Menambah atau menghapus subnet

Anda dapat memilih satu subnet per Availability Zone untuk titik akhir antarmuka Anda. Jika Anda menambahkan subnet, kami membuat antarmuka jaringan endpoint di subnet dan menetapkannya alamat IP pribadi dari rentang alamat IP subnet. Jika Anda menghapus subnet, kami menghapus antarmuka jaringan endpoint-nya. Untuk informasi selengkapnya, lihat the section called “Subnet dan Availability Zone”.

Untuk mengubah subnet menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola subnet.
5. Pilih atau batal pilihan Availability Zones sesuai kebutuhan. Untuk setiap Availability Zone, pilih satu subnet. Secara default, kami memilih alamat IP dari rentang alamat IP subnet dan menetapkannya ke antarmuka jaringan titik akhir. Untuk memilih alamat IP untuk antarmuka jaringan titik akhir, pilih Tentukan alamat IP dan masukkan alamat IPv4 dari rentang alamat

subnet. Jika layanan endpoint mendukung IPv6, Anda juga dapat memasukkan alamat IPv6 dari rentang alamat subnet.

Jika Anda menentukan alamat IP untuk subnet yang sudah memiliki antarmuka jaringan endpoint untuk titik akhir VPC ini, kami mengganti antarmuka jaringan endpoint dengan yang baru. Proses ini untuk sementara memutuskan subnet dan titik akhir VPC.

6. Pilih Ubah subnet.

Untuk mengubah subnet menggunakan baris perintah

- memodifikasi-vpc-titik akhir ()AWS CLI
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Grup keamanan asosiasi

Anda dapat mengubah grup keamanan yang terkait dengan antarmuka jaringan untuk titik akhir antarmuka Anda. Aturan grup keamanan mengontrol lalu lintas yang diizinkan ke antarmuka jaringan titik akhir dari sumber daya di VPC Anda.

Untuk mengubah grup keamanan menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola grup keamanan.
5. Pilih atau batalkan pilihan grup keamanan sesuai kebutuhan.
6. Pilih Ubah grup keamanan.

Untuk mengubah grup keamanan menggunakan baris perintah

- memodifikasi-vpc-titik akhir ()AWS CLI
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Edit kebijakan titik akhir VPC

Jika Layanan AWS mendukung kebijakan titik akhir, Anda dapat mengedit kebijakan titik akhir untuk titik akhir. Setelah memperbarui kebijakan titik akhir, perlu beberapa menit agar perubahan diterapkan. Untuk informasi selengkapnya, lihat Kebijakan titik akhir.

Untuk mengubah kebijakan titik akhir menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola kebijakan.
5. Pilih Akses Penuh untuk mengizinkan akses penuh ke layanan, atau pilih Kustom dan lampirkan kebijakan kustom.
6. Pilih Simpan.

Untuk mengubah kebijakan endpoint menggunakan baris perintah

- memodifikasi-vpc-titik akhir ()AWS CLI
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Aktifkan nama DNS pribadi

Kami menyarankan Anda mengaktifkan nama DNS pribadi untuk titik akhir VPC Anda. Layanan AWS Ini memastikan bahwa permintaan yang menggunakan titik akhir layanan publik, seperti permintaan yang dibuat melalui AWS SDK, diselesaikan ke titik akhir VPC Anda.

Untuk menggunakan nama DNS pribadi, Anda harus mengaktifkan nama host DNS dan resolusi DNS untuk VPC Anda. Setelah Anda mengaktifkan nama DNS pribadi, mungkin diperlukan beberapa menit agar alamat IP pribadi tersedia. Catatan DNS yang kami buat saat Anda mengaktifkan nama DNS pribadi bersifat pribadi. Oleh karena itu, nama DNS pribadi tidak dapat diselesaikan secara publik.

Untuk mengubah opsi nama DNS pribadi menggunakan konsol

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

2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Ubah nama DNS pribadi.
5. Pilih atau hapus Aktifkan untuk titik akhir ini sesuai kebutuhan.
6. Jika layanannya Amazon S3, memilih Aktifkan untuk titik akhir ini di langkah sebelumnya juga memilih Aktifkan DNS pribadi hanya untuk titik akhir masuk. Jika Anda lebih suka fungsi DNS pribadi standar, hapus Aktifkan DNS pribadi hanya untuk titik akhir masuk. Jika Anda tidak memiliki titik akhir gateway untuk Amazon S3 selain titik akhir antarmuka untuk Amazon S3, dan Anda memilih Aktifkan DNS pribadi hanya untuk titik akhir masuk, Anda akan menerima kesalahan saat menyimpan perubahan di langkah berikutnya. Untuk informasi selengkapnya, lihat the section called “DNS privat”.
7. Pilih Simpan perubahan.

Untuk mengubah opsi nama DNS pribadi menggunakan baris perintah

- memodifikasi-vpc-titik akhir ()AWS CLI
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Kelola tanda

Anda dapat menandai titik akhir antarmuka Anda untuk membantu Anda mengidentifikasi atau mengkategorikannya sesuai dengan kebutuhan organisasi Anda.

Untuk mengelola tag menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola tag.
5. Untuk setiap tag untuk menambahkan pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih Hapus di sebelah kanan kunci tag dan nilai.
7. Pilih Simpan.

Untuk mengelola tag menggunakan baris perintah

- buat-tag dan hapus-tag ()AWS CLI
- New-EC2Tagdan Remove-EC2Tag(Alat untuk Windows PowerShell)

Menerima peringatan untuk acara titik akhir antarmuka

Anda dapat membuat notifikasi untuk menerima peringatan untuk peristiwa tertentu yang terkait dengan titik akhir antarmuka Anda. Misalnya, Anda dapat menerima email saat permintaan koneksi diterima atau ditolak.

Tugas

- Buat notifikasi SNS
- Menambahkan kebijakan akses
- Menambahkan kebijakan kunci

Buat notifikasi SNS

Gunakan prosedur berikut untuk membuat topik Amazon SNS untuk notifikasi dan berlangganan topik tersebut.

Untuk membuat notifikasi untuk titik akhir antarmuka menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Dari tab Notifikasi, pilih Buat notifikasi.
5. Untuk ARN Pemberitahuan, pilih Nama Sumber Daya Amazon (ARN) untuk topik SNS yang Anda buat.
6. Untuk berlangganan acara, pilih dari Acara.
   - Connect — Konsumen layanan membuat titik akhir antarmuka. Ini mengirimkan permintaan koneksi ke penyedia layanan.
   - Terima — Penyedia layanan menerima permintaan koneksi.
   - Tolak — Penyedia layanan menolak permintaan koneksi.

- Hapus — Konsumen layanan menghapus titik akhir antarmuka.

7. Pilih Buat notifikasi.

Untuk membuat notifikasi untuk titik akhir antarmuka menggunakan baris perintah

- buat-vpc-endpoint-koneksi-notifikasi ()AWS CLI
- New-EC2VpcEndpointConnectionNotification(Alat untuk Windows PowerShell)

Menambahkan kebijakan akses

Tambahkan kebijakan akses ke topik Amazon SNS yang memungkinkan AWS PrivateLink untuk mempublikasikan notifikasi atas nama Anda, seperti berikut ini. Untuk informasi selengkapnya, lihat Bagaimana cara mengedit kebijakan akses topik Amazon SNS saya? Gunakan kunci kondisi `aws:SourceArn` dan `aws:SourceAccount` global untuk melindungi dari masalah wakil yang membingungkan.

JSON

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

```
}
```

Menambahkan kebijakan kunci

Jika Anda menggunakan topik SNS terenkripsi, kebijakan sumber daya untuk kunci KMS harus dipercaya AWS PrivateLink untuk memanggil operasi API. AWS KMS Berikut ini adalah contoh kebijakan kunci.

JSON

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

Hapus titik akhir antarmuka

Setelah selesai dengan titik akhir VPC, Anda dapat menghapusnya. Menghapus titik akhir antarmuka juga menghapus antarmuka jaringan titik akhir.

Untuk menghapus titik akhir antarmuka menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta mengonfirmasi, pilih **`delete`**.
6. Pilih Hapus.

Untuk menghapus titik akhir antarmuka menggunakan baris perintah

- hapus-vpc-titik akhir ()AWS CLI
- Remove-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Titik akhir Gateway

Titik akhir VPC Gateway menyediakan konektivitas yang andal ke Amazon S3 dan DynamoDB tanpa memerlukan gateway internet atau perangkat NAT untuk VPC Anda. Titik akhir Gateway tidak digunakan AWS PrivateLink, tidak seperti jenis titik akhir VPC lainnya.

Amazon S3 dan DynamoDB mendukung titik akhir gateway dan titik akhir antarmuka. Untuk perbandingan opsi, lihat yang berikut ini:

- Jenis titik akhir VPC untuk Amazon S3
- Jenis titik akhir VPC untuk Amazon DynamoDB

Harga

Tidak dikenakan biaya tambahan untuk menggunakan titik akhir gateway.

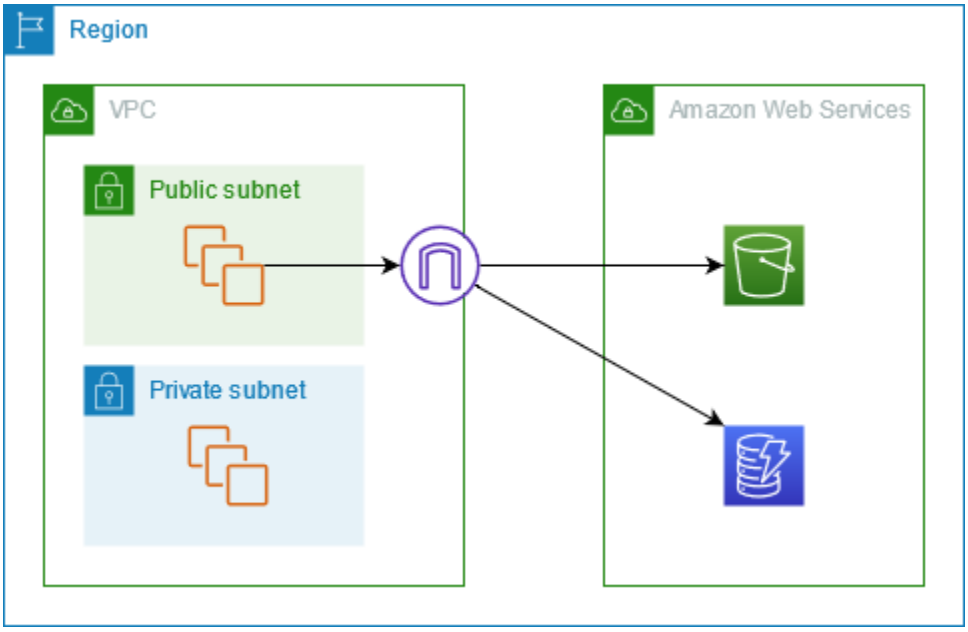
Daftar Isi

Ikhtisar

Anda dapat mengakses Amazon S3 dan DynamoDB melalui titik akhir layanan publik mereka atau melalui titik akhir gateway. Ikhtisar ini membandingkan metode ini.

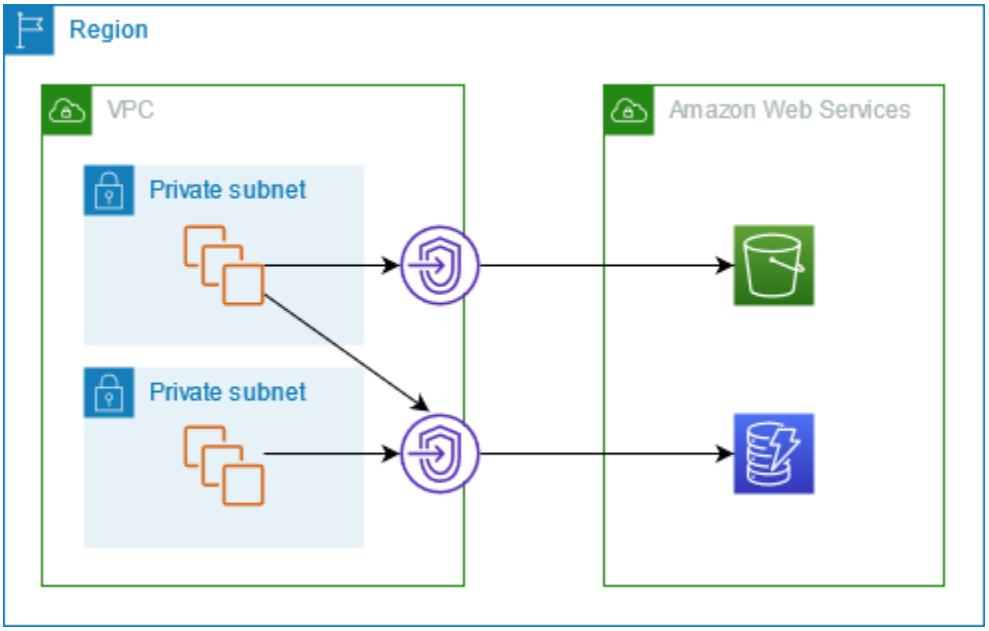
Akses melalui gateway internet

Diagram berikut menunjukkan cara instans mengakses Amazon S3 dan DynamoDB melalui titik akhir layanan publiknya. Lalu lintas ke Amazon S3 atau DynamoDB dari instance di subnet publik dirutekan ke gateway internet untuk VPC dan kemudian ke layanan. Instans di subnet pribadi tidak dapat mengirim lalu lintas ke Amazon S3 atau DynamoDB, karena menurut definisi subnet pribadi tidak memiliki rute ke gateway internet. Untuk mengaktifkan instance di subnet pribadi untuk mengirim lalu lintas ke Amazon S3 atau DynamoDB, Anda akan menambahkan perangkat NAT ke subnet publik dan merutekan lalu lintas di subnet pribadi ke perangkat NAT. Sementara lalu lintas ke Amazon S3 atau DynamoDB melintasi gateway internet, itu tidak meninggalkan jaringan. AWS



Akses melalui titik akhir gateway

Diagram berikut menunjukkan cara instance mengakses Amazon S3 dan DynamoDB melalui titik akhir gateway. Lalu lintas dari VPC Anda ke Amazon S3 atau DynamoDB dirutekan ke titik akhir gateway. Setiap tabel rute subnet harus memiliki rute yang mengirimkan lalu lintas yang ditujukan untuk layanan ke titik akhir gateway menggunakan daftar awalan untuk layanan. Untuk informasi selengkapnya, lihat daftar awalan AWS-terkelola di Panduan Pengguna Amazon VPC.



Perutean

Saat Anda membuat titik akhir gateway, Anda memilih tabel rute VPC untuk subnet yang Anda aktifkan. Rute berikut secara otomatis ditambahkan ke setiap tabel rute yang Anda pilih. Tujuan adalah daftar awalan untuk layanan yang dimiliki oleh AWS dan targetnya adalah titik akhir gateway.

Destinasi	Target
prefix_list_id	*gateway_endpoint_id*

Pertimbangan-pertimbangan

- Anda dapat meninjau rute titik akhir yang kami tambahkan ke tabel rute Anda, tetapi Anda tidak dapat memodifikasi atau menghapusnya. Untuk menambahkan rute titik akhir ke tabel rute, kaitkan dengan titik akhir gateway. Kami menghapus rute titik akhir saat Anda memisahkan tabel rute dari titik akhir gateway atau saat Anda menghapus titik akhir gateway.

- Semua instance dalam subnet yang terkait dengan tabel rute yang terkait dengan titik akhir gateway secara otomatis menggunakan titik akhir gateway untuk mengakses layanan. Instance dalam subnet yang tidak terkait dengan tabel rute ini menggunakan titik akhir layanan publik, bukan titik akhir gateway.
- Tabel rute dapat memiliki rute titik akhir ke Amazon S3 dan rute titik akhir ke DynamoDB. Anda dapat memiliki rute titik akhir ke layanan yang sama (Amazon S3 atau DynamoDB) di beberapa tabel rute. Anda tidak dapat memiliki beberapa rute titik akhir ke layanan yang sama (Amazon S3 atau DynamoDB) dalam satu tabel rute.
- Kami menggunakan rute paling spesifik yang cocok dengan lalu lintas untuk menentukan cara merutekan lalu lintas (kecocokan awalan terpanjang). Untuk tabel rute dengan rute titik akhir, ini berarti sebagai berikut:
  - Jika ada rute yang mengirimkan semua lalu lintas internet (0.0.0. 0/0) ke gateway internet, rute titik akhir diutamakan untuk lalu lintas yang ditujukan untuk layanan (Amazon S3 atau DynamoDB) di Wilayah saat ini. Lalu lintas yang ditujukan untuk yang berbeda Layanan AWS menggunakan gateway internet.
  - Lalu lintas yang ditujukan untuk layanan (Amazon S3 atau DynamoDB) di Wilayah lain masuk ke gateway internet karena daftar awalan khusus untuk Wilayah.
  - Jika ada rute yang menentukan rentang alamat IP yang tepat untuk layanan (Amazon S3 atau DynamoDB) di Wilayah yang sama, rute tersebut lebih diutamakan daripada rute titik akhir.

Keamanan

Saat instans Anda mengakses Amazon S3 atau DynamoDB melalui titik akhir gateway, instans mengakses layanan menggunakan titik akhir publiknya. Grup keamanan untuk contoh ini harus mengizinkan lalu lintas ke dan dari layanan. Berikut ini adalah contoh aturan outbound. Ini mereferensikan ID daftar awalan untuk layanan.

Destinasi	Protokol	Rentang port
prefix_list_id	TCP	443

ACL jaringan untuk subnet untuk instance ini juga harus memungkinkan lalu lintas ke dan dari layanan. Berikut ini adalah contoh aturan outbound. Anda tidak dapat mereferensikan daftar awalan dalam aturan ACL jaringan, tetapi Anda bisa mendapatkan rentang alamat IP untuk layanan dari daftar awalannya.

Destinasi	Protokol	Rentang port
service_cidr_block_1	TCP	443
service_cidr_block_2	TCP	443
service_cidr_block_3	TCP	443

Jenis alamat IP

Jenis alamat IP menentukan daftar awalan mana yang terkait dengan tabel rute Anda.

Persyaratan untuk mengaktifkan IPv6 untuk titik akhir gateway

- Jenis alamat IP dari titik akhir gateway harus kompatibel dengan subnet untuk titik akhir gateway, seperti yang dijelaskan di sini:
  - IPv4 - Tambahkan daftar awalan IPv4 layanan ke tabel rute Anda.
  - IPv6 - Tambahkan daftar awalan IPv6 layanan ke tabel rute Anda. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6.
  - Dualstack - Tambahkan daftar awalan IPv4 layanan ke tabel rute Anda dan tambahkan daftar awalan IPv6 layanan ke tabel rute Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6.

Jenis IP catatan DNS

Secara default, titik akhir gateway mengembalikan catatan DNS berdasarkan titik akhir layanan yang Anda panggil. Jika Anda membuat titik akhir gateway menggunakan titik akhir layanan IPv4, seperti, Amazon `s3.us-east-2.amazonaws.com` S3 mengembalikan catatan A ke klien Anda, dan semua subnet dalam tabel rute Anda menggunakan IPv4.

Sebaliknya, jika Anda membuat titik akhir gateway menggunakan endpoint layanan dualstack, seperti, Amazon `s3.dualstack.us-east-2.amazonaws.com` S3 mengembalikan catatan A dan AAAA ke klien Anda, dan subnet dalam tabel rute Anda menggunakan IPv4 dan IPv6.

> **Note**
>
> Untuk bucket direktori, atau S3 Express One Zone, titik akhir gateway untuk bidang data akan menjadi `s3express-use2-az1.us-east-2.amazonaws.com` dan masing-masing. `s3express-use2-az1.dualstack.us-east-2.amazonaws.com`

Jenis IP rekaman DNS memengaruhi cara lalu lintas diarahkan ke klien Anda. Jika Anda membuat titik akhir gateway menggunakan titik akhir layanan IPv4 dan kemudian memanggil titik akhir layanan dualstack, lalu lintas yang menggunakan catatan AAAA tidak akan dirutekan melalui titik akhir gateway. Lalu lintas akan dijatuhkan atau diarahkan melalui IPv6-compatible jalur jika ada. Jika Anda menggunakan jenis IP rekaman DNS yang ditentukan layanan, pastikan layanan Anda dapat menangani panggilan variabel dari beberapa titik akhir layanan.

Alih-alih pengaturan tipe IP rekaman DNS default yang ditentukan layanan, Anda dapat menyesuaikan jenis IP rekaman DNS untuk memilih catatan mana yang dikembalikan untuk titik akhir tertentu. Tabel berikut menunjukkan jenis IP rekaman DNS yang didukung dan jenis rekaman yang dikembalikan:

Jenis IP catatan DNS	Jenis catatan yang dikembalikan
IPv4	A
IPv6	AAAA
Tumpukan ganda	A dan AAAA
ditetapkan layanan	Catatan tergantung pada titik akhir layanan

Untuk memilih jenis IP rekaman DNS, Anda harus menggunakan jenis alamat IP yang kompatibel untuk layanan titik akhir. Tabel berikut menunjukkan jenis IP rekaman DNS yang didukung untuk setiap jenis alamat IP untuk titik akhir gateway:

Jenis alamat IP	Jenis IP rekaman DNS yang didukung
IPv4	IPv4, ditentukan layanan*
IPv6	IPv6, ditentukan layanan*

Jenis alamat IP	Jenis IP rekaman DNS yang didukung
Tumpukan ganda	IPv4, IPv6, Dualstack, ditentukan layanan*

* Merupakan tipe IP catatan DNS default.

> **Note**
>
> Untuk menggunakan jenis IP rekaman DNS selain yang ditentukan layanan untuk titik akhir Gateway Anda, Anda harus mengizinkan `enableDnsSupport` dan atribut `enableDnsHostnames` dalam pengaturan VPC Anda.

Anda tidak dapat mengubah jenis IP rekaman DNS untuk titik akhir gateway DynamoDB. DynamoDB hanya mendukung jenis IP rekaman DNS yang ditentukan layanan.

Perilaku tipe IP rekaman DNS berbeda untuk titik akhir antarmuka. Untuk informasi selengkapnya, lihat Jenis IP rekaman DNS untuk titik akhir antarmuka.

Titik akhir gateway untuk Amazon S3

Anda dapat mengakses Amazon S3 dari VPC menggunakan titik akhir VPC gateway. Setelah membuat titik akhir gateway, Anda dapat menambahkannya sebagai target di tabel rute untuk lalu lintas yang ditujukan dari VPC Anda ke Amazon S3.

Tidak dikenakan biaya tambahan untuk menggunakan titik akhir gateway.

Amazon S3 mendukung titik akhir gateway dan titik akhir antarmuka. Dengan titik akhir gateway, Anda dapat mengakses Amazon S3 dari VPC Anda, tanpa memerlukan gateway internet atau perangkat NAT untuk VPC Anda, dan tanpa biaya tambahan. Namun, titik akhir gateway tidak mengizinkan akses dari jaringan lokal, dari VPC peered di AWS Wilayah lain, atau melalui gateway transit. Untuk skenario tersebut, Anda harus menggunakan titik akhir antarmuka, yang tersedia dengan biaya tambahan. Untuk informasi selengkapnya, lihat Jenis titik akhir VPC untuk Amazon S3 di Panduan Pengguna Amazon S3.

Daftar Isi

- DNS privat
- Buat titik akhir gateway
- Kontrol akses menggunakan kebijakan bucket
- Tabel rute asosiasi
- Edit kebijakan titik akhir VPC
- Hapus titik akhir gateway

Pertimbangan-pertimbangan

- Titik akhir gateway hanya tersedia di Wilayah tempat Anda membuatnya. Pastikan untuk membuat titik akhir gateway Anda di Wilayah yang sama dengan bucket S3 Anda.
- Jika Anda menggunakan server DNS Amazon, Anda harus mengaktifkan nama host DNS dan resolusi DNS untuk VPC Anda. Jika Anda menggunakan server DNS Anda sendiri, pastikan bahwa permintaan ke Amazon S3 diselesaikan dengan benar ke alamat IP yang dikelola oleh. AWS
- Aturan untuk grup keamanan untuk instans Anda yang mengakses Amazon S3 melalui titik akhir gateway harus mengizinkan lalu lintas ke dan dari Amazon S3. Anda dapat mereferensikan ID daftar awalan untuk Amazon S3 dalam aturan grup keamanan.
- ACL jaringan untuk subnet untuk instans Anda yang mengakses Amazon S3 melalui titik akhir gateway harus mengizinkan lalu lintas ke dan dari Amazon S3. Anda tidak dapat mereferensikan daftar awalan dalam aturan ACL jaringan, tetapi Anda bisa mendapatkan rentang alamat IP untuk Amazon S3 dari daftar awalan untuk Amazon S3.
- Periksa apakah Anda menggunakan Layanan AWS yang memerlukan akses ke bucket S3. Misalnya, layanan mungkin memerlukan akses ke bucket yang berisi file log, atau mungkin mengharuskan Anda mengunduh driver atau agen ke instans EC2 Anda. Jika demikian, pastikan bahwa kebijakan titik akhir Anda mengizinkan sumber daya Layanan AWS atau mengakses bucket ini menggunakan tindakan. `s3:GetObject`
- Anda tidak dapat menggunakan `aws:SourceIp` kondisi dalam kebijakan identitas atau kebijakan bucket untuk permintaan ke Amazon S3 yang melintasi titik akhir VPC. Sebaliknya, gunakan `aws:VpcSourceIp` kondisinya. Atau, Anda dapat menggunakan tabel rute untuk mengontrol instans EC2 mana yang dapat mengakses Amazon S3 melalui titik akhir VPC.
- Sumber alamat IPv4 atau IPv6 dari instans di subnet Anda yang terpengaruh seperti yang diterima oleh Amazon S3 berubah dari alamat publik ke alamat pribadi di VPC Anda. Titik akhir mengalihkan rute jaringan, dan memutus koneksi TCP terbuka. Koneksi sebelumnya yang menggunakan alamat publik tidak dilanjutkan. Kami menyarankan agar Anda tidak menjalankan

tugas penting apa pun saat membuat atau memodifikasi titik akhir; atau Anda menguji untuk memastikan bahwa perangkat lunak Anda dapat terhubung kembali secara otomatis ke Amazon S3 setelah koneksi putus.

- Koneksi titik akhir tidak dapat diperpanjang dari VPC. Sumber daya di sisi lain koneksi VPN, koneksi peering VPC, gateway transit, atau Direct Connect koneksi di VPC Anda tidak dapat menggunakan titik akhir gateway untuk berkomunikasi dengan Amazon S3.
- Akun Anda memiliki kuota default 20 titik akhir gateway per Wilayah, yang dapat disesuaikan. Ada juga batas 255 titik akhir gateway per VPC.

DNS privat

Anda dapat mengonfigurasi DNS pribadi untuk mengoptimalkan biaya saat membuat titik akhir gateway dan titik akhir antarmuka untuk Amazon S3.

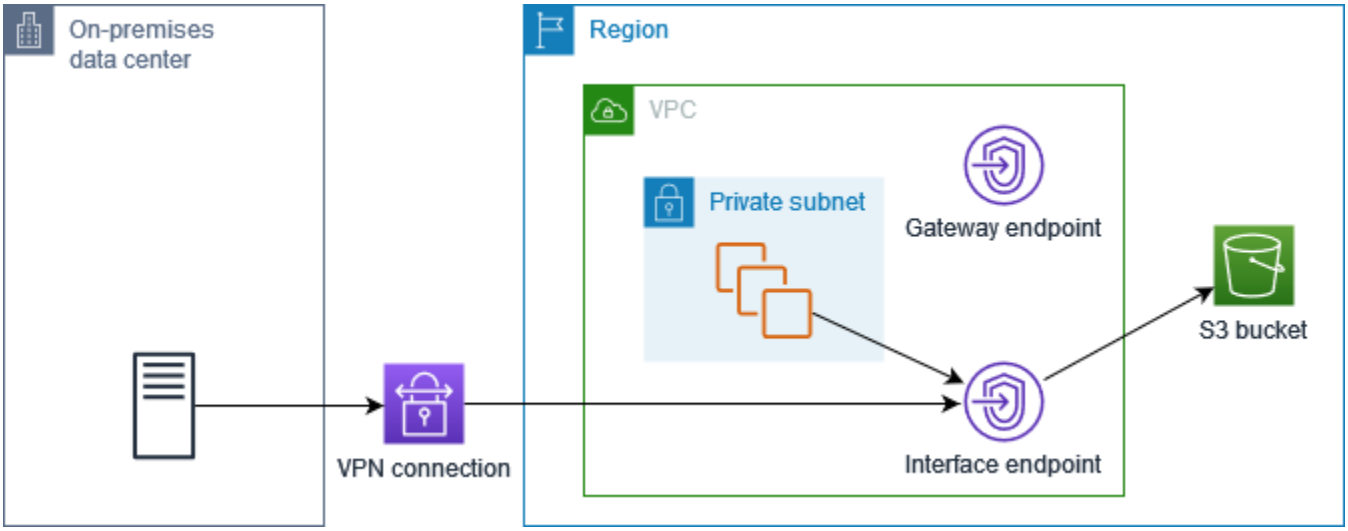
Resolver Rute 53

Amazon menyediakan server DNS, yang disebut Resolver Route 53, untuk VPC Anda. Resolver Route 53 secara otomatis menyelesaikan nama domain dan catatan VPC lokal di zona host pribadi. Namun, Anda tidak dapat menggunakan Resolver Route 53 dari luar VPC Anda. Route 53 menyediakan titik akhir Resolver dan aturan Resolver sehingga Anda dapat menggunakan Resolver Route 53 dari luar VPC Anda. Titik akhir Resolver masuk meneruskan kueri DNS dari jaringan lokal ke Resolver Route 53. Titik akhir Resolver keluar meneruskan kueri DNS dari Resolver Route 53 ke jaringan lokal.

Saat Anda mengonfigurasi titik akhir antarmuka untuk Amazon S3 agar menggunakan DNS pribadi hanya untuk titik akhir Resolver masuk, kami membuat titik akhir Resolver masuk. Titik akhir Resolver masuk menyelesaikan kueri DNS ke Amazon S3 dari lokal ke alamat IP pribadi titik akhir antarmuka. Kami juga menambahkan catatan ALIAS untuk Resolver Route 53 ke zona yang dihosting publik untuk Amazon S3, sehingga kueri DNS dari VPC Anda diselesaikan ke alamat IP publik Amazon S3, yang merutekan lalu lintas ke titik akhir gateway.

DNS privat

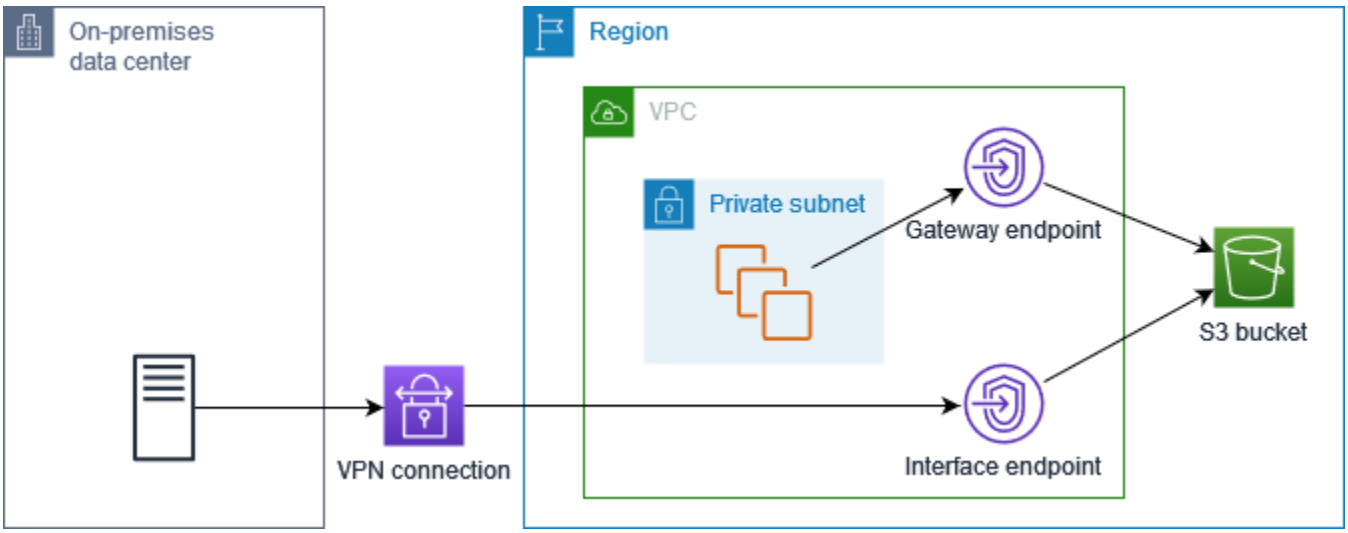
Jika Anda mengonfigurasi DNS pribadi untuk titik akhir antarmuka untuk Amazon S3 tetapi tidak mengonfigurasi DNS pribadi hanya untuk titik akhir Resolver masuk, permintaan dari jaringan lokal dan VPC menggunakan titik akhir antarmuka untuk mengakses Amazon S3. Oleh karena itu, Anda membayar untuk menggunakan titik akhir antarmuka untuk lalu lintas dari VPC, alih-alih menggunakan titik akhir gateway tanpa biaya tambahan.



DNS pribadi hanya untuk titik akhir Resolver masuk

Jika Anda mengonfigurasi DNS pribadi hanya untuk titik akhir Resolver masuk, permintaan dari jaringan lokal menggunakan titik akhir antarmuka untuk mengakses Amazon S3, dan permintaan dari VPC Anda menggunakan titik akhir gateway untuk mengakses Amazon S3. Oleh karena itu, Anda mengoptimalkan biaya Anda, karena Anda membayar untuk menggunakan titik akhir antarmuka hanya untuk lalu lintas yang tidak dapat menggunakan titik akhir gateway.

Untuk mengonfigurasi ini, jenis IP catatan DNS dari titik akhir gateway harus cocok dengan titik akhir antarmuka atau be. `service-defined` AWS PrivateLink tidak mendukung kombinasi lainnya. Untuk informasi selengkapnya, lihat the section called “Jenis IP catatan DNS”.



Konfigurasikan DNS pribadi

Anda dapat mengonfigurasi DNS pribadi untuk titik akhir antarmuka untuk Amazon S3 saat Anda membuatnya atau setelah Anda membuatnya. Untuk informasi selengkapnya, lihat the section called "Buat VPC endpoint" (konfigurasi selama pembuatan) atau the section called "Aktifkan nama DNS pribadi" (konfigurasi setelah pembuatan).

Buat titik akhir gateway

Gunakan prosedur berikut untuk membuat titik akhir gateway yang terhubung ke Amazon S3.

Untuk membuat titik akhir gateway menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Kategori layanan, pilih Layanan AWS.
5. Untuk Layanan, tambahkan filter Type = Gateway.

   Jika data Amazon S3 Anda disimpan dalam bucket tujuan umum, pilih com.amazonaws.*region*.s3.

   Jika data Amazon S3 Anda disimpan dalam bucket direktori, pilih com.amazonaws.*region*.s3express.
6. Untuk VPC, pilih VPC tempat membuat titik akhir.
7. Untuk jenis alamat IP, pilih dari opsi berikut:

   - IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan layanan menerima permintaan IPv4.
   - IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6 dan layanan menerima permintaan IPv6.
   - Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan endpoint. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6 dan layanan menerima permintaan IPv4 dan IPv6.
8. Untuk Tabel rute, pilih tabel rute yang akan digunakan oleh titik akhir. Kami secara otomatis menambahkan rute yang mengarahkan lalu lintas yang ditujukan untuk layanan ke antarmuka jaringan titik akhir.

9. Untuk Kebijakan, pilih Akses penuh untuk mengizinkan semua operasi oleh semua prinsipal di semua sumber daya melalui titik akhir VPC. Jika tidak, pilih Kustom untuk melampirkan kebijakan titik akhir VPC yang mengontrol izin yang dimiliki kepala sekolah untuk melakukan tindakan pada sumber daya melalui titik akhir VPC.
10. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
11. Pilih Buat titik akhir.

Untuk membuat titik akhir gateway menggunakan baris perintah

- buat-vpc-titik akhir ()AWS CLI
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Kontrol akses menggunakan kebijakan bucket

Anda dapat menggunakan kebijakan bucket untuk mengontrol akses ke bucket dari titik akhir tertentu, VPC, rentang alamat IP, dan. Akun AWS Contoh-contoh ini mengasumsikan bahwa ada juga pernyataan kebijakan yang memungkinkan akses yang diperlukan untuk kasus penggunaan Anda.

Example Contoh: Batasi akses ke titik akhir tertentu

Anda dapat membuat kebijakan bucket yang membatasi akses ke titik akhir tertentu dengan menggunakan kunci kondisi AWS:sourceVPCE. Kebijakan berikut menolak akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan kecuali titik akhir gateway yang ditentukan digunakan. Perhatikan bahwa kebijakan ini memblokir akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan melalui Konsol Manajemen AWS.

JSON

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

```
                "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example Contoh: Batasi akses ke VPC tertentu

Anda dapat membuat kebijakan bucket yang membatasi akses ke VPC tertentu dengan menggunakan kunci kondisi AWS:sourceVPC. Ini berguna jika Anda memiliki beberapa titik akhir yang dikonfigurasi dalam VPC yang sama. Kebijakan berikut menolak akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan kecuali permintaan tersebut berasal dari VPC yang ditentukan. Perhatikan bahwa kebijakan ini memblokir akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan melalui Konsol Manajemen AWS.

JSON

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

Example Contoh: Batasi akses ke rentang alamat IP tertentu

Anda dapat membuat kebijakan yang membatasi akses ke rentang alamat IP tertentu dengan menggunakan kunci VpcSourceIp kondisi aws:. Kebijakan berikut menolak akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan kecuali permintaan berasal dari alamat IP yang ditentukan. Perhatikan bahwa kebijakan ini memblokir akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan melalui Konsol Manajemen AWS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC-CIDR",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
    }
  ]
}
```

Example Contoh: Batasi akses ke bucket di tempat tertentu Akun AWS

Anda dapat membuat kebijakan yang membatasi akses ke bucket S3 Akun AWS secara spesifik menggunakan kunci kondisi. `s3:ResourceAccount` Kebijakan berikut menolak akses ke bucket S3 menggunakan tindakan yang ditentukan kecuali jika dimiliki oleh yang ditentukan. Akun AWS

JSON

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

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

Tabel rute asosiasi

Anda dapat mengubah tabel rute yang terkait dengan titik akhir gateway. Saat Anda mengaitkan tabel rute, kami secara otomatis menambahkan rute yang mengarahkan lalu lintas yang ditujukan untuk layanan ke antarmuka jaringan titik akhir. Saat Anda memisahkan tabel rute, kami secara otomatis menghapus rute titik akhir dari tabel rute.

Untuk mengaitkan tabel rute menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Kelola tabel rute.
5. Pilih atau batalkan pilihan tabel rute sesuai kebutuhan.
6. Pilih Ubah tabel rute.

Untuk mengaitkan tabel rute menggunakan baris perintah

- memodifikasi-vpc-titik akhir ()AWS CLI
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Edit kebijakan titik akhir VPC

Anda dapat mengedit kebijakan titik akhir untuk titik akhir gateway, yang mengontrol akses ke Amazon S3 dari VPC melalui titik akhir. Setelah memperbarui kebijakan titik akhir, perlu beberapa menit agar perubahan diterapkan. Kebijakan default memungkinkan akses penuh. Untuk informasi selengkapnya, lihat Kebijakan titik akhir.

Untuk mengubah kebijakan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Kelola kebijakan.
5. Pilih Akses Penuh untuk mengizinkan akses penuh ke layanan, atau pilih Kustom dan lampirkan kebijakan kustom.
6. Pilih Simpan.

Berikut ini adalah contoh kebijakan endpoint untuk mengakses Amazon S3.

Example Contoh: Batasi akses ke bucket tertentu

Anda dapat membuat kebijakan yang membatasi akses ke bucket S3 tertentu saja. Ini berguna jika Anda memiliki yang lain Layanan AWS di VPC Anda yang menggunakan bucket S3.

JSON

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

```
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
      ]
    }
  ]
}
```

Example Contoh: Batasi akses ke peran IAM tertentu

Anda dapat membuat kebijakan yang membatasi akses ke peran IAM tertentu. Anda harus menggunakan `aws:PrincipalArn` untuk memberikan akses ke kepala sekolah.

JSON

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

Example Contoh: Batasi akses ke pengguna di akun tertentu

Anda dapat membuat kebijakan yang membatasi akses ke akun tertentu.

JSON

```
{
```

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

Hapus titik akhir gateway

Setelah selesai dengan titik akhir gateway, Anda dapat menghapusnya. Saat Anda menghapus titik akhir gateway, kami menghapus rute titik akhir dari tabel rute subnet.

Anda tidak dapat menghapus titik akhir gateway jika DNS pribadi diaktifkan.

Untuk menghapus titik akhir gateway menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta mengonfirmasi, pilih **delete**.
6. Pilih Hapus.

Untuk menghapus titik akhir gateway menggunakan baris perintah

- hapus-vpc-titik akhir ()AWS CLI
- Remove-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Titik akhir Gateway untuk Amazon DynamoDB

Anda dapat mengakses Amazon DynamoDB dari VPC Anda menggunakan titik akhir VPC gateway. Setelah Anda membuat titik akhir gateway, Anda dapat menambahkannya sebagai target dalam tabel rute Anda untuk lalu lintas yang ditujukan dari VPC Anda ke DynamoDB.

Tidak dikenakan biaya tambahan untuk menggunakan titik akhir gateway.

DynamoDB mendukung titik akhir gateway dan titik akhir antarmuka. Dengan titik akhir gateway, Anda dapat mengakses DynamoDB dari VPC Anda, tanpa memerlukan gateway internet atau perangkat NAT untuk VPC Anda, dan tanpa biaya tambahan. Namun, titik akhir gateway tidak mengizinkan akses dari jaringan lokal, dari VPC peered di AWS Wilayah lain, atau melalui gateway transit. Untuk skenario tersebut, Anda harus menggunakan titik akhir antarmuka, yang tersedia dengan biaya tambahan. Untuk informasi selengkapnya, lihat Jenis titik akhir VPC untuk DynamoDB di Panduan Pengembang Amazon DynamoDB.

Daftar Isi

Pertimbangan-pertimbangan

- Titik akhir gateway hanya tersedia di Wilayah tempat Anda membuatnya. Pastikan untuk membuat titik akhir gateway Anda di Wilayah yang sama dengan tabel DynamoDB Anda.
- Jika Anda menggunakan server DNS Amazon, Anda harus mengaktifkan nama host DNS dan resolusi DNS untuk VPC Anda. Jika Anda menggunakan server DNS Anda sendiri, pastikan bahwa permintaan ke DynamoDB diselesaikan dengan benar ke alamat IP yang dikelola oleh. AWS
- Aturan untuk grup keamanan untuk instance Anda yang mengakses DynamoDB melalui titik akhir gateway harus mengizinkan lalu lintas ke dan dari DynamoDB. Anda dapat mereferensikan ID daftar awalan untuk DynamoDB dalam aturan grup keamanan.
- ACL jaringan untuk subnet untuk instance Anda yang mengakses DynamoDB melalui titik akhir gateway harus mengizinkan lalu lintas ke dan dari DynamoDB. Anda tidak dapat mereferensikan

daftar awalan dalam aturan ACL jaringan, tetapi Anda bisa mendapatkan rentang alamat IP untuk DynamoDB dari daftar awalan untuk DynamoDB.

- Jika Anda menggunakan AWS CloudTrail untuk mencatat operasi DynamoDB, file log berisi alamat IP pribadi instans EC2 di VPC konsumen layanan dan ID titik akhir gateway untuk setiap permintaan yang dilakukan melalui titik akhir.
- Titik akhir Gateway hanya mendukung lalu lintas IPv4.
- Alamat IPv4 sumber dari instance di subnet Anda yang terpengaruh berubah dari alamat IPv4 publik ke alamat IPv4 pribadi dari VPC Anda. Titik akhir mengalihkan rute jaringan dan memutus koneksi TCP terbuka. Koneksi sebelumnya yang menggunakan alamat IPv4 publik tidak dilanjutkan. Sebaiknya Anda tidak menjalankan tugas penting saat membuat atau memodifikasi titik akhir gateway. Atau, uji untuk memastikan bahwa perangkat lunak Anda dapat secara otomatis terhubung kembali ke DynamoDB jika koneksi terputus.
- Koneksi titik akhir tidak dapat diperpanjang dari VPC. Sumber daya di sisi lain koneksi VPN, koneksi peering VPC, gateway transit, atau Direct Connect koneksi di VPC Anda tidak dapat menggunakan titik akhir gateway untuk berkomunikasi dengan DynamoDB.
- Akun Anda memiliki kuota default 20 titik akhir gateway per Wilayah, yang dapat disesuaikan. Ada juga batas 255 titik akhir gateway per VPC.

Buat titik akhir gateway

Gunakan prosedur berikut untuk membuat titik akhir gateway yang terhubung ke DynamoDB.

Untuk membuat titik akhir gateway menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Kategori layanan, pilih Layanan AWS.
5. Untuk Layanan, tambahkan filter Type = Gateway dan pilih com.amazonaws. *region*.dinamodb.
6. Untuk VPC, pilih VPC tempat membuat titik akhir.
7. Untuk Tabel rute, pilih tabel rute yang akan digunakan oleh titik akhir. Kami secara otomatis menambahkan rute yang mengarahkan lalu lintas yang ditujukan untuk layanan ke antarmuka jaringan titik akhir.
8. Untuk Kebijakan, pilih Akses penuh untuk mengizinkan semua operasi oleh semua prinsipal di semua sumber daya melalui titik akhir VPC. Jika tidak, pilih Kustom untuk melampirkan kebijakan

titik akhir VPC yang mengontrol izin yang dimiliki kepala sekolah untuk melakukan tindakan pada sumber daya melalui titik akhir VPC.

9. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
10. Pilih Buat titik akhir.

Untuk membuat titik akhir gateway menggunakan baris perintah

- buat-vpc-titik akhir ()AWS CLI
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Kontrol akses menggunakan kebijakan IAM

Anda dapat membuat kebijakan IAM untuk mengontrol prinsipal IAM mana yang dapat mengakses tabel DynamoDB menggunakan titik akhir VPC tertentu.

Example Contoh: Batasi akses ke titik akhir tertentu

Anda dapat membuat kebijakan yang membatasi akses ke titik akhir VPC tertentu dengan menggunakan kunci kondisi AWS:sourceVPCE. Kebijakan berikut menolak akses ke tabel DynamoDB di akun kecuali titik akhir VPC yang ditentukan digunakan. Contoh ini mengasumsikan bahwa ada juga pernyataan kebijakan yang memungkinkan akses yang diperlukan untuk kasus penggunaan Anda.

JSON

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

```
            }
        }
    ]
}
```

Example Contoh: Izinkan akses dari peran IAM tertentu

Anda dapat membuat kebijakan yang mengizinkan akses menggunakan peran IAM tertentu. Kebijakan berikut memberikan akses ke peran IAM yang ditentukan.

JSON

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

Example Contoh: Memungkinkan akses dari akun tertentu

Anda dapat membuat kebijakan yang mengizinkan akses dari akun tertentu saja. Kebijakan berikut memberikan akses ke pengguna di akun yang ditentukan.

JSON

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

```
   "Statement": [
      {
         "Sid": "Allow-access-from-account",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "aws:PrincipalAccount": "111122223333"
            }
         }
      }
   ]
}
```

Tabel rute asosiasi

Anda dapat mengubah tabel rute yang terkait dengan titik akhir gateway. Saat Anda mengaitkan tabel rute, kami secara otomatis menambahkan rute yang mengarahkan lalu lintas yang ditujukan untuk layanan ke antarmuka jaringan titik akhir. Saat Anda memisahkan tabel rute, kami secara otomatis menghapus rute titik akhir dari tabel rute.

Untuk mengaitkan tabel rute menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Kelola tabel rute.
5. Pilih atau batalkan pilihan tabel rute sesuai kebutuhan.
6. Pilih Ubah tabel rute.

Untuk mengaitkan tabel rute menggunakan baris perintah

- memodifikasi-vpc-titik akhir ()AWS CLI
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Edit kebijakan titik akhir VPC

Anda dapat mengedit kebijakan titik akhir untuk titik akhir gateway, yang mengontrol akses ke DynamoDB dari VPC melalui titik akhir. Setelah memperbarui kebijakan titik akhir, perlu beberapa menit agar perubahan diterapkan. Kebijakan default memungkinkan akses penuh. Untuk informasi selengkapnya, lihat Kebijakan titik akhir.

Untuk mengubah kebijakan titik akhir menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Kelola kebijakan.
5. Pilih Akses Penuh untuk mengizinkan akses penuh ke layanan, atau pilih Kustom dan lampirkan kebijakan kustom.
6. Pilih Simpan.

Untuk memodifikasi titik akhir gateway menggunakan baris perintah

- memodifikasi-vpc-titik akhir ()AWS CLI
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Berikut ini adalah contoh kebijakan endpoint untuk mengakses DynamoDB.

Example Contoh: Izinkan akses hanya-baca

Anda dapat membuat kebijakan yang membatasi akses ke akses hanya-baca. Kebijakan berikut memberikan izin untuk membuat daftar dan mendeskripsikan tabel DynamoDB.

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

```
      ],
      "Resource": "*"
    }
  ]
}
```

Example Contoh: Batasi akses ke tabel tertentu

Anda dapat membuat kebijakan yang membatasi akses ke tabel DynamoDB tertentu. Kebijakan berikut memungkinkan akses ke tabel DynamoDB yang ditentukan.

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

Hapus titik akhir gateway

Setelah selesai dengan titik akhir gateway, Anda dapat menghapusnya. Saat Anda menghapus titik akhir gateway, kami menghapus rute titik akhir dari tabel rute subnet.

Untuk menghapus titik akhir gateway menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir gateway.
4. Pilih Tindakan, Hapus titik akhir VPC.

5. Saat diminta mengonfirmasi, pilih **delete**.
6. Pilih Hapus.

Untuk menghapus titik akhir gateway menggunakan baris perintah

- hapus-vpc-titik akhir ()AWS CLI
- Remove-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Akses produk SaaS melalui AWS PrivateLink

Dengan menggunakan AWS PrivateLink, Anda dapat mengakses produk SaaS secara pribadi, seolah-olah mereka berjalan di VPC Anda sendiri.

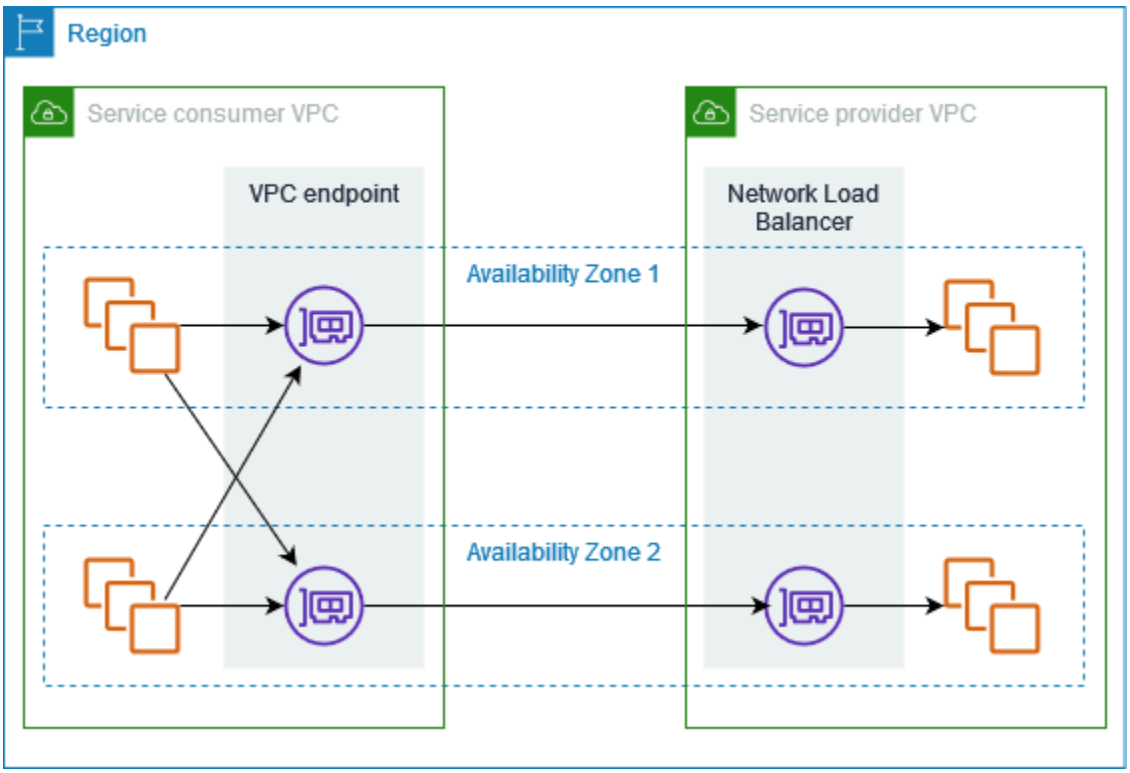
Daftar Isi

Ikhtisar

Anda dapat menemukan, membeli, dan menyediakan produk SaaS yang didukung oleh melalui AWS PrivateLink . AWS Marketplace Untuk informasi selengkapnya, lihat Mengakses aplikasi SaaS secara aman dan pribadi. AWS PrivateLink

Anda juga dapat menemukan produk SaaS yang didukung oleh AWS PrivateLink dari AWS Mitra. Untuk informasi lebih lanjut, lihat AWS PrivateLink Mitra.

Diagram berikut menunjukkan bagaimana Anda menggunakan titik akhir VPC untuk terhubung ke produk SaaS. Penyedia layanan membuat layanan endpoint dan memberikan pelanggan mereka akses ke layanan endpoint. Sebagai konsumen layanan, Anda membuat titik akhir VPC antarmuka, yang membuat koneksi antara satu atau lebih subnet di VPC Anda dan layanan endpoint.



Membuat sebuah titik akhir antarmuka

Gunakan prosedur berikut untuk membuat titik akhir VPC antarmuka yang terhubung ke produk SaaS.

Persyaratan

Berlangganan layanan.

Untuk membuat titik akhir antarmuka ke layanan mitra

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Jika Anda membeli layanan dari AWS Marketplace, lakukan hal berikut:
    a. Untuk Jenis, pilih AWS Marketplace layanan.
    b. Pilih layanan.
5. Jika Anda berlangganan layanan dengan penunjukan Siap AWS Layanan, lakukan hal berikut:

a. Untuk Jenis, pilih Layanan mitra PrivateLink siap pakai.

b. Masukkan nama layanan, lalu pilih Verifikasi layanan.

6. Untuk VPC, pilih VPC dari mana Anda akan mengakses produk.
7. Untuk Subnet, pilih subnet untuk membuat antarmuka jaringan titik akhir.
8. Untuk grup Keamanan, pilih grup keamanan untuk dikaitkan dengan antarmuka jaringan titik akhir. Aturan grup keamanan harus mengizinkan lalu lintas antara sumber daya di VPC dan antarmuka jaringan titik akhir.
9. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
10. Pilih Buat titik akhir.

Untuk mengkonfigurasi titik akhir antarmuka

Untuk informasi tentang mengonfigurasi titik akhir antarmuka Anda, lihat. the section called “Konfigurasikan titik akhir antarmuka”

Akses peralatan virtual melalui AWS PrivateLink

Anda dapat menggunakan Load Balancer Gateway untuk mendistribusikan lalu lintas ke armada peralatan virtual jaringan. Peralatan dapat digunakan untuk inspeksi keamanan, kepatuhan, kontrol kebijakan, dan layanan jaringan lainnya. Anda menentukan Load Balancer Gateway saat membuat layanan endpoint VPC. AWS Prinsipal lain mengakses layanan endpoint dengan membuat titik akhir Gateway Load Balancer.

Harga

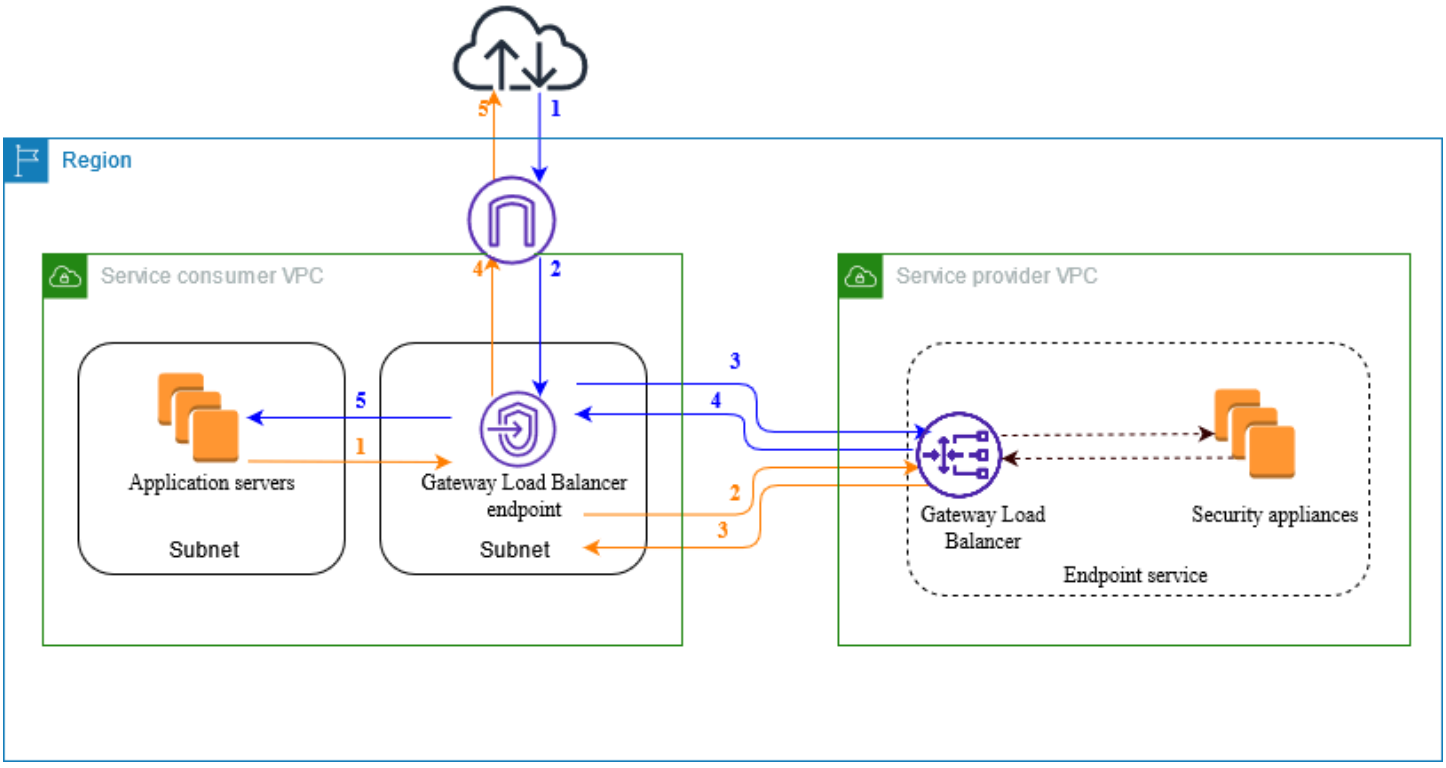
Anda ditagih untuk setiap jam dimana titik akhir Load Balancer Gateway Anda disediakan di setiap Availability Zone. Anda juga ditagih per GB data yang diproses. Untuk informasi selengkapnya, silakan lihat AWS PrivateLink Harga.

Daftar Isi

Untuk informasi selengkapnya, lihat Gateway Load Balancers.

Ikhtisar

Diagram berikut menunjukkan bagaimana server aplikasi mengakses peralatan keamanan melalui AWS PrivateLink. Server aplikasi berjalan di subnet dari VPC konsumen layanan. Anda membuat titik akhir Load Balancer Gateway di subnet lain dari VPC yang sama. Semua lalu lintas yang memasuki VPC konsumen layanan melalui gateway internet pertama-tama diarahkan ke titik akhir Gateway Load Balancer untuk diperiksa dan kemudian diarahkan ke subnet tujuan. Demikian pula, semua lalu lintas yang meninggalkan server aplikasi dialihkan ke titik akhir Gateway Load Balancer untuk diperiksa sebelum dialihkan kembali melalui gateway internet.



Lalu lintas dari internet ke server aplikasi (panah biru):

1. Lalu lintas memasuki VPC konsumen layanan melalui gateway internet.
2. Lalu lintas dikirim ke titik akhir Load Balancer Gateway, berdasarkan konfigurasi tabel rute.
3. Lalu lintas dikirim ke Load Balancer Gateway untuk diperiksa melalui alat keamanan.
4. Lalu lintas dikirim kembali ke titik akhir Load Balancer Gateway setelah pemeriksaan.
5. Lalu lintas dikirim ke server aplikasi, berdasarkan konfigurasi tabel rute.

Lalu lintas dari server aplikasi ke internet (panah oranye):

1. Lalu lintas dikirim ke titik akhir Load Balancer Gateway, berdasarkan konfigurasi tabel rute.
2. Lalu lintas dikirim ke Load Balancer Gateway untuk diperiksa melalui alat keamanan.
3. Lalu lintas dikirim kembali ke titik akhir Load Balancer Gateway setelah pemeriksaan.
4. Lalu lintas dikirim ke gateway internet berdasarkan konfigurasi tabel rute.
5. Lalu lintas dialihkan kembali ke internet.

Jenis alamat IP

Penyedia layanan dapat membuat titik akhir layanan mereka tersedia untuk konsumen layanan melalui IPv4, IPv6, atau IPv4 dan IPv6, bahkan jika peralatan keamanan mereka hanya mendukung IPv4. Jika Anda mengaktifkan dukungan dualstack, konsumen yang ada dapat terus menggunakan IPv4 untuk mengakses layanan Anda dan konsumen baru dapat memilih untuk menggunakan IPv6 untuk mengakses layanan Anda.

Jika titik akhir Load Balancer Gateway mendukung IPv4, antarmuka jaringan endpoint memiliki alamat IPv4. Jika titik akhir Load Balancer Gateway mendukung IPv6, antarmuka jaringan endpoint memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Jika Anda mendeskripsikan antarmuka jaringan endpoint dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Persyaratan untuk mengaktifkan IPv6 untuk layanan endpoint

- VPC dan subnet untuk layanan endpoint harus memiliki blok CIDR IPv6 terkait.
- Load Balancer Gateway untuk layanan endpoint harus menggunakan tipe alamat IP dualstack. Peralatan keamanan tidak perlu mendukung lalu lintas IPv6.

Persyaratan untuk mengaktifkan IPv6 untuk titik akhir Load Balancer Gateway

- Layanan endpoint harus memiliki jenis alamat IP yang mencakup dukungan IPv6.
- Jenis alamat IP dari titik akhir Load Balancer Gateway harus kompatibel dengan subnet untuk titik akhir Gateway Load Balancer, seperti yang dijelaskan di sini:
  - IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4.
  - IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6.
  - Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan endpoint Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6.
- Tabel rute untuk subnet di VPC konsumen layanan harus merutekan lalu lintas IPv6 dan ACL jaringan untuk subnet ini harus memungkinkan lalu lintas IPv6.

Perutean

Untuk merutekan lalu lintas ke layanan endpoint, tentukan titik akhir Load Balancer Gateway sebagai target dalam tabel rute Anda, menggunakan ID-nya. Untuk diagram di atas, tambahkan rute ke tabel rute sebagai berikut. Saat menggunakan titik akhir Load Balancer Gateway sebagai target, Anda tidak dapat menentukan daftar awalan sebagai tujuan. Dalam tabel ini, rute IPv6 disertakan untuk konfigurasi dualstack.

Tabel rute untuk gateway internet

Tabel rute ini harus memiliki rute yang mengirimkan lalu lintas yang ditujukan untuk server aplikasi ke titik akhir Load Balancer Gateway.

Destinasi	Target
VPC IPv4 CIDR	Lokal:
VPC IPv6 CIDR	Lokal:
Application subnet IPv4 CIDR	*vpc-endpoint-id*
Application subnet IPv6 CIDR	*vpc-endpoint-id*

Tabel rute untuk subnet dengan server aplikasi

Tabel rute ini harus memiliki rute yang mengirimkan semua lalu lintas dari server aplikasi ke titik akhir Load Balancer Gateway.

Destinasi	Target
VPC IPv4 CIDR	Lokal:
VPC IPv6 CIDR	Lokal:
0.0.0. 0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Tabel rute untuk subnet dengan titik akhir Gateway Load Balancer

Tabel rute ini harus mengirim lalu lintas yang dikembalikan dari inspeksi ke tujuan akhirnya. Untuk lalu lintas yang berasal dari internet, rute lokal mengirimkan lalu lintas ke server aplikasi. Untuk lalu lintas yang berasal dari server aplikasi, tambahkan rute yang mengirimkan semua lalu lintas ke gateway internet.

Destinasi	Target
VPC IPv4 CIDR	Lokal:
VPC IPv6 CIDR	Lokal:
0.0.0. 0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

Membuat sistem inspeksi sebagai layanan titik akhir Load Balancer Gateway

Anda dapat membuat layanan Anda sendiri yang didukung oleh AWS PrivateLink, yang dikenal sebagai layanan endpoint. Anda adalah penyedia layanan, dan AWS prinsip yang membuat koneksi ke layanan Anda adalah konsumen layanan.

Layanan endpoint memerlukan Network Load Balancer atau Gateway Load Balancer. Dalam hal ini, Anda akan membuat layanan endpoint menggunakan Load Balancer Gateway. Untuk informasi selengkapnya tentang membuat layanan endpoint menggunakan Network Load Balancer, lihat. Buat layanan endpoint

Daftar Isi

Pertimbangan-pertimbangan

- Layanan endpoint tersedia di Wilayah tempat Anda membuatnya.

- Ketika konsumen layanan mengambil informasi tentang layanan endpoint, mereka hanya dapat melihat Availability Zone yang mereka miliki bersama dengan penyedia layanan. Ketika penyedia layanan dan konsumen layanan berada di akun yang berbeda, nama Availability Zone, sepertius-east-1a, mungkin dipetakan ke Availability Zone fisik yang berbeda di masing-masing Akun AWS akun. Anda dapat menggunakan ID AZ untuk secara konsisten mengidentifikasi Availability Zone untuk layanan Anda. Untuk informasi selengkapnya, lihat ID AZ di Panduan Pengguna Amazon EC2.
- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat AWS PrivateLink kuota.

Prasyarat

- Buat VPC penyedia layanan dengan setidaknya dua subnet di Availability Zone di mana layanan harus tersedia. Satu subnet adalah untuk instance alat keamanan dan yang lainnya untuk Load Balancer Gateway.
- Buat Load Balancer Gateway di VPC penyedia layanan Anda. Jika Anda berencana untuk mengaktifkan dukungan IPv6 pada layanan endpoint Anda, Anda harus mengaktifkan dukungan dualstack pada Load Balancer Gateway Anda. Untuk informasi selengkapnya, lihat Memulai dengan Gateway Load Balancers.
- Luncurkan peralatan keamanan di VPC penyedia layanan dan daftarkan ke grup target penyeimbang beban.

Buat layanan endpoint

Gunakan prosedur berikut untuk membuat layanan endpoint menggunakan Load Balancer Gateway.

Untuk membuat layanan endpoint menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih Buat layanan titik akhir.
4. Untuk jenis Load balancer, pilih Gateway.
5. Untuk penyeimbang beban yang tersedia, pilih Load Balancer Gateway Anda.

6. Untuk Memerlukan penerimaan untuk titik akhir, pilih Penerimaan yang diperlukan untuk mengharuskan permintaan koneksi ke layanan titik akhir Anda diterima secara manual. Kalau tidak, mereka diterima secara otomatis.
7. Untuk jenis alamat IP yang Didukung, lakukan salah satu hal berikut:
   - Pilih IPv4 - Aktifkan layanan endpoint untuk menerima permintaan IPv4.
   - Pilih IPv6 — Aktifkan layanan endpoint untuk menerima permintaan IPv6.
   - Pilih IPv4 dan IPv6 — Aktifkan layanan endpoint untuk menerima permintaan IPv4 dan IPv6.
8. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
9. Pilih Buat.

Untuk membuat layanan endpoint menggunakan baris perintah

- buat-vpc-endpoint-service-configuration ()AWS CLI
- New-EC2VpcEndpointServiceConfiguration(Alat untuk Windows PowerShell)

Jadikan layanan endpoint Anda tersedia

Penyedia layanan harus melakukan hal berikut untuk membuat layanan mereka tersedia bagi konsumen layanan.

- Tambahkan izin yang memungkinkan setiap konsumen layanan terhubung ke layanan endpoint Anda. Untuk informasi selengkapnya, lihat the section called “Kelola izin”.
- Berikan konsumen layanan dengan nama layanan Anda dan Availability Zone yang didukung sehingga mereka dapat membuat titik akhir antarmuka untuk terhubung ke layanan Anda. Untuk informasi lebih lanjut, lihat prosedur di bawah ini.
- Terima permintaan koneksi titik akhir dari konsumen layanan. Untuk mengetahui informasi selengkapnya, lihat the section called “Menerima atau menolak permintaan koneksi”.

AWS prinsipal dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir Load Balancer Gateway. Untuk informasi selengkapnya, lihat Buat titik akhir Load Balancer Gateway.

Mengakses sistem inspeksi menggunakan titik akhir Gateway Load Balancer

Anda dapat membuat titik akhir Load Balancer Gateway untuk terhubung ke layanan endpoint yang didukung oleh. AWS PrivateLink

Untuk setiap subnet yang Anda tentukan dari VPC Anda, kami membuat antarmuka jaringan endpoint di subnet dan menetapkannya alamat IP pribadi dari rentang alamat subnet. Antarmuka jaringan endpoint adalah antarmuka jaringan yang dikelola pemohon; Anda dapat melihatnya di Anda Akun AWS, tetapi Anda tidak dapat mengelolanya sendiri.

Anda ditagih untuk penggunaan per jam dan biaya pemrosesan data. Untuk informasi selengkapnya, lihat harga titik akhir Load Balancer Gateway.

Daftar Isi

Pertimbangan-pertimbangan

- Anda hanya dapat memilih satu Availability Zone di VPC konsumen layanan. Anda tidak dapat mengubah subnet ini nanti. Untuk menggunakan titik akhir Load Balancer Gateway di subnet yang berbeda, Anda harus membuat titik akhir Load Balancer Gateway baru.
- Anda dapat membuat satu titik akhir Load Balancer Gateway per Availability Zone per layanan, dan Anda harus memilih Availability Zone yang didukung oleh Load Balancer Gateway. Ketika penyedia layanan dan konsumen layanan berada di akun yang berbeda, nama Availability Zone, sepertius-east-1a, mungkin dipetakan ke Availability Zone fisik yang berbeda di masing-masing Akun AWS akun. Anda dapat menggunakan ID AZ untuk secara konsisten mengidentifikasi Availability Zone untuk layanan Anda. Untuk informasi selengkapnya, lihat ID AZ di Panduan Pengguna Amazon EC2.

- Sebelum Anda dapat menggunakan layanan endpoint, penyedia layanan harus menerima permintaan koneksi. Layanan tidak dapat memulai permintaan ke sumber daya di VPC Anda melalui titik akhir VPC. Titik akhir hanya mengembalikan respons terhadap lalu lintas yang diprakarsai oleh sumber daya di VPC Anda.
- Setiap titik akhir Load Balancer Gateway dapat mendukung bandwidth hingga 10 Gbps per Availability Zone dan secara otomatis menskalakan hingga 100 Gbps.
- Jika layanan endpoint dikaitkan dengan beberapa Load Balancer Gateway, titik akhir Load Balancer Gateway akan membuat koneksi dengan hanya satu penyeimbang beban per Availability Zone.
- Untuk menjaga lalu lintas dalam Availability Zone yang sama, kami sarankan Anda membuat titik akhir Load Balancer Gateway di setiap Availability Zone tempat Anda akan mengirim lalu lintas.
- Pelestarian IP klien Network Load Balancer tidak didukung ketika lalu lintas dirutekan melalui titik akhir Gateway Load Balancer, bahkan jika target berada di VPC yang sama dengan Network Load Balancer.
- Jika server aplikasi dan titik akhir Load Balancer Gateway berada di subnet yang sama, aturan NACL dievaluasi untuk lalu lintas dari server aplikasi ke titik akhir Load Balancer Gateway.
- Jika Anda menggunakan Load Balancer Gateway dengan gateway internet khusus egres, lalu lintas IPv6 dijatuhkan. Sebagai gantinya, gunakan gateway internet dan aturan firewall masuk.
- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat AWS PrivateLink kuota.

Prasyarat

- Buat VPC konsumen layanan dengan setidaknya dua subnet di Availability Zone tempat Anda akan mengakses layanan. Satu subnet adalah untuk server aplikasi dan yang lainnya untuk titik akhir Gateway Load Balancer.
- Untuk memverifikasi Availability Zones yang didukung oleh layanan endpoint, jelaskan layanan endpoint menggunakan konsol atau perintah describe-vpc-endpoint-services.
- Jika sumber daya Anda berada dalam subnet dengan ACL jaringan, verifikasi bahwa ACL jaringan memungkinkan lalu lintas antara antarmuka jaringan titik akhir dan sumber daya di VPC.

Buat titik akhir

Gunakan prosedur berikut untuk membuat titik akhir Load Balancer Gateway yang terhubung ke layanan endpoint untuk sistem inspeksi.

Untuk membuat titik akhir Load Balancer Gateway menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Jenis, pilih layanan Endpoint yang menggunakan NLB dan GWLB.
5. Untuk nama Layanan, masukkan nama layanan, lalu pilih Verifikasi layanan.
6. Untuk VPC, pilih VPC dari mana Anda akan mengakses layanan endpoint.
7. Untuk Subnet, pilih satu subnet untuk membuat antarmuka jaringan endpoint.
8. Untuk jenis alamat IP, pilih dari opsi berikut:
   - IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika subnet yang dipilih memiliki rentang alamat IPv4.
   - IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan endpoint. Opsi ini didukung hanya jika subnet yang dipilih adalah subnet IPv6 saja.
   - Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan endpoint. Opsi ini didukung hanya jika subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6.
9. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
10. Pilih Buat titik akhir. Status awal adalah `pending acceptance`.

Untuk membuat titik akhir Load Balancer Gateway menggunakan baris perintah

- buat-vpc-titik akhir ()AWS CLI
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Konfigurasikan perutean

Gunakan prosedur berikut untuk mengonfigurasi tabel rute untuk VPC konsumen layanan. Hal ini memungkinkan peralatan keamanan untuk melakukan pemeriksaan keamanan untuk lalu lintas

masuk yang ditujukan untuk server aplikasi. Untuk informasi selengkapnya, lihat the section called "Perutean".

Untuk mengonfigurasi perutean menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Tabel Rute.
3. Pilih tabel rute untuk gateway internet dan lakukan hal berikut:
   a. Pilih Tindakan, Sunting rute.
   b. Jika Anda mendukung IPv4, pilih Tambahkan rute. Untuk Tujuan, masukkan blok IPv4 CIDR subnet untuk server aplikasi. Untuk Target, pilih titik akhir VPC.
   c. Jika Anda mendukung IPv6, pilih Tambahkan rute. Untuk Tujuan, masukkan blok IPv6 CIDR subnet untuk server aplikasi. Untuk Target, pilih titik akhir VPC.
   d. Pilih Simpan perubahan.
4. Pilih tabel rute untuk subnet dengan server aplikasi dan lakukan hal berikut:
   a. Pilih Tindakan, Sunting rute.
   b. Jika Anda mendukung IPv4, pilih Tambahkan rute. Untuk Tujuan, masukkan**`0.0.0.0/0`**. Untuk Target, pilih titik akhir VPC.
   c. Jika Anda mendukung IPv6, pilih Tambahkan rute. Untuk Tujuan, masukkan**`::/0`**. Untuk Target, pilih titik akhir VPC.
   d. Pilih Simpan perubahan.
5. Pilih tabel rute untuk subnet dengan titik akhir Gateway Load Balancer, dan lakukan hal berikut:
   a. Pilih Tindakan, Sunting rute.
   b. Jika Anda mendukung IPv4, pilih Tambahkan rute. Untuk Tujuan, masukkan**`0.0.0.0/0`**. Untuk Target, pilih gateway internet.
   c. Jika Anda mendukung IPv6, pilih Tambahkan rute. Untuk Tujuan, masukkan**`::/0`**. Untuk Target, pilih gateway internet.
   d. Pilih Simpan perubahan.

Untuk mengkonfigurasi routing menggunakan command line

- create-route (AWS CLI)

- New-EC2Route(Alat untuk Windows PowerShell)

Kelola tanda

Anda dapat menandai titik akhir Load Balancer Gateway Anda untuk membantu Anda mengidentifikasi atau mengkategorikannya sesuai dengan kebutuhan organisasi Anda.

Untuk mengelola tag menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola tag.
5. Untuk setiap tag untuk menambahkan pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih Hapus di sebelah kanan kunci tag dan nilai.
7. Pilih Simpan.

Untuk mengelola tag menggunakan baris perintah

- buat-tag dan hapus-tag ()AWS CLI
- New-EC2Tagdan Remove-EC2Tag(Alat untuk Windows PowerShell)

Menghapus titik akhir Load Balancer Gateway

Setelah selesai dengan titik akhir, Anda dapat menghapusnya. Menghapus titik akhir Load Balancer Gateway juga menghapus antarmuka jaringan titik akhir. Anda tidak dapat menghapus titik akhir Load Balancer Gateway jika ada rute dalam tabel rute yang mengarah ke titik akhir.

Untuk menghapus titik akhir Load Balancer Gateway

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Endpoints dan pilih endpoint Anda.
3. Pilih Tindakan, Hapus Titik Akhir.
4. Di layar konfirmasi, pilih Ya, Hapus.

Untuk menghapus titik akhir Load Balancer Gateway

- hapus-vpc-titik akhir ()AWS CLI
- Remove-EC2VpcEndpoint (AWS Tools for Windows PowerShell)

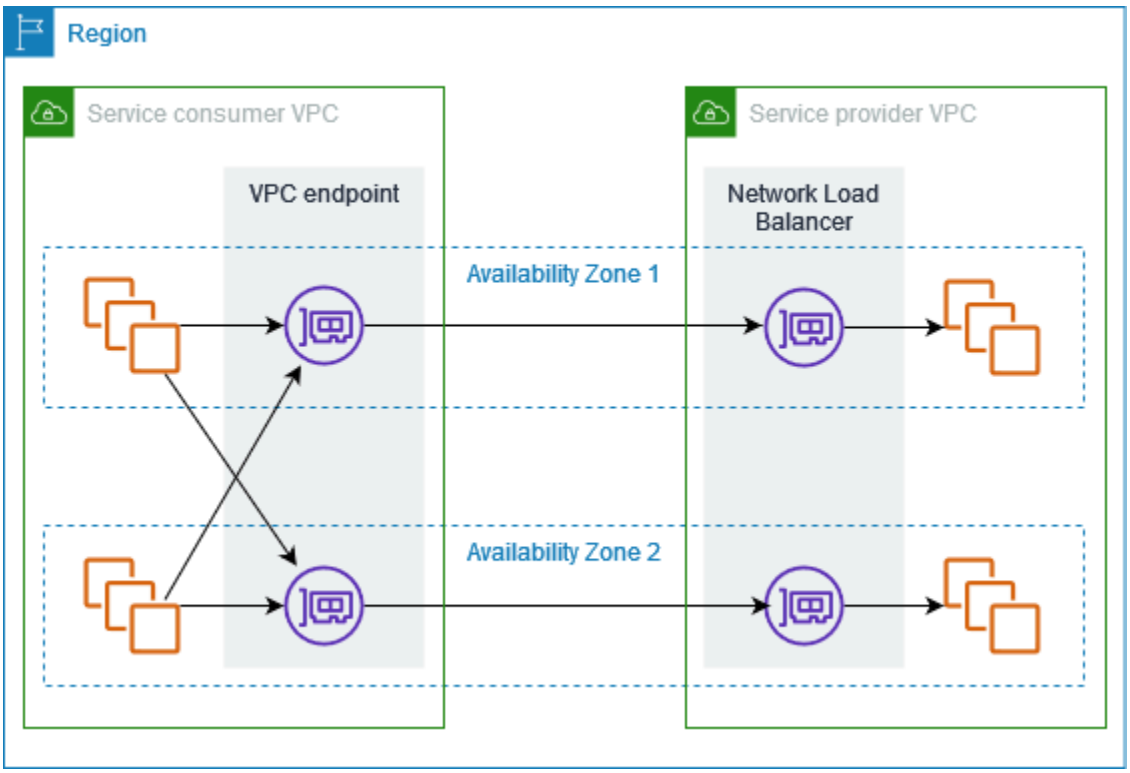
Bagikan layanan Anda melalui AWS PrivateLink

Anda dapat meng-host layanan AWS PrivateLink bertenaga Anda sendiri, yang dikenal sebagai layanan titik akhir, dan membagikannya dengan AWS pelanggan lain.

Daftar Isi

Ikhtisar

Diagram berikut menunjukkan bagaimana Anda membagikan layanan yang di-host AWS dengan AWS pelanggan lain, dan bagaimana pelanggan tersebut terhubung ke layanan Anda. Sebagai penyedia layanan, Anda membuat Network Load Balancer di VPC Anda sebagai front end layanan. Anda kemudian memilih penyeimbang beban ini ketika Anda membuat konfigurasi layanan titik akhir VPC. Anda memberikan izin kepada AWS prinsipal tertentu sehingga mereka dapat terhubung ke layanan Anda. Sebagai konsumen layanan, pelanggan membuat titik akhir VPC antarmuka, yang menetapkan koneksi antara subnet yang mereka pilih dari VPC mereka dan layanan titik akhir Anda. Penyeimbang beban menerima permintaan dari konsumen layanan dan mengarahkannya ke target yang menghosting layanan Anda.



Untuk latensi rendah dan ketersediaan tinggi, kami sarankan Anda menyediakan layanan Anda di setidaknya dua Availability Zone.

Nama host DNS

Saat penyedia layanan membuat layanan titik akhir VPC, AWS buat nama host DNS khusus titik akhir untuk layanan tersebut. Nama-nama ini memiliki sintaks berikut:

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

Berikut ini adalah contoh nama host DNS untuk layanan titik akhir VPC di Wilayah us-east-2:

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

Ketika konsumen layanan membuat titik akhir VPC antarmuka, kami membuat nama DNS Regional dan zona yang dapat digunakan konsumen layanan untuk berkomunikasi dengan layanan endpoint. Nama daerah memiliki sintaks berikut:

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

Nama zona memiliki sintaks berikut:

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

DNS privat

Penyedia layanan juga dapat mengaitkan nama DNS pribadi untuk layanan endpoint mereka, sehingga konsumen layanan dapat terus mengakses layanan menggunakan nama DNS yang ada. Jika penyedia layanan mengaitkan nama DNS pribadi dengan layanan endpoint mereka, maka konsumen layanan dapat mengaktifkan nama DNS pribadi untuk titik akhir antarmuka mereka. Jika penyedia layanan tidak mengaktifkan DNS pribadi, maka konsumen layanan mungkin perlu memperbarui aplikasi mereka untuk menggunakan nama DNS publik dari layanan titik akhir VPC. Untuk informasi selengkapnya, lihat Kelola nama DNS.

Subnet dan Availability Zone

Layanan endpoint Anda tersedia di Availability Zones yang Anda aktifkan untuk Network Load Balancer Anda. Untuk ketersediaan dan ketahanan yang tinggi, kami sarankan Anda mengaktifkan penyeimbang beban di setidaknya dua Availability Zone, menerapkan instans EC2 di setiap zona yang diaktifkan, dan mendaftarkan instans ini ke grup target penyeimbang beban Anda.

Anda dapat mengaktifkan penyeimbangan beban lintas zona sebagai alternatif untuk menghosting layanan titik akhir Anda di beberapa Availability Zone. Namun, konsumen akan kehilangan akses ke layanan endpoint dari kedua zona jika zona yang menghosting layanan endpoint gagal. Juga pertimbangkan bahwa ketika Anda mengaktifkan penyeimbangan beban lintas zona untuk Network Load Balancer, biaya transfer data EC2 berlaku.

Konsumen dapat membuat titik akhir VPC antarmuka di Availability Zones tempat layanan endpoint Anda tersedia. Kami membuat antarmuka jaringan titik akhir di setiap subnet yang dikonfigurasi konsumen untuk titik akhir VPC. Kami menetapkan alamat IP ke setiap antarmuka jaringan titik akhir dari subnetnya, berdasarkan jenis alamat IP dari titik akhir VPC. Ketika permintaan menggunakan titik akhir regional untuk layanan titik akhir VPC, kami memilih antarmuka jaringan titik akhir yang sehat, menggunakan algoritma round robin untuk bergantian antara antarmuka jaringan di Availability Zone yang berbeda. Kami kemudian menyelesaikan lalu lintas ke alamat IP dari antarmuka jaringan titik akhir yang dipilih.

Konsumen dapat menggunakan titik akhir zona untuk titik akhir VPC jika kasus penggunaannya lebih baik untuk menjaga lalu lintas di Availability Zone yang sama.

Cross-Region akses

Penyedia layanan dapat meng-host layanan di satu Wilayah dan membuatnya tersedia dalam satu set Wilayah yang didukung. Konsumen layanan memilih Wilayah layanan saat membuat titik akhir.

Izin

- Secara default, entitas IAM tidak memiliki izin untuk membuat layanan endpoint tersedia di beberapa Wilayah atau mengakses layanan endpoint di seluruh Wilayah. Untuk memberikan izin yang diperlukan untuk akses lintas wilayah, administrator IAM dapat membuat kebijakan IAM yang mengizinkan tindakan khusus izin. `vpce:AllowMultiRegion`
- Untuk mengontrol Wilayah yang dapat ditentukan oleh entitas IAM sebagai Wilayah yang didukung saat membuat layanan titik akhir, gunakan kunci `ec2:VpceSupportedRegion` kondisi.
- Untuk mengontrol Wilayah yang dapat ditentukan oleh entitas IAM sebagai Wilayah layanan saat membuat titik akhir VPC, gunakan `ec2:VpceServiceRegion` kunci kondisi.

Pertimbangan-pertimbangan

- Penyedia layanan harus memilih masuk ke Wilayah keikutsertaan sebelum menambahkannya sebagai Wilayah yang didukung untuk layanan titik akhir.
- Layanan endpoint Anda harus dapat diakses dari Wilayah tuan rumahnya. Anda tidak dapat menghapus Wilayah host dari kumpulan Wilayah yang didukung. Untuk redundansi, Anda dapat menerapkan layanan endpoint Anda di beberapa Wilayah dan mengaktifkan akses lintas wilayah untuk setiap layanan endpoint.
- Konsumen layanan harus memilih masuk ke Wilayah keikutsertaan sebelum memilihnya sebagai Wilayah layanan untuk titik akhir. Jika memungkinkan, kami menyarankan agar konsumen layanan mengakses layanan menggunakan konektivitas intra-wilayah, bukan konektivitas lintas wilayah. Intra-Region konektivitas memberikan latensi yang lebih rendah dan biaya yang lebih rendah.
- Jika penyedia layanan menghapus Wilayah dari kumpulan Wilayah yang didukung, konsumen layanan tidak dapat memilih Wilayah tersebut sebagai Wilayah layanan saat mereka membuat titik akhir baru. Perhatikan bahwa ini tidak memengaruhi akses ke layanan titik akhir dari titik akhir yang ada yang menggunakan Wilayah ini sebagai Wilayah layanan.
- Untuk ketersediaan tinggi, penyedia harus menggunakan setidaknya dua Availability Zone. Cross-Region akses tidak mengharuskan penyedia dan konsumen menggunakan Availability Zone yang sama.

- Cross-Region akses tidak didukung untuk Availability Zone berikut:`use1-az3`,`usw1-az2`,`apne1-az3`,`apne2-az2`, dan`apne2-az4`.
- Dengan akses lintas wilayah, AWS PrivateLink mengelola failover antara Availability Zones. Itu tidak mengelola failover di seluruh Wilayah.
- Cross-Region akses tidak didukung untuk Network Load Balancers dengan nilai kustom yang dikonfigurasi untuk batas waktu idle TCP.
- Cross-Region akses tidak didukung dengan fragmentasi UDP.
- Cross-Region akses hanya didukung untuk layanan yang Anda bagikan AWS PrivateLink.

Jenis alamat IP

Penyedia layanan dapat membuat titik akhir layanan mereka tersedia untuk konsumen layanan melalui IPv4, IPv6, atau IPv4 dan IPv6, bahkan jika server backend mereka hanya mendukung IPv4. Jika Anda mengaktifkan dukungan dualstack, konsumen yang ada dapat terus menggunakan IPv4 untuk mengakses layanan Anda dan konsumen baru dapat memilih untuk menggunakan IPv6 untuk mengakses layanan Anda.

Jika antarmuka VPC endpoint mendukung IPv4, antarmuka jaringan endpoint memiliki alamat IPv4. Jika antarmuka VPC endpoint mendukung IPv6, antarmuka jaringan endpoint memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Jika Anda mendeskripsikan antarmuka jaringan endpoint dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Persyaratan untuk mengaktifkan IPv6 untuk layanan endpoint

- VPC dan subnet untuk layanan endpoint harus memiliki blok CIDR IPv6 terkait.
- Semua Network Load Balancer untuk layanan endpoint harus menggunakan tipe alamat IP dualstack. Target tidak perlu mendukung lalu lintas IPv6. Jika layanan memproses alamat IP sumber dari header protokol proxy versi 2, itu harus memproses alamat IPv6.

Persyaratan untuk mengaktifkan IPv6 untuk titik akhir antarmuka

- Layanan endpoint harus mendukung permintaan IPv6.
- Jenis alamat IP dari titik akhir antarmuka harus kompatibel dengan subnet untuk titik akhir antarmuka, seperti yang dijelaskan di sini:

- IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4.
- IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6.
- Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan endpoint Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6.

Jenis alamat IP rekaman DNS untuk titik akhir antarmuka

Jenis alamat IP rekaman DNS yang didukung oleh titik akhir antarmuka menentukan catatan DNS yang kita buat. Jenis alamat IP rekaman DNS dari titik akhir antarmuka harus kompatibel dengan jenis alamat IP dari titik akhir antarmuka, seperti yang dijelaskan di sini:

- IPv4 — Buat catatan untuk nama DNS pribadi, Regional, dan zona. Jenis alamat IP harus IPv4 atau Dualstack.
- IPv6 — Buat catatan AAAA untuk nama DNS pribadi, Regional, dan zona. Jenis alamat IP harus IPv6 atau Dualstack.
- Dualstack — Buat catatan A dan AAAA untuk nama DNS pribadi, Regional, dan zona. Jenis alamat IP harus Dualstack.

Buat layanan yang didukung oleh AWS PrivateLink

Anda dapat membuat layanan Anda sendiri yang didukung oleh AWS PrivateLink, yang dikenal sebagai layanan endpoint. Anda adalah penyedia layanan, dan AWS prinsip yang membuat koneksi ke layanan Anda adalah konsumen layanan.

Layanan endpoint memerlukan Network Load Balancer atau Gateway Load Balancer. Penyeimbang beban menerima permintaan dari konsumen layanan dan mengarahkan mereka ke layanan Anda. Dalam hal ini, Anda akan membuat layanan endpoint menggunakan Network Load Balancer. Untuk informasi selengkapnya tentang membuat layanan endpoint menggunakan Load Balancer Gateway, lihat. Akses peralatan virtual

Daftar Isi

- Jadikan layanan endpoint Anda tersedia untuk konsumen layanan
- Connect ke layanan endpoint sebagai konsumen layanan

Pertimbangan-pertimbangan

- Layanan endpoint tersedia di Wilayah tempat Anda membuatnya. Konsumen dapat mengakses layanan Anda dari Wilayah lain jika Anda mengaktifkan akses lintas wilayah, atau jika mereka menggunakan peering VPC atau gateway transit.
- Ketika konsumen layanan mengambil informasi tentang layanan endpoint, mereka hanya dapat melihat Availability Zone yang mereka miliki bersama dengan penyedia layanan. Ketika penyedia layanan dan konsumen layanan berada di akun yang berbeda, nama Availability Zone, sepertius-east-1a, mungkin dipetakan ke Availability Zone fisik yang berbeda di masing-masing Akun AWS akun. Anda dapat menggunakan ID AZ untuk secara konsisten mengidentifikasi Availability Zone untuk layanan Anda. Untuk informasi selengkapnya, lihat ID AZ di Panduan Pengguna Amazon EC2.
- Ketika konsumen layanan mengirim lalu lintas ke layanan melalui titik akhir antarmuka, alamat IP sumber yang diberikan ke aplikasi adalah alamat IP pribadi dari node penyeimbang beban, bukan alamat IP konsumen layanan. Jika Anda mengaktifkan protokol proxy pada penyeimbang beban, Anda dapat memperoleh alamat konsumen layanan dan ID titik akhir antarmuka dari header protokol proxy. Untuk informasi selengkapnya, lihat Protokol proxy di Panduan Pengguna untuk Network Load Balancers.
- Network Load Balancer dapat dikaitkan dengan layanan endpoint tunggal, tetapi layanan endpoint dapat dikaitkan dengan beberapa Network Load Balancer.
- Jika layanan endpoint dikaitkan dengan beberapa Network Load Balancer, setiap antarmuka jaringan endpoint dikaitkan dengan satu penyeimbang beban. Ketika koneksi pertama dari antarmuka jaringan endpoint dimulai, kita memilih salah satu Network Load Balancers di Availability Zone yang sama dengan antarmuka jaringan endpoint secara acak. Semua permintaan koneksi berikutnya dari antarmuka jaringan titik akhir ini menggunakan penyeimbang beban yang dipilih. Kami menyarankan Anda menggunakan konfigurasi listener dan grup target yang sama untuk semua load balancer untuk layanan endpoint, sehingga konsumen dapat menggunakan layanan endpoint dengan sukses terlepas dari load balancer mana yang dipilih.
- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat AWS PrivateLink kuota.

Prasyarat

- Buat VPC untuk layanan endpoint Anda dengan setidaknya satu subnet di setiap Availability Zone di mana layanan harus tersedia.
- Untuk memungkinkan konsumen layanan membuat titik akhir VPC antarmuka IPv6 untuk layanan titik akhir Anda, VPC dan subnet harus memiliki blok CIDR IPv6 yang terkait.
- Buat Network Load Balancer di VPC Anda. Pilih satu subnet per Availability Zone di mana layanan harus tersedia untuk konsumen layanan. Untuk latensi rendah dan toleransi kesalahan, kami sarankan Anda menyediakan layanan Anda di setidaknya dua Availability Zone di Region.
- Jika Network Load Balancer Anda memiliki grup keamanan, itu harus memungkinkan lalu lintas masuk dari alamat IP klien. Atau, Anda dapat mematikan evaluasi aturan grup keamanan masuk untuk lalu lintas AWS PrivateLink. Untuk informasi selengkapnya, lihat Grup keamanan di Panduan Pengguna untuk Network Load Balancer.
- Untuk mengaktifkan layanan endpoint Anda menerima permintaan IPv6, Network Load Balancers harus menggunakan tipe alamat IP dualstack. Target tidak perlu mendukung lalu lintas IPv6. Untuk informasi selengkapnya, lihat Jenis alamat IP di Panduan Pengguna untuk Network Load Balancers.

  Jika Anda memproses alamat IP sumber dari header protokol proxy versi 2, verifikasi bahwa Anda dapat memproses alamat IPv6.
- Luncurkan instance di setiap Availability Zone di mana layanan harus tersedia dan daftarkan ke grup target load balancer. Jika Anda tidak meluncurkan instans di semua Availability Zone yang diaktifkan, Anda dapat mengaktifkan penyeimbangan beban lintas zona untuk mendukung konsumen layanan yang menggunakan nama host DNS zona untuk mengakses layanan. Biaya transfer data regional berlaku saat Anda mengaktifkan penyeimbangan beban lintas zona. Untuk informasi selengkapnya, lihat Cross-zone load balancing di Panduan Pengguna untuk Network Load Balancer.

Buat layanan endpoint

Gunakan prosedur berikut untuk membuat layanan endpoint menggunakan Network Load Balancer.

Untuk membuat layanan endpoint menggunakan konsol

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

3. Pilih Buat layanan endpoint.
4. Untuk jenis Load balancer, pilih Network.
5. Untuk penyeimbang beban yang tersedia, pilih Network Load Balancers untuk dikaitkan dengan layanan endpoint. Untuk melihat Availability Zone yang diaktifkan untuk load balancer yang Anda pilih, lihat Detail penyeimbang beban yang dipilih, Termasuk Availability Zone. Layanan endpoint Anda akan tersedia di Availability Zone ini.
6. (Opsional) Untuk membuat layanan endpoint Anda tersedia dari Wilayah selain Wilayah tempat layanan tersebut di-host, pilih Wilayah dari Wilayah Layanan. Untuk informasi selengkapnya, lihat the section called “Cross-Region akses”.
7. Untuk Memerlukan penerimaan untuk titik akhir, pilih Penerimaan yang diperlukan untuk mengharuskan permintaan koneksi ke layanan titik akhir Anda diterima secara manual. Jika tidak, permintaan ini diterima secara otomatis.
8. Untuk Aktifkan nama DNS pribadi, pilih Kaitkan nama DNS pribadi dengan layanan untuk mengaitkan nama DNS pribadi yang dapat digunakan konsumen layanan untuk mengakses layanan Anda, lalu masukkan nama DNS pribadi. Jika tidak, konsumen layanan dapat menggunakan nama DNS spesifik titik akhir yang disediakan oleh. AWS Sebelum konsumen layanan dapat menggunakan nama DNS pribadi, penyedia layanan harus memverifikasi bahwa mereka memiliki domain. Untuk informasi selengkapnya, lihat Kelola nama DNS.
9. Untuk jenis alamat IP yang Didukung, lakukan salah satu hal berikut:
   - Pilih IPv4 - Aktifkan layanan endpoint untuk menerima permintaan IPv4.
   - Pilih IPv6 — Aktifkan layanan endpoint untuk menerima permintaan IPv6.
   - Pilih IPv4 dan IPv6 — Aktifkan layanan endpoint untuk menerima permintaan IPv4 dan IPv6.
10. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
11. Pilih Buat.

Untuk membuat layanan endpoint menggunakan baris perintah

- buat-vpc-endpoint-service-configuration ()AWS CLI
- New-EC2VpcEndpointServiceConfiguration(Alat untuk Windows PowerShell)

Jadikan layanan endpoint Anda tersedia untuk konsumen layanan

AWS prinsipal dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat antarmuka VPC endpoint. Penyedia layanan harus melakukan hal berikut untuk membuat layanan mereka tersedia bagi konsumen layanan.

- Tambahkan izin yang memungkinkan setiap konsumen layanan terhubung ke layanan endpoint Anda. Untuk informasi selengkapnya, lihat the section called “Kelola izin”.
- Berikan konsumen layanan dengan nama layanan Anda dan Availability Zone yang didukung sehingga mereka dapat membuat titik akhir antarmuka untuk terhubung ke layanan Anda. Untuk informasi selengkapnya, lihat the section called “Connect ke layanan endpoint sebagai konsumen layanan”.
- Terima permintaan koneksi titik akhir dari konsumen layanan. Untuk informasi selengkapnya, lihat the section called “Menerima atau menolak permintaan koneksi”.

Connect ke layanan endpoint sebagai konsumen layanan

Konsumen layanan menggunakan prosedur berikut untuk membuat titik akhir antarmuka untuk terhubung ke layanan endpoint Anda.

Untuk membuat titik akhir antarmuka menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Jenis, pilih layanan Endpoint yang menggunakan NLB dan GWLB.
5. Untuk nama Layanan, masukkan nama layanan (misalnya,`com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`), lalu pilih Verifikasi layanan.
6. (Opsional) Untuk terhubung ke layanan titik akhir yang tersedia di Wilayah selain Wilayah titik akhir, pilih Wilayah Layanan, Aktifkan titik akhir Lintas Wilayah, lalu pilih Wilayah. Untuk informasi selengkapnya, lihat the section called “Cross-Region akses”.
7. Untuk VPC, pilih VPC dari mana Anda akan mengakses layanan endpoint.
8. Untuk Subnet, pilih subnet untuk membuat antarmuka jaringan titik akhir.
9. Untuk jenis alamat IP, pilih dari opsi berikut:

- IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan layanan titik akhir menerima permintaan IPv4.
- IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6 dan layanan endpoint menerima permintaan IPv6.
- Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan endpoint. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6 dan layanan endpoint menerima permintaan IPv4 dan IPv6.

10. Untuk jenis IP rekaman DNS, pilih dari opsi berikut:

    - IPv4 — Buat catatan untuk nama DNS pribadi, Regional, dan zona. Jenis alamat IP harus IPv4 atau Dualstack.
    - IPv6 — Buat catatan AAAA untuk nama DNS pribadi, Regional, dan zona. Jenis alamat IP harus IPv6 atau Dualstack.
    - Dualstack — Buat catatan A dan AAAA untuk nama DNS pribadi, Regional, dan zona. Jenis alamat IP harus Dualstack.
    - Layanan didefinisikan - Buat catatan untuk nama DNS pribadi, Regional, dan zona serta catatan AAAA untuk nama DNS Regional dan zona. Jenis alamat IP harus Dualstack.
11. Untuk grup Keamanan, pilih grup keamanan untuk diasosiasikan dengan antarmuka jaringan titik akhir.
12. Pilih Buat titik akhir.

Untuk membuat titik akhir antarmuka menggunakan baris perintah

- buat-vpc-titik akhir ()AWS CLI
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Konfigurasikan layanan endpoint

Setelah Anda membuat layanan endpoint, Anda dapat memperbarui konfigurasinya.

Tugas

- Kelola izin

- Menerima atau menolak permintaan koneksi
- Kelola penyeimbang beban
- Kaitkan nama DNS pribadi
- Ubah Wilayah yang didukung
- Ubah jenis alamat IP yang didukung
- Kelola tanda

Kelola izin

Kombinasi pengaturan izin dan penerimaan membantu Anda mengontrol konsumen layanan (AWS prinsipal) mana yang dapat mengakses layanan endpoint Anda. Misalnya, Anda dapat memberikan izin kepada prinsipal tertentu yang Anda percayai dan secara otomatis menerima semua permintaan koneksi, atau Anda dapat memberikan izin kepada kelompok prinsipal yang lebih luas dan secara manual menerima permintaan koneksi tertentu yang Anda percayai.

Secara default, layanan endpoint Anda tidak tersedia untuk konsumen layanan. Anda harus menambahkan izin yang memungkinkan AWS prinsipal tertentu untuk membuat titik akhir VPC antarmuka untuk terhubung ke layanan titik akhir Anda. Untuk menambahkan izin untuk AWS prinsipal, Anda memerlukan Nama Sumber Daya Amazon (ARN). Daftar berikut mencakup contoh ARN untuk AWS prinsipal yang didukung.

ARN untuk kepala sekolah AWS

Akun AWS (termasuk semua kepala sekolah di akun)

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

Peran

arn:aws:iam: ::peran/*account_idrole_name*

Pengguna

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

Semua kepala sekolah di semua Akun AWS

*

Pertimbangan-pertimbangan

- Jika Anda memberikan izin kepada semua orang untuk mengakses layanan endpoint dan mengonfigurasi layanan endpoint untuk menerima semua permintaan, penyeimbang beban Anda akan bersifat publik meskipun tidak memiliki alamat IP publik.
- Jika Anda menghapus izin, itu tidak memengaruhi koneksi yang ada antara titik akhir dan layanan yang sebelumnya diterima.

Untuk mengelola izin untuk layanan titik akhir Anda menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint dan pilih tab Allow principals.
4. Untuk menambahkan izin, pilih Izinkan prinsipal. Agar Kepala Sekolah dapat ditambahkan, masukkan ARN kepala sekolah. Untuk menambahkan prinsipal lain, pilih Tambah prinsipal. Setelah selesai menambahkan prinsipal, pilih Izinkan prinsipal.
5. Untuk menghapus izin, pilih prinsipal dan pilih Tindakan, Hapus. Saat diminta konfirmasi, masukkan **`delete`**, lalu pilih Hapus.

Untuk menambahkan izin untuk layanan endpoint Anda menggunakan baris perintah

- modify-vpc-endpoint-service-permissions ()AWS CLI
- Edit-EC2EndpointServicePermission(Alat untuk Windows PowerShell)

Menerima atau menolak permintaan koneksi

Kombinasi pengaturan izin dan penerimaan membantu Anda mengontrol konsumen layanan (AWS prinsipal) mana yang dapat mengakses layanan endpoint Anda. Misalnya, Anda dapat memberikan izin kepada prinsipal tertentu yang Anda percayai dan secara otomatis menerima semua permintaan koneksi, atau Anda dapat memberikan izin kepada kelompok prinsipal yang lebih luas dan secara manual menerima permintaan koneksi tertentu yang Anda percayai.

Anda dapat mengonfigurasi layanan endpoint Anda untuk menerima permintaan koneksi secara otomatis. Jika tidak, Anda harus menerima atau menolaknya secara manual. Jika Anda tidak menerima permintaan koneksi, konsumen layanan tidak dapat mengakses layanan endpoint Anda.

Jika Anda memberikan izin kepada semua orang untuk mengakses layanan endpoint dan mengonfigurasi layanan endpoint untuk menerima semua permintaan, penyeimbang beban Anda akan bersifat publik meskipun tidak memiliki alamat IP publik.

Anda dapat menerima pemberitahuan ketika permintaan koneksi diterima atau ditolak. Untuk informasi selengkapnya, lihat the section called “Menerima peringatan untuk acara layanan titik akhir”.

Untuk mengubah pengaturan penerimaan menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint.
4. Pilih Tindakan, Ubah pengaturan penerimaan titik akhir.
5. Pilih atau hapus Penerimaan diperlukan.
6. Pilih Save changes (Simpan perubahan)

Untuk memodifikasi pengaturan penerimaan menggunakan baris perintah

- memodifikasi-vpc-endpoint-service-configuration ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Alat untuk Windows PowerShell)

Untuk menerima atau menolak permintaan koneksi menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint.
4. Dari tab Koneksi titik akhir, pilih koneksi titik akhir.
5. Untuk menerima permintaan koneksi, pilih Tindakan, Terima permintaan koneksi titik akhir. Saat diminta konfirmasi, masukkan **`accept`** lalu pilih Terima.
6. Untuk menolak permintaan koneksi, pilih Tindakan, Tolak permintaan koneksi titik akhir. Saat diminta konfirmasi, masukkan lalu **`reject`** pilih Tolak.

Untuk menerima atau menolak permintaan koneksi menggunakan baris perintah

- terima-vpc-endpoint-koneksi atau tolak-vpc-endpoint-koneksi ()AWS CLI
- Approve-EC2EndpointConnectionatau Deny-EC2EndpointConnection(Alat untuk Windows PowerShell)

Kelola penyeimbang beban

Anda dapat mengelola penyeimbang beban yang terkait dengan layanan endpoint Anda. Anda tidak dapat memisahkan penyeimbang beban jika ada titik akhir yang terhubung ke layanan titik akhir Anda.

Jika Anda mengaktifkan Availability Zone lain untuk penyeimbang beban Anda, Availability Zone akan muncul di bawah tab Load Balancers pada halaman layanan Endpoint. Namun, itu tidak akan diaktifkan untuk layanan endpoint atau tercantum di tab Detail layanan endpoint Anda di. Konsol Manajemen AWS Anda perlu mengaktifkan layanan endpoint untuk Availability Zone yang baru.

Mungkin perlu beberapa menit agar Availability Zone penyeimbang beban siap untuk layanan endpoint Anda. Jika Anda menggunakan otomatisasi, sebaiknya tambahkan tunggu dalam proses otomatisasi sebelum mengaktifkan layanan endpoint untuk Availability Zone yang baru.

Untuk mengelola penyeimbang beban untuk layanan titik akhir Anda menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint.
4. Pilih Actions, Associate, atau disassociate load balancer.
5. Ubah konfigurasi layanan endpoint sesuai kebutuhan. Contoh:
   - Pilih kotak centang untuk penyeimbang beban untuk mengaitkannya dengan layanan titik akhir.
   - Kosongkan kotak centang untuk penyeimbang beban untuk memisahkannya dari layanan titik akhir. Anda harus memilih setidaknya satu penyeimbang beban.
6. Pilih Save changes (Simpan perubahan)

   Layanan endpoint akan diaktifkan untuk Availability Zone baru yang Anda tambahkan ke load balancer Anda. Availability Zone baru tercantum di bawah tab Load Balancers dan tab Detail dari layanan endpoint.

Setelah Anda mengaktifkan Availability Zone untuk layanan endpoint, konsumen layanan dapat menambahkan subnet dari Availability Zone tersebut ke titik akhir VPC antarmuka mereka.

Untuk mengelola penyeimbang beban untuk layanan endpoint Anda menggunakan baris perintah

- memodifikasi-vpc-endpoint-service-configuration ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Alat untuk Windows PowerShell)

Untuk mengaktifkan layanan endpoint di Availability Zone yang baru-baru ini diaktifkan untuk penyeimbang beban, cukup panggil perintah dengan ID layanan endpoint.

Kaitkan nama DNS pribadi

Anda dapat mengaitkan nama DNS pribadi dengan layanan endpoint Anda. Setelah Anda mengaitkan nama DNS pribadi, Anda harus memperbarui entri untuk domain di server DNS Anda. Sebelum konsumen layanan dapat menggunakan nama DNS pribadi, penyedia layanan harus memverifikasi bahwa mereka memiliki domain. Untuk informasi selengkapnya, lihat Kelola nama DNS.

Untuk memodifikasi layanan endpoint nama DNS pribadi menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint.
4. Pilih Tindakan, Ubah nama DNS pribadi.
5. Pilih Kaitkan nama DNS pribadi dengan layanan dan masukkan nama DNS pribadi.
   - Nama domain harus menggunakan huruf kecil.
   - Anda dapat menggunakan wildcard dalam nama domain (misalnya,**`*.myexampleservice.com`**).
6. Pilih Simpan perubahan.
7. Nama DNS pribadi siap digunakan oleh konsumen layanan ketika status verifikasi diverifikasi. Jika status verifikasi berubah, permintaan koneksi baru ditolak tetapi koneksi yang ada tidak terpengaruh.

Untuk memodifikasi layanan endpoint nama DNS pribadi menggunakan baris perintah

- memodifikasi-vpc-endpoint-service-configuration ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Alat untuk Windows PowerShell)

Untuk memulai proses verifikasi domain menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint.
4. Pilih Tindakan, Verifikasi kepemilikan domain untuk nama DNS pribadi.
5. Saat diminta konfirmasi, masukkan **`verify`** lalu pilih Verifikasi.

Untuk memulai proses verifikasi domain menggunakan baris perintah

- start-vpc-endpoint-service-private-dns-verifikasi ()AWS CLI
- Start-EC2VpcEndpointServicePrivateDnsVerification(Alat untuk Windows PowerShell)

Ubah Wilayah yang didukung

Anda dapat mengubah kumpulan Wilayah yang didukung untuk layanan endpoint Anda. Sebelum Anda dapat menambahkan Wilayah keikutsertaan, Anda harus ikut serta. Anda tidak dapat menghapus Wilayah yang menghosting layanan endpoint Anda.

Setelah Anda menghapus Wilayah, konsumen layanan tidak dapat membuat titik akhir baru yang menetapkannya sebagai Wilayah layanan. Menghapus Wilayah tidak memengaruhi titik akhir yang ada yang menetapkannya sebagai Wilayah layanan. Saat Anda menghapus Region, sebaiknya Anda menolak koneksi endpoint yang ada dari Region tersebut.

Untuk mengubah Wilayah yang didukung untuk layanan titik akhir Anda

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint.
4. Pilih Tindakan, Ubah Wilayah yang didukung.

5. Pilih dan batal pilihan Wilayah sesuai kebutuhan.
6. Pilih Simpan perubahan.

Ubah jenis alamat IP yang didukung

Anda dapat mengubah jenis alamat IP yang didukung oleh layanan endpoint Anda.

Pertimbangan

Untuk mengaktifkan layanan endpoint Anda menerima permintaan IPv6, Network Load Balancers harus menggunakan tipe alamat IP dualstack. Target tidak perlu mendukung lalu lintas IPv6. Untuk informasi selengkapnya, lihat Jenis alamat IP di Panduan Pengguna untuk Network Load Balancers.

Untuk mengubah jenis alamat IP yang didukung menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan titik akhir VPC.
4. Pilih Tindakan, Ubah jenis alamat IP yang didukung.
5. Untuk jenis alamat IP yang Didukung, lakukan salah satu hal berikut:
   - Pilih IPv4 - Aktifkan layanan endpoint untuk menerima permintaan IPv4.
   - Pilih IPv6 — Aktifkan layanan endpoint untuk menerima permintaan IPv6.
   - Pilih IPv4 dan IPv6 — Aktifkan layanan endpoint untuk menerima permintaan IPv4 dan IPv6.
6. Pilih Simpan perubahan.

Untuk memodifikasi jenis alamat IP yang didukung menggunakan baris perintah

- memodifikasi-vpc-endpoint-service-configuration ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Alat untuk Windows PowerShell)

Kelola tanda

Anda dapat menandai sumber daya Anda untuk membantu Anda mengidentifikasi mereka atau mengkategorikannya sesuai dengan kebutuhan organisasi Anda.

Untuk mengelola tag untuk layanan endpoint Anda menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan titik akhir VPC.
4. Pilih Tindakan, Kelola tag.
5. Untuk setiap tag yang akan ditambahkan, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih Hapus di sebelah kanan kunci tag dan nilai.
7. Pilih Simpan.

Untuk mengelola tag untuk koneksi titik akhir Anda menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan titik akhir VPC dan kemudian pilih tab Koneksi titik akhir.
4. Pilih koneksi titik akhir dan kemudian pilih Tindakan, Kelola tag.
5. Untuk setiap tag yang akan ditambahkan, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih Hapus di sebelah kanan kunci tag dan nilai.
7. Pilih Simpan.

Untuk mengelola tag untuk izin layanan titik akhir Anda menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan titik akhir VPC dan kemudian pilih tab Izinkan prinsipal.
4. Pilih prinsipal dan kemudian pilih Tindakan, Kelola tag.
5. Untuk setiap tag yang akan ditambahkan, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih Hapus di sebelah kanan kunci tag dan nilai.
7. Pilih Simpan.

Untuk menambah dan menghapus tag menggunakan baris perintah

- buat-tag dan hapus-tag ()AWS CLI
- New-EC2Tagdan Remove-EC2Tag(Alat untuk Windows PowerShell)

Mengelola nama DNS untuk layanan titik akhir VPC

Penyedia layanan dapat mengonfigurasi nama DNS pribadi untuk layanan titik akhir mereka. Misalkan penyedia layanan membuat layanan mereka tersedia melalui titik akhir publik dan sebagai layanan titik akhir. Jika penyedia layanan menggunakan nama DNS dari titik akhir publik sebagai nama DNS pribadi dari layanan endpoint, maka konsumen layanan dapat mengakses titik akhir publik atau layanan endpoint menggunakan aplikasi klien yang sama, tanpa modifikasi. Jika permintaan berasal dari VPC konsumen layanan, server DNS pribadi menyelesaikan nama DNS ke alamat IP antarmuka jaringan titik akhir. Jika tidak, server DNS publik menyelesaikan nama DNS ke titik akhir publik.

Sebelum Anda dapat mengonfigurasi nama DNS pribadi untuk layanan endpoint Anda, Anda harus membuktikan bahwa Anda memiliki domain dengan melakukan pemeriksaan verifikasi kepemilikan domain.

Pertimbangan-pertimbangan

- Layanan endpoint hanya dapat memiliki satu nama DNS pribadi.
- Saat konsumen membuat titik akhir antarmuka untuk terhubung ke layanan Anda, kami membuat zona host pribadi dan mengaitkannya dengan VPC konsumen layanan. Kami membuat catatan CNAME di zona host pribadi yang memetakan nama DNS pribadi layanan titik akhir ke nama DNS regional titik akhir VPC. Ketika konsumen mengirim permintaan ke nama DNS publik layanan, server DNS pribadi menyelesaikan permintaan ke alamat IP dari antarmuka jaringan titik akhir.
- Untuk memverifikasi domain, Anda harus memiliki nama host publik atau penyedia DNS publik.
- Anda dapat memverifikasi domain subdomain. Misalnya, Anda dapat memverifikasi example.com, bukan a.example.com. Setiap label DNS dapat memiliki hingga 63 karakter dan seluruh nama domain tidak boleh melebihi panjang total 255 karakter.

  Jika Anda menambahkan subdomain tambahan, Anda harus memverifikasi subdomain, atau domain. Misalnya, katakanlah Anda memiliki.example.com, dan memverifikasi example.com. Anda sekarang menambahkan b.example.com sebagai nama DNS pribadi. Anda harus memverifikasi

example.com atau b.example.com sebelum konsumen layanan dapat menggunakan nama tersebut.

- Nama DNS pribadi tidak didukung untuk titik akhir Gateway Load Balancer.

Verifikasi kepemilikan domain

Domain Anda dikaitkan dengan sekumpulan data layanan nama domain (DNS) yang Anda kelola melalui penyedia DNS Anda. Catatan TXT adalah tipe catatan DNS yang menyediakan informasi tambahan tentang domain Anda. Ini terdiri dari nama dan nilai. Sebagai bagian dari proses verifikasi, Anda harus menambahkan catatan TXT ke server DNS untuk domain publik Anda.

Verifikasi kepemilikan domain selesai ketika kami mendeteksi keberadaan catatan TXT di pengaturan DNS domain Anda.

Setelah menambahkan catatan, Anda dapat memeriksa status proses verifikasi domain menggunakan konsol Amazon VPC. Di panel navigasi, pilih Layanan titik akhir. Pilih layanan endpoint dan periksa nilai status verifikasi Domain di tab Detail. Jika verifikasi domain tertunda, tunggu beberapa menit dan segarkan layar. Jika diperlukan, Anda dapat memulai proses verifikasi secara manual. Pilih Tindakan, Verifikasi kepemilikan domain untuk nama DNS pribadi.

Nama DNS pribadi siap digunakan oleh konsumen layanan ketika status verifikasi diverifikasi. Jika status verifikasi berubah, permintaan koneksi baru ditolak tetapi koneksi yang ada tidak terpengaruh.

Jika status verifikasi gagal, lihatthe section called “Memecahkan masalah verifikasi domain”.

Dapatkan nama dan nilainya

Kami memberi Anda nama dan nilai yang Anda gunakan dalam catatan TXT. Misalnya, informasi tersedia di Konsol Manajemen AWS. Pilih layanan endpoint dan lihat Nama verifikasi domain dan nilai verifikasi Domain pada tab Detail untuk layanan endpoint. Anda juga dapat menggunakan AWS CLI perintah describe-vpc-endpoint-service-configurations berikut untuk mengambil informasi tentang konfigurasi nama DNS pribadi untuk layanan endpoint yang ditentukan.

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

Berikut ini adalah output contoh. Anda akan menggunakan `Value` dan `Name` ketika Anda membuat catatan TXT.

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

Misalnya, misalkan nama domain Anda adalah example.com dan itu `Value` dan seperti `Name` yang ditunjukkan pada contoh keluaran sebelumnya. Tabel berikut adalah contoh pengaturan catatan TXT.

Nama	Tipe	Nilai
_6e86v84tqgqubxbwi i1m.example.com	TXT	vpce:l6p0 ERxlTt45jevFwOCp

Kami menyarankan Anda menggunakan `Name` sebagai subdomain rekaman karena nama domain dasar mungkin sudah digunakan. Namun, jika penyedia DNS Anda tidak mengizinkan nama catatan DNS berisi garis bawah, Anda dapat menghilangkan “_6e86v84tqgqubxbwii1m” dan cukup gunakan “example.com” dalam catatan TXT.

Setelah kami memverifikasi “_6e86v84tqgqubxbwii1m.example.com”, konsumen layanan dapat menggunakan “example.com” atau subdomain (misalnya, “service.example.com” atau “my.service.example.com”).

Tambahkan catatan TXT ke server DNS domain Anda

Prosedur untuk menambahkan catatan TXT ke server DNS domain tergantung pada siapa yang menyediakan layanan DNS Anda. Penyedia DNS Anda mungkin Amazon Route 53 atau pencatat nama domain lainnya.

Amazon Route 53

Buat catatan untuk zona yang dihosting publik menggunakan kebijakan perutean sederhana. Gunakan nilai berikut:

- Untuk nama Rekam masukkan domain atau subdomain.

- Untuk Tipe catatan, pilih TXT.
- Untuk Value/Route lalu lintas ke, masukkan nilai verifikasi domain.
- Untuk TTL (detik), masukkan**`1800`**.

Untuk informasi selengkapnya, lihat Membuat catatan menggunakan konsol di Panduan Pengembang Amazon Route 53.

Prosedur umum

Buka situs web untuk penyedia DNS Anda dan masuk ke akun Anda. Temukan halaman untuk memperbarui catatan DNS untuk domain Anda. Tambahkan catatan TXT dengan nama dan nilai yang kami berikan. Diperlukan waktu hingga 48 jam agar pembaruan catatan DNS diterapkan, tetapi seringkali berlaku lebih cepat.

Untuk petunjuk yang lebih spesifik, lihat dokumentasi dari penyedia DNS Anda. Tabel berikut menyediakan tautan ke dokumentasi untuk beberapa penyedia DNS umum. Daftar ini tidak dimaksudkan untuk menjadi komprehensif, juga tidak dimaksudkan sebagai rekomendasi dari produk atau layanan yang disediakan oleh perusahaan-perusahaan ini.

DNS/Hosting penyedia	Tautan dokumentasi
GoDaddy	Tambahkan catatan TXT
Dreamhost	Menambahkan catatan DNS kustom
Cloudflare	Mengelola catatan DNS
HostGator	Mengelola Rekaman DNS dengan HostGator/eNom
Namecheap	Bagaimana cara menambahkan TXT/SPF/DKIM/DMARC catatan untuk domain saya?
Names.co.uk	Mengubah pengaturan DNS domain Anda
Wix	Menambahkan atau Memperbarui Catatan TXT di Akun Wix Anda

Periksa apakah catatan TXT diterbitkan

Anda dapat memverifikasi bahwa catatan TXT verifikasi kepemilikan domain nama DNS pribadi Anda dipublikasikan dengan benar ke server DNS Anda menggunakan langkah-langkah berikut. Anda akan menjalankan nslookup perintah, yang tersedia untuk Windows dan Linux.

Anda akan menanyakan server DNS yang melayani domain Anda karena server tersebut berisi informasi terbaru untuk domain Anda. Informasi domain Anda membutuhkan waktu untuk menyebar ke server DNS lain.

Untuk memverifikasi bahwa catatan TXT Anda dipublikasikan ke server DNS Anda

1. Temukan server nama untuk domain Anda menggunakan perintah berikut.

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

   Output mencantumkan server nama yang melayani domain Anda. Anda akan menanyakan salah satu server ini di langkah berikutnya.

2. Verifikasi bahwa catatan TXT diterbitkan dengan benar menggunakan perintah berikut, di *name_server* mana salah satu server nama yang Anda temukan di langkah sebelumnya.

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

3. Dalam output dari langkah sebelumnya, verifikasi bahwa string yang mengikuti `text =` cocok dengan nilai TXT.

   Dalam contoh kita, jika catatan diterbitkan dengan benar, outputnya mencakup yang berikut ini.

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

Memecahkan masalah verifikasi domain

Jika proses verifikasi domain gagal, informasi berikut dapat membantu Anda memecahkan masalah.

- Periksa apakah penyedia DNS Anda mengizinkan garis bawah dalam nama catatan TXT. Jika penyedia DNS Anda tidak mengizinkan garis bawah, Anda dapat menghilangkan nama verifikasi domain (misalnya, “_6e86v84tqgqubxbwii1m”) dari catatan TXT.

- Periksa apakah penyedia DNS Anda menambahkan nama domain ke akhir catatan TXT. Beberapa penyedia DNS secara otomatis menambahkan nama domain Anda ke nama atribut catatan TXT. Untuk menghindari duplikasi nama domain ini, tambahkan titik ke akhir nama domain saat Anda membuat catatan TXT. Ini memberi tahu penyedia DNS Anda bahwa tidak perlu menambahkan nama domain ke catatan TXT.
- Periksa apakah penyedia DNS Anda memodifikasi nilai catatan DNS agar hanya menggunakan huruf kecil. Kami memverifikasi domain Anda hanya jika ada catatan verifikasi dengan nilai atribut yang sama persis dengan nilai yang kami berikan. Jika penyedia DNS mengubah nilai rekaman TXT Anda untuk hanya menggunakan huruf kecil, hubungi mereka untuk bantuan.
- Anda mungkin perlu memverifikasi domain Anda lebih dari sekali karena Anda mendukung beberapa Wilayah atau beberapa Akun AWS. Jika penyedia DNS Anda tidak mengizinkan Anda memiliki lebih dari satu catatan TXT dengan nama atribut yang sama, periksa apakah penyedia DNS Anda mengizinkan Anda menetapkan beberapa nilai atribut ke catatan TXT yang sama. Misalnya, jika DNS Anda dikelola oleh Amazon Route 53, Anda dapat menggunakan prosedur berikut.

  1. Di konsol Route 53, pilih data TXT yang Anda buat saat memverifikasi domain di Wilayah pertama.
  2. Untuk Nilai, pergi ke akhir nilai atribut yang ada, dan kemudian tekan Enter.
  3. Tambahkan nilai atribut untuk Wilayah tambahan, lalu simpan set rekaman.

  Jika penyedia DNS Anda tidak mengizinkan Anda menetapkan beberapa nilai ke catatan TXT yang sama, Anda dapat memverifikasi domain satu kali dengan nilai dalam nama atribut catatan TXT, dan satu kali lagi dengan nilai yang dihapus dari nama atribut. Namun, Anda hanya dapat memverifikasi domain yang sama dua kali.

Menerima peringatan untuk acara layanan titik akhir

Anda dapat membuat notifikasi untuk menerima peringatan untuk acara tertentu yang terkait dengan layanan endpoint Anda. Misalnya, Anda dapat menerima email saat permintaan koneksi diterima atau ditolak.

Tugas

- Buat notifikasi SNS
- Menambahkan kebijakan akses
- Menambahkan kebijakan kunci

Buat notifikasi SNS

Gunakan prosedur berikut untuk membuat topik Amazon SNS untuk notifikasi dan berlangganan topik tersebut.

Untuk membuat notifikasi untuk layanan endpoint menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint.
4. Dari tab Notifikasi, pilih Buat notifikasi.
5. Untuk Notification ARN, pilih ARN untuk topik SNS yang Anda buat.
6. Untuk berlangganan acara, pilih dari Acara.
   - Connect — Konsumen layanan membuat titik akhir antarmuka. Ini mengirimkan permintaan koneksi ke penyedia layanan.
   - Terima — Penyedia layanan menerima permintaan koneksi.
   - Tolak — Penyedia layanan menolak permintaan koneksi.
   - Hapus — Konsumen layanan menghapus titik akhir antarmuka.
7. Pilih Buat notifikasi.

Untuk membuat notifikasi untuk layanan endpoint menggunakan command line

- buat-vpc-endpoint-koneksi-notifikasi ()AWS CLI
- New-EC2VpcEndpointConnectionNotification(Alat untuk Windows PowerShell)

Menambahkan kebijakan akses

Tambahkan kebijakan akses ke topik SNS yang memungkinkan AWS PrivateLink untuk mempublikasikan pemberitahuan atas nama Anda, seperti berikut ini. Untuk informasi selengkapnya, lihat Bagaimana cara mengedit kebijakan akses topik Amazon SNS saya? Gunakan kunci kondisi `aws:SourceArn` dan `aws:SourceAccount` global untuk melindungi dari masalah wakil yang membingungkan.

JSON

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

Menambahkan kebijakan kunci

Jika Anda menggunakan topik SNS terenkripsi, kebijakan sumber daya untuk kunci KMS harus dipercaya AWS PrivateLink untuk memanggil operasi API. AWS KMS Berikut ini adalah contoh kebijakan kunci.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
```

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

Hapus layanan endpoint

Setelah selesai dengan layanan endpoint, Anda dapat menghapusnya. Anda tidak dapat menghapus layanan titik akhir jika ada titik akhir yang terhubung ke layanan titik akhir yang berada dalam status atau. `available` `pending-acceptance`

Menghapus layanan endpoint tidak menghapus penyeimbang beban terkait dan tidak memengaruhi server aplikasi yang terdaftar dengan grup target penyeimbang beban.

Untuk menghapus layanan endpoint menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint.
4. Pilih Tindakan, Hapus layanan titik akhir.
5. Saat diminta konfirmasi, masukkan **`delete`**, lalu pilih Hapus.

Untuk menghapus layanan endpoint menggunakan baris perintah

- hapus-vpc-endpoint-service-configurations ()AWS CLI

- Remove-EC2EndpointServiceConfiguration(Alat untuk Windows PowerShell)

Akses sumber daya VPC melalui AWS PrivateLink

Anda dapat mengakses sumber daya VPC secara pribadi di VPC lain menggunakan titik akhir VPC sumber daya (titik akhir sumber daya). Titik akhir sumber daya memungkinkan Anda mengakses sumber daya VPC secara pribadi dan aman seperti database, instans Amazon EC2, titik akhir aplikasi, target nama domain, atau alamat IP yang mungkin ada di subnet pribadi di VPC lain atau di lingkungan di lokasi. Tanpa titik akhir sumber daya, Anda harus menambahkan gateway internet ke VPC Anda atau mengakses sumber daya menggunakan titik akhir antarmuka dan AWS PrivateLink Network Load Balancer. Titik akhir sumber daya tidak memerlukan penyeimbang beban, sehingga Anda dapat mengakses sumber daya VPC secara langsung. Sumber daya VPC diwakili oleh konfigurasi sumber daya. Konfigurasi sumber daya dikaitkan dengan gateway sumber daya.

Harga

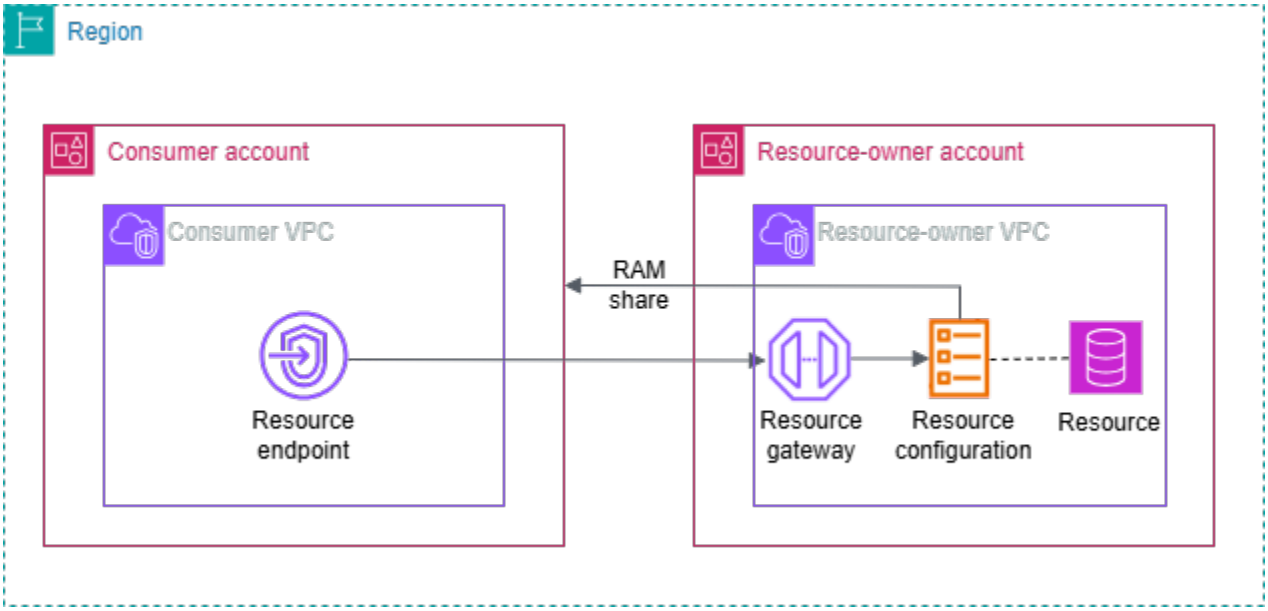
Saat mengakses sumber daya menggunakan titik akhir sumber daya, Anda ditagih untuk setiap jam titik akhir VPC sumber daya Anda disediakan. Anda juga ditagih per GB data yang diproses saat Anda mengakses sumber daya. Untuk informasi selengkapnya, lihat harga AWS PrivateLink. Saat mengaktifkan akses ke sumber daya menggunakan konfigurasi sumber daya dan gateway sumber daya, Anda akan ditagih per data GB yang diproses oleh gateway sumber daya Anda. Untuk informasi selengkapnya, lihat harga Amazon VPC Lattice.

Daftar Isi

Ikhtisar

Anda dapat mengakses sumber daya di akun Anda atau yang telah dibagikan dengan Anda dari akun lain. Untuk mengakses sumber daya, Anda membuat titik akhir VPC sumber daya, yang membuat koneksi antara subnet di VPC Anda dan sumber daya menggunakan antarmuka jaringan. Lalu lintas yang ditujukan untuk sumber daya diselesaikan ke alamat IP pribadi dari antarmuka jaringan titik akhir sumber daya menggunakan DNS. Kemudian, lalu lintas dikirim ke sumber daya menggunakan koneksi antara titik akhir VPC dan sumber daya melalui gateway sumber daya.

Gambar berikut menunjukkan titik akhir sumber daya di akun konsumen yang mengakses sumber daya yang dimiliki oleh akun lain dan dibagikan melalui: AWS RAM



Pertimbangan-pertimbangan

- Lalu lintas TCP didukung. Lalu lintas UDP tidak didukung.
- Koneksi jaringan harus dimulai dari VPC yang berisi titik akhir sumber daya, dan bukan dari VPC yang memiliki sumber daya. VPC sumber daya tidak dapat memulai koneksi jaringan ke VPC endpoint.
- Satu-satunya ARN-based sumber daya yang didukung adalah sumber daya Amazon RDS.
- Setidaknya satu Availability Zone dari titik akhir VPC dan gateway sumber daya harus tumpang tindih.

Nama host DNS

Dengan AWS PrivateLink, Anda mengirim lalu lintas ke sumber daya menggunakan titik akhir pribadi. Saat Anda membuat titik akhir VPC sumber daya, kami membuat nama DNS Regional (disebut nama DNS default) yang dapat Anda gunakan untuk berkomunikasi dengan sumber daya dari VPC Anda dan dari tempat. Kami menyarankan Anda menggunakan DNS alih-alih IP endpoint untuk terhubung ke sumber daya Anda. Nama DNS default untuk titik akhir VPC sumber daya Anda memiliki sintaks berikut:

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

Saat Anda membuat titik akhir VPC sumber daya untuk konfigurasi sumber daya tertentu yang menggunakan ARN, Anda dapat mengaktifkan DNS pribadi. Dengan DNS pribadi, Anda dapat terus membuat permintaan ke sumber daya menggunakan nama DNS yang disediakan untuk sumber daya oleh AWS layanan, sambil memanfaatkan konektivitas pribadi melalui titik akhir VPC sumber daya. Untuk informasi selengkapnya, lihat the section called “Resolusi DNS”.

Perintah deskripsi-vpc-endpoint-associations berikut menampilkan entri DNS untuk titik akhir sumber daya.

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

Berikut ini adalah contoh output untuk titik akhir sumber daya untuk database Amazon RDS dengan nama DNS pribadi diaktifkan. Nama DNS pertama adalah nama DNS default. Nama DNS kedua berasal dari zona host pribadi tersembunyi, yang menyelesaikan permintaan ke titik akhir publik ke alamat IP pribadi dari antarmuka jaringan titik akhir.

```
[
    [
        "vpce-rsc-asc-abcd1234abcd",
        "vpce-123456789abcdefgh",
        "Accessible",
        {
            "DnsName": "vpce-1234567890abcdefg-
snra-1234567890abcdefg.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-
east-1.on.aws",
            "HostedZoneId": "ABCDEFGH123456789000"
        },
```

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

Resolusi DNS

Catatan DNS yang kami buat untuk titik akhir VPC sumber daya Anda bersifat publik. Oleh karena itu, nama-nama DNS ini dapat diselesaikan secara publik. Namun, permintaan DNS dari luar VPC masih mengembalikan alamat IP pribadi dari antarmuka jaringan titik akhir sumber daya. Anda dapat menggunakan nama DNS ini untuk mengakses sumber daya dari tempat, selama Anda memiliki akses ke VPC tempat titik akhir sumber daya berada, melalui VPN atau Direct Connect.

DNS privat

Jika Anda mengaktifkan DNS pribadi untuk titik akhir VPC sumber daya Anda untuk konfigurasi sumber daya tertentu yang menggunakan ARN, dan VPC Anda mengaktifkan nama host DNS dan resolusi DNS, kami membuat zona host pribadi terkelola AWS tersembunyi untuk konfigurasi sumber daya dengan nama DNS kustom. Zona yang dihosting berisi kumpulan catatan untuk nama DNS default untuk sumber daya yang menyelesaikannya ke alamat IP pribadi antarmuka jaringan titik akhir sumber daya di VPC Anda.

Amazon menyediakan server DNS untuk VPC Anda, yang disebut Resolver Route 53. Resolver Route 53 secara otomatis menyelesaikan nama domain VPC lokal dan merekam di zona host pribadi. Namun, Anda tidak dapat menggunakan Resolver Route 53 dari luar VPC Anda. Jika ingin mengakses titik akhir VPC dari jaringan lokal, Anda dapat menggunakan nama DNS kustom atau Anda dapat menggunakan titik akhir Route 53 Resolver dan aturan Resolver. Untuk informasi selengkapnya, lihat Mengintegrasikan AWS Transit Gateway dengan AWS PrivateLink dan Amazon Route 53 Resolver.

Subnet dan Availability Zone

Anda dapat mengonfigurasi titik akhir VPC Anda dengan satu subnet per Availability Zone. Kami membuat antarmuka jaringan endpoint untuk titik akhir VPC di subnet Anda. Kami menetapkan alamat IP ke setiap antarmuka jaringan titik akhir dari subnetnya, berdasarkan jenis alamat IP dari titik akhir VPC. Dalam lingkungan produksi, untuk ketersediaan dan ketahanan yang tinggi, kami merekomendasikan untuk mengonfigurasi setidaknya dua Availability Zone untuk setiap titik akhir VPC.

Jenis alamat IP

Endpoint sumber daya dapat mendukung alamat IPv4, IPv6, atau dualstack. Titik akhir yang mendukung IPv6 dapat merespons kueri DNS dengan catatan AAAA. Jenis alamat IP dari titik akhir sumber daya harus kompatibel dengan subnet untuk titik akhir sumber daya, seperti yang dijelaskan di sini:

- IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4.
- IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6.
- Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan endpoint Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6.

Jika titik akhir VPC sumber daya mendukung IPv4, antarmuka jaringan titik akhir memiliki alamat IPv4. Jika titik akhir VPC sumber daya mendukung IPv6, antarmuka jaringan titik akhir memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Jika Anda mendeskripsikan antarmuka jaringan endpoint dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Mengakses sumber daya melalui titik akhir VPC sumber daya

Anda dapat mengakses sumber daya VPC seperti nama domain, alamat IP, atau database Amazon RDS menggunakan titik akhir sumber daya. Titik akhir sumber daya menyediakan akses pribadi ke sumber daya. Saat Anda membuat titik akhir sumber daya, Anda menentukan konfigurasi sumber daya tipe tunggal, grup, atau ARN. Titik akhir sumber daya dapat dikaitkan dengan hanya

satu konfigurasi sumber daya. Konfigurasi sumber daya dapat mewakili satu sumber daya atau sekelompok sumber daya.

Prasyarat

Untuk membuat titik akhir sumber daya, Anda harus memenuhi prasyarat berikut.

- Anda harus memiliki konfigurasi sumber daya yang Anda buat atau akun lain yang dibuat dan dibagikan dengan Anda AWS RAM.
- Jika konfigurasi sumber daya dibagikan dengan Anda dari akun lain, Anda harus meninjau dan menerima pembagian sumber daya yang berisi konfigurasi sumber daya. Untuk informasi selengkapnya, lihat Menerima dan menolak undangan di Panduan Pengguna.AWS RAM

Buat titik akhir sumber daya VPC

Gunakan prosedur berikut untuk membuat titik akhir sumber daya VPC. Setelah membuat titik akhir sumber daya, Anda hanya dapat memodifikasi grup atau tag keamanannya.

Untuk membuat titik akhir sumber daya VPC

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Anda dapat menentukan nama untuk membuatnya lebih mudah untuk menemukan dan mengelola endpoint.
5. Untuk Jenis, pilih Sumber Daya.
6. Untuk konfigurasi Sumber Daya, pilih konfigurasi sumber daya.
7. Untuk pengaturan Jaringan, pilih VPC dari mana Anda akan mengakses sumber daya.
8. Jika, Anda ingin mengonfigurasi dukungan DNS pribadi untuk konfigurasi sumber daya, pilih Pengaturan tambahan, Aktifkan nama DNS. Untuk menggunakan fitur ini, pastikan atribut Aktifkan nama host DNS dan Aktifkan dukungan DNS diaktifkan untuk VPC Anda. Untuk informasi selengkapnya, lihat the section called “Nama domain khusus untuk konsumen sumber daya”.
9. Untuk Subnet, pilih subnet untuk membuat antarmuka jaringan endpoint di.

Dalam lingkungan produksi, untuk ketersediaan dan ketahanan yang tinggi, kami merekomendasikan untuk mengonfigurasi setidaknya dua Availability Zone untuk setiap titik akhir VPC.

10. Untuk grup Keamanan, pilih grup keamanan.

    Jika Anda tidak menentukan grup keamanan, kami mengaitkan grup keamanan default untuk VPC.

11. Pilih Buat titik akhir.

Untuk membuat titik akhir sumber daya menggunakan baris perintah

- buat-vpc-titik akhir ()AWS CLI
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Kelola titik akhir sumber daya

Setelah membuat titik akhir sumber daya, Anda dapat mengelola grup atau tag keamanannya.

Tugas

- Hapus titik akhir
- Perbarui titik akhir

Hapus titik akhir

Setelah selesai dengan titik akhir VPC, Anda dapat menghapusnya.

Untuk menghapus titik akhir menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta mengonfirmasi, pilih **`delete`**.
6. Pilih Hapus.

Untuk menghapus titik akhir menggunakan baris perintah

- hapus-vpc-titik akhir ()AWS CLI
- Remove-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Perbarui titik akhir

Anda dapat memperbarui titik akhir VPC.

Untuk memperbarui titik akhir menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir.
4. Pilih Tindakan, dan opsi yang sesuai.
5. Ikuti langkah-langkah konsol untuk mengirimkan pembaruan.

Untuk memperbarui titik akhir menggunakan baris perintah

- memodifikasi-vpc-titik akhir ()AWS CLI
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Konfigurasi sumber daya untuk sumber daya VPC

Konfigurasi sumber daya mewakili sumber daya atau sekelompok sumber daya yang ingin Anda buat dapat diakses oleh klien di VPC dan akun lain. Dengan mendefinisikan konfigurasi sumber daya, Anda dapat mengizinkan konektivitas jaringan pribadi, aman, searah ke sumber daya di VPC Anda dari klien di VPC dan akun lain. Konfigurasi sumber daya dikaitkan dengan gateway sumber daya yang melaluinya ia menerima lalu lintas.

Daftar Isi

- Nama domain khusus untuk pemilik jaringan layanan
- Definisi sumber daya
- Protokol
- Rentang pelabuhan
- Mengakses sumber daya
- Asosiasi dengan jenis jaringan layanan
- Jenis jaringan layanan
- Berbagi konfigurasi sumber daya melalui AWS RAM
- Memantau
- Membuat konfigurasi sumber daya di VPC Lattice
- Mengelola pengaitan konfigurasi sumber daya VPC Lattice

Jenis konfigurasi sumber daya

Konfigurasi sumber daya dapat terdiri dari beberapa jenis. Jenis yang berbeda membantu mewakili berbagai jenis sumber daya. Jenisnya adalah:

- Konfigurasi sumber daya tunggal: Alamat IP atau nama domain. Itu dapat dibagikan secara independen.
- Konfigurasi sumber daya grup: Kumpulan konfigurasi sumber daya anak. Itu dapat dibagikan secara independen.
- Konfigurasi sumber daya anak: Anggota konfigurasi sumber daya Grup. Ini mewakili alamat IP atau nama domain. Itu tidak dapat dibagikan secara independen; dan hanya dapat dibagikan sebagai bagian dari grup. Itu dapat ditambahkan dan dihapus dari grup dengan mulus. Ketika ditambahkan, secara otomatis dapat diakses oleh mereka yang dapat mengakses grup.
- Konfigurasi sumber daya ARN: Merupakan tipe sumber daya yang didukung yang disediakan oleh layanan. AWS Misalnya, database Amazon RDS. Konfigurasi sumber daya anak dikelola secara otomatis oleh AWS.

Gateway sumber daya

Konfigurasi sumber daya dikaitkan dengan gateway sumber daya. Resource gateway adalah satu set ENI yang berfungsi sebagai titik masuknya ke dalam VPC di mana sumber daya berada. Beberapa

konfigurasi sumber daya dapat dikaitkan dengan gateway sumber daya yang sama. Ketika klien di VPC atau akun lain mengakses sumber daya di VPC Anda, sumber daya melihat lalu lintas yang datang secara lokal dari gateway sumber daya di VPC tersebut.

Nama domain khusus untuk penyedia sumber daya

Penyedia sumber daya dapat melampirkan nama domain khusus ke konfigurasi sumber daya, sepertiexample.com, sumber daya yang dapat digunakan konsumen untuk mengakses konfigurasi sumber daya. Nama domain kustom dapat dimiliki dan diverifikasi oleh penyedia sumber daya, atau dapat berupa pihak ketiga atau AWS domain. Penyedia sumber daya dapat menggunakan konfigurasi sumber daya untuk berbagi cluster cache dan cluster Kafka, TLS-based aplikasi, atau sumber daya lainnya. AWS

Pertimbangan berikut berlaku untuk penyedia konfigurasi sumber daya:

- Konfigurasi sumber daya hanya dapat memiliki satu domain khusus.
- Nama domain kustom dari konfigurasi sumber daya tidak dapat diubah.
- Nama domain kustom dapat dilihat oleh semua konsumen konfigurasi sumber daya.
- Anda dapat memverifikasi nama domain kustom Anda menggunakan proses verifikasi nama domain di VPC Lattice. Untuk informasi lebih lanjut Untuk informasi lebih lanjut, lihathttps://docs.aws.amazon.com/vpc-lattice/latest/ug/create-and-verify.html.
- Untuk konfigurasi sumber daya grup tipe dan anak, Anda harus terlebih dahulu menentukan domain grup pada konfigurasi sumber daya grup. Setelah itu, konfigurasi sumber daya anak dapat memiliki domain kustom yang merupakan subdomain dari domain grup. Jika grup tidak memiliki domain grup, Anda dapat menggunakan nama domain khusus apa pun untuk anak, tetapi VPC Lattice tidak akan menyediakan zona yang dihosting untuk nama domain anak di VPC konsumen sumber daya.

Nama domain khusus untuk konsumen sumber daya

Ketika konsumen sumber daya mengaktifkan konektivitas ke konfigurasi sumber daya yang memiliki nama domain khusus, mereka dapat mengizinkan VPC Lattice untuk mengelola zona host pribadi Route 53 di VPC mereka. Konsumen sumber daya memiliki opsi terperinci untuk domain mana yang ingin mereka izinkan VPC Lattice mengelola zona host pribadi.

Konsumen sumber daya dapat mengatur `private-dns-enabled` parameter saat mengaktifkan konektivitas ke konfigurasi sumber daya melalui titik akhir sumber daya, titik akhir jaringan layanan,

atau asosiasi VPC jaringan layanan. Seiring dengan `private-dns-enabled` parameter, konsumen dapat menggunakan opsi DNS untuk menentukan domain mana yang mereka inginkan untuk VPC Lattice untuk mengelola zona host pribadi. Konsumen dapat memilih antara preferensi DNS pribadi berikut:

`ALL_DOMAINS`

VPC Lattice menyediakan zona host pribadi untuk semua nama domain kustom.

`VERIFIED_DOMAINS_ONLY`

VPC Lattice menyediakan zona host pribadi hanya jika nama domain kustom telah diverifikasi oleh penyedia.

`VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`

VPC Lattice menyediakan zona host pribadi untuk semua nama domain kustom terverifikasi dan nama domain lain yang ditentukan oleh konsumen sumber daya. Konsumen sumber daya menentukan nama domain dalam `private DNS specified domains` parameter.

`SPECIFIED_DOMAINS_ONLY`

VPC Lattice menyediakan zona host pribadi untuk nama domain yang ditentukan oleh konsumen sumber daya. Konsumen sumber daya menentukan nama domain dalam `private DNS specified domains` parameter.

Saat Anda mengaktifkan DNS pribadi, VPC Lattice membuat zona host pribadi di VPC Anda untuk nama domain kustom yang terkait dengan konfigurasi sumber daya. Secara default, preferensi DNS pribadi diatur ke`VERIFIED_DOMAINS_ONLY`. Ini berarti bahwa zona host pribadi dibuat hanya jika nama domain kustom telah diverifikasi oleh penyedia sumber daya. Jika Anda menyetel preferensi DNS pribadi Anda ke `ALL_DOMAINS` atau `SPECIFIED_DOMAINS_ONLY` kemudian VPC Lattice membuat zona yang dihosting pribadi terlepas dari status verifikasi nama domain kustom. Ketika zona host pribadi dibuat untuk domain tertentu, semua lalu lintas ke domain tersebut dari VPC Anda dirutekan melalui VPC Lattice. Kami menyarankan Anda menggunakan`ALL_DOMAINS`,`VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`, atau `SPECIFIED_DOMAINS_ONLY` preferensi hanya ketika Anda ingin lalu lintas ke nama domain kustom ini melalui VPC Lattice.

Kami menyarankan agar konsumen sumber daya menetapkan preferensi DNS pribadi mereka. `VERIFIED_DOMAINS_ONLY` Hal ini memungkinkan konsumen memperketat perimeter keamanan

mereka dengan hanya mengizinkan VPC Lattice untuk menyediakan zona host pribadi untuk domain terverifikasi di akun konsumen sumber daya.

Untuk memilih domain di domain yang ditentukan DNS pribadi, konsumen sumber daya dapat memasukkan nama domain yang sepenuhnya memenuhi syarat, seperti `my.example.com` atau menggunakan wildcard seperti. `*.example.com`

Pertimbangan berikut berlaku untuk konsumen konfigurasi sumber daya:

- Parameter berkemampuan DNS pribadi tidak dapat diubah.
- DNS pribadi harus diaktifkan pada asosiasi sumber daya jaringan layanan untuk host pribadi yang akan dibuat dalam VPC. Untuk konfigurasi sumber daya, status DNS pribadi yang diaktifkan dari asosiasi sumber daya jaringan layanan akan mengesampingkan status diaktifkan DNS pribadi dari titik akhir jaringan layanan atau asosiasi VPC jaringan layanan.

Untuk konfigurasi sumber daya yang merupakan target nama domain, entri zona host pribadi tidak dibuat jika berikut ini benar:

- Resource gateway berada di VPC yang sama dengan asosiasi VPC jaringan VPC endpoint/service jaringan layanan.
- Resolusi DNS diatur ke IN_VPC pada gateway sumber daya.
- Nama domain kustom atau domain grup adalah domain tingkat yang sama atau lebih tinggi dari target nama domain.

Nama domain khusus untuk pemilik jaringan layanan

Properti berkemampuan DNS pribadi dari asosiasi sumber daya jaringan layanan mengesampingkan properti berkemampuan DNS pribadi dari titik akhir jaringan layanan dan asosiasi VPC jaringan layanan.

Jika pemilik jaringan layanan membuat asosiasi sumber daya jaringan layanan dan tidak mengaktifkan DNS pribadi, VPC Lattice tidak akan menyediakan zona yang dihosting pribadi untuk konfigurasi sumber daya tersebut di VPC mana pun yang terhubung dengan jaringan layanan, meskipun DNS pribadi diaktifkan pada titik akhir jaringan layanan atau asosiasi VPC jaringan layanan.

Untuk konfigurasi sumber daya tipe ARN, bendera DNS pribadi benar dan tidak dapat diubah.

Definisi sumber daya

Dalam konfigurasi sumber daya, identifikasi sumber daya dengan salah satu cara berikut:

- Dengan Nama Sumber Daya Amazon (ARN): Jenis sumber daya yang didukung yang disediakan oleh layanan AWS , dapat diidentifikasi oleh ARN mereka. Hanya database Amazon RDS yang didukung. Anda tidak dapat membuat konfigurasi sumber daya untuk klaster yang dapat diakses publik.
- Dengan target nama domain: Anda dapat menggunakan nama domain apa pun. Jika Anda menggunakan server DNS pribadi atau domain Anda berada di zona host pribadi Route53, maka gateway sumber daya harus memiliki resolusi DNS yang disetel ke IN_VPC. Jika nama domain Anda menunjuk ke IP yang berada di luar VPC Anda, Anda harus memiliki gateway NAT di VPC Anda.
- Dengan IP-address: Untuk IPv4, tentukan IP pribadi dari rentang berikut: 10.0.0. 0/8, 100.64.0. 0/10, 172.16.0. 0/12, 192.168.0. 0/16. Untuk IPv6, tentukan IP dari VPC. IP publik tidak didukung.

Protokol

Saat Anda membuat konfigurasi sumber daya, Anda dapat menentukan protokol yang akan didukung oleh sumber daya. Saat ini, hanya protokol TCP yang didukung.

Rentang pelabuhan

Saat Anda membuat konfigurasi sumber daya, Anda dapat menentukan port yang akan menerima permintaan. Akses klien pada port lain tidak akan diizinkan.

Mengakses sumber daya

Konsumen dapat mengakses konfigurasi sumber daya langsung dari VPC mereka menggunakan titik akhir VPC atau melalui jaringan layanan. Sebagai konsumen, Anda dapat mengaktifkan akses dari VPC Anda ke konfigurasi sumber daya yang ada di akun Anda atau yang telah dibagikan dengan Anda dari akun lain melalui. AWS RAM

- Mengakses konfigurasi sumber daya secara langsung

  Anda dapat membuat titik akhir AWS PrivateLink VPC dari sumber daya tipe (titik akhir sumber daya) di VPC Anda untuk mengakses konfigurasi sumber daya secara pribadi dari VPC Anda.

Untuk informasi selengkapnya tentang cara membuat titik akhir sumber daya, lihat Mengakses sumber daya VPC di panduan pengguna.AWS PrivateLink

- Mengakses konfigurasi sumber daya melalui jaringan layanan

  Anda dapat mengaitkan konfigurasi sumber daya ke jaringan layanan, dan menghubungkan VPC Anda ke jaringan layanan. Anda dapat menghubungkan VPC Anda ke jaringan layanan baik melalui asosiasi atau menggunakan titik akhir VPC AWS PrivateLink jaringan layanan.

  Untuk informasi selengkapnya tentang asosiasi jaringan layanan, lihat Mengelola asosiasi untuk jaringan layanan VPC Lattice.

  Untuk informasi selengkapnya tentang titik akhir VPC jaringan layanan, lihat Mengakses jaringan layanan di panduan pengguna.AWS PrivateLink

Saat DNS pribadi diaktifkan untuk VPC, Anda tidak dapat membuat titik akhir sumber daya dan titik akhir jaringan layanan untuk konfigurasi sumber daya yang sama.

Asosiasi dengan jenis jaringan layanan

Ketika Anda berbagi konfigurasi sumber daya dengan akun konsumen, misalnya, melalui Account-B AWS RAM, Account-B dapat mengakses konfigurasi sumber daya baik secara langsung melalui titik akhir VPC sumber daya, atau melalui jaringan layanan.

Untuk mengakses konfigurasi sumber daya melalui jaringan layanan, harus Account-B mengaitkan konfigurasi sumber daya dengan jaringan layanan. Jaringan layanan dapat dibagikan antar akun. Jadi, Account-B dapat berbagi jaringan layanan mereka (yang terkait dengan konfigurasi sumber daya) Account-C, membuat sumber daya Anda dapat diakses dari Account-C.

Untuk mencegah berbagi transitif tersebut, Anda dapat menentukan bahwa konfigurasi sumber daya Anda tidak dapat ditambahkan ke jaringan layanan yang dapat dibagikan antar akun. Jika Anda menentukan ini, maka Account-B tidak akan dapat menambahkan konfigurasi sumber daya Anda ke jaringan layanan yang dibagikan atau dapat dibagikan dengan akun lain di masa mendatang.

Jenis jaringan layanan

Ketika Anda berbagi konfigurasi sumber daya dengan akun lain, misalnya Account-B, melalui AWS RAM, Account-B dapat mengakses sumber daya dalam salah satu dari tiga cara:

- Menggunakan titik akhir VPC dari sumber daya tipe (titik akhir VPC sumber daya).

- Menggunakan titik akhir VPC dari jenis jaringan layanan (titik akhir VPC jaringan layanan).
- Menggunakan asosiasi VPC jaringan layanan.

  Bila Anda menggunakan asosiasi jaringan layanan, setiap sumber daya diberi IP per subnet dari 129.224.0. 0/17 blok, yang AWS dimiliki dan tidak dapat dirutekan. Ini merupakan tambahan dari daftar awalan terkelola yang digunakan VPC Lattice untuk merutekan lalu lintas ke layanan melalui jaringan VPC Lattice. Kedua IP ini diperbarui ke tabel rute VPC Anda.

Untuk titik akhir VPC jaringan layanan dan asosiasi VPC jaringan layanan, konfigurasi sumber daya harus dimasukkan ke dalam jaringan layanan. Account-B Jaringan layanan dapat dibagikan antar akun. Jadi, Account-B dapat berbagi jaringan layanan mereka (yang berisi konfigurasi sumber daya) dengan Account-C, membuat sumber daya Anda dapat diakses dari Account-C. Untuk mencegah berbagi transitif seperti itu, Anda dapat melarang konfigurasi sumber daya Anda ditambahkan ke jaringan layanan yang dapat dibagikan antar akun. Jika Anda melarang ini, maka tidak Account-B akan dapat menambahkan konfigurasi sumber daya Anda ke jaringan layanan yang dibagikan atau dapat dibagikan dengan akun lain.

Berbagi konfigurasi sumber daya melalui AWS RAM

Konfigurasi sumber daya terintegrasi dengan AWS Resource Access Manager. Anda dapat membagikan konfigurasi sumber daya Anda dengan akun lain melalui AWS RAM. Saat Anda berbagi konfigurasi sumber daya dengan AWS akun, klien di akun tersebut dapat mengakses sumber daya secara pribadi. Anda dapat berbagi konfigurasi sumber daya menggunakan pembagian sumber daya di AWS RAM.

Gunakan AWS RAM konsol, untuk melihat pembagian sumber daya yang telah ditambahkan, sumber daya bersama yang dapat Anda akses, dan AWS akun yang telah berbagi sumber daya dengan Anda. Untuk informasi selengkapnya, lihat Sumber daya yang dibagikan dengan Anda di Panduan AWS RAM Pengguna.

Untuk mengakses sumber daya dari VPC lain di akun yang sama dengan konfigurasi sumber daya, Anda tidak perlu membagikan konfigurasi sumber daya. AWS RAM

Memantau

Anda dapat mengaktifkan log pemantauan pada konfigurasi sumber daya Anda. Anda dapat memilih tujuan untuk mengirim log ke.

Membuat konfigurasi sumber daya di VPC Lattice

Buat konfigurasi sumber daya.

Konsol Manajemen AWS

Untuk membuat konfigurasi sumber daya menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih Konfigurasi sumber daya.
3. Pilih Buat konfigurasi sumber daya.
4. Masukkan nama yang unik di AWS akun Anda. Anda tidak dapat mengubah nama ini setelah konfigurasi sumber daya dibuat.
5. Untuk jenis Konfigurasi, pilih Sumber daya untuk sumber daya tunggal atau turunan atau grup Sumber daya untuk grup sumber daya anak.
6. Pilih gateway sumber daya yang sebelumnya Anda buat atau buat sekarang.
7. (Opsional) Untuk memasukkan nama domain khusus, lakukan salah satu hal berikut:
   - Jika Anda memiliki konfigurasi sumber daya tipe tunggal, Anda dapat memasukkan nama domain khusus. Konsumen sumber daya dapat menggunakan nama domain ini untuk mengakses konfigurasi sumber daya Anda.
   - Jika Anda memiliki konfigurasi sumber daya tipe grup dan anak, Anda harus terlebih dahulu menentukan domain grup pada konfigurasi sumber daya grup. Selanjutnya, konfigurasi sumber daya anak dapat memiliki domain kustom yang merupakan subdomain dari domain grup.
8. (Opsional) Masukkan ID verifikasi.

   Berikan ID verifikasi jika Anda ingin nama domain Anda diverifikasi. Ini memungkinkan konsumen sumber daya tahu bahwa Anda memiliki nama domain.
9. Pilih pengenal sumber daya yang Anda inginkan untuk diwakili oleh konfigurasi sumber daya ini.
10. Pilih rentang port di mana Anda ingin berbagi sumber daya.
11. Untuk pengaturan Asosiasi, tentukan apakah konfigurasi sumber daya ini dapat dikaitkan dengan jaringan layanan yang dapat dibagikan.
12. Untuk konfigurasi sumber daya Bagikan, pilih pembagian sumber daya yang mengidentifikasi prinsipal yang dapat mengakses sumber daya ini.

13. (Opsional) Untuk Pemantauan, aktifkan log akses Sumber Daya dan tujuan pengiriman jika Anda ingin memantau permintaan dan tanggapan ke dan dari konfigurasi sumber daya.
14. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
15. Pilih Buat konfigurasi sumber daya.

AWS CLI

Perintah create-resource-configuration berikut membuat konfigurasi sumber daya tunggal dan mengaitkannya dengan nama domain kustom. `example.com`

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

Perintah create-resource-configuration berikut membuat konfigurasi sumber daya grup dan mengaitkannya dengan nama domain kustom. `example.com`

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

Perintah create-resource-configuration berikut membuat konfigurasi sumber daya anak dan mengaitkannya dengan nama domain kustom. `child.example.com`

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

Mengelola pengaitan konfigurasi sumber daya VPC Lattice

Akun konsumen tempat Anda berbagi konfigurasi sumber daya dan klien di akun Anda dapat mengakses konfigurasi sumber daya baik secara langsung menggunakan titik akhir VPC sumber daya atau melalui titik akhir jaringan layanan. Akibatnya konfigurasi sumber daya Anda akan memiliki asosiasi titik akhir dan asosiasi jaringan layanan.

Kelola asosiasi sumber daya jaringan layanan

Membuat atau menghapus asosiasi jaringan layanan.

> **Note**
>
> Jika Anda menerima pesan yang ditolak akses saat membuat asosiasi antara jaringan layanan dan konfigurasi sumber daya, periksa versi AWS RAM kebijakan Anda dan pastikan bahwa itu adalah versi 2. Untuk informasi selengkapnya, lihat panduan AWS RAM pengguna.

Untuk mengelola asosiasi layanan-jaringan menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih Konfigurasi sumber daya.
3. Pilih nama konfigurasi sumber daya untuk membuka halaman detailnya.
4. Pilih tab Asosiasi jaringan layanan.
5. Pilih Buat asosiasi.
6. Pilih jaringan layanan dari jaringan layanan VPC Lattice. Untuk membuat jaringan layanan, pilih Buat jaringan kisi VPC.
7. (Opsional) Untuk menambahkan tag, perluas tag asosiasi layanan, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
8. (Opsional) Untuk mengaktifkan nama DNS pribadi untuk asosiasi sumber daya jaringan layanan ini pilih aktifkan nama DNS pribadi. Untuk informasi selengkapnya, lihat the section called “Nama domain khusus untuk pemilik jaringan layanan”.
9. Pilih Simpan perubahan.
10. Untuk menghapus asosiasi, pilih kotak centang untuk asosiasi, lalu pilih Tindakan, Hapus. Saat diminta konfirmasi, masukkan **`confirm`**, lalu pilih Hapus.

Untuk membuat asosiasi jaringan layanan menggunakan AWS CLI

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

Untuk menghapus asosiasi jaringan layanan menggunakan AWS CLI

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

Kelola asosiasi titik akhir VPC sumber daya

Akun konsumen dengan akses ke konfigurasi sumber daya atau klien di akun Anda dapat mengakses konfigurasi sumber daya menggunakan titik akhir VPC sumber daya. Jika konfigurasi sumber daya Anda memiliki nama domain khusus, Anda dapat menggunakan aktifkan DNS pribadi untuk mengizinkan VPC Lattice menyediakan zona yang dihosting pribadi untuk titik akhir sumber daya atau titik akhir jaringan layanan Anda. Dengan ini, klien dapat langsung menggulung nama domain untuk mengakses konfigurasi sumber daya. Untuk informasi selengkapnya, lihat the section called “Nama domain khusus untuk konsumen sumber daya”.

Konsol Manajemen AWS

1. Untuk membuat asosiasi endpoint baru, buka PrivateLink dan Lattice di panel navigasi kiri dan pilih Endpoints.
2. Pilih Buat titik akhir.
3. Pilih konfigurasi sumber daya yang ingin Anda sambungkan ke VPC Anda.
4. Pilih VPC, subnet, dan grup keamanan.
5. (Opsional) Untuk mengaktifkan DNS pribadi dan mengkonfigurasi opsi DNS, pilih Aktifkan nama DNS.
6. (Opsional) Untuk menandai titik akhir VPC Anda, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
7. Pilih Buat titik akhir.

AWS CLI

Perintah create-vpc-endpoint berikut membuat titik akhir VPC yang menggunakan DNS pribadi. Preferensi DNS pribadi diatur ke `VERIFIED_AND_SELECTED` dan domain yang dipilih adalah `example.com` dan. `example.org` VPC Lattice hanya menyediakan zona host pribadi untuk domain terverifikasi atau atau. `example.com` `example.org`

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

Untuk membuat asosiasi titik akhir VPC menggunakan AWS CLI

Gunakan perintah create-vpc-endpoint.

Untuk menghapus asosiasi titik akhir VPC menggunakan AWS CLI

Gunakan perintah delete-vpc-endpoint.

Gateway sumber daya di VPC Lattice

Gateway sumber daya adalah titik lalu lintas masuk ke VPC tempat sumber daya berada. Ini mencakup beberapa Availability Zone.

VPC harus memiliki gateway sumber daya jika Anda berencana membuat sumber daya di dalam VPC dapat diakses dari VPC atau akun lain. Setiap sumber daya yang Anda bagikan dikaitkan dengan gateway sumber daya. Ketika klien di VPC atau akun lain mengakses sumber daya di VPC Anda, sumber daya melihat lalu lintas yang datang secara lokal dari gateway sumber daya di VPC tersebut. IP sumber lalu lintas adalah alamat IP dari gateway sumber daya. Anda dapat menetapkan beberapa alamat IP ke gateway sumber daya untuk memungkinkan lebih banyak koneksi jaringan dengan sumber daya. Beberapa sumber daya dalam VPC dapat dikaitkan dengan gateway sumber daya yang sama.

Gateway sumber daya tidak menyediakan kemampuan penyeimbangan beban.

Daftar Isi

- Alamat IPv4 per ENI
- Resolusi DNS Konfigurasi Sumber Daya
- Membuat gateway sumber daya di VPC Lattice
- Menghapus gateway sumber daya di VPC Lattice

Pertimbangan-pertimbangan

Pertimbangan berikut berlaku untuk gateway sumber daya:

- Agar sumber daya dapat diakses dari semua Availability Zone, Anda harus membuat gateway sumber daya untuk menjangkau sebanyak mungkin Availability Zone.
- Setidaknya satu Availability Zone dari titik akhir VPC dan gateway sumber daya harus tumpang tindih.
- VPC dapat memiliki maksimal 100 gateway sumber daya. Untuk informasi selengkapnya, lihat Kuota untuk Kisi VPC.
- Anda tidak dapat membuat gateway sumber daya di subnet bersama.

Grup keamanan

Anda dapat melampirkan grup keamanan ke gateway sumber daya. Aturan grup keamanan untuk gateway sumber daya mengontrol lalu lintas keluar dari gateway sumber daya ke sumber daya.

Aturan keluar yang disarankan untuk lalu lintas yang mengalir dari gateway sumber daya ke sumber daya database

Agar lalu lintas mengalir dari gateway sumber daya ke sumber daya, Anda harus membuat aturan keluar untuk protokol pendengar dan rentang port sumber daya yang diterima.

Destinasi	Protokol	Rentang port	Komentar
CIDR range for resource	TCP	3306	Mengizinkan lalu lintas dari gateway sumber daya ke database.

Jenis alamat IP

Gateway sumber daya dapat memiliki alamat IPv4, IPv6 atau dual-stack. Jenis alamat IP dari gateway sumber daya harus kompatibel dengan subnet gateway sumber daya dan jenis alamat IP sumber daya, seperti yang dijelaskan di sini:

- IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan gateway Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4, dan sumber daya juga memiliki alamat IPv4.
- IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan gateway Anda. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6, dan sumber daya juga memiliki alamat IPv6.
- Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan gateway Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6, dan sumber daya memiliki alamat IPv4 atau IPv6.

Jenis alamat IP dari gateway sumber daya tidak tergantung pada jenis alamat IP klien atau titik akhir VPC tempat sumber daya diakses.

Alamat IPv4 per ENI

Jika gateway sumber daya Anda memiliki IPv4 atau tipe alamat IP dual-stack, Anda dapat mengonfigurasi jumlah alamat IPv4 yang ditetapkan untuk setiap ENI gateway sumber daya Anda. Saat Anda membuat gateway sumber daya, Anda memilih dari 1 hingga 62 alamat IPv4. Setelah Anda mengatur jumlah alamat IPv4, nilainya tidak dapat diubah.

Alamat IPv4 digunakan untuk terjemahan alamat jaringan dan menentukan jumlah maksimum koneksi IPv4 bersamaan ke sumber daya. Secara default, semua gateway sumber daya ditetapkan 16 alamat IPv4 per ENI. Ini adalah jumlah IP yang cocok untuk membentuk koneksi dengan sumber daya backend Anda.

Jika gateway sumber daya Anda menggunakan jenis alamat IPv6, gateway sumber daya secara otomatis menerima /80 CIDR per ENI. Nilai ini tidak dapat diubah.

Resolusi DNS Konfigurasi Sumber Daya

Anda dapat menentukan bagaimana gateway sumber daya melakukan resolusi DNS untuk konfigurasi sumber daya yang merupakan target nama domain. Properti ini tetap. Anda dapat memilih:

- PUBLIC (default) - Nama domain diselesaikan menggunakan resolver DNS publik.
- IN_VPC - Nama domain diselesaikan menggunakan server DNS yang dikonfigurasi dalam kumpulan opsi DHCP dari VPC tempat gateway sumber daya berada. Anda harus menggunakan ini jika Anda menggunakan server DNS privat atau target nama domain Anda berada di zona yang di-hosting secara privat Route53.

Jika resolusi DNS adalah IN_VPC, Anda tidak dapat melampirkan konfigurasi sumber daya yang ditentukan oleh ARN ke gateway sumber daya. Anda tidak dapat menyetel Resolusi DNS ke IN_VPC jika gateway sumber daya menggunakan subnet. IPv6-only

Membuat gateway sumber daya di VPC Lattice

Gunakan konsol untuk membuat gateway sumber daya.

Untuk membuat gateway sumber daya menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih gateway sumber daya.
3. Pilih Buat gateway sumber daya.
4. Masukkan nama yang unik di AWS akun Anda.
5. Pilih jenis alamat IP untuk gateway sumber daya.
6. Untuk jenis alamat IP, pilih jenis alamat IP untuk gateway sumber daya.

    - Jika Anda memilih IPv4 atau Dualstack untuk jenis alamat IP, Anda dapat memasukkan jumlah alamat IPv4 per ENI untuk gateway sumber daya Anda.

      Defaultnya adalah 16 alamat IPv4 per ENI. Ini adalah jumlah IP yang cocok untuk membentuk koneksi dengan sumber daya backend Anda.
7. Pilih VPC tempat sumber daya berada.
8. Untuk grup Keamanan, pilih hingga lima grup keamanan untuk mengontrol lalu lintas masuk dari VPC ke jaringan layanan.
9. Untuk Resolusi DNS Konfigurasi Sumber Daya, pilih cara DNS diselesaikan untuk target nama domain.

    - Jika Anda menggunakan server DNS pribadi atau target nama domain Anda berada di zona host pribadi Route53, atur ke IN_VPC

10. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
11. Pilih Buat gateway sumber daya.

Untuk membuat gateway sumber daya menggunakan AWS CLI

Gunakan perintah create-resource-gateway.

Menghapus gateway sumber daya di VPC Lattice

Gunakan konsol untuk menghapus gateway sumber daya.

Untuk menghapus gateway sumber daya menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih gateway sumber daya.
3. Pilih kotak centang untuk gateway sumber daya yang ingin Anda hapus dan pilih Tindakan, Hapus. Saat diminta konfirmasi, masukkan **`confirm`**, lalu pilih Hapus.

Untuk menghapus gateway sumber daya menggunakan AWS CLI

Gunakan perintah delete-resource-gateway.

Akses jaringan layanan melalui AWS PrivateLink

Anda dapat terhubung secara pribadi ke jaringan layanan dari VPC Anda menggunakan titik akhir VPC jaringan layanan (titik akhir jaringan layanan). Endpoint jaringan layanan memungkinkan Anda mengakses sumber daya dan layanan yang terkait dengan jaringan layanan secara pribadi dan aman. Dengan cara ini, Anda dapat mengakses beberapa sumber daya dan layanan secara pribadi melalui satu titik akhir VPC.

Jaringan layanan adalah kumpulan logis konfigurasi sumber daya dan layanan VPC Lattice. Dengan menggunakan titik akhir jaringan layanan, Anda dapat menghubungkan jaringan layanan ke VPC, dan mengakses sumber daya dan layanan tersebut secara pribadi dari VPC atau dari lokal. Endpoint jaringan layanan memungkinkan Anda terhubung ke satu jaringan layanan. Untuk terhubung ke beberapa jaringan layanan dari VPC Anda, Anda dapat membuat beberapa titik akhir jaringan layanan, masing-masing menunjuk ke jaringan layanan yang berbeda.

Jaringan layanan terintegrasi dengan AWS Resource Access Manager (AWS RAM). Anda dapat berbagi jaringan layanan Anda dengan akun lain melalui AWS RAM. Ketika Anda berbagi jaringan layanan dengan AWS akun lain, akun tersebut dapat membuat titik akhir jaringan layanan untuk terhubung ke jaringan layanan. Anda dapat berbagi jaringan layanan menggunakan pembagian sumber daya di AWS RAM.

Gunakan AWS RAM konsol, untuk melihat pembagian sumber daya yang telah ditambahkan, jaringan layanan bersama yang dapat Anda akses, dan AWS akun yang telah berbagi sumber daya dengan Anda. Untuk informasi selengkapnya, lihat Sumber daya yang dibagikan dengan Anda di Panduan AWS RAM Pengguna.

Harga

Anda ditagih setiap jam untuk konfigurasi sumber daya yang terkait dengan jaringan layanan Anda. Anda juga ditagih per GB data yang diproses saat mengakses sumber daya melalui titik akhir VPC jaringan layanan. Anda tidak ditagih setiap jam untuk titik akhir VPC jaringan layanan itu sendiri. Untuk informasi selengkapnya, lihat harga Amazon VPC Lattice.

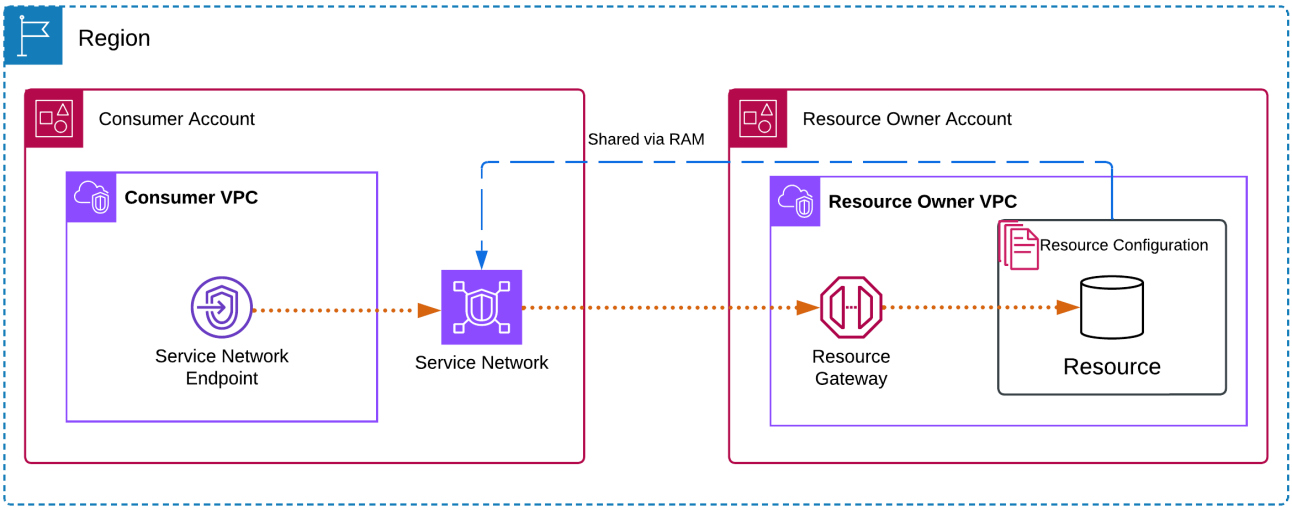
Daftar Isi

- Subnet dan Availability Zone
- Jenis alamat IP
- Mengakses jaringan layanan melalui titik akhir jaringan layanan
- Kelola titik akhir jaringan layanan

Ikhtisar

Anda dapat membuat jaringan layanan Anda sendiri, atau jaringan layanan dapat dibagikan dengan Anda dari akun lain. Either way, Anda dapat membuat endpoint jaringan layanan untuk menghubungkannya dari VPC Anda. Untuk informasi selengkapnya tentang cara membuat jaringan layanan dan mengaitkan konfigurasi sumber daya dengannya, lihat Panduan Pengguna Amazon VPC Lattice.

Diagram berikut menunjukkan bagaimana titik akhir jaringan layanan di VPC Anda mengakses jaringan layanan.



Koneksi jaringan hanya dapat dimulai dari VPC yang memiliki titik akhir jaringan layanan ke sumber daya dan layanan di jaringan layanan. VPC dengan sumber daya dan layanan tidak dapat memulai koneksi jaringan ke VPC endpoint.

Nama host DNS

Dengan AWS PrivateLink, Anda mengirim lalu lintas ke jaringan layanan menggunakan titik akhir pribadi. Saat Anda membuat titik akhir VPC jaringan layanan, kami membuat nama DNS Regional

(disebut nama DNS default) untuk setiap sumber daya dan layanan yang dapat Anda gunakan untuk berkomunikasi dengan sumber daya dan layanan dari VPC Anda dan dari tempat. Alamat IP yang terkait dengan titik akhir dapat berubah. Kami menyarankan Anda menggunakan DNS alih-alih IP endpoint untuk terhubung ke jaringan layanan Anda.

Nama DNS default untuk sumber daya di jaringan layanan memiliki sintaks berikut:

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

Nama DNS default untuk layanan Lattice di jaringan layanan memiliki sintaks berikut:

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

Jika Anda menggunakan Konsol Manajemen AWS, Anda dapat menemukan nama DNS di bawah tab Asosiasi. Jika Anda menggunakan AWS CLI, gunakan perintah describe-vpc-endpoint-associations.

Anda hanya dapat mengaktifkan DNS pribadi ketika jaringan layanan Anda memiliki konfigurasi ARN-type sumber daya ke layanan database Amazon RDS. Dengan DNS pribadi, Anda dapat terus membuat permintaan ke sumber daya menggunakan nama DNS yang disediakan untuk sumber daya oleh AWS layanan, sambil memanfaatkan konektivitas pribadi melalui titik akhir VPC jaringan layanan. Untuk informasi selengkapnya, lihat the section called “Resolusi DNS”.

Resolusi DNS

Saat Anda membuat endpoint jaringan layanan, kami membuat nama DNS untuk setiap konfigurasi sumber daya dan layanan Lattice yang terkait dengan jaringan layanan. Catatan DNS ini bersifat publik. Oleh karena itu, nama-nama DNS ini dapat diselesaikan secara publik. Namun, permintaan DNS dari luar VPC masih mengembalikan alamat IP pribadi dari antarmuka jaringan titik akhir jaringan layanan. Anda dapat menggunakan nama DNS ini untuk mengakses sumber daya dan layanan dari tempat, selama Anda memiliki akses ke VPC tempat titik akhir jaringan layanan berada, melalui VPN atau Direct Connect.

DNS privat

Jika Anda mengaktifkan DNS pribadi untuk titik akhir VPC jaringan layanan Anda, dan VPC Anda mengaktifkan nama host DNS dan resolusi DNS, kami membuat zona host pribadi terkelola AWS

tersembunyi untuk konfigurasi sumber daya yang memiliki nama DNS khusus. Zona yang dihosting berisi kumpulan catatan untuk nama DNS default untuk sumber daya yang menyelesaikannya ke alamat IP pribadi antarmuka jaringan titik akhir jaringan layanan di VPC Anda.

Amazon menyediakan server DNS untuk VPC Anda, yang disebut Resolver Route 53. Resolver Route 53 secara otomatis menyelesaikan nama domain VPC lokal dan merekam di zona host pribadi. Namun, Anda tidak dapat menggunakan Resolver Route 53 dari luar VPC Anda. Jika ingin mengakses titik akhir VPC dari jaringan lokal, Anda dapat menggunakan nama DNS default atau Anda dapat menggunakan titik akhir Route 53 Resolver dan aturan Resolver. Untuk informasi selengkapnya, lihat Mengintegrasikan AWS Transit Gateway dengan AWS PrivateLink dan Amazon Route 53 Resolver.

Subnet dan Availability Zone

Anda dapat mengonfigurasi titik akhir VPC Anda dengan satu subnet per Availability Zone. Kami membuat sebuah elastic network interface untuk endpoint VPC di subnet Anda. Kami menetapkan alamat IP untuk setiap elastic network interface dari subnetnya dalam kelipatan/28, jika jenis alamat IP dari titik akhir VPC adalah IPv4. Jumlah alamat IP yang ditetapkan di setiap subnet tergantung pada jumlah konfigurasi sumber daya dan kami menambahkan IP tambahan di/28 blok sesuai kebutuhan. Dalam lingkungan produksi, untuk ketersediaan dan ketahanan yang tinggi, kami merekomendasikan untuk mengonfigurasi setidaknya dua Availability Zone untuk setiap titik akhir VPC dan memiliki IP yang berdekatan.

Jenis alamat IP

Service-network endpoint dapat mendukung alamat IPv4, IPv6, atau dual-stack. Titik akhir yang mendukung IPv6 dapat merespons kueri DNS dengan catatan AAAA. Jenis alamat IP dari titik akhir jaringan layanan harus kompatibel dengan subnet untuk titik akhir sumber daya, seperti yang dijelaskan di sini:

- IPv4 — Tetapkan alamat IPv4 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4.
- IPv6 — Tetapkan alamat IPv6 ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih hanya subnet IPv6.
- Dualstack — Tetapkan alamat IPv4 dan IPv6 ke antarmuka jaringan endpoint Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang alamat IPv4 dan IPv6.

Jika titik akhir VPC jaringan layanan mendukung IPv4, antarmuka jaringan titik akhir memiliki alamat IPv4. Jika titik akhir VPC jaringan layanan mendukung IPv6, antarmuka jaringan titik akhir memiliki alamat IPv6. Alamat IPv6 untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Jika Anda menggambarkan antarmuka jaringan titik akhir dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Mengakses jaringan layanan melalui titik akhir jaringan layanan

Anda dapat mengakses jaringan layanan menggunakan titik akhir jaringan layanan. Endpoint jaringan layanan menyediakan akses pribadi ke konfigurasi sumber daya dan layanan di jaringan layanan.

Prasyarat

Untuk membuat titik akhir jaringan layanan, Anda harus memenuhi prasyarat berikut.

- Anda harus memiliki jaringan layanan yang dibuat oleh Anda atau dibagikan dengan Anda dari akun lain melalui AWS RAM.
- Jika jaringan layanan dibagikan dengan Anda dari akun lain, Anda harus meninjau dan menerima pembagian sumber daya yang berisi jaringan layanan. Untuk informasi selengkapnya, lihat Menerima dan menolak undangan di Panduan Pengguna.AWS RAM
- Titik akhir jaringan layanan awalnya memerlukan blok /28 alamat IPv4 yang berdekatan yang tersedia di Availability Zone. Jika Anda menambahkan konfigurasi sumber daya ke jaringan layanan yang terkait dengan titik akhir Anda, Anda memerlukan blok /28 tambahan yang tersedia di subnet yang sama, karena setiap sumber daya mengkonsumsi IP unik per Availability Zone.

  Jika Anda berencana menambahkan lebih dari 16 konfigurasi sumber daya ke jaringan layanan, blok /28 tambahan akan digunakan pada titik akhir jaringan layanan untuk mengakomodasi sumber daya baru. Sebaiknya jika Anda perlu menghindari penggunaan IP VPC CIDR, Anda menggunakan asosiasi VPC jaringan layanan. Untuk informasi selengkapnya, lihat Mengelola asosiasi titik akhir VPC di Panduan Pengguna Amazon VPC Lattice.

Buat titik akhir jaringan layanan

Buat titik akhir jaringan layanan untuk mengakses jaringan layanan yang dibagikan dengan Anda. Setelah membuat endpoint jaringan layanan, Anda hanya dapat memodifikasi grup atau tag keamanannya.

Untuk membuat titik akhir jaringan layanan

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih Endpoints.
3. Pilih Buat titik akhir.
4. Anda dapat menentukan nama untuk membuatnya lebih mudah untuk menemukan dan mengelola endpoint.
5. Untuk Jenis, pilih Jaringan layanan.
6. Untuk jaringan Layanan, pilih jaringan layanan.
7. Untuk pengaturan Jaringan, pilih VPC Anda dari mana Anda akan mengakses jaringan layanan.
8. Jika, Anda ingin mengonfigurasi dukungan DNS pribadi, pilih Pengaturan tambahan, Aktifkan nama DNS pribadi. Untuk menggunakan fitur ini, pastikan atribut Aktifkan nama host DNS dan Aktifkan dukungan DNS diaktifkan untuk VPC Anda.
9. Untuk Subnet, pilih subnet untuk membuat antarmuka jaringan endpoint di.

   Dalam lingkungan produksi, untuk ketersediaan dan ketahanan yang tinggi, kami merekomendasikan untuk mengonfigurasi setidaknya dua Availability Zone untuk setiap titik akhir VPC.
10. Untuk grup Keamanan, pilih grup keamanan.

    Jika Anda tidak menentukan grup keamanan, kami mengaitkan grup keamanan default untuk VPC.
11. Pilih Buat titik akhir.

Untuk membuat endpoint layanan-jaringan menggunakan baris perintah

- buat-vpc-titik akhir ()AWS CLI
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Kelola titik akhir jaringan layanan

Setelah membuat titik akhir jaringan layanan, Anda dapat memperbarui grup atau tag keamanannya.

Tugas

- Hapus titik akhir

- Memperbarui titik akhir jaringan layanan

Hapus titik akhir

Setelah selesai dengan titik akhir VPC, Anda dapat menghapusnya.

Untuk menghapus titik akhir menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir jaringan layanan.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta mengonfirmasi, pilih **`delete`**.
6. Pilih Hapus.

Untuk menghapus titik akhir menggunakan baris perintah

- hapus-vpc-titik akhir ()AWS CLI
- Remove-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Memperbarui titik akhir jaringan layanan

Anda dapat memperbarui titik akhir VPC.

Untuk memperbarui titik akhir menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir.
4. Pilih Tindakan, dan opsi yang sesuai.
5. Ikuti langkah-langkah konsol untuk mengirimkan pembaruan.

Untuk memperbarui titik akhir menggunakan baris perintah

- memodifikasi-vpc-titik akhir ()AWS CLI

- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Identitas dan manajemen akses untuk AWS PrivateLink

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. AWS PrivateLink IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Daftar Isi

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan. AWS PrivateLink

Pengguna layanan — Jika Anda menggunakan AWS PrivateLink layanan untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak AWS PrivateLink fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda.

Administrator layanan — Jika Anda bertanggung jawab atas AWS PrivateLink sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS PrivateLink. Tugas Anda adalah menentukan AWS PrivateLink fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda sebaiknya mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke AWS PrivateLink.

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensil dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensional. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensil dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk

informasi selengkapnya, lihat Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh

identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCP) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana AWS PrivateLink bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses AWS PrivateLink, pelajari fitur IAM yang tersedia untuk digunakan. AWS PrivateLink

Fitur IAM	AWS PrivateLink dukungan
Identity-based kebijakan	Ya
Resource-based kebijakan	Ya
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Service-linked peran	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara AWS PrivateLink dan Layanan AWS pekerjaan lainnya dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Identity-based kebijakan untuk AWS PrivateLink

Mendukung kebijakan berbasis identitas: Ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. 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 Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan 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. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Identity-based contoh kebijakan untuk AWS PrivateLink

Untuk melihat contoh kebijakan AWS PrivateLink berbasis identitas, lihat. Identity-based contoh kebijakan untuk AWS PrivateLink

Resource-based kebijakan dalam AWS PrivateLink

Mendukung kebijakan berbasis sumber daya: Ya

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. 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 principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

AWS PrivateLink Layanan mendukung satu jenis kebijakan berbasis sumber daya, yang dikenal sebagai kebijakan titik akhir. Kebijakan endpoint mengontrol AWS prinsipal mana yang dapat

menggunakan endpoint untuk mengakses layanan endpoint. Untuk informasi selengkapnya, lihat the section called “Kebijakan titik akhir”.

Tindakan kebijakan untuk AWS PrivateLink

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan di namespace ec2

Beberapa tindakan untuk AWS PrivateLink adalah bagian dari Amazon EC2 API. Tindakan kebijakan ini menggunakan `ec2` awalan. Untuk informasi selengkapnya, lihat AWS PrivateLink tindakan di Referensi API Amazon EC2.

Tindakan di namespace vpce

AWS PrivateLink juga menyediakan tindakan `AllowMultiRegion` hanya izin. Tindakan kebijakan ini menggunakan `vpce` awalan.

Sumber daya kebijakan untuk AWS PrivateLink

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Kunci kondisi kebijakan untuk AWS PrivateLink

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. 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. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Kunci kondisi berikut khusus untuk AWS PrivateLink:

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

Untuk informasi selengkapnya, lihat Kunci kondisi untuk Amazon EC2.

ACL di AWS PrivateLink

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal 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.

ABAC dengan AWS PrivateLink

Mendukung ABAC (tanda dalam kebijakan): Ya

Attribute-based Access Control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut yang disebut tag. Anda dapat melampirkan tag ke entitas dan AWS sumber daya

IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda 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 Tentukan izin dengan otorisasi 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 AWS PrivateLink

Mendukung kredensial sementara: Ya

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Cross-service izin utama untuk AWS PrivateLink

Mendukung sesi akses terusan (FAS): Ya

Sesi akses teruskan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

Peran layanan untuk AWS PrivateLink

Mendukung peran layanan: Tidak

Peran layanan adalah 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 Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

Service-linked peran untuk AWS PrivateLink

Mendukung peran terkait layanan: Tidak

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

Identity-based contoh kebijakan untuk AWS PrivateLink

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau mengubah sumber daya AWS PrivateLink . Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS PrivateLink, termasuk format ARN untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk Amazon EC2 di Referensi Otorisasi Layanan.

Contoh

- Kontrol penggunaan titik akhir VPC
- Kontrol pembuatan titik akhir VPC berdasarkan pemilik layanan
- Kontrol nama DNS pribadi yang dapat ditentukan untuk layanan titik akhir VPC
- Kontrol nama layanan yang dapat ditentukan untuk layanan titik akhir VPC

Kontrol penggunaan titik akhir VPC

Secara default, pengguna tidak memiliki izin untuk bekerja dengan titik akhir. Anda dapat membuat kebijakan berbasis identitas yang memberikan izin kepada pengguna untuk membuat, memodifikasi, mendeskripsikan, dan menghapus titik akhir. Berikut adalah contohnya.

JSON

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

```
    "Statement":[
        {
            "Effect": "Allow",
            "Action":"ec2:*VpcEndpoint*",
            "Resource":"*"
        }
    ]
}
```

Untuk informasi tentang mengontrol akses ke layanan menggunakan titik akhir VPC, lihat. the section called “Kebijakan titik akhir”

Kontrol pembuatan titik akhir VPC berdasarkan pemilik layanan

Anda dapat menggunakan tombol `ec2:VpceServiceOwner` kondisi untuk mengontrol titik akhir VPC apa yang dapat dibuat berdasarkan siapa yang memiliki layanan (`amazon`,`aws-marketplace`, atau ID akun). Contoh berikut memberikan izin untuk membuat titik akhir VPC dengan pemilik layanan yang ditentukan. Untuk menggunakan contoh ini, ganti Wilayah, ID akun, dan pemilik layanan.

JSON

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

```
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceOwner": [
                        "amazon"
                    ]
                }
            }
        }
    ]
}
```

Kontrol nama DNS pribadi yang dapat ditentukan untuk layanan titik akhir VPC

Anda dapat menggunakan tombol `ec2:VpceServicePrivateDnsName` kondisi untuk mengontrol layanan titik akhir VPC apa yang dapat dimodifikasi atau dibuat berdasarkan nama DNS pribadi yang terkait dengan layanan titik akhir VPC. Contoh berikut memberikan izin untuk membuat layanan titik akhir VPC dengan nama DNS pribadi yang ditentukan. Untuk menggunakan contoh ini, ganti Region, ID akun, dan nama DNS pribadi.

JSON

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

```
            }
        }
    ]
}
```

Kontrol nama layanan yang dapat ditentukan untuk layanan titik akhir VPC

Anda dapat menggunakan tombol `ec2:VpceServiceName` kondisi untuk mengontrol titik akhir VPC apa yang dapat dibuat berdasarkan nama layanan titik akhir VPC. Contoh berikut memberikan izin untuk membuat titik akhir VPC dengan nama layanan yang ditentukan. Untuk menggunakan contoh ini, ganti Region, ID akun, dan nama layanan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc/*",
                "arn:aws:ec2:us-east-1:111111111111:security-group/*",
                "arn:aws:ec2:us-east-1:111111111111:subnet/*",
                "arn:aws:ec2:us-east-1:111111111111:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.111111111111.s3"
                    ]
                }
            }
        }
```

```
    ]
}
```

Kontrol akses ke titik akhir VPC menggunakan kebijakan titik akhir

Kebijakan endpoint adalah kebijakan berbasis sumber daya yang Anda lampirkan ke titik akhir VPC untuk mengontrol AWS prinsipal mana yang dapat menggunakan titik akhir untuk mengakses. Layanan AWS

Kebijakan endpoint tidak mengesampingkan atau mengganti kebijakan berbasis identitas atau kebijakan berbasis sumber daya. Misalnya, jika Anda menggunakan titik akhir antarmuka untuk terhubung ke Amazon S3, Anda juga dapat menggunakan kebijakan bucket Amazon S3 untuk mengontrol akses ke bucket dari titik akhir tertentu atau VPC tertentu.

Daftar Isi

Pertimbangan-pertimbangan

- Kebijakan endpoint adalah dokumen kebijakan JSON yang menggunakan bahasa kebijakan IAM. Itu harus mengandung elemen Principal. Ukuran kebijakan endpoint tidak boleh melebihi 20.480 karakter, termasuk spasi putih.
- Saat membuat antarmuka atau titik akhir gateway untuk sebuah Layanan AWS, Anda dapat melampirkan kebijakan titik akhir tunggal ke titik akhir. Anda dapat memperbarui kebijakan endpoint kapan saja. Jika Anda tidak melampirkan kebijakan endpoint, kami melampirkan kebijakan endpoint default.
- Tidak semua Layanan AWS mendukung kebijakan titik akhir. Jika Layanan AWS tidak mendukung kebijakan titik akhir, kami mengizinkan akses penuh ke titik akhir apa pun untuk layanan. Untuk informasi selengkapnya, lihat the section called “Lihat dukungan kebijakan titik akhir”.
- Saat Anda membuat titik akhir VPC untuk layanan endpoint selain layanan Layanan AWS, kami mengizinkan akses penuh ke titik akhir.

- Anda tidak dapat menggunakan karakter wildcard (* atau?) atau operator kondisi numerik dengan kunci konteks global yang mereferensikan pengidentifikasi yang dihasilkan sistem (misalnya, atau). `aws:PrincipalAccount` `aws:SourceVpc`
- Bila Anda menggunakan operator kondisi string, Anda harus menggunakan setidaknya enam karakter berturut-turut sebelum atau setelah setiap karakter wildcard.
- Saat Anda menentukan ARN dalam elemen sumber daya atau kondisi, bagian akun ARN dapat menyertakan ID akun atau karakter wildcard, tetapi tidak keduanya.
- Setelah memperbarui kebijakan titik akhir, perlu beberapa menit agar perubahan diterapkan.

Kebijakan titik akhir default

Kebijakan endpoint default memberikan akses penuh ke titik akhir.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Kebijakan untuk titik akhir antarmuka

Misalnya kebijakan titik akhir untuk Layanan AWS, lihatthe section called “Layanan yang terintegrasi”. Kolom pertama dalam tabel berisi tautan ke AWS PrivateLink dokumentasi untuk masing-masing Layanan AWS. Jika Layanan AWS mendukung kebijakan titik akhir, dokumentasinya menyertakan contoh kebijakan titik akhir.

Prinsip untuk titik akhir gateway

Dengan titik akhir gateway, `Principal` elemen harus diatur ke*. Untuk menentukan prinsipal, gunakan tombol `aws:PrincipalArn` kondisi.

```
"Condition": {
```

```
    "StringEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
    }
}
```

Jika Anda menentukan prinsipal dalam format berikut, akses diberikan kepada Pengguna root akun AWS satu-satunya, tidak semua pengguna dan peran untuk akun.

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

Misalnya kebijakan titik akhir untuk titik akhir gateway, lihat berikut ini:

- Titik akhir untuk Amazon S3
- Titik akhir untuk DynamoDB

Memperbarui kebijakan titik akhir VPC

Gunakan prosedur berikut untuk memperbarui kebijakan titik akhir untuk. Layanan AWS Setelah memperbarui kebijakan titik akhir, perlu beberapa menit agar perubahan diterapkan.

Untuk memperbarui kebijakan titik akhir menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir VPC.
4. Pilih Tindakan, Kelola kebijakan.
5. Pilih Akses Penuh untuk mengizinkan akses penuh ke layanan, atau pilih Kustom dan lampirkan kebijakan kustom.
6. Pilih Simpan.

Untuk memperbarui kebijakan titik akhir menggunakan baris perintah

- memodifikasi-vpc-titik akhir ()AWS CLI
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

AWS kebijakan terkelola untuk AWS PrivateLink

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, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

AWS PrivateLink pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS PrivateLink sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat AWS PrivateLink dokumen.

Ubah	Deskripsi	Date
AWS PrivateLink mulai melacak perubahan	AWS PrivateLink mulai melacak perubahan untuk kebijakan AWS terkelolanya.	1 Maret 2021

CloudWatch metrik untuk AWS PrivateLink

AWS PrivateLink menerbitkan titik data ke Amazon CloudWatch untuk titik akhir antarmuka Anda, titik akhir Load Balancer Gateway, dan layanan titik akhir. CloudWatch memungkinkan Anda untuk mengambil statistik tentang titik-titik data tersebut sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Anggap metrik sebagai variabel untuk memantau, dan titik data sebagai nilai variabel tersebut dari waktu ke waktu. Setiap titik data memiliki timestamp terkait dan pengukuran unit opsional.

Anda dapat menggunakan metrik untuk memverifikasi bahwa sistem Anda bekerja sesuai harapan. Misalnya, Anda dapat membuat CloudWatch alarm untuk memantau metrik tertentu dan memulai tindakan (seperti mengirim pemberitahuan ke alamat email) jika metrik berada di luar rentang yang Anda anggap dapat diterima.

Metrik diterbitkan untuk semua titik akhir antarmuka, titik akhir Load Balancer Gateway, dan layanan titik akhir. Mereka tidak dipublikasikan untuk titik akhir gateway atau untuk konsumen layanan titik akhir yang menggunakan akses lintas wilayah. Secara default, AWS PrivateLink kirimkan metrik ke CloudWatch dalam interval satu menit, tanpa biaya tambahan.

Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Daftar Isi

Metrik dan dimensi titik akhir

`AWS/PrivateLinkEndpoints`Namespace menyertakan metrik berikut untuk titik akhir antarmuka dan titik akhir Gateway Load Balancer.

Metrik	Deskripsi
`ActiveConnections`	Jumlah koneksi aktif bersamaan. Ini termasuk koneksi dalam status SYN_SENT dan DESIGN.

Metrik	Deskripsi
	Kriteria pelaporan: Titik akhir menerima lalu lintas selama periode satu menit. Statistics: Statistik yang paling berguna adalah `Average`, `Maximum`, dan `Minimum`. Dimensi • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`BytesProcessed`	Jumlah byte yang dipertukarkan antara titik akhir dan layanan titik akhir, digabungkan di kedua arah. Ini adalah jumlah byte yang ditagih ke pemilik titik akhir. Tagihan menampilkan nilai ini dalam GB. Kriteria pelaporan: Titik akhir menerima lalu lintas selama periode satu menit. Statistik: Statistik yang paling berguna adalah`Average`,`Sum`,`Maximum`, dan`Minimum`. Dimensi • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Metrik	Deskripsi
`NewConnections`	Jumlah koneksi baru yang dibuat melalui titik akhir. Kriteria pelaporan: Titik akhir menerima lalu lintas selama periode satu menit. Statistik: Statistik yang paling berguna adalah`Average`,`Sum`,`Maximum`, dan`Minimum`. Dimensi • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`PacketsDropped`	Jumlah paket yang dijatuhkan oleh titik akhir. Metrik ini mungkin tidak menangkap semua drop paket. Peningkatan nilai dapat menunjukkan bahwa layanan endpoint atau endpoint tidak sehat. Kriteria pelaporan: Titik akhir menerima lalu lintas selama periode satu menit. Statistics: Statistik yang paling berguna adalah `Average`, `Sum`, dan `Maximum`. Dimensi • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Metrik	Deskripsi
`RstPacketsReceived`	Jumlah paket RST yang diterima oleh endpoint. Peningkatan nilai dapat menunjukkan bahwa layanan endpoint tidak sehat. Kriteria pelaporan: Titik akhir menerima lalu lintas selama periode satu menit. Statistics: Statistik yang paling berguna adalah `Average`, `Sum`, dan `Maximum`. Dimensi • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Untuk memfilter metrik ini, gunakan dimensi berikut.

Dimensi	Deskripsi
`Endpoint Type`	Memfilter data metrik berdasarkan tipe titik akhir (`Interface` |`GatewayLoadBalancer`).
`Service Name`	Memfilter data metrik berdasarkan nama layanan.
`Subnet Id`	Filter data metrik dengan subnet.
`VPC Endpoint Id`	Memfilter data metrik berdasarkan titik akhir VPC.
`VPC Id`	Memfilter data metrik oleh VPC.

Metrik dan dimensi layanan titik akhir

`AWS/PrivateLinkServices`Namespace menyertakan metrik berikut untuk layanan titik akhir.

Metrik	Deskripsi
`ActiveConnections`	Jumlah maksimum koneksi aktif dari klien ke target melalui titik akhir. Peningkatan nilai dapat menunjukkan perlunya menambahkan target ke penyeimbang beban. Kriteria pelaporan: Titik akhir yang terhubung ke layanan titik akhir mengirim lalu lintas selama periode satu menit. Statistik: Statistik yang paling berguna adalah `Average` dan `Maximum`. Dimensi • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`BytesProcessed`	Jumlah byte yang dipertukarkan antara layanan endpoint dan endpoint, di kedua arah. Kriteria pelaporan: Titik akhir yang terhubung ke layanan titik akhir mengirim lalu lintas selama periode satu menit. Statistics: Statistik yang paling berguna adalah `Average`, `Sum`, dan `Maximum`. Dimensi • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`EndpointsCount`	Jumlah titik akhir yang terhubung ke layanan endpoint.

Metrik	Deskripsi
	Kriteria pelaporan: Ada nilai bukan nol selama periode lima menit. Statistik: Statistik yang paling berguna adalah `Average` dan `Maximum`. Dimensi • `Service Id`
`NewConnections`	Jumlah koneksi baru yang dibuat dari klien ke target melalui titik akhir. Peningkatan nilai dapat menunjukkan perlunya menambahkan target ke penyeimbang beban. Kriteria pelaporan: Titik akhir yang terhubung ke layanan titik akhir mengirim lalu lintas selama periode satu menit. Statistics: Statistik yang paling berguna adalah `Average`, `Sum`, dan `Maximum`. Dimensi • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Metrik	Deskripsi
`RstPacketsSent`	Jumlah paket RST yang dikirim ke endpoint oleh layanan endpoint. Peningkatan nilai dapat menunjukkan bahwa ada target yang tidak sehat. Kriteria pelaporan: Titik akhir yang terhubung ke layanan titik akhir mengirim lalu lintas selama periode satu menit. Statistics: Statistik yang paling berguna adalah `Average`, `Sum`, dan `Maximum`. Dimensi • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Untuk memfilter metrik ini, gunakan dimensi berikut.

Dimensi	Deskripsi
`Az`	Memfilter data metrik berdasarkan Availability Zone.
`Load Balancer Arn`	Memfilter data metrik berdasarkan penyeimbang beban.
`Service Id`	Memfilter data metrik berdasarkan layanan titik akhir.
`VPC Endpoint Id`	Memfilter data metrik berdasarkan titik akhir VPC.

Lihat CloudWatch metrik

Anda dapat melihat CloudWatch metrik ini menggunakan konsol VPC Amazon, konsol, atau CloudWatch sebagai AWS CLI berikut.

Untuk melihat metrik menggunakan konsol VPC Amazon

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Titik akhir. Pilih titik akhir Anda dan kemudian pilih tab Monitoring.
3. Di panel navigasi, pilih Layanan titik akhir. Pilih layanan endpoint Anda dan kemudian pilih tab Monitoring.

Untuk melihat metrik menggunakan konsol CloudWatch

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Metrik.
3. Pilih AWS/PrivateLinkEndpointsnamespace.
4. Pilih AWS/PrivateLinkServicesnamespace.

Untuk melihat metrik menggunakan AWS CLI

Gunakan perintah daftar-metrik berikut untuk mencantumkan metrik yang tersedia untuk titik akhir antarmuka dan titik akhir Load Balancer Gateway:

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

Gunakan perintah list-metrics berikut untuk mencantumkan metrik yang tersedia untuk layanan endpoint:

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

Gunakan aturan Wawasan Kontributor bawaan

AWS PrivateLink menyediakan aturan Contributor Insights bawaan untuk layanan endpoint Anda guna membantu Anda menemukan titik akhir mana yang merupakan kontributor terbesar untuk setiap metrik yang didukung. Untuk informasi selengkapnya, lihat Wawasan Kontributor di CloudWatch Panduan Pengguna Amazon.

AWS PrivateLink memberikan aturan berikut:

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1`— Memberi peringkat titik akhir berdasarkan jumlah koneksi aktif.

- `VpcEndpointService-BytesByEndpointId-v1`— Peringkat titik akhir dengan jumlah byte yang diproses.
- `VpcEndpointService-NewConnectionsByEndpointId-v1`— Peringkat titik akhir dengan jumlah koneksi baru.
- `VpcEndpointService-RstPacketsByEndpointId-v1`— Peringkat titik akhir dengan jumlah paket RST yang dikirim ke titik akhir.

Sebelum Anda dapat menggunakan aturan bawaan, Anda harus mengaktifkannya. Setelah Anda mengaktifkan aturan, aturan mulai mengumpulkan data kontributor. Untuk informasi tentang biaya untuk Wawasan Kontributor, lihat Harga Amazon CloudWatch .

Anda harus memiliki izin berikut untuk menggunakan Contributor Insights:

- `cloudwatch:DeleteInsightRules`— Untuk menghapus aturan Contributor Insights.
- `cloudwatch:DisableInsightRules`— Untuk menonaktifkan aturan Contributor Insights.
- `cloudwatch:GetInsightRuleReport`— Untuk mendapatkan datanya.
- `cloudwatch:ListManagedInsightRules`— Untuk mencantumkan aturan Contributor Insights yang tersedia.
- `cloudwatch:PutManagedInsightRules`— Untuk mengaktifkan aturan Contributor Insights.

Tugas

- Aktifkan aturan Contributor Insights
- Nonaktifkan aturan Wawasan Kontributor
- Hapus aturan Wawasan Kontributor

Aktifkan aturan Contributor Insights

Gunakan prosedur berikut untuk mengaktifkan aturan bawaan untuk AWS PrivateLink menggunakan salah satu Konsol Manajemen AWS atau AWS CLI.

Untuk mengaktifkan aturan Contributor Insights untuk AWS PrivateLink menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint Anda.

4. Pada tab Contributor Insights, pilih Aktifkan.
5. (Opsional) Secara default, semua aturan diaktifkan. Untuk mengaktifkan hanya aturan tertentu, pilih aturan yang tidak boleh diaktifkan dan kemudian pilih Tindakan, Nonaktifkan aturan. Ketika dimintai konfirmasi, pilih Nonaktifkan.

Untuk mengaktifkan aturan Contributor Insights untuk menggunakan AWS PrivateLink AWS CLI

1. Gunakan perintah list-managed-insight-rules sebagai berikut untuk menghitung aturan yang tersedia. Untuk `--resource-arn` opsi, tentukan ARN dari layanan endpoint Anda.

```
aws cloudwatch list-managed-insight-rules --resource-arn
 arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. Dalam output `list-managed-insight-rules` perintah, salin nama template dari `TemplateName` bidang. Berikut ini adalah contoh dari bidang ini.

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. Gunakan perintah put-managed-insight-rules sebagai berikut untuk mengaktifkan aturan. Anda harus menentukan nama template dan ARN dari layanan endpoint Anda.

```
aws cloudwatch put-managed-insight-rules --managed-rules
 TemplateName=VpcEndpointService-NewConnectionsByEndpointId-
v1,ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

Nonaktifkan aturan Wawasan Kontributor

Anda dapat menonaktifkan aturan bawaan AWS PrivateLink kapan saja. Setelah Anda menonaktifkan aturan, aturan berhenti mengumpulkan data kontributor, tetapi data kontributor yang ada disimpan hingga berusia 15 hari. Setelah Anda menonaktifkan aturan, Anda dapat mengaktifkannya lagi untuk melanjutkan pengumpulan data kontributor.

Untuk menonaktifkan aturan Contributor Insights untuk AWS PrivateLink menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint Anda.

4. Pada tab Contributor Insights, pilih Nonaktifkan semua untuk menonaktifkan semua aturan. Atau, perluas panel Aturan, pilih aturan yang akan dinonaktifkan, lalu pilih Tindakan, Nonaktifkan aturan
5. Ketika dimintai konfirmasi, pilih Nonaktifkan.

Untuk menonaktifkan aturan Contributor Insights untuk menggunakan AWS PrivateLink AWS CLI

Gunakan perintah disable-insight-rules untuk menonaktifkan aturan.

Hapus aturan Wawasan Kontributor

Gunakan prosedur berikut untuk menghapus aturan bawaan untuk AWS PrivateLink menggunakan salah satu Konsol Manajemen AWS atau AWS CLI. Setelah Anda menghapus aturan, aturan berhenti mengumpulkan data kontributor dan kami menghapus data kontributor yang ada.

Untuk menghapus aturan Contributor Insights untuk AWS PrivateLink menggunakan konsol

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Wawasan Wawasan Kontributor.
3. Perluas panel Aturan dan pilih aturan.
4. Pilih Tindakan, Hapus aturan.
5. Saat diminta konfirmasi, pilih Hapus.

Untuk menghapus aturan Contributor Insights untuk menggunakan AWS PrivateLink AWS CLI

Gunakan perintah delete-insight-rules untuk menghapus aturan.

AWS PrivateLink kuota

AWS Akun Anda memiliki kuota default, sebelumnya disebut sebagai batas, untuk setiap layanan. AWS Kecuali dinyatakan lain, setiap kuota adalah Region-specific. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan. Jika Anda meminta penambahan kuota yang berlaku per sumber daya, kami meningkatkan kuota untuk semua sumber daya di Wilayah.

Untuk meminta penambahan kuota, lihat Meminta penambahan kuota di Panduan Pengguna Service Quotas.

Permintaan throttling

Tindakan API untuk AWS PrivateLink adalah bagian dari Amazon EC2 API. Amazon EC2 membatasi permintaan API-nya di level tersebut. Akun AWS Untuk informasi selengkapnya, lihat Meminta pembatasan di Panduan Pengembang Amazon EC2. Selain itu, permintaan API juga dibatasi di tingkat organisasi untuk membantu kinerja. AWS PrivateLink Jika Anda menggunakan AWS Organizations dan menerima kode `RequestLimitExceeded` kesalahan saat Anda masih dalam batas API tingkat akun, lihat Cara mengidentifikasi AWS akun yang melakukan banyak panggilan API. Jika Anda memerlukan bantuan, hubungi tim akun Anda atau buka kasus dukungan teknis menggunakan layanan VPC dan kategori Titik Akhir VPC. Pastikan untuk melampirkan gambar kode `RequestLimitExceeded` kesalahan.

Kuota titik akhir VPC

AWS Akun Anda memiliki kuota berikut yang terkait dengan titik akhir VPC.

Nama	Default	Dapat disesuaikan	Komentar
Titik akhir antara muka dan Penyeimbang Beban Gateway per VPC	50	Ya	Ini adalah kuota gabungan untuk titik akhir antarmuka dan titik akhir Load Balancer Gateway
Titik akhir VPC Gateway per Wilayah	20	Ya	Anda dapat membuat hingga 255 titik akhir gateway per VPC

Nama	Default	Dapat disesuaikan	Komentar
Sumber daya VPC endpoint untuk VPC	200	Ya	
Layanan jaringan VPC endpoint untuk VPC	50	Ya	
Karakter per kebijakan VPC endpoint	20,480	Tidak	Ukuran maksimum kebijakan titik akhir VPC, termasuk spasi putih

Pertimbangan berikut berlaku untuk lalu lintas yang melewati titik akhir VPC:

- Secara default, setiap titik akhir VPC dapat mendukung bandwidth hingga 10 Gbps per Availability Zone, dan secara otomatis menskalakan hingga 100 Gbps. Bandwidth maksimum untuk titik akhir VPC, saat mendistribusikan beban di semua Availability Zone, adalah jumlah Availability Zone dikalikan dengan 100 Gbps. Jika aplikasi Anda membutuhkan throughput yang lebih tinggi, hubungi AWS dukungan.
- Unit transmisi maksimum (MTU) dari koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang diizinkan yang dapat dilewatkan melalui titik akhir VPC. Semakin besar MTU, semakin banyak data yang dapat dilewatkan dalam satu paket tunggal. VPC endpoint mendukung MTU 8500 byte. Paket dengan ukuran lebih besar dari 8500 byte yang tiba di VPC endpoint akan dijatuhkan.
- Path MTU Discovery (PMTUD) tidak didukung. Titik akhir VPC tidak menghasilkan pesan ICMP berikut: `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (Tipe 3, Kode 4).
- Titik akhir VPC memberlakukan penjepitan Ukuran Segmen Maksimum (MSS) untuk semua paket. Untuk informasi lebih lanjut, lihat RFC879.

Riwayat dokumen untuk AWS PrivateLink

Tabel berikut menjelaskan rilis untuk AWS PrivateLink.

Perubahan	Deskripsi	Tanggal
Akses sumber daya dan jaringan layanan	AWS PrivateLink mendukung akses sumber daya dan jaringan layanan di seluruh VPC dan batas akun.	Desember 1, 2024
Cross-Region akses	Penyedia layanan dapat meng-host layanan di satu Wilayah dan membuatnya tersedia dalam satu set AWS Wilayah. Konsumen layanan memilih Wilayah layanan saat membuat titik akhir.	November 26, 2024
Alamat IP yang ditunjuk	Anda dapat menentukan alamat IP untuk antarmuka jaringan titik akhir Anda saat membuat atau memodifikasi titik akhir VPC Anda.	17 Agustus 2023
Dukungan IPv6	Anda dapat mengonfigurasi layanan titik akhir Load Balancer Gateway dan titik akhir Load Balancer Gateway untuk mendukung alamat IPv4 dan IPv6 atau hanya alamat IPv6.	12 Desember 2022
Wawasan Kontributor	Anda dapat menggunakan aturan Contributor Insights bawaan untuk mengident ifikasi titik akhir tertentu	18 Agustus 2022

	yang merupakan kontributor teratas untuk metrik tersebut. CloudWatch AWS PrivateLink	
Dukungan IPv6	Penyedia layanan dapat mengaktifkan layanan endpoint mereka untuk menerima permintaan IPv6, bahkan jika layanan backend mereka hanya mendukung IPv4. Jika layanan endpoint menerima permintaan IPv6, konsumen layanan dapat mengaktifkan dukungan IPv6 untuk titik akhir antarmuka mereka sehingga mereka dapat mengakses layanan endpoint melalui IPv6.	Mei 11, 2022
CloudWatch metrik	AWS PrivateLink menerbitk an CloudWatch metrik untuk titik akhir antarmuka Anda, titik akhir Load Balancer Gateway, dan layanan titik akhir.	27 Januari 2022
Titik akhir Load Balancer Gateway	Anda dapat membuat endpoint Gateway Load Balancer di VPC Anda untuk mengarahk an lalu lintas ke layanan VPC endpoint yang Anda konfigura si menggunakan Gateway Load Balancer.	10 November 2020

Kebijakan titik akhir VPC	Anda dapat melampirkan kebijakan IAM ke titik akhir VPC antarmuka untuk layanan untuk AWS mengontrol akses ke layanan.	23 Maret 2020
Kunci kondisi untuk titik akhir VPC dan layanan titik akhir	Anda dapat menggunakan tombol kondisi EC2 untuk mengontrol akses ke titik akhir VPC dan layanan titik akhir.	6 Maret 2020
Menandai titik akhir VPC dan layanan endpoint pada pembuatan	Anda dapat menambahkan tag saat membuat titik akhir VPC dan layanan titik akhir.	5 Februari 2020
Nama DNS pribadi	Anda dapat mengakses layanan AWS PrivateLink berbasis dari dalam VPC Anda menggunakan nama DNS pribadi.	6 Januari 2020
Layanan titik akhir VPC	Anda dapat membuat layanan titik akhir Anda sendiri dan memungkinkan orang lain Akun AWS dan pengguna untuk terhubung ke layanan Anda melalui titik akhir VPC antarmuka. Anda dapat menawarkan layanan endpoint Anda untuk berlangganan di. AWS Marketplace	28 November 2017

Antarmuka titik akhir VPC untuk Layanan AWS	Anda dapat membuat titik akhir antarmuka untuk terhubung ke Layanan AWS yang terintegrasi dengan AWS PrivateLink tanpa menggunakan gateway internet atau perangkat NAT.	8 November 2017
Titik akhir VPC untuk DynamoDB	Anda dapat membuat titik akhir VPC gateway untuk mengakses Amazon DynamoDB dari VPC Anda tanpa menggunakan gateway internet atau perangkat NAT.	16 Agustus 2017
Titik akhir VPC untuk Amazon S3	Anda dapat membuat titik akhir VPC gateway untuk mengakses Amazon S3 dari VPC Anda tanpa menggunakan gateway internet atau perangkat NAT.	11 Mei 2015

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