AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

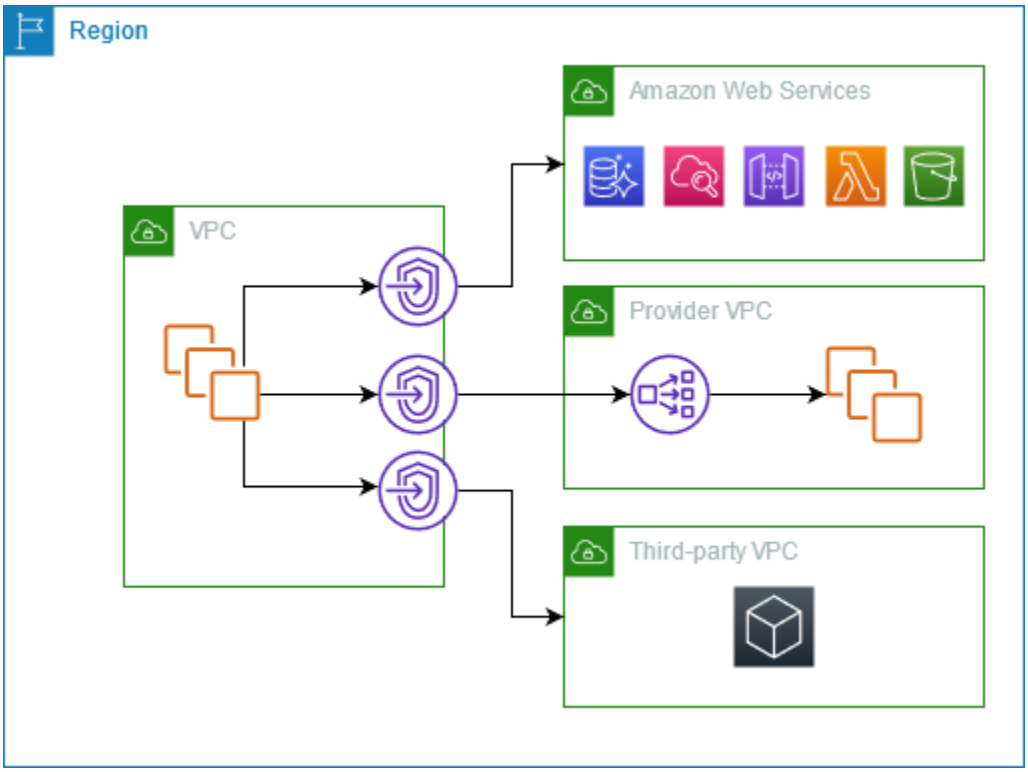
Apa itu AWS PrivateLink?

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

Kasus penggunaan

Anda dapat membuat titik akhir VPC untuk menghubungkan sumber daya di VPC Anda ke layanan 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 instance EC2 di subnet pribadi dan tiga titik akhir VPC antarmuka. Titik akhir VPC paling atas terhubung ke file. Layanan AWS Titik akhir VPC tengah terhubung ke layanan yang dihosting oleh layanan lain Akun AWS (layanan titik akhir VPC). Titik akhir VPC bawah terhubung ke layanan mitra. AWS Marketplace



Pelajari selengkapnya

- the section called “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:

- AWS Management ConsoleMenyediakan 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.
- AWS 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: :Pemberitahuan VPC EndpointConnection
  - AWS: :EC2: :VPC EndpointService
  - AWS: :EC2: :Izin VPC EndpointService
  - 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 selengkapnya, lihat Alat untuk Dibangun 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, ini mengharuskan aplikasi Anda 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

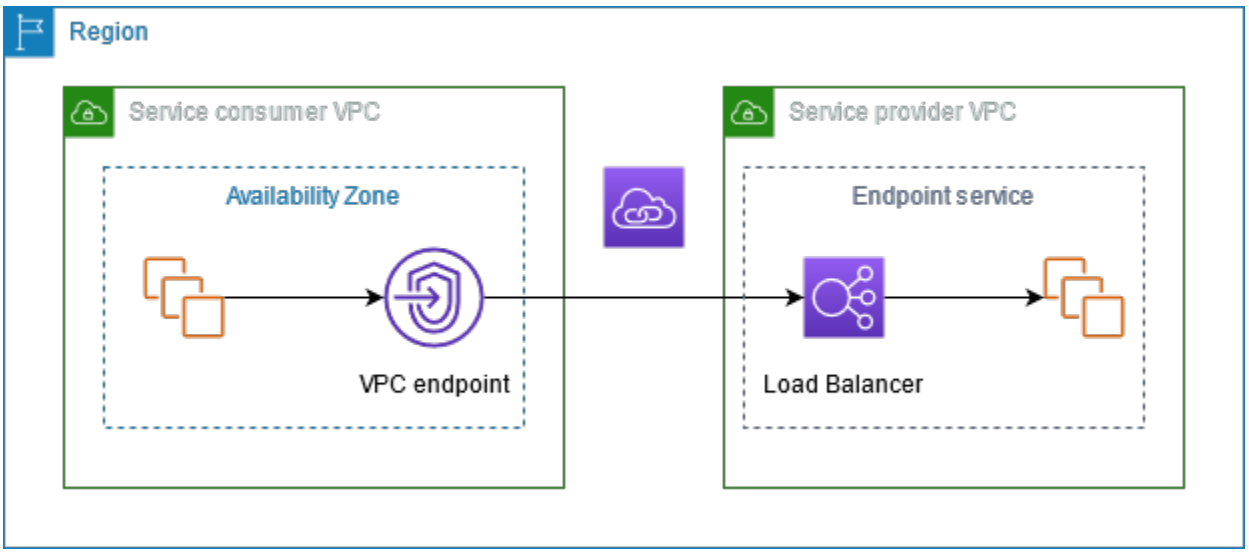
Anda dapat menggunakan Amazon VPC untuk mendefinisikan virtual private cloud (VPC), yang merupakan jaringan virtual yang terisolasi secara logis. Anda dapat meluncurkan AWS sumber daya di VPC Anda. Anda dapat mengizinkan sumber daya di VPC Anda terhubung ke sumber daya di luar VPC itu. Misalnya, tambahkan 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 sumber daya di VPC Anda terhubung ke layanan di VPC lain menggunakan alamat IP pribadi, seolah-olah layanan 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 layanan membuat titik akhir VPC antarmuka untuk terhubung ke layanan endpoint yang di-host oleh penyedia layanan.



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.

Konsep

- Layanan titik akhir
- Nama layanan
- Status layanan

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:

- `Pending`- Layanan endpoint sedang dibuat.
- `Available`- Layanan endpoint tersedia.
- `Failed`- Layanan endpoint tidak dapat dibuat.
- `Deleting`- Penyedia layanan menghapus layanan endpoint dan penghapusan sedang berlangsung.
- `Deleted`- Layanan endpoint dihapus.

Konsumen layanan

Pengguna suatu layanan adalah konsumen layanan. Konsumen layanan dapat mengakses layanan endpoint dari AWS sumber daya, seperti instans EC2, atau dari server lokal.

Konsep

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

Titik akhir VPC

Konsumen layanan membuat titik akhir VPC untuk menghubungkan VPC mereka ke layanan endpoint. Konsumen layanan harus menentukan nama layanan layanan titik akhir saat membuat titik akhir VPC. Ada beberapa jenis titik akhir VPC. Anda harus membuat jenis titik akhir VPC yang diperlukan oleh layanan endpoint.

- `Interface`- Buat titik akhir antarmuka untuk mengirim lalu lintas TCP 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.

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. Untuk setiap subnet yang Anda tentukan saat Anda membuat titik akhir VPC, kami membuat antarmuka jaringan endpoint di subnet.

Jika titik akhir VPC mendukung IPv4, antarmuka jaringan titik akhir memiliki alamat IPv4. Jika titik akhir VPC mendukung IPv6, antarmuka jaringan endpoint-nya 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.

Alamat IP dari antarmuka jaringan endpoint tidak akan berubah selama masa pakai titik akhir VPC-nya.

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, 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. `Available`

Berikut ini adalah status yang mungkin untuk titik akhir VPC:

- `PendingAcceptance`- Permintaan koneksi tertunda. Ini adalah status awal jika permintaan diterima secara manual.
- `Pending`- 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.
- `Available`- Titik akhir VPC tersedia untuk digunakan.
- `Rejected`- Penyedia layanan menolak permintaan koneksi. Penyedia layanan juga dapat menolak koneksi setelah tersedia untuk digunakan.
- `Expired`- Permintaan koneksi kedaluwarsa.
- `Failed`- Titik akhir VPC tidak dapat dibuat tersedia.
- `Deleting`- Konsumen layanan menghapus titik akhir VPC dan penghapusan sedang berlangsung.
- `Deleted`- Titik akhir VPC dihapus.

AWS PrivateLink koneksi

Lalu lintas dari VPC Anda dikirim ke layanan endpoint menggunakan koneksi antara titik akhir VPC dan layanan endpoint. Lalu lintas antara titik akhir VPC dan layanan endpoint 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.

Dengan titik akhir VPC antarmuka, konsumen layanan dapat menggunakan kebijakan titik akhir untuk mengontrol prinsip IAM mana yang dapat menggunakan titik akhir VPC untuk mengakses layanan 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.

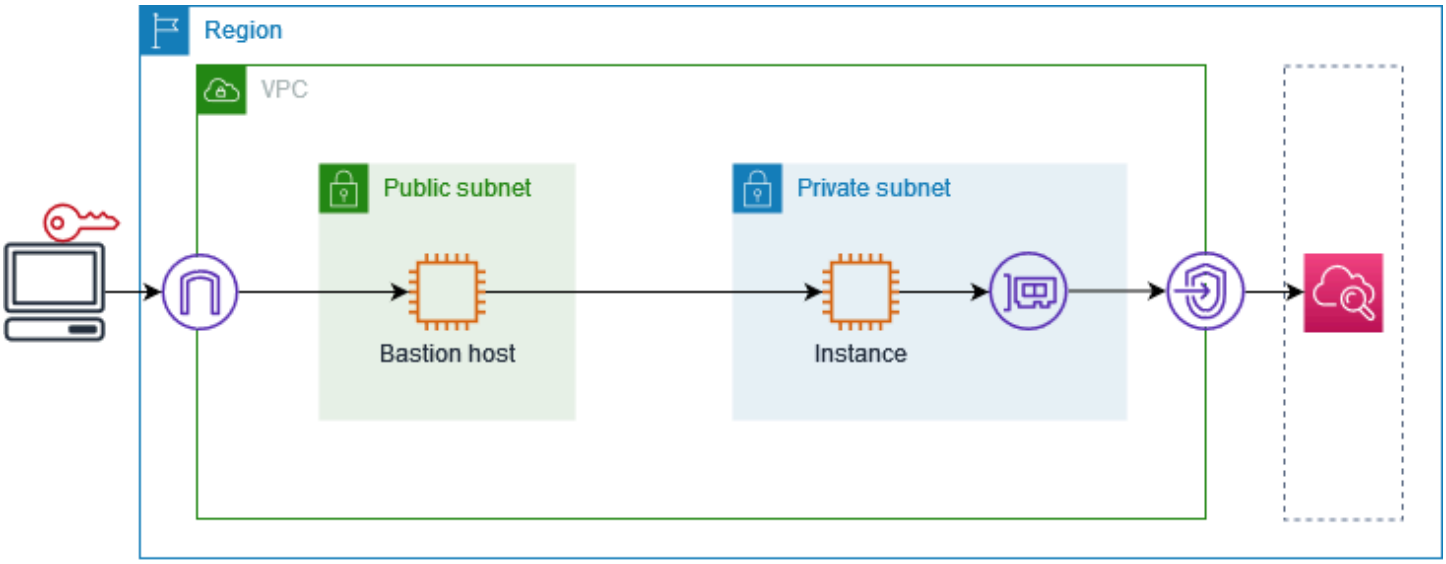
Anda dapat mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas domain ke titik akhir VPC. Untuk informasi selengkapnya, lihat Merutekan lalu lintas ke titik akhir VPC menggunakan nama domain Anda.

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 Amazon VPC 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.
- 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 kebijakan CloudWatchReadOnlyAccess.

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 Auto-assign IP 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 Auto-assign IP 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 adalah 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 Amazon VPC 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. ***wilayah*** .monitoring.
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 Amazon VPC 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 Harga AWS PrivateLink.

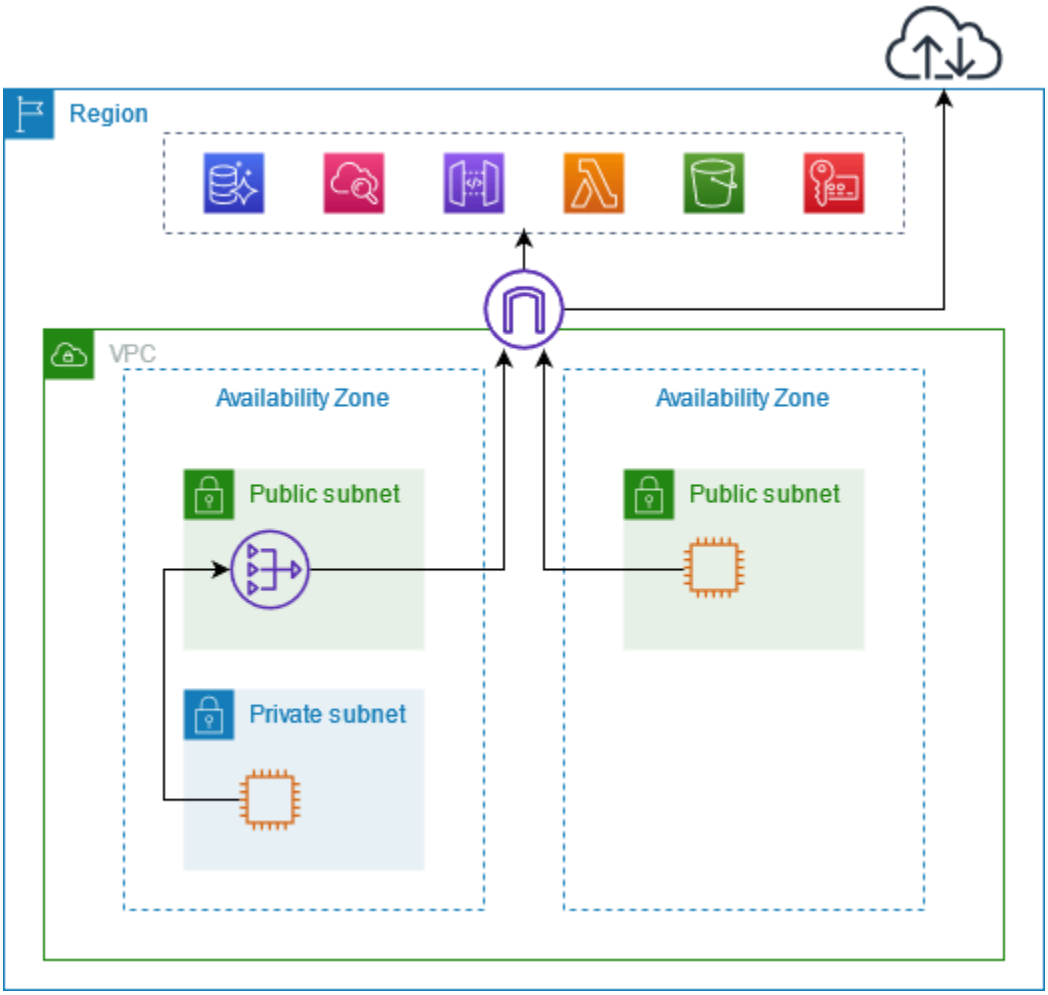
Daftar Isi

Gambaran Umum

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.

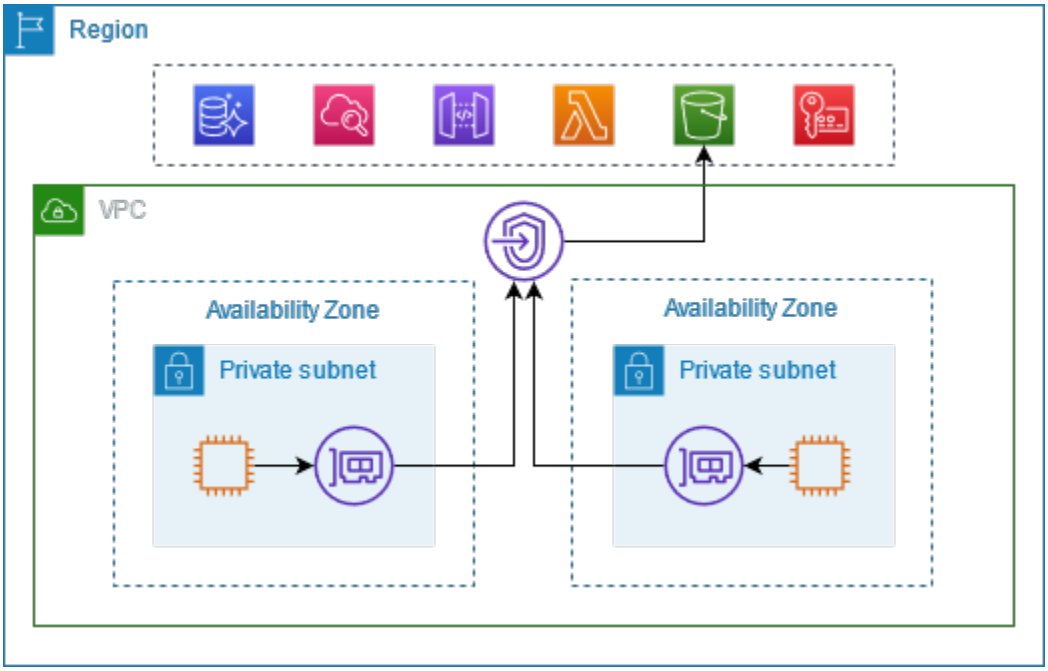
Akses melalui titik akhir layanan publik

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.

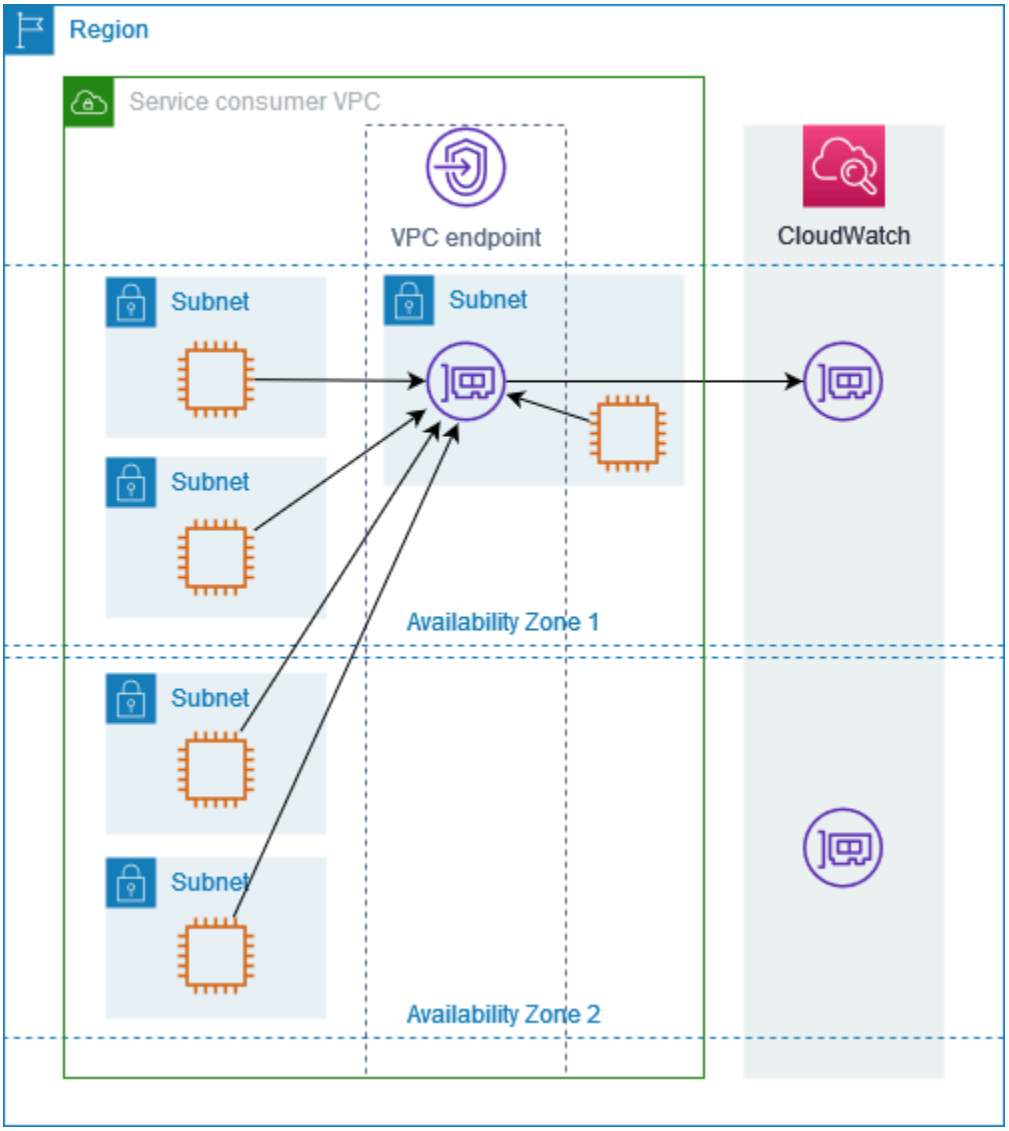
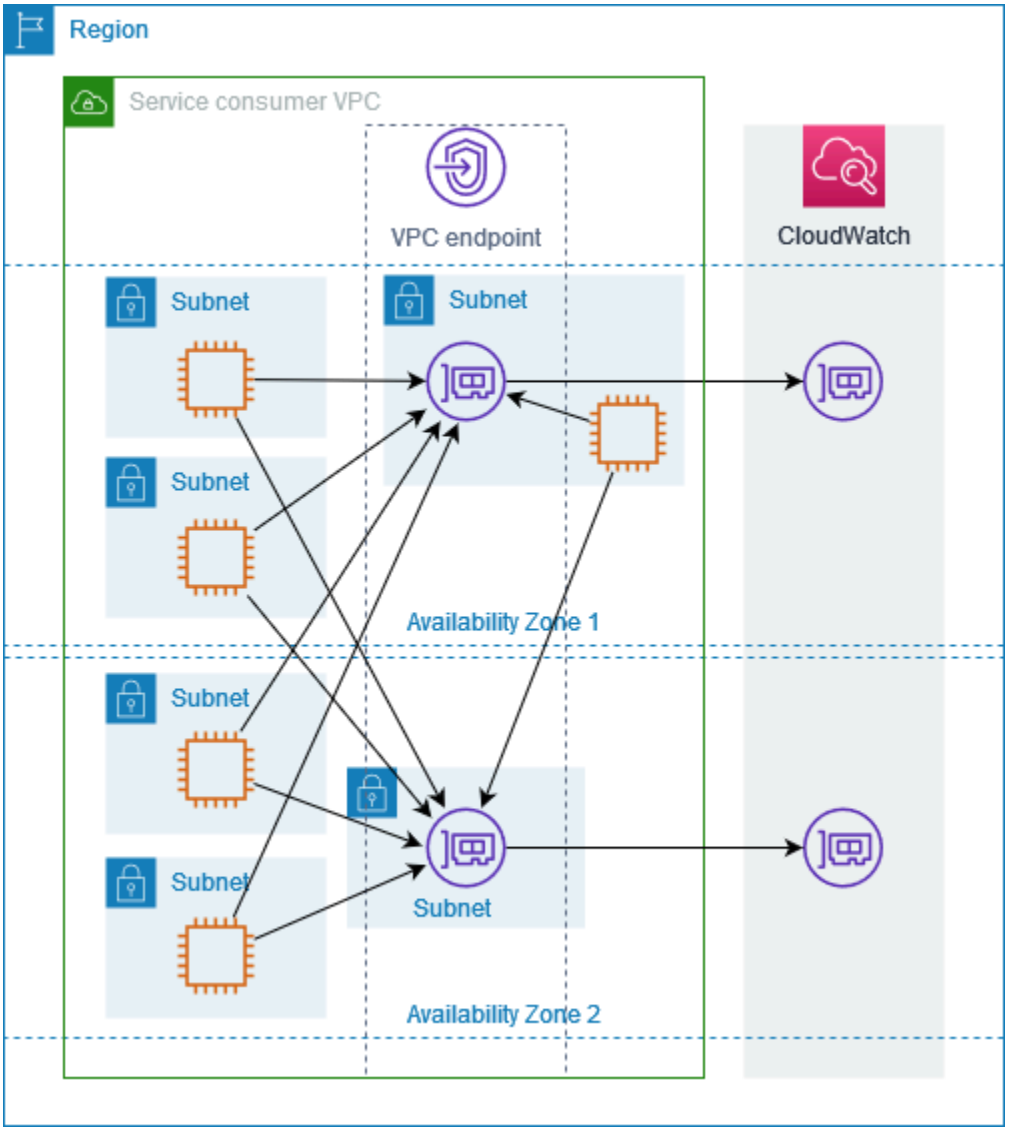
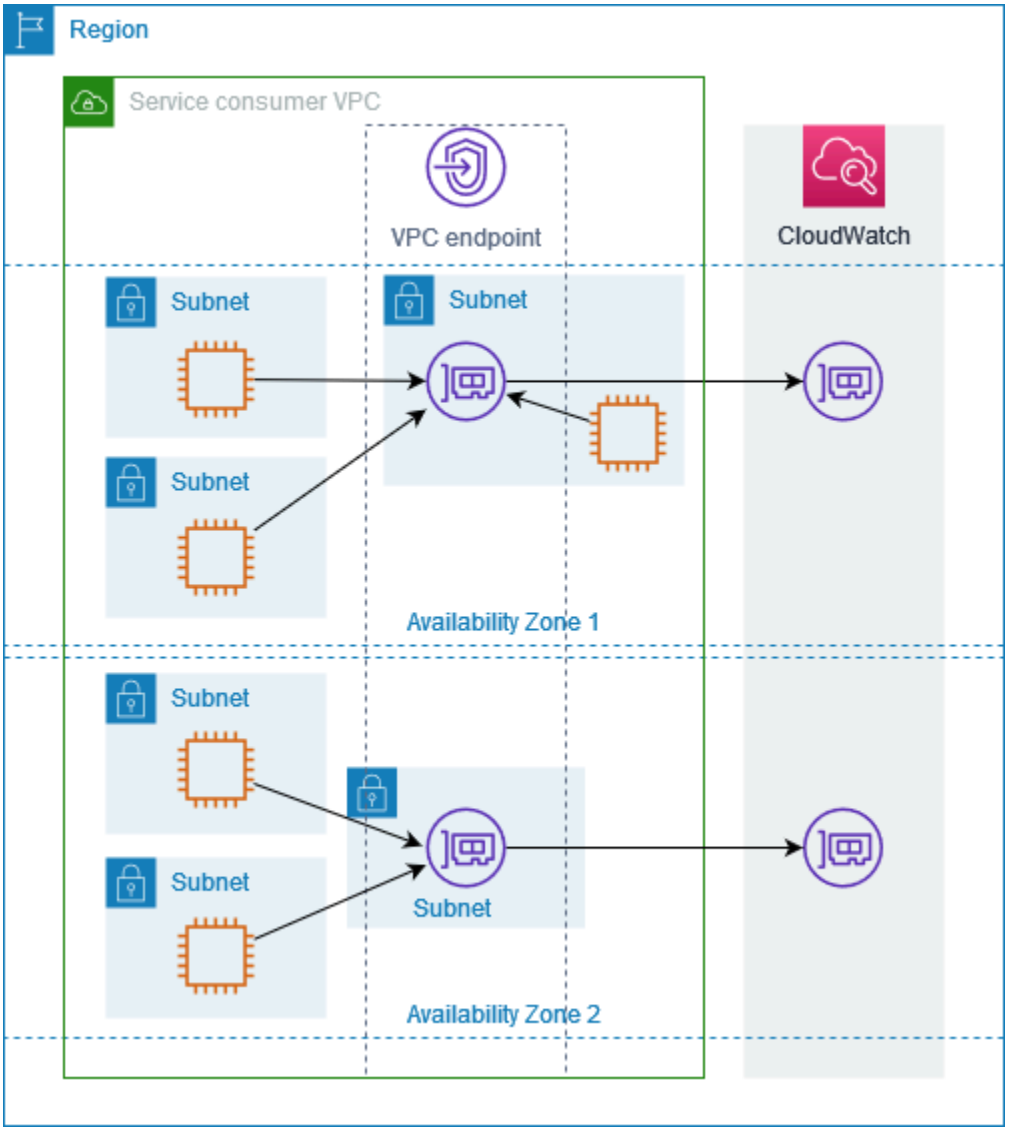


Diagram berikut menunjukkan titik akhir VPC untuk Amazon CloudWatch dengan antarmuka jaringan titik akhir di dua Availability Zones. Ketika sumber daya apa pun di subnet apa pun di VPC mengakses CloudWatch Amazon dengan menggunakan titik akhir publiknya, kami memilih antarmuka jaringan titik akhir yang 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 menggambarkan antarmuka jaringan titik akhir dengan alamat IPv6, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

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
Penganalisis Akses	com.amazonaws. *wilayah* *.access-analyzer*
AWS Account Management	com.amazonaws. *wilayah.akun*
Amazon API Gateway	com.amazonaws. *wilayah* *.execute-api*
AWS AppConfig	com.amazonaws. *wilayah* *.appconfig*
	com.amazonaws. *wilayah* *.appconfigdata*
AWS App Mesh	com.amazonaws. *wilayah* *.appmesh*
	com.amazonaws. *wilayah* *.appmesh-envoy-management*

Layanan AWS	Nama layanan
AWS Pelari Aplikasi	com.amazonaws. *wilayah* .apprunner
AWS Layanan Pelari Aplikasi	com.amazonaws. *wilayah* *.apprunner.requests*
Application Auto Scaling	com.amazonaws. *wilayah* *.application-autoscaling*
AWS Layanan Migrasi Aplikasi	com.amazonaws. *wilayah* .mgn
Amazon AppStream 2.0	com.amazonaws. *wilayah* *.appstream.api*
	com.amazonaws. *wilayah* *.appstream.streaming*
AWS AppSync	com.amazonaws. *wilayah* .appsync-api
Amazon Athena	com.amazonaws. *wilayah* *.athena*
AWS Audit Manager	com.amazonaws. *wilayah* *.auditmanager*
Amazon Aurora	com.amazonaws. *wilayah* .rds
AWS Auto Scaling	com.amazonaws. *wilayah* *.autoscaling-plan*
AWS Pertukaran Data B2B	com.amazonaws. *wilayah* *.b2bi*
AWS Backup	com.amazonaws. *wilayah.cadangan*
	com.amazonaws. *wilayah* *.backup-gateway*
AWS Batch	com.amazonaws. *wilayah* .batch
Batuan Dasar Amazon	com.amazonaws. *wilayah* *.bedrock*
	com.amazonaws. *wilayah* *.bedrock-agent*
	com.amazonaws. *wilayah* *.bedrock-agent-runtime*

Layanan AWS	Nama layanan
	com.amazonaws. *wilayah* *.bedrock-runtime*
AWS Billing Conductor	com.amazonaws. *wilayah* *.billingconductor*
Amazon Braket	com.amazonaws. *wilayah* *.braket*
AWS Kamar Bersih	com.amazonaws. *wilayah.cleanrooms*
AWS Kamar Bersih ML	com.amazonaws. *wilayah.cleanrooms-ml*
AWS Cloud Control API	com.amazonaws. *wilayah* *.cloudcontrolapi*
	com.amazonaws. *wilayah* *.cloudcontrolapi-fips*
Amazon Cloud Directory	com.amazonaws. *wilayah* *.clouddirectory*
AWS CloudFormation	com.amazonaws. *wilayah* *.cloudformation*
AWS CloudHSM	com.amazonaws. *wilayah* *.cloudhsmv2*
AWS Cloud Map	com.amazonaws. *wilayah* *.servicediscovery*
	com.amazonaws. *wilayah* *.servicediscovery-fips*
	com.amazonaws. *wilayah* *.data-servicediscovery*
	com.amazonaws. *wilayah* *.data-servicediscovery-fips*
AWS CloudTrail	com.amazonaws. *wilayah* *.cloudtrail*
Amazon CloudWatch	com.amazonaws. *wilayah* .jelas
	com.amazonaws. *wilayah* *.evidently-dataplane*

Layanan AWS	Nama layanan
	com.amazonaws. *wilayah.monitoring*
	com.amazonaws. *wilayah* .rum
	com.amazonaws. *wilayah .rum-dataplane*
	com.amazonaws. *wilayah.sintetis*
CloudWatch Log Amazon	com.amazonaws. *wilayah.logs*
Monitor CloudWatch Jaringan Amazon	com.amazonaws. *wilayah .networkmonitor*
AWS CodeArtifact	com.amazonaws. *wilayah .codeartifact.api*
	com.amazonaws. *wilayah .codeartifact.repositori*
AWS CodeBuild	com.amazonaws. *wilayah .codebuild*
	com.amazonaws. *wilayah .codebuild-fips*
AWS CodeCommit	com.amazonaws. *wilayah .codecommit*
	com.amazonaws. *wilayah .codecommit-fips*
	com.amazonaws. *wilayah* .git-codecommit
	com.amazonaws. *wilayah .git-codecommit-fips*
AWS CodeConnections	com.amazonaws. *wilayah .codeconnections.api*
	com.amazonaws. *wilayah .codestar-connections.api*
AWS CodeDeploy	com.amazonaws. *wilayah .codedeploy*

Layanan AWS	Nama layanan
	com.amazonaws. *wilayah* *.codedeploy-commands-secure*
Amazon CodeGuru Profiler	com.amazonaws. *wilayah* *.codeguru-profiler*
CodeGuru Peninjau Amazon	com.amazonaws. *wilayah* *.codeguru-reviewer*
AWS CodePipeline	com.amazonaws. *wilayah* *.codepipeline*
Amazon CodeWhisperer	com.amazonaws. *wilayah* *.codewhisperer*
Amazon Comprehend	com.amazonaws. *wilayah* *.comprehend*
Amazon Comprehend Medical	com.amazonaws. *wilayah* *.comprehendmedical*
AWS Config	com.amazonaws. *wilayah* *.config*
Amazon Connect	com.amazonaws. *wilayah.app-integrasi*
	com.amazonaws. *wilayah.kasus*
	com.amazonaws. *wilayah.connect-campaign*
	com.amazonaws. *wilayah.profil*
	com.amazonaws. *wilayah* *.voiceid*
	com.amazonaws. *wilayah* .kebijaksanaan
AWS Connector Service	com.amazonaws. *wilayah* *.awsconnector*
AWS Katalog Kontrol	com.amazonaws. *wilayah* *.controlcatalog*
AWS Data Exchange	com.amazonaws. *wilayah* *.dataexchange*
Amazon Data Firehose	com.amazonaws. *wilayah* *.kinesis-firehose*
AWS Database Migration Service	com.amazonaws. *wilayah.dms*
	com.amazonaws. *wilayah* .dms-fips

Layanan AWS	Nama layanan
AWS DataSync	com.amazonaws. *wilayah.datasync*
Amazon DataZone	com.amazonaws. *wilayah .datazone*
AWS Deadline Cloud	com.amazonaws. *wilayah .deadline.management*
	com.amazonaws. *wilayah .deadline.scheduling*
DevOpsGuru Amazon	com.amazonaws. *wilayah .devops-guru*
AWS Directory Service	com.amazonaws. *wilayah* .ds
Amazon DynamoDB	com.amazonaws. *wilayah .dynamodb*
API langsung Amazon EBS	com.amazonaws. *wilayah* .ebs
Amazon EC2	com.amazonaws. *wilayah .ec2*
Amazon EC2 Auto Scaling	com.amazonaws. *wilayah .autoscaling*
EC2 Image Builder	com.amazonaws. *wilayah .imagebuilder*
Amazon ECR	com.amazonaws. *wilayah .ecr.api*
	com.amazonaws. *wilayah .ecr.dkr*
Amazon ECS	com.amazonaws. *wilayah .ecs*
	com.amazonaws. *wilayah .ecs-agent*
	com.amazonaws. *wilayah .ecs-telemetri*
Amazon EKS	com.amazonaws. *wilayah* .eks
	com.amazonaws. *wilayah .eks-auth*
AWS Elastic Beanstalk	com.amazonaws. *wilayah .elasticbeanstalk*

Layanan AWS	Nama layanan
	com.amazonaws. *wilayah* *.elasticbeanstalk-health*
AWS Elastic Disaster Recovery	com.amazonaws. *wilayah* *.drs*
Amazon Elastic File System	com.amazonaws. *wilayah* *.elasticfilesystem*
	com.amazonaws. *wilayah* *.elasticfilesystem-fips*
Amazon Elastic Inference	com.amazonaws. *wilayah* *.elastic-inference.runtime*
Elastic Load Balancing	com.amazonaws. *wilayah* *.elasticloadbalancing*
Amazon ElastiCache	com.amazonaws. *wilayah* *.elasticache*
	com.amazonaws. *wilayah* *.elasticache-fips*
AWS Elemental MediaConnect	com.amazonaws. *wilayah* *.mediaconnect*
Amazon EMR	com.amazonaws. *wilayah* *.elasticmapreduce*
Amazon EMR di EKS	com.amazonaws. *wilayah* *.emr-kontainer*
Amazon EMR Tanpa Server	com.amazonaws. *wilayah* *.emr-serverless*
Amazon EMR WAL	com.amazonaws. *wilayah* *.emrwal.prod*
Resolusi Entitas AWS	com.amazonaws. *wilayah* *.entityresolution*
Amazon EventBridge	com.amazonaws. *wilayah.event*
	com.amazonaws. *wilayah.pipes-data*
AWS Fault Injection Service	com.amazonaws. *wilayah* .fis
Amazon FinSpace	com.amazonaws. *wilayah* *.finspace*

Layanan AWS	Nama layanan
	com.amazonaws. *wilayah* *.finspace-api*
Amazon Forecast	com.amazonaws. *wilayah* .forecast
	com.amazonaws. *wilayah* *.forecastquery*
	com.amazonaws. *wilayah* *.forecast-fips*
	com.amazonaws. *wilayah* *.forecastquery-fips*
Amazon Fraud Detector	com.amazonaws. *wilayah* *.frauddetector*
Amazon FSx	com.amazonaws. *wilayah* *.fsx*
	com.amazonaws. *wilayah* *.fsx-fips*
AWS Glue	com.amazonaws. *wilayah.lem*
AWS Glue DataBrew	com.amazonaws. *wilayah* *.databrew*
Grafana yang Dikelola Amazon	com.amazonaws. *wilayah* *.grafana*
	com.amazonaws. *wilayah* *.grafana-ruang* kerja
AWS Ground Station	com.amazonaws. *wilayah* *.groundstation*
Amazon GuardDuty	com.amazonaws. *wilayah* *.guardduty-data*
	com.amazonaws. *wilayah* *.guardduty-data-fips*
AWS HealthImaging	com.amazonaws. *wilayah* .dicom-medical-imaging
	com.amazonaws. *wilayah* *.medical-imaging*
	com.amazonaws. *wilayah* *.runtime-medical-imaging*
AWS HealthLake	com.amazonaws. *wilayah* *.healthlake*

Layanan AWS	Nama layanan
AWS HealthOmics	com.amazonaws. *wilayah* *.analytics-omics*
	com.amazonaws. *wilayah* *.control-storage-omics*
	com.amazonaws. *wilayah* *.storage-omics*
	com.amazonaws. *wilayah* *.tags-omics*
	com.amazonaws. *wilayah* *.workflows-omics*
Pusat Identitas IAM	com.amazonaws. *wilayah* *.identitystore*
Peran IAM Di Mana Saja	com.amazonaws. *wilayah* *.rolesanywhere*
Amazon Inspector	com.amazonaws. *wilayah* *.inspector2*
AWS IoT Core	com.amazonaws. *wilayah* *.iot.data*
	com.amazonaws. *wilayah* *.iot.credentials*
	com.amazonaws. *wilayah* *.iot.fleethub.api*
AWS IoT Core Device Advisor	com.amazonaws. *wilayah* *.deviceadvisor.iot*
AWS IoT Core for LoRaWAN	com.amazonaws. *wilayah* *.iotwireless.api*
	com.amazonaws. *wilayah* *.lorawan.cups*
	com.amazonaws. *wilayah* *.lorawan.lns*
AWS IoT FleetWise	com.amazonaws. *wilayah* .iotfleetwise
AWS IoT Greengrass	com.amazonaws. *wilayah* *.greengrass*
AWS IoT RoboRunner	com.amazonaws. *wilayah* .iotroborunner
AWS IoT SiteWise	com.amazonaws. *wilayah* *.iotsitewise.api*
	com.amazonaws. *wilayah* *.iotsitewise.data*

Layanan AWS	Nama layanan
AWS IoT TwinMaker	com.amazonaws. *wilayah* .iottwinmaker.api
	com.amazonaws. *wilayah* .iottwinmaker.data
Amazon Kendra	com.amazonaws. *wilayah .kendra*
	aws.api. *wilayah .kendra-ranking*
AWS Key Management Service	com.amazonaws. *wilayah* .kms
	com.amazonaws. *wilayah* .kms-fips
Amazon Keyspaces (untuk Apache Cassandra)	com.amazonaws. *wilayah .cassandra*
	com.amazonaws. *wilayah .cassandra-fips*
Amazon Kinesis Data Streams	com.amazonaws. *wilayah .kinesis-streams*
AWS Lake Formation	com.amazonaws. *wilayah .lakeformation*
AWS Lambda	com.amazonaws. *wilayah .lambda*
Amazon Lex	com.amazonaws. *wilayah .models-v2-lex*
	com.amazonaws. *wilayah .runtime-v2-lex*
AWS License Manager	com.amazonaws. *wilayah.license-manager*
	com.amazonaws. *wilayah .license-manager-fips*
	com.amazonaws. *region .license-manager-user-subscriptions*
Amazon Lookout for Equipment	com.amazonaws. *wilayah .lookoutequipment*
Amazon Lookout for Metrics	com.amazonaws. *wilayah .lookoutmetrics*
Amazon Lookout for Vision	com.amazonaws. *wilayah .lookoutvision*

Layanan AWS	Nama layanan
Amazon Macie	com.amazonaws. *wilayah* *.macie2*
AWS Mainframe Modernization	com.amazonaws. *wilayah* .m2
Amazon Managed Blockchain	com.amazonaws. *wilayah* *.managedblockchain-query*
	com.amazonaws. *wilayah* *.managedblockchain.bitcoin.mainnet*
	com.amazonaws. *wilayah* *.managedblockchain.bitcoin.testnet*
Layanan Dikelola Amazon untuk Prometheus	com.amazonaws. *wilayah* .aps
	com.amazonaws. *wilayah* .aps-workspaces
Alur Kerja Terkelola Amazon untuk Apache Airflow	com.amazonaws. *wilayah* *.airflow.api*
	com.amazonaws. *wilayah* *.airflow.env*
	com.amazonaws. *wilayah* *.airflow.ops*
AWS Management Console	com.amazonaws. *wilayah.console*
	com.amazonaws. *wilayah.signin*
Amazon MemoryDB for Redis	com.amazonaws. *wilayah* *.memory-db*
	com.amazonaws. *wilayah* *.memorydb-fips*
Orkestrator AWS Migration Hub	com.amazonaws. *wilayah* *.migrationhub-orchestrator*
AWS Migration Hub Refactor Spaces	com.amazonaws. *wilayah* *.refactor-spaces*
Rekomendasi Strategi Migrasi Hub	com.amazonaws. *wilayah* *.migrationhub-strategy*

Layanan AWS	Nama layanan
Analisis Amazon Neptunus	com.amazonaws. *wilayah* .neptune-grafik
Amazon Nimble Studio	com.amazonaws. *wilayah* .gesit
OpenSearch Layanan Amazon	Titik akhir ini dikelola layanan
AWS Organizations	com.amazonaws. *wilayah*.organisasi
	com.amazonaws. *wilayah* .organisasi-fips
AWS Outposts	com.amazonaws. *wilayah*.pos terdepan
AWS Panorama	com.amazonaws. *wilayah* .panorama
AWS Kriptografi Pembayaran	com.amazonaws. *wilayah* .payment-cryptography.controlplane
	com.amazonaws. *wilayah* .payment-cryptography.dataplane
Amazon Personalisasi	com.amazonaws. *wilayah*.personalisasi
	com.amazonaws. *wilayah* .personalize-event
	com.amazonaws. *wilayah* .personalize-runtime
Rantai Pasokan AWS	com.amazonaws. *wilayah* .scn
Amazon Pinpoint	com.amazonaws. *wilayah*.pinpoint
	com.amazonaws. *wilayah* .pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws. *wilayah* .polly
AWS 5G pribadi	com.amazonaws. *wilayah*.private-jaringan
AWS Private Certificate Authority	com.amazonaws. *wilayah* .acm-pca

Layanan AWS	Nama layanan
	com.amazonaws. *wilayah* *.pca-connector-ad*
AWS Proton	com.amazonaws. *wilayah* *.proton*
Amazon Q Bisnis	aws.api. *wilayah* *.qbusiness*
Amazon QLDB	com.amazonaws. *wilayah* *.qldb.session*
Amazon QuickSight	com.amazonaws. *wilayah.situs* *web* quicksight-
Amazon RDS	com.amazonaws. *wilayah* .rds
API Data Amazon RDS	com.amazonaws. *wilayah* .rds-data
AWS Re: Post Pribadi	com.amazonaws. *wilayah* *.repostspace*
Amazon Redshift	com.amazonaws. *wilayah* *.redshift*
	com.amazonaws. *wilayah* *.redshift-fips*
API Data Pergeseran Merah Amazon	com.amazonaws. *wilayah* *.redshift-data*
	com.amazonaws. *wilayah* *.redshift-data-fips*
Amazon Rekognition	com.amazonaws. *wilayah* *.rekognition*
	com.amazonaws. *wilayah* *.rekognition-fips*
	com.amazonaws. *wilayah* *.streaming-rekognition*
	com.amazonaws. *wilayah* *.streaming-rekognition-fips*
AWS RoboMaker	com.amazonaws. *wilayah* *.robomaker*
Amazon S3	com.amazonaws. *wilayah* .s3
Titik Akses Multi-Wilayah Amazon S3	com.amazonaws.s3-global.accesspoint

Layanan AWS	Nama layanan
Amazon S3 di Outposts	com.amazonaws. *wilayah* .s3-pos terdepan
Amazon SageMaker	aws.sagemaker. *wilayah.notebook*
	aws.sagemaker. *wilayah* .studio
	com.amazonaws. *wilayah .sagemaker.api*
	com.amazonaws. *wilayah .sagemaker.feature store-runtime*
	com.amazonaws. *wilayah .sagemaker.metrics*
	com.amazonaws. *wilayah .sagemaker.runtime*
	com.amazonaws. *wilayah .sagemaker.runtime-fips*
AWS Secrets Manager	com.amazonaws. *wilayah .secretsmanager*
AWS Security Hub	com.amazonaws. *wilayah .securityhub*
AWS Security Token Service	com.amazonaws. *wilayah* .sts
Service Catalog	com.amazonaws. *wilayah .servicecatalog*
	com.amazonaws. *wilayah .servicecatalog-appregistry*
Amazon SES	com.amazonaws. *wilayah .email-smtp*
AWS SimSpace Weaver	com.amazonaws. *wilayah .simspaceweaver*
AWS Snow Device Management	com.amazonaws. *wilayah .snow-device-management*
Amazon SNS	com.amazonaws. *wilayah* .sns
Amazon SQS	com.amazonaws. *wilayah.sqs*

Layanan AWS	Nama layanan
Amazon SWF	com.amazonaws. *wilayah* .swf
	com.amazonaws. *wilayah* .swf-fips
AWS Step Functions	com.amazonaws. *wilayah* .states
	com.amazonaws. *wilayah* .sync-states
AWS Storage Gateway	com.amazonaws. *wilayah* .storagegateway
AWS Systems Manager	com.amazonaws. *wilayah* .ec2messages
	com.amazonaws. *wilayah* .ssm
	com.amazonaws. *wilayah* .ssm-kontak
	com.amazonaws. *wilayah* .ssm-insiden
	com.amazonaws. *wilayah* .ssmmessages
AWS Pembangun Jaringan Telekomunikasi	com.amazonaws. *wilayah* .tnb
Amazon Texttract	com.amazonaws. *wilayah* .textract
	com.amazonaws. *wilayah* .textract-fips
Amazon Timestream	com.amazonaws. *wilayah* .timestream.ingest-sel
	com.amazonaws. *wilayah* .timestream.query-sel
Amazon Timestream untuk InfluxDB	com.amazonaws. *wilayah* .timestream-influxdb
Amazon Transcribe	com.amazonaws. *wilayah* .transcribe

Layanan AWS	Nama layanan
	com.amazonaws. *wilayah* *.transcribestreaming*
Amazon Transcribe Medis	com.amazonaws. *wilayah* *.transcribe*
	com.amazonaws. *wilayah* *.transcribestreaming*
AWS Transfer for SFTP	com.amazonaws. *wilayah.transfer*
	com.amazonaws. *wilayah* *.transfer.server*
Amazon Translate	com.amazonaws. *wilayah* .translate
AWS Trusted Advisor	com.amazonaws. *wilayah* *.trustedadvisor*
Izin Terverifikasi Amazon	com.amazonaws. *wilayah* *.verifiedpermissions*
Kisi VPC Amazon	com.amazonaws. *wilayah* *.vpc-kisi*
Amazon WorkSpaces	com.amazonaws. *wilayah.ruang* kerja
Klien WorkSpaces Tipis Amazon	com.amazonaws. *wilayah* *.thinclient.api*
AWS X-Ray	com.amazonaws. *wilayah* .xray

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:

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

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"
                }
            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": [],
            "PrivateDnsNameVerificationState": "verified",
            "SupportedIpAddressTypes": [
                "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.

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

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.

```
[
    "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.cleanrooms",
    "com.amazonaws.us-east-1.cleanrooms-ml",
    "com.amazonaws.us-east-1.cloudtrail",
    "com.amazonaws.us-east-1.codeguru-profiler",
    "com.amazonaws.us-east-1.codeguru-reviewer",
    "com.amazonaws.us-east-1.codepipeline",
    "com.amazonaws.us-east-1.codewhisperer",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.datazone",
    "com.amazonaws.us-east-1.deadline.management",
    "com.amazonaws.us-east-1.deadline.scheduling",
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.elastic-inference.runtime",
    "com.amazonaws.us-east-1.email-smtp",
    "com.amazonaws.us-east-1.grafana-workspace",
    "com.amazonaws.us-east-1.iot.credentials",
    "com.amazonaws.us-east-1.iot.data",
    "com.amazonaws.us-east-1.iotwireless.api",
    "com.amazonaws.us-east-1.lorawan.cups",
    "com.amazonaws.us-east-1.lorawan.lns",
    "com.amazonaws.us-east-1.macie2",
    "com.amazonaws.us-east-1.neptune-graph",
    "com.amazonaws.us-east-1.nimble",
    "com.amazonaws.us-east-1.organizations",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.redshift-data",
    "com.amazonaws.us-east-1.redshift-data-fips",
    "com.amazonaws.us-east-1.refactor-spaces",
    "com.amazonaws.us-east-1.sagemaker.runtime-fips",
    "com.amazonaws.us-east-1.storagegateway",
    "com.amazonaws.us-east-1.transfer",
```

```
    "com.amazonaws.us-east-1.transfer.server",
    "com.amazonaws.us-east-1.verifiedpermissions"
]
```

Lihat dukungan IPv6

Anda 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:

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "com.amazonaws.us-east-1.athena",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.timestream-influxdb"
]
```

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 Layanan AWS

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 nama Layanan, pilih layanan. Untuk informasi selengkapnya, lihat the section called “Layanan yang terintegrasi”.
6. Untuk VPC, pilih VPC dari mana Anda akan mengakses file. Layanan AWS
7. 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.
8. Untuk Subnet, pilih satu subnet per Availability Zone dari mana Anda akan mengakses. Layanan AWS Anda tidak dapat memilih beberapa subnet dari Availability Zone yang sama. Untuk informasi selengkapnya, lihat the section called “Subnet dan Availability Zone”.

   Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda pilih. 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. 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.
9. Untuk jenis alamat IP, pilih dari opsi berikut:

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

10. Untuk grup Keamanan, pilih grup keamanan yang akan dikaitkan dengan antarmuka jaringan titik akhir untuk titik akhir VPC. Secara default, kami mengaitkan grup keamanan default untuk VPC.
11. 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. Opsi ini hanya tersedia jika layanan mendukung kebijakan titik akhir VPC. Untuk informasi selengkapnya, lihat Kebijakan titik akhir.
12. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
13. 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. Namun, Anda dapat menggunakan titik akhir VPC di subnet yang dibagikan dengan Anda.

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 tag

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 Amazon VPC 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 Amazon VPC 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 Amazon VPC 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 Amazon VPC 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 tag

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 Amazon VPC 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.

Untuk membuat notifikasi untuk titik akhir antarmuka 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 antarmuka.
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 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.

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

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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id",
      "Condition": {
```

```
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint/endpoint-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

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 Amazon VPC 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.

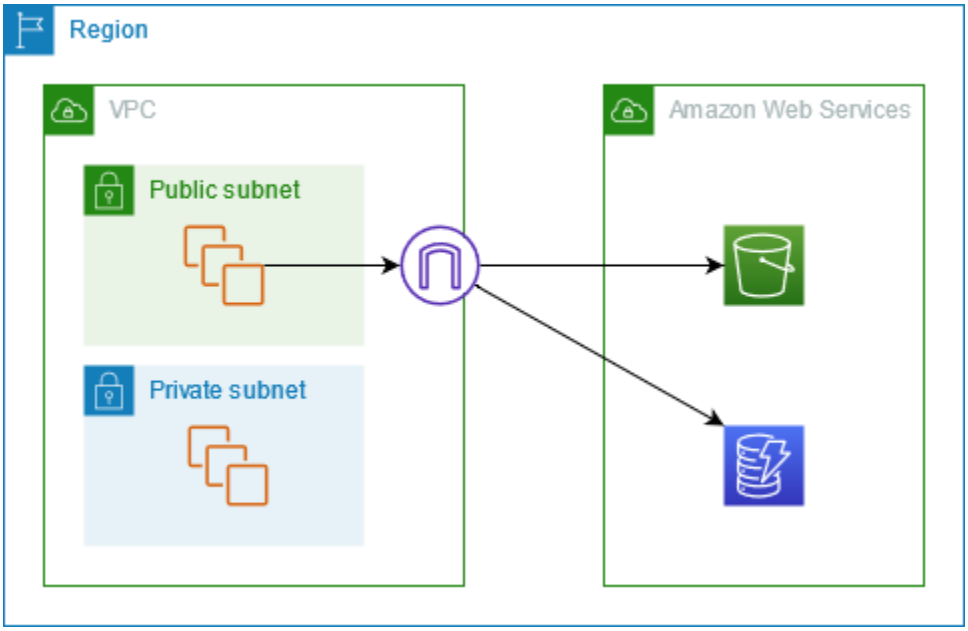
Daftar Isi

Gambaran Umum

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

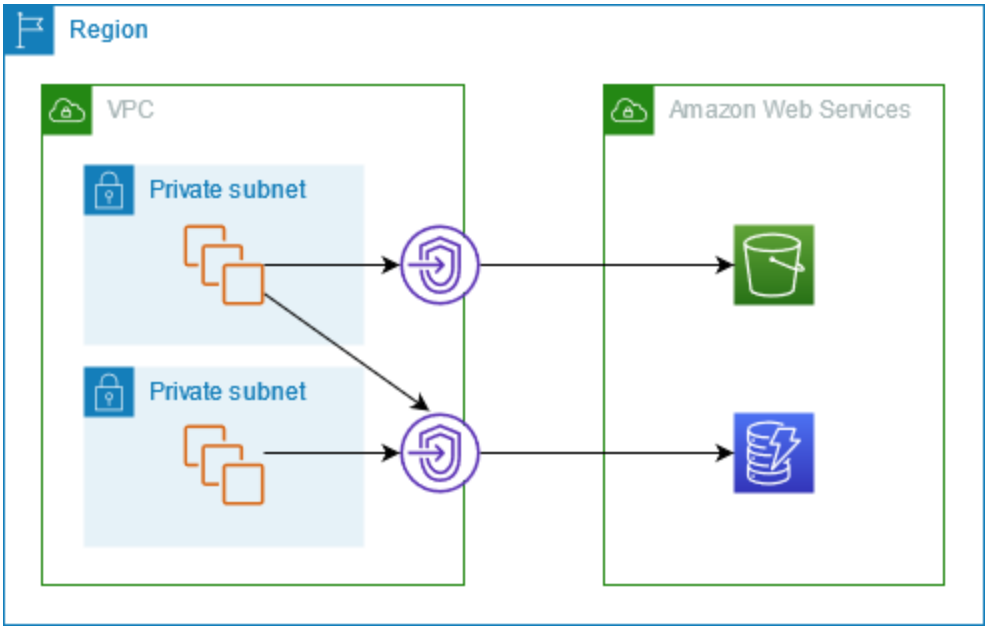
Akses melalui gateway internet

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.

Tujuan	Target
prefix_list_id	*gateway_endpoint_id*

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.

Tujuan	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.

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

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

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.

- Titik akhir Gateway hanya mendukung lalu lintas IPv4.
- Alamat IPv4 sumber dari instance di subnet Anda yang terpengaruh seperti yang diterima oleh Amazon S3 berubah dari alamat IPv4 publik ke alamat IPv4 pribadi di VPC Anda. Titik akhir mengalihkan rute jaringan, dan memutus koneksi TCP terbuka. Koneksi sebelumnya yang menggunakan alamat IPv4 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 AWS 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.

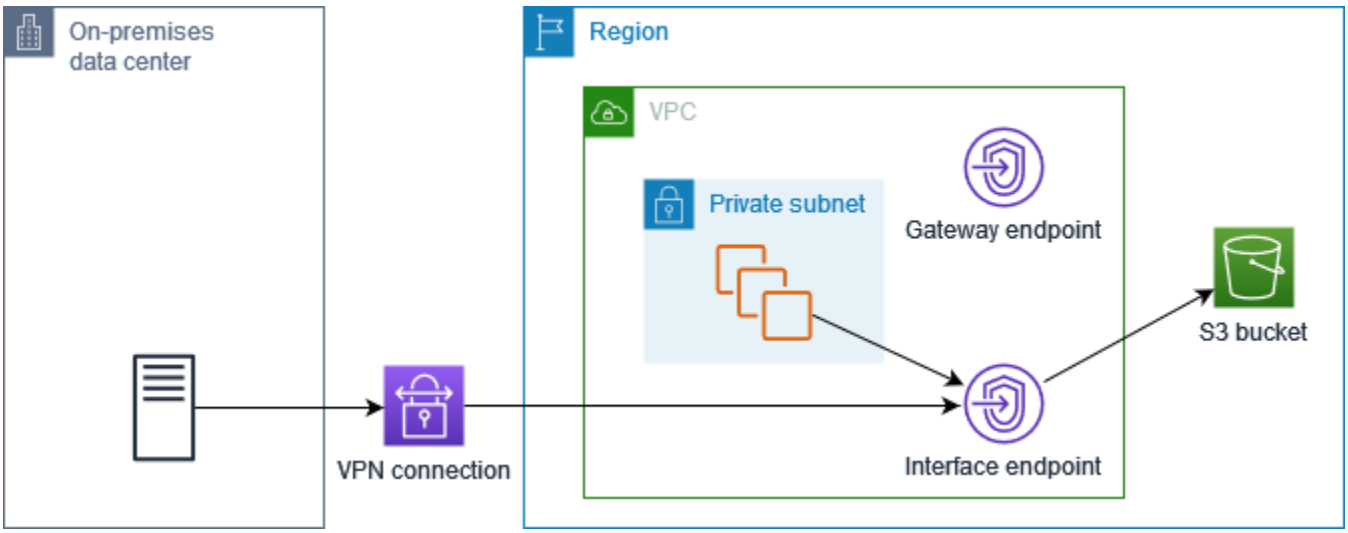
Resolver Rute 53

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.

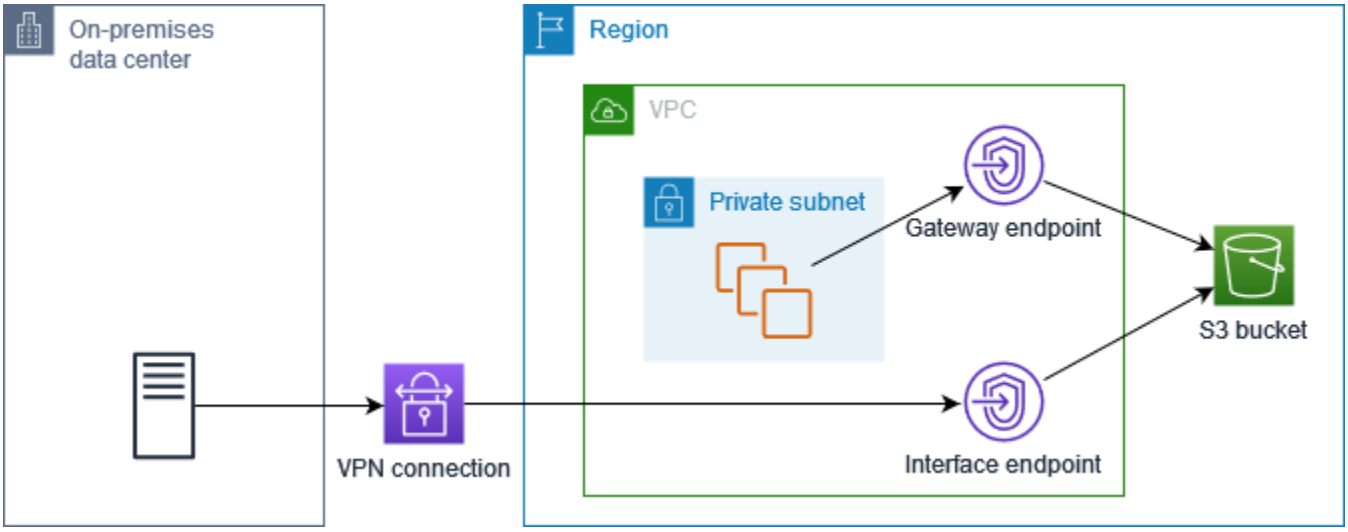
DNS privat

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.



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 dan pilih com.amazonaws. *wilayah* .s3.
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 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 AWS Management Console.

```
{
  "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 AWS Management Console.

```
{
  "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 kondisi aws: VpcSource Ip. 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 AWS Management Console.

```
{
  "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

```
{
  "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. 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 khusus.
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.

```
{
  "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.

```
{
  "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.

```
{
```

```
  "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

- 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 AWS 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. *wilayah* .dynamodb.
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.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-endpoint",
         "Effect": "Deny",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:region:account-id: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.

```
{
   "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.

```
{
   "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. 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 khusus.
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.

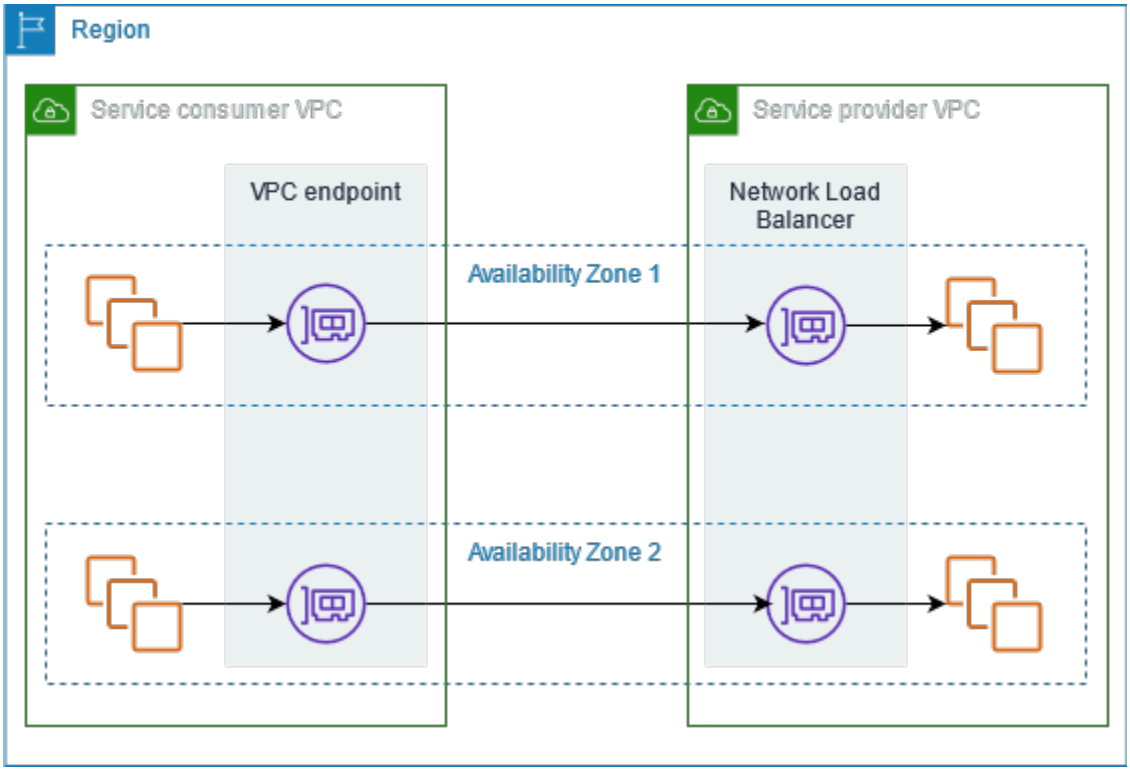
Daftar Isi

Gambaran Umum

Anda dapat menemukan, membeli, dan menyediakan produk SaaS yang didukung oleh melalui AWS PrivateLink . AWS Marketplace Untuk informasi lebih lanjut, lihat AWS Marketplace: - 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 kategori Layanan, pilih AWS Marketplace layanan.
    b. Masukkan nama layanan.
5. Jika Anda berlangganan layanan dengan penunjukan Siap AWS Layanan, lakukan hal berikut:

   a. Untuk kategori Layanan, pilih Layanan mitra PrivateLink siap pakai.
   b. Masukkan nama layanan dan pilih Verifikasi layanan.
6. Untuk VPC, pilih VPC dari mana Anda akan mengakses produk.
7. Untuk Subnet, pilih satu subnet per Availability Zone dari mana Anda akan mengakses produk.
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

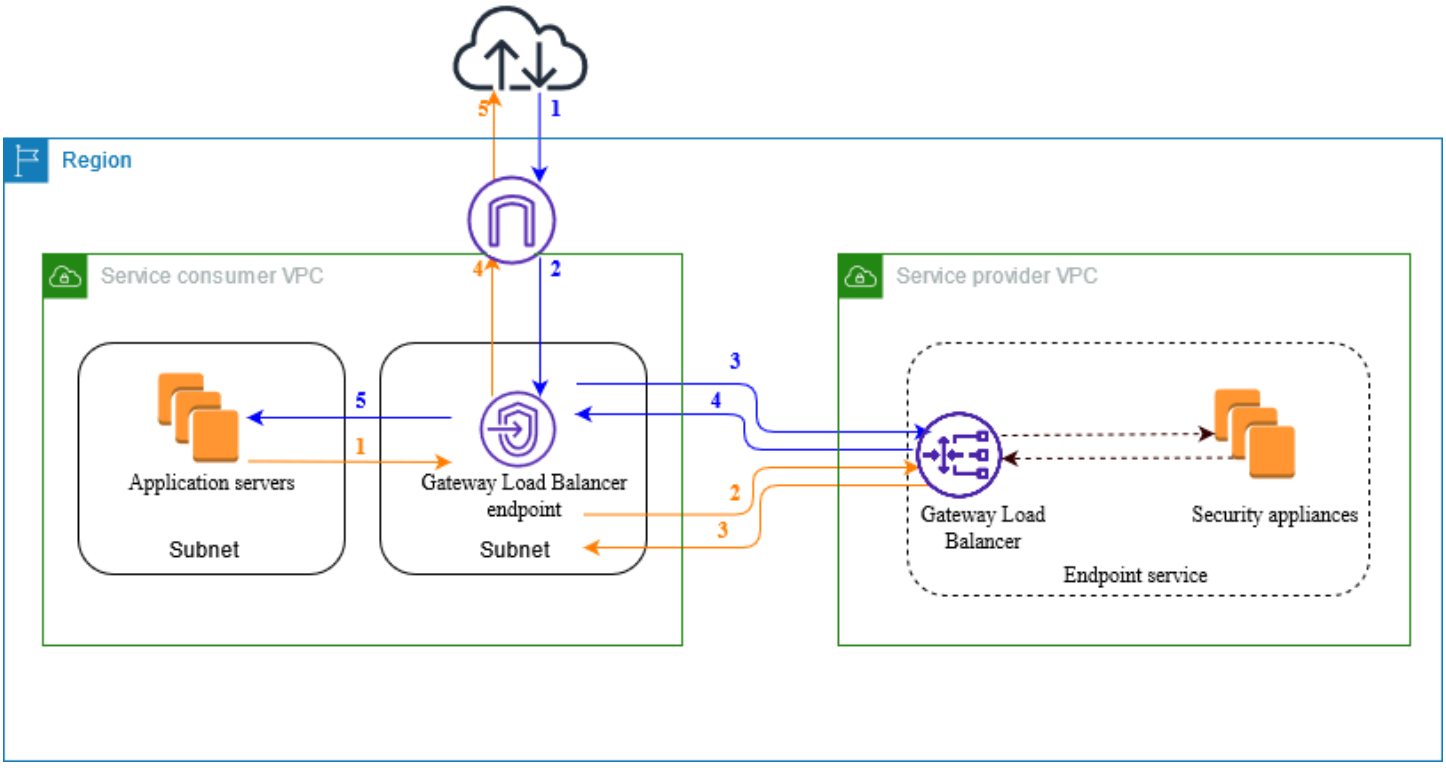
Anda ditagih untuk setiap jam dimana titik akhir Load Balancer Gateway Anda disediakan di setiap Availability Zone. Anda juga ditagih per GB data yang diproses. Untuk informasi selengkapnya, silakan lihat Harga AWS PrivateLink.

Daftar Isi

Untuk informasi selengkapnya, lihat Gateway Load Balancers.

Gambaran Umum

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 dialihkan 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. Perhatikan bahwa 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.

Tujuan	Target
VPC IPv4 CIDR	Lokal:
VPC IPv6 CIDR	Lokal:
Aplikasi subnet IPv4 CIDR	*vpc-titik akhir id*
Aplikasi subnet IPv6 CIDR	*vpc-titik akhir 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.

Tujuan	Target
VPC IPv4 CIDR	Lokal:
VPC IPv6 CIDR	Lokal:
0.0.0.0/0	*vpc-titik akhir id*
::/0	*vpc-titik akhir 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.

Tujuan	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

- 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 Amazon VPC 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 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 “Mengelola 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

- 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.
- 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 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 endpoint lainnya.
5. Untuk nama Layanan, masukkan nama layanan, lalu pilih Verifikasi layanan.
6. Untuk VPC, pilih VPC tempat membuat titik akhir.
7. Untuk Subnet, pilih subnet untuk membuat titik akhir.
8. Untuk jenis alamat IP, pilih dari opsi berikut:

   - 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.
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 Amazon VPC 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 tag

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 Amazon VPC 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 Amazon VPC 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)

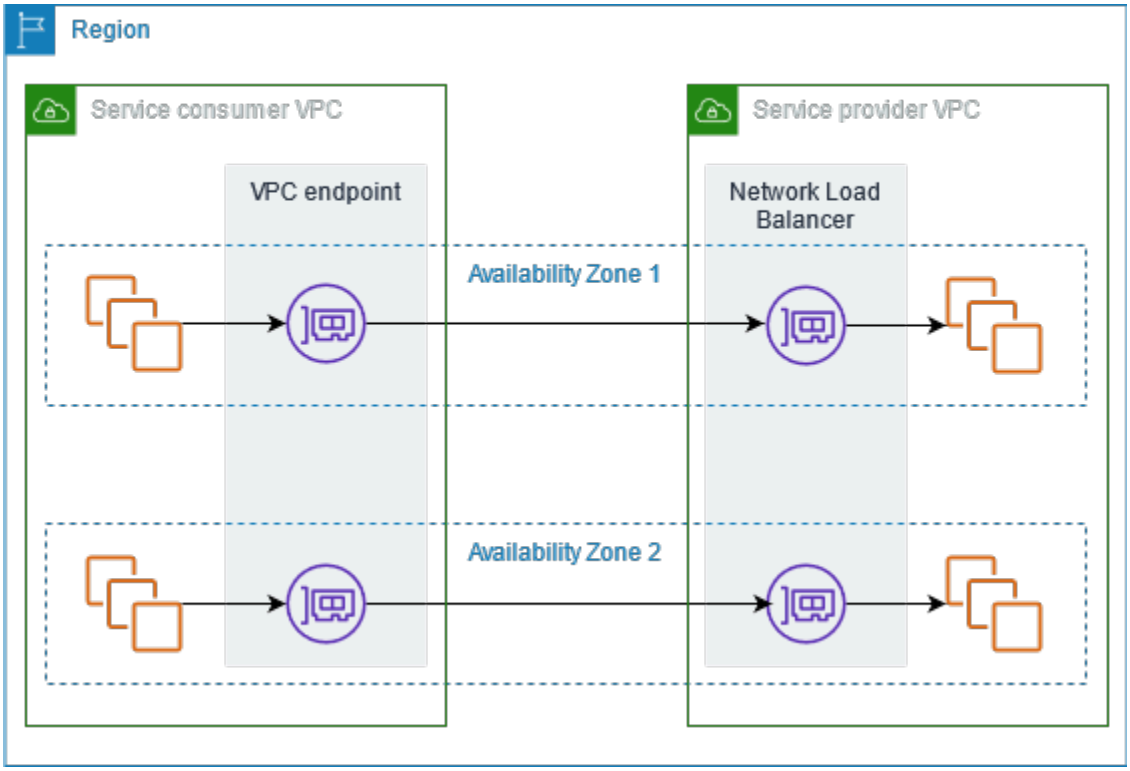
Bagikan layanan Anda melalui AWS PrivateLink

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

Daftar Isi

Gambaran Umum

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.region.vpce.amazonaws.com
```

Nama zona memiliki sintaks berikut:

```
endpoint_id-zone.endpoint_service_id.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.

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

- Prasyarat
- Buat layanan endpoint
- Jadikan layanan endpoint Anda tersedia untuk konsumen layanan

Pertimbangan

- Layanan endpoint tersedia di Wilayah tempat Anda membuatnya. Anda dapat mengakses layanan endpoint dari Wilayah lain menggunakan VPC peering.
- Layanan endpoint mendukung lalu lintas hanya melalui TCP.
- 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.
- 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 Penyeimbangan beban lintas zona di Panduan Pengguna untuk Penyeimbang Beban Jaringan.

Buat layanan endpoint

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

Untuk membuat 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 Buat layanan titik akhir.
4. Untuk jenis Load balancer, pilih Network.
5. Untuk penyeimbang beban yang tersedia, pilih Network Load Balancers untuk dikaitkan dengan layanan endpoint. Zona Ketersediaan yang disertakan mencantumkan Availability Zone yang diaktifkan untuk Network Load Balancer yang dipilih. Layanan endpoint Anda akan tersedia di Availability Zone ini.
6. 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.
7. 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.
8. 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.
9. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
10. 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 “Mengelola 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 berikut.
- 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 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 endpoint lainnya.
5. Untuk nama Layanan, masukkan nama layanan (misalnya,`com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`), dan pilih Verifikasi layanan.
6. Untuk VPC, pilih VPC untuk membuat titik akhir.
7. Untuk Subnet, pilih subnet (Availability Zones) dari mana Anda akan mengakses layanan endpoint.
8. Untuk jenis alamat IP, pilih dari opsi berikut:

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

9. 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.
10. Untuk grup Keamanan, pilih grup keamanan untuk dikaitkan dengan antarmuka jaringan titik akhir.
11. 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

- Mengelola izin
- Menerima atau menolak permintaan koneksi
- Kelola penyeimbang beban
- Kaitkan nama DNS pribadi
- Ubah jenis alamat IP yang didukung
- Kelola tag

Mengelola 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:: account_id:root
```

Peran

```
arn:aws:iam:: account_id:peran/role_name
```

Pengguna

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

Semua kepala sekolah di semua Akun AWS

```
*
```

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 Amazon VPC 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.

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

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 menolak permintaan yang sudah diterima, itu tidak mempengaruhi koneksi antara titik akhir dan layanan.

Untuk memodifikasi pengaturan penerimaan 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 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 Amazon VPC 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 Network Load Balancer, Anda juga dapat mengaktifkan Availability Zone untuk layanan endpoint Anda. 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 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 endpoint.
4. Pilih Actions, Associate, atau disassociate load balancer.
5. Ubah konfigurasi layanan endpoint sesuai kebutuhan. Sebagai 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.
   - Jika Anda baru-baru ini mengaktifkan Availability Zone lain untuk penyeimbang beban Anda, itu akan muncul di Zona Ketersediaan Termasuk. Jika Anda menyimpan perubahan pada langkah berikutnya, ini memungkinkan layanan endpoint untuk Availability Zone baru.
6. Pilih Save changes (Simpan perubahan)

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 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 tag

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. Ketika penyedia layanan menggunakan nama DNS publik yang ada sebagai nama DNS pribadi untuk layanan endpoint mereka, maka konsumen layanan tidak perlu mengubah aplikasi apa pun yang menggunakan nama DNS publik yang ada. 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

- Layanan endpoint hanya dapat memiliki satu nama DNS pribadi.
- Anda tidak boleh membuat catatan A untuk nama DNS pribadi, sehingga hanya server di VPC konsumen layanan yang dapat menyelesaikan nama DNS pribadi.
- Nama DNS pribadi tidak didukung untuk titik akhir Gateway Load Balancer.
- 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.

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 AWS Management Console. 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:L6P0E 45jevfwocp RxlTt

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 host publik Anda. Gunakan nilai berikut:

- Untuk Tipe catatan, pilih TXT.
- Untuk TTL (detik), masukkan**`1800`**.
- Untuk kebijakan Routing, pilih Perutean sederhana.
- Untuk nama Rekam masukkan domain atau subdomain.
- Untuk lalu lintas Nilai/Rute ke, masukkan nilai verifikasi domain.

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.

Penyedia DNS/Hosting	Tautan dokumentasi
GoDaddy	Tambahkan catatan TXT
Dreamhost	Menambahkan catatan DNS kustom
Cloudflare	Mengelola catatan DNS
HostGator	Mengelola Rekaman DNS HostGator dengan/eNom
Namecheap	Bagaimana cara menambahkan catatan TXT/SPF/DKIM/DMARC untuk domain saya?
Names.co.uk	Mengubah pengaturan DNS domain
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 up-to-date informasi paling banyak 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 mana *name_server* adalah 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 Region 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.

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

```
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint-service/service-
id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

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.

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

```
      }
    }
  ]
}
```

Menghapus 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)

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, 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 Basic IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses ke AWS PrivateLink.

Mengautentikasi dengan identitas

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

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensil yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas

yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensi yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna

memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.

- Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna IAM atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
- Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan

diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

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

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

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

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya 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 prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal 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.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. 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 yang dapat Anda gunakan AWS PrivateLink

Fitur IAM	AWS PrivateLink dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	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 prinsipal	Ya

Fitur IAM	AWS PrivateLink dukungan
Peran layanan	Tidak
Peran terkait layanan	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.

Kebijakan berbasis identitas untuk AWS PrivateLink

Mendukung kebijakan berbasis identitas	Ya

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

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk AWS PrivateLink

Untuk melihat contoh kebijakan AWS PrivateLink berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS PrivateLink

Kebijakan berbasis sumber daya dalam AWS PrivateLink

Mendukung kebijakan berbasis sumber daya	Ya

Kebijakan berbasis sumber daya 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 prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal 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 prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya 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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan

hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

AWS PrivateLink berbagi namespace API-nya dengan Amazon EC2. Tindakan kebijakan AWS PrivateLink menggunakan awalan berikut sebelum tindakan:

```
ec2
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Describe`, sertakan tindakan berikut:

```
"Action": "ec2:Describe*"
```

Untuk melihat daftar tindakan, lihat AWS PrivateLink AWS PrivateLink tindakan di Referensi API Amazon EC2. Untuk informasi selengkapnya, lihat Tindakan yang Ditentukan oleh Amazon EC2 di Referensi Otorisasi Layanan.

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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan

sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, 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	Ya

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

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

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

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

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

Kunci kondisi berikut khusus untuk AWS PrivateLink:

- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`

Untuk mempelajari tindakan dan sumber daya mana untuk gunakan kunci syarat, lihat Tindakan yang Ditentukan oleh Amazon EC2.

ACL di AWS PrivateLink

Mendukung ACL	Tidak

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

ABAC dengan AWS PrivateLink

Mendukung ABAC (tanda dalam kebijakan)	Ya

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

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

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

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

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

Menggunakan kredensyal sementara dengan AWS PrivateLink

Mendukung penggunaan kredensial sementara	Ya

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

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

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

Izin utama lintas layanan untuk AWS PrivateLink

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk

menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk AWS PrivateLink

Mendukung peran layanan	Tidak

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

Peran terkait layanan untuk AWS PrivateLink

Mendukung peran terkait layanan	Tidak

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

Contoh kebijakan berbasis identitas untuk AWS PrivateLink

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

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

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh 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.

```
{
    "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.

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

```
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id: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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
```

```
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id: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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc-endpoint/*"
            ],
            "Condition": {
```

```
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.region.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

- 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.

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 Amazon VPC 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)

CloudWatch metrik untukAWS PrivateLink

AWS PrivateLinkmenerbitkan titik data ke Amazon CloudWatch untuk titik akhir antarmuka Anda, titik akhir Gateway Load Balancer, dan layanan endpoint. CloudWatch memungkinkan Anda mengambil statistik tentang titik data yang diurutkan, yang diurutkan, yang diurutkan, yang diurutkan, yang diurutkan, yang diurutkan, yang diurutkan, yang diurutkan, yang diurutkan 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 notifikasi ke alamat email) jika metrik berada di luar rentang yang menurut Anda dapat diterima.

Metrik dipublikasikan untuk semua titik akhir antarmuka, titik akhir Gateway Load Balancer, dan layanan endpoint. Mereka tidak dipublikasikan untuk titik akhir gateway. Secara default,AWS PrivateLink mengirimkan 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 mencakup metrik berikut untuk titik akhir antarmuka dan titik akhir Load Balancer Gateway.

Metrik	Deskripsi
`ActiveConnections`	Jumlah koneksi aktif bersamaan. Ini termasuk koneksi dalam keadaan SYN_SENT dan ESTABLISHED.

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 dipertukarkan antara endpoint dan layanan endpoint, dikumpulkan 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 tetes 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 titik akhir. 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`	Menyaring data metrik menurut tipe titik akhir (`Interface` |`GatewayLoadBalancer`).
`Service Name`	Memfilter data metrik berdasarkan nama Layanan.
`Subnet Id`	Memfilter data metrik berdasarkan subnet.
`VPC Endpoint Id`	Memfilter data metrik berdasarkan titik akhir VPC.
`VPC Id`	Memfilter data metrik berdasarkan VPC.

Metrik dan dimensi Layanan titik akhir

`AWS/PrivateLinkServices`Namespace mencakup 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 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 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 Amazon VPC, CloudWatch konsol, atauAWS CLI sebagai berikut.

Untuk melihat metrik menggunakan konsol Amazon VPC

1. Buka konsol Amazon VPC 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 CloudWatch konsol

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Metrik.
3. Pilih AWS/PrivateLinkEndpoints namespace.
4. Pilih AWS/PrivateLinkServices namespace.

Untuk melihat metrik menggunakan AWS CLI

Gunakan perintah metrik list-metrics untuk mencantumkan metrik yang tersedia untuk titik akhir antarmuka dan titik akhir Load Balancer Gateway:

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

Gunakan perintah metrik list-metrics untuk mencantumkan metrik yang tersedia untuk Layanan titik akhir:

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

Menggunakan aturan Contributor Insights bawaan

AWS PrivateLinkmenyediakan aturan Contributor Insights bawaan untuk layanan endpoint Anda untuk membantu Anda menemukan titik akhir mana yang merupakan kontributor terbesar untuk setiap metrik yang didukung. Untuk informasi selengkapnya, lihat Contributor Insights di Panduan CloudWatch Pengguna Amazon.

AWS PrivateLinkmemberikan aturan berikut:

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1`- Peringkat endpoint dengan jumlah koneksi aktif.

- `VpcEndpointService-BytesByEndpointId-v1`- Peringkat endpoint dengan jumlah byte diproses.
- `VpcEndpointService-NewConnectionsByEndpointId-v1`- Peringkat endpoint dengan jumlah koneksi baru.
- `VpcEndpointService-RstPacketsByEndpointId-v1`- Peringkat endpoint dengan jumlah paket RST dikirim ke endpoint.

Sebelum Anda dapat menggunakan aturan bawaan, Anda harus mengaktifkannya. Setelah Anda mengaktifkan aturan, aturan mulai mengumpulkan data kontributor. Untuk informasi tentang Wawasan Kontributor, lihat CloudWatch Harga Amazon.

Anda harus memiliki izin berikut untuk menggunakan Wawasan Kontributor:

- `cloudwatch:DeleteInsightRules`- Untuk menghapus Wawasan Kontributor.
- `cloudwatch:DisableInsightRules`- Untuk menonaktifkan Wawasan Kontributor.
- `cloudwatch:GetInsightRuleReport`- Untuk mendapatkan data.
- `cloudwatch:ListManagedInsightRules`- Untuk mencantumkan aturan Contributor Insights yang tersedia.
- `cloudwatch:PutManagedInsightRules`- Untuk mengaktifkan Wawasan Kontributor.

Tugas

- Aktifkan Wawasan Kontributor
- Wawasan Kontributor
- Hapus Wawasan Kontributor

Aktifkan Wawasan Kontributor

Gunakan prosedur berikut untuk mengaktifkan aturan bawaan untukAWS PrivateLink menggunakan salah satuAWS Management Console atauAWS CLI.

Untuk mengaktifkan aturan Contributor Insights untukAWS PrivateLink 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 Anda.

4. Pada tab Contributor Insights, pilih Aktifkan.
5. (Opsional) Secara bawaan, semua aturan diaktifkan. Untuk mengaktifkan aturan tertentu saja, pilih aturan yang tidak boleh diaktifkan, lalu pilih Tindakan, Nonaktifkan aturan. Ketika dimintai konfirmasi, pilih Nonaktifkan.

Untuk mengaktifkan aturan Contributor Insights untukAWS PrivateLink menggunakanAWS CLI

1. Gunakan list-managed-insight-rulesperintah sebagai berikut untuk menghitung aturan yang tersedia. Untuk`--resource-arn` opsi, tentukan ARN 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 bidang ini.

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. Gunakan put-managed-insight-rulesperintah sebagai berikut untuk mengaktifkan aturan. Anda harus menentukan nama template dan ARN 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
```

Wawasan Kontributor

Anda dapat menonaktifkan aturan bawaanAWS PrivateLink kapan saja. Setelah Anda menonaktifkan aturan, aturan berhenti mengumpulkan data kontributor, tetapi data kontributor yang ada disimpan hingga berusia 15 hari. Setelah menonaktifkan aturan, Anda dapat mengaktifkannya lagi untuk melanjutkan pengumpulan data kontributor.

Untuk menonaktifkan aturan Contributor Insights untukAWS PrivateLink 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 Anda.

4. Pada tab Contributor Insights, pilih Nonaktifkan semua untuk menonaktifkan semua aturan. Atau, luaskan panel Aturan, pilih aturan yang akan dinonaktifkan, lalu pilih Tindakan, Nonaktifkan aturan
5. Ketika dimintai konfirmasi, pilih Nonaktifkan.

Untuk menonaktifkan aturan Contributor Insights untukAWS PrivateLink menggunakanAWS CLI

Gunakan disable-insight-rulesperintah untuk menonaktifkan aturan.

Hapus Wawasan Kontributor

Gunakan prosedur berikut untuk menghapus aturan bawaan untukAWS PrivateLink menggunakan salah satuAWS Management Console atauAWS CLI. Setelah Anda menghapus aturan, aturan berhenti mengumpulkan data kontributor dan kami menghapus data kontributor yang ada.

Menghapus aturan Contributor Insights untukAWS PrivateLink menggunakan konsol

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Wawasan.
3. Perluas panel Aturan dan pilih aturan.
4. Pilih Tindakan, Hapus aturan.
5. Saat diminta konfirmasi, pilih Delete (Hapus).

Untuk menghapus aturan Contributor Insights untukAWS PrivateLink menggunakanAWS CLI

Gunakan delete-insight-rulesperintah untuk menghapus aturan.

AWS PrivateLink kuota

Tabel berikut mencantumkan kuota, yang sebelumnya disebut sebagai batas, untuk AWS PrivateLink sumber daya per Wilayah untuk akun Anda. Kecuali disebutkan lain, Anda dapat meminta penambahan untuk kuota ini. Untuk informasi selengkapnya, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

Jika Anda meminta penambahan kuota yang berlaku per sumber daya, kami meningkatkan kuota untuk semua sumber daya di Wilayah.

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
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
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 yang merupakan kontributor teratas untuk metrik tersebut. CloudWatch AWS PrivateLink	18 Agustus 2022
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	Mei 11, 2022

	mengaktifkan dukungan IPv6 untuk titik akhir antarmuka mereka sehingga mereka dapat mengakses layanan endpoint melalui IPv6.	
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 menggunak an 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.