AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

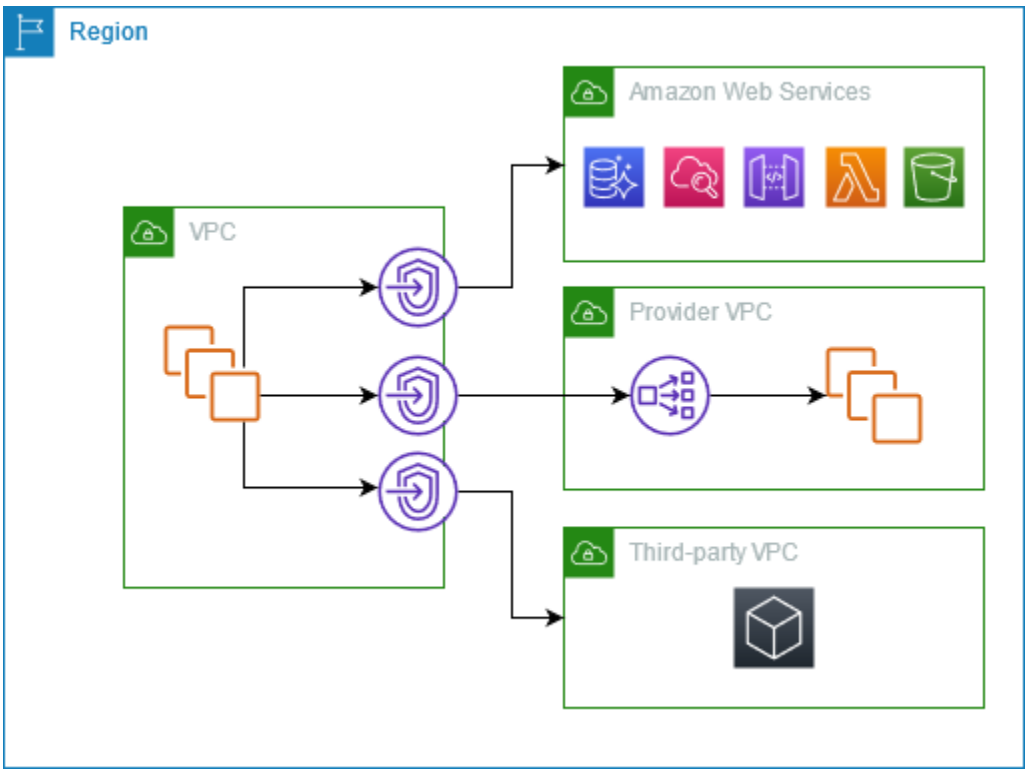
Apa itu AWS PrivateLink?

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

Kasus penggunaan

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

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



Pelajari selengkapnya

- the section called “Konsep”
- Akses Layanan AWS
- Akses produk SaaS
- Akses peralatan virtual
- Bagikan layanan Anda

Bekerja dengan titik VPC akhir

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

- AWS Management ConsoleMenyediakan antarmuka web yang dapat Anda gunakan untuk mengakses AWS PrivateLink sumber daya Anda. Buka VPC konsol Amazon 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::VPCEndpointConnectionNotification
  - AWS::EC2::VPCEndpointService
  - AWS::EC2::VPCEndpointServicePermissions
  - AWS:: ElasticLoadBalancing V2:: LoadBalancer
- AWS SDKs— Menyediakan bahasa khususAPIs. SDKsMengurus banyak detail koneksi, seperti menghitung tanda tangan, menangani percobaan ulang permintaan, dan menangani kesalahan. Untuk informasi lebih lanjut, lihat Alat untuk Membangun di AWS.
- Kueri API — Menyediakan API tindakan tingkat rendah yang Anda panggil menggunakan HTTPS permintaan. Menggunakan Query API adalah cara paling langsung untuk mengakses AmazonVPC. 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 EC2APIReferensi Amazon.

Harga

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

AWS PrivateLink konsep

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

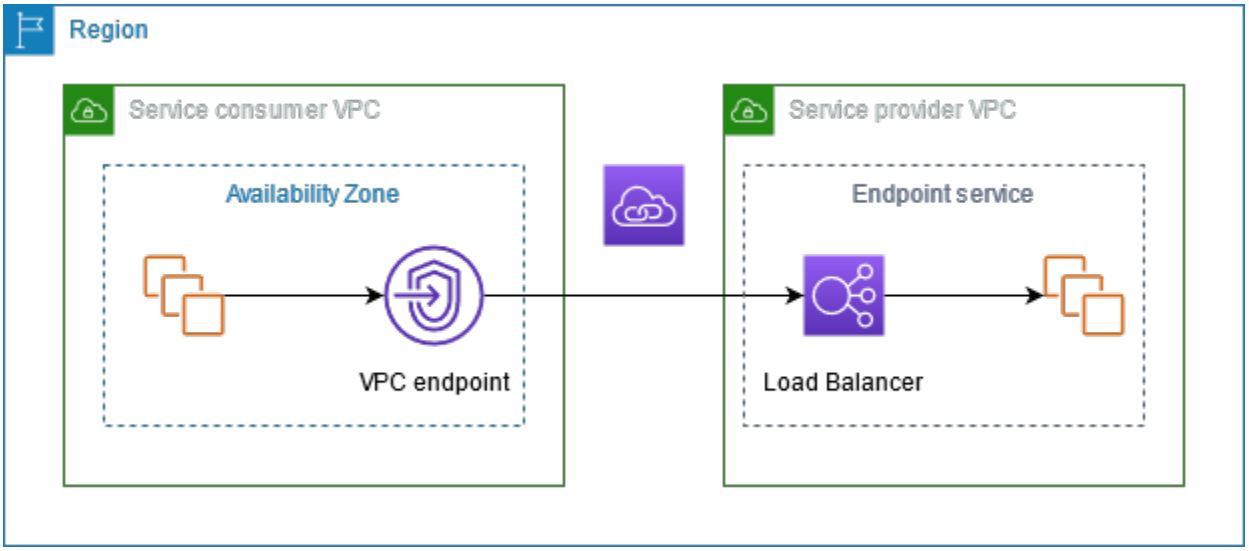
Berikut ini adalah konsep penting untuk dipahami saat Anda mulai menggunakan AWS PrivateLink.

Daftar Isi

- Penyedia
- Konsumen layanan atau sumber daya
- AWS PrivateLink koneksi
- Zona host pribadi

Diagram arsitektur

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



Penyedia

Memahami konsep yang terkait dengan penyedia.

Penyedia layanan

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

Penyedia sumber daya

Pemilik sumber daya, misalnya database, cluster node, atau instance, adalah penyedia sumber daya. Penyedia sumber daya mencakup AWS layanan, AWS Mitra, dan AWS akun lainnya. Penyedia sumber daya dapat meng-host sumber daya mereka di dalam VPCs atau di tempat.

Konsep

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

Layanan titik akhir

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

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

Nama layanan

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

Konfigurasi sumber daya

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

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

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

Gerbang sumber daya

Sebuah gateway sumber daya adalah titik masuknya ke dalam VPC dari mana sumber daya sedang dibagikan. Penyedia membuat gateway sumber daya untuk berbagi sumber daya dariVPC.

Konsumen layanan atau sumber daya

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

Konsep

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

Titik akhir VPC

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

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

Ada jenis VPC endpoint lain`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 VPC akhir lainnya. Untuk informasi selengkapnya, lihat the section called “Titik akhir Gateway”.

Antarmuka jaringan titik akhir

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

Jika VPC endpoint mendukungIPv4, antarmuka jaringan endpoint nya memiliki alamat. IPv4 Jika VPC endpoint mendukungIPv6, antarmuka jaringan endpoint nya memiliki alamat. IPv6 IPv6Alamat untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Saat Anda mendeskripsikan antarmuka jaringan titik akhir dengan IPv6 alamat, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Kebijakan titik akhir

Kebijakan VPCendpoint adalah kebijakan IAM sumber daya yang Anda lampirkan ke titik VPC akhir. Ini menentukan prinsipal mana yang dapat menggunakan titik akhir untuk mengakses VPC layanan

titik akhir. Kebijakan VPC endpoint default memungkinkan semua tindakan oleh semua prinsipal pada semua sumber daya di atas titik akhir. VPC

Status titik akhir

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

Berikut ini adalah status yang mungkin untuk VPC titik akhir:

- `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. VPCTitik akhir kembali ke status ini jika konsumen layanan memodifikasi titik akhir. VPC
- `Available`- VPC Titik akhir tersedia untuk digunakan.
- `Rejected`- Penyedia layanan menolak permintaan koneksi. Penyedia layanan juga dapat menolak koneksi setelah tersedia untuk digunakan.
- `Expired`- Permintaan koneksi kedaluwarsa.
- `Failed`- VPC Titik akhir tidak dapat dibuat tersedia.
- `Deleting`- Konsumen layanan menghapus VPC titik akhir dan penghapusan sedang berlangsung.
- `Deleted`- VPC Titik akhir dihapus.

AWS PrivateLink koneksi

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

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

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

Zona host pribadi

Zona yang dihosting adalah wadah untuk DNS catatan 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 tempat AndaVPCs.

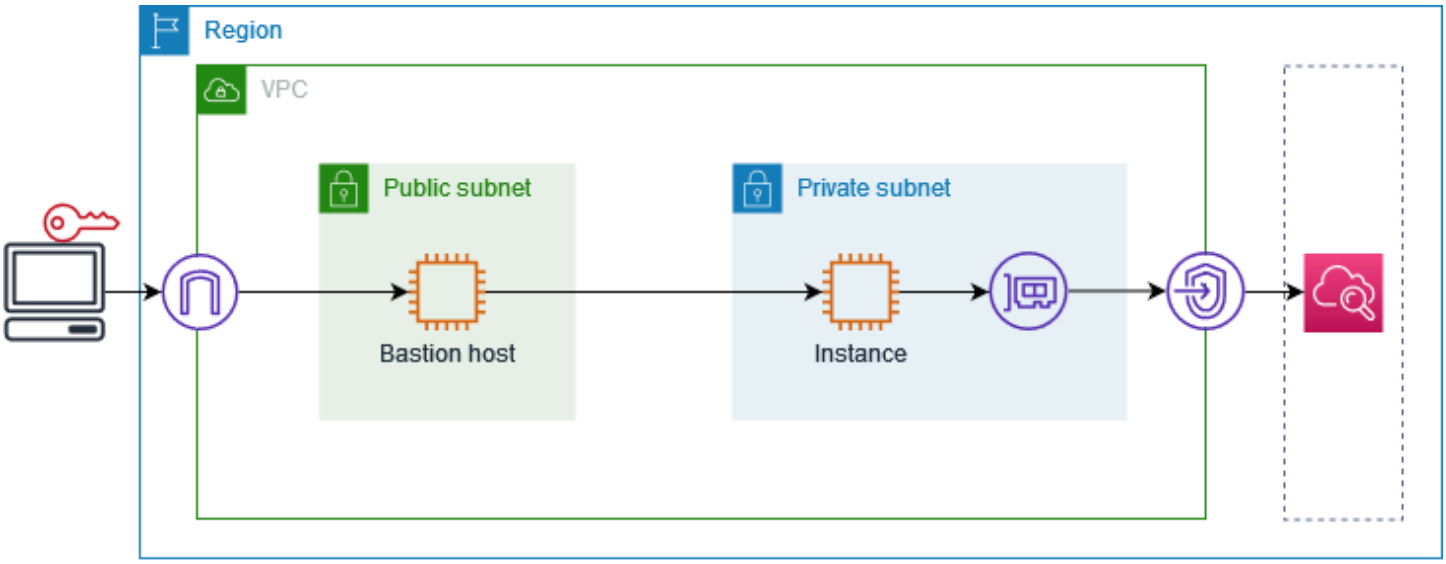
Anda dapat mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas domain ke VPC titik akhir. Untuk informasi selengkapnya, lihat Merutekan lalu lintas ke VPC titik akhir menggunakan nama domain Anda.

Anda dapat menggunakan Route 53 untuk mengonfigurasi split-horizonDNS, di mana Anda menggunakan nama domain yang sama untuk situs web publik dan layanan endpoint yang didukung oleh. AWS PrivateLink DNSpermintaan untuk nama host publik dari VPC penyelesaian konsumen ke alamat IP pribadi dari antarmuka jaringan titik akhir, tetapi permintaan dari luar VPC terus diselesaikan ke titik akhir publik. Untuk informasi selengkapnya, lihat DNSMekanisme untuk Lalu Lintas Perutean dan Mengaktifkan Failover untuk Penerapan. AWS PrivateLink

Memulai dengan AWS PrivateLink

Tutorial ini menunjukkan cara mengirim permintaan dari EC2 instance di subnet pribadi ke Amazon CloudWatch menggunakan. 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 SSH kunci. Kemudian, Anda dapat terhubung ke instance dari host bastion tanpa menentukan `.pem` file dalam perintah. ssh Setelah Anda menyiapkan VPC titik akhir untuk CloudWatch, lalu lintas dari instance yang ditakdirkan akan diselesaikan ke antarmuka jaringan titik akhir dan kemudian dikirim ke CloudWatch menggunakan titik akhir. CloudWatch VPC



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 VPC titik akhir untuk mengakses CloudWatch

Langkah 1: Buat VPC dengan subnet

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

Untuk membuat VPC

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Pilih BuatVPC.
3. Agar Sumber Daya dapat dibuat, pilih, VPCdan lainnya.
4. Untuk pembuatan otomatis tag 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 BuatVPC.

Langkah 2: Luncurkan instance

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

Prasyarat

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

Untuk meluncurkan host benteng

1. Buka EC2 konsol Amazon 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 AndaVPC.
    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 EC2 konsol Amazon 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 AndaVPC.
    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. IAMMisalnya profil, pilih profil IAM instans 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 SSH agen menggunakan perintah berikut, di *key.pem* mana 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 instance.

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

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

   ```
   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 VPC konfigurasi saat ini.

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

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

Langkah 4: Buat VPC titik akhir untuk mengakses CloudWatch

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

Prasyarat

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

Untuk membuat VPC titik akhir untuk CloudWatch

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk tag Nama, masukkan nama untuk titik akhir.
5. Untuk Kategori layanan, pilih Layanan AWS.
6. Untuk Layanan, pilih com.amazonaws. ***region***.pemantauan.
7. Untuk VPC, pilihVPC.
8. Untuk Subnet, pilih Availability Zone dan kemudian pilih subnet pribadi.
9. Untuk grup Keamanan, pilih grup keamanan untuk VPC titik akhir.
10. Untuk Kebijakan, pilih Akses penuh untuk mengizinkan semua operasi oleh semua prinsipal pada semua sumber daya di atas 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 VPC akhir

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

Untuk menguji titik VPC akhir

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

```
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 bahwa instance memiliki IAM peran 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 VPC akhir.

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 EC2 konsol Amazon 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 VPC titik akhir, Anda dapat menghapusnya.

Untuk menghapus titik VPC akhir

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih VPC titik akhir.
4. Pilih Tindakan, Hapus VPC titik akhir.
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 Anda VPC sehingga lalu lintas dapat berpindah dari VPC ke. Layanan AWS Jika konfigurasi ini tidak berfungsi dengan persyaratan keamanan jaringan Anda, Anda dapat menggunakan AWS PrivateLink VPC untuk menghubungkan Anda Layanan AWS seolah-olah mereka ada di AndaVPC, tanpa menggunakan gateway internet.

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

Harga

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

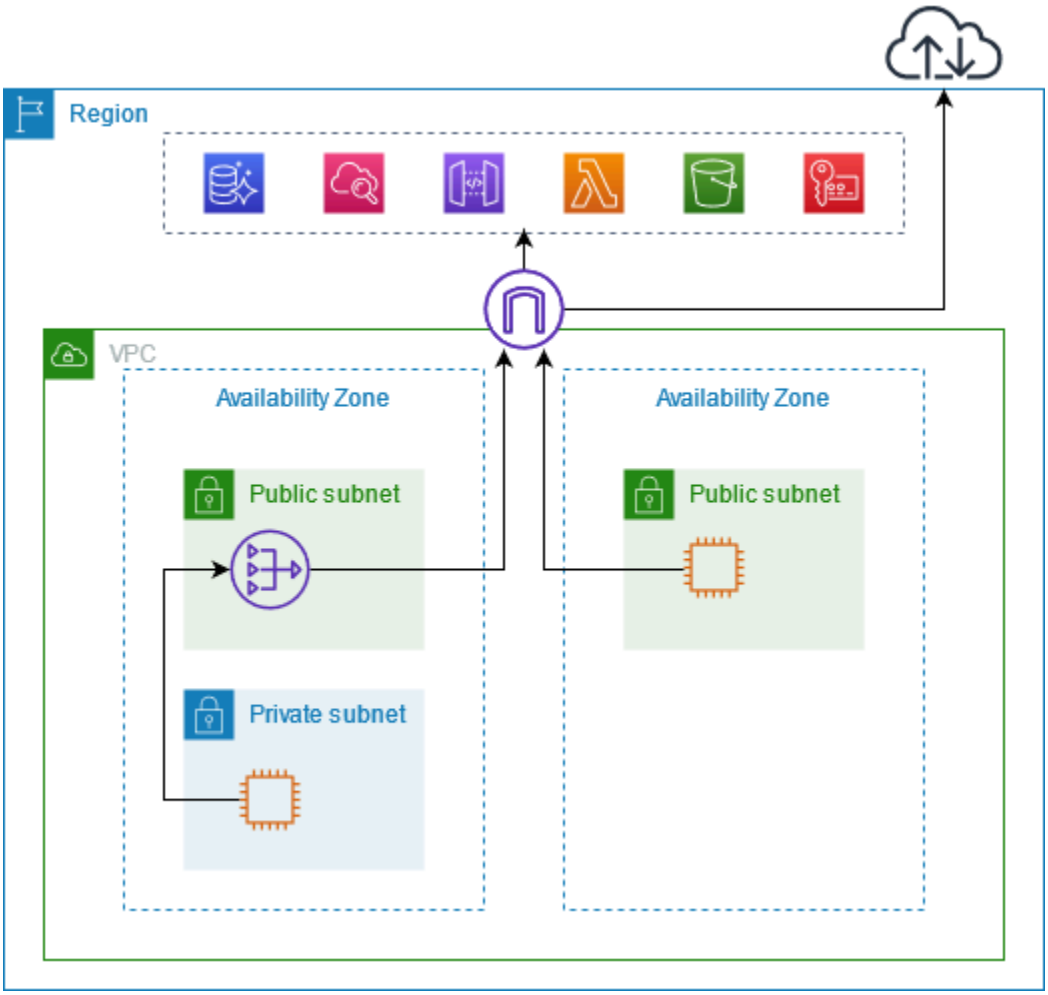
Daftar Isi

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.

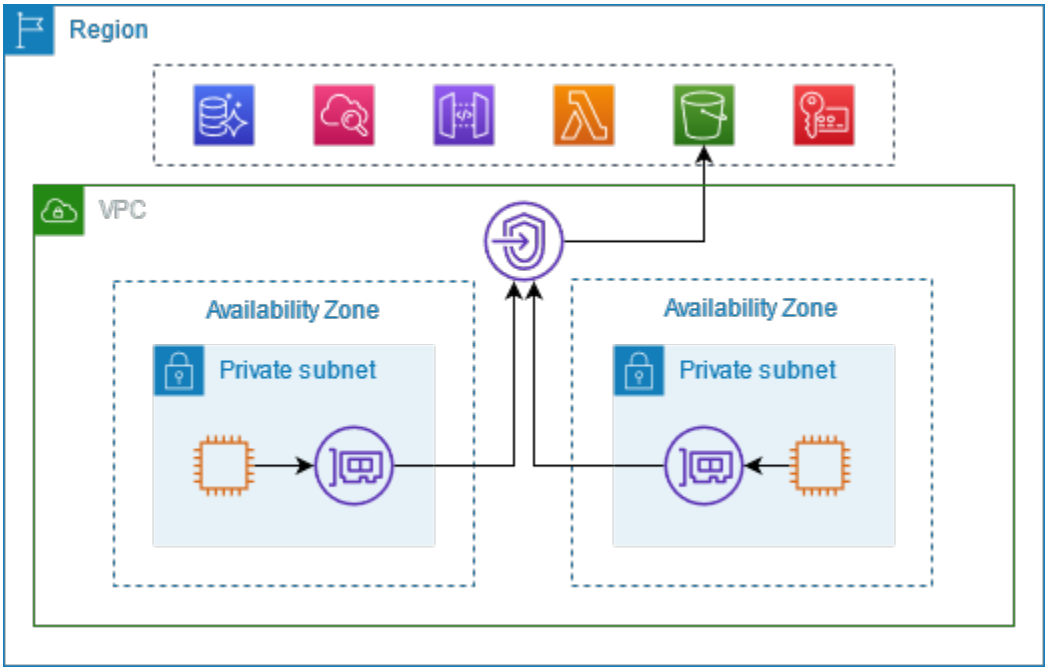
Akses melalui titik akhir layanan publik

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 NAT gateway, lalu ke gateway internet untukVPC, 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 VPC titik akhir antarmuka, yang membuat koneksi antara subnet di antarmuka jaringan Anda VPC dan yang Layanan AWS menggunakan. Lalu lintas yang Layanan AWS ditujukan untuk diselesaikan ke alamat IP pribadi dari antarmuka jaringan titik akhir menggunakanDNS, dan kemudian dikirim ke Layanan AWS menggunakan koneksi antara titik VPC akhir dan. Layanan AWS



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

DNSnama host

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 VPC titik akhir antarmuka, kami membuat DNS nama Regional dan zona yang dapat Anda gunakan untuk berkomunikasi dengan Layanan AWS dari Anda. VPC

DNSNama Regional untuk VPC titik akhir antarmuka Anda memiliki sintaks berikut:

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

DNSNama-nama zona memiliki sintaks berikut:

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

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

describe-vpc-endpointsPerintah berikut menampilkan DNS entri 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 DNS nama 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"
        }
    ]
]
```

DNSresolusi

DNSCatatan yang kami buat untuk VPC titik akhir antarmuka Anda bersifat publik. Oleh karena itu, DNS nama-nama ini dapat diselesaikan secara publik. Namun, DNS permintaan 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 layanan. VPC

Pribadi DNS

Jika Anda mengaktifkan private DNS untuk VPC endpoint antarmuka Anda, dan DNSnama host dan DNS resolusi Anda VPC diaktifkan, kami membuat zona host pribadi AWS terkelola yang tersembunyi untuk Anda. Zona yang dihosting berisi kumpulan catatan untuk DNS nama default untuk layanan yang menyelesaikannya ke alamat IP pribadi dari antarmuka jaringan titik akhir di Anda. VPC 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 DNS nama pribadi untuk VPC Layanan AWS titik akhir Anda. Ini memastikan bahwa permintaan yang menggunakan titik akhir layanan publik, seperti permintaan yang dibuat melalui AWS SDK, diselesaikan ke titik VPC akhir Anda.

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

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

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

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

Diagram berikut menunjukkan VPC titik akhir untuk Amazon CloudWatch dengan antarmuka jaringan endpoint dalam Availability Zone tunggal. Ketika sumber daya apa pun di subnet apa pun di VPC mengakses Amazon CloudWatch 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.

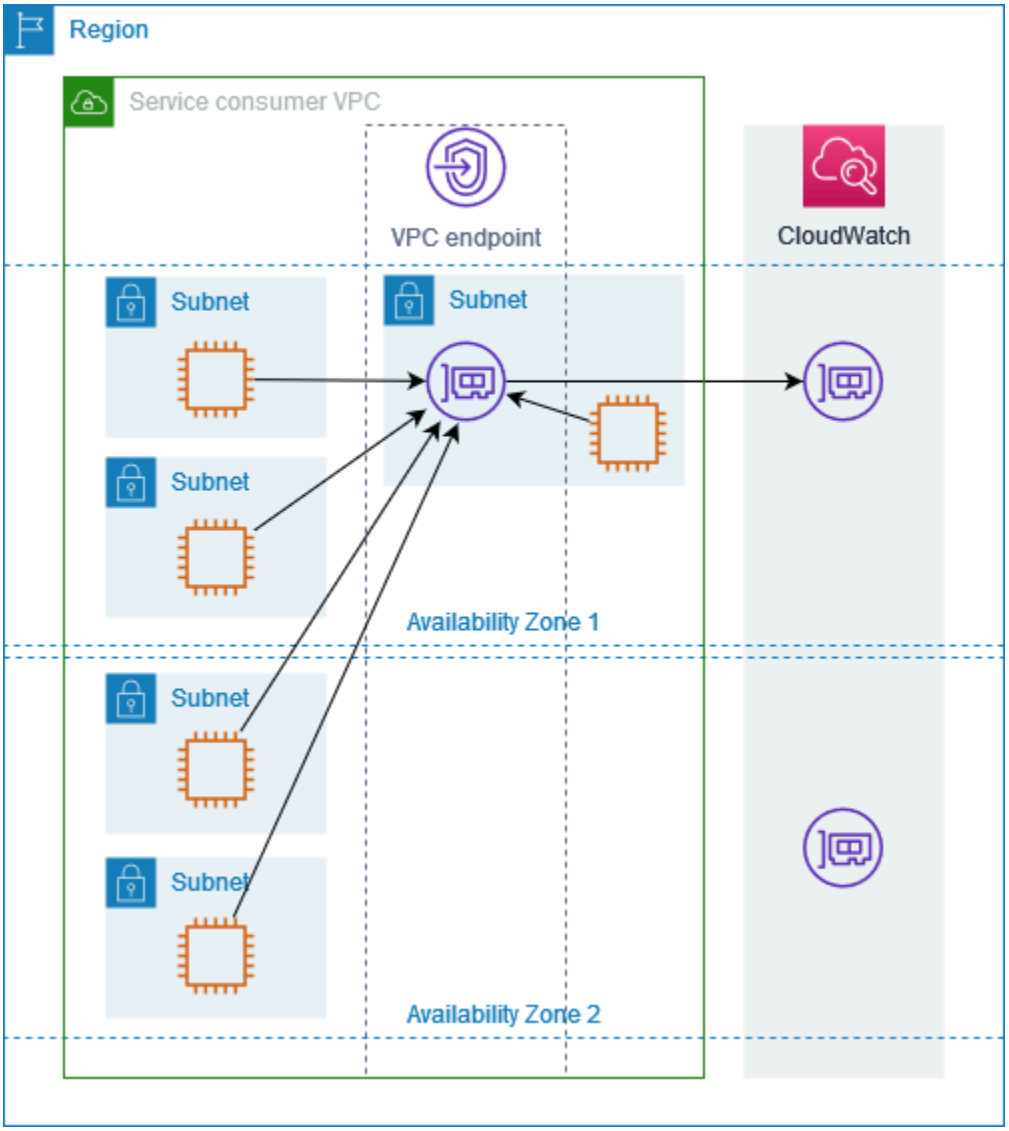
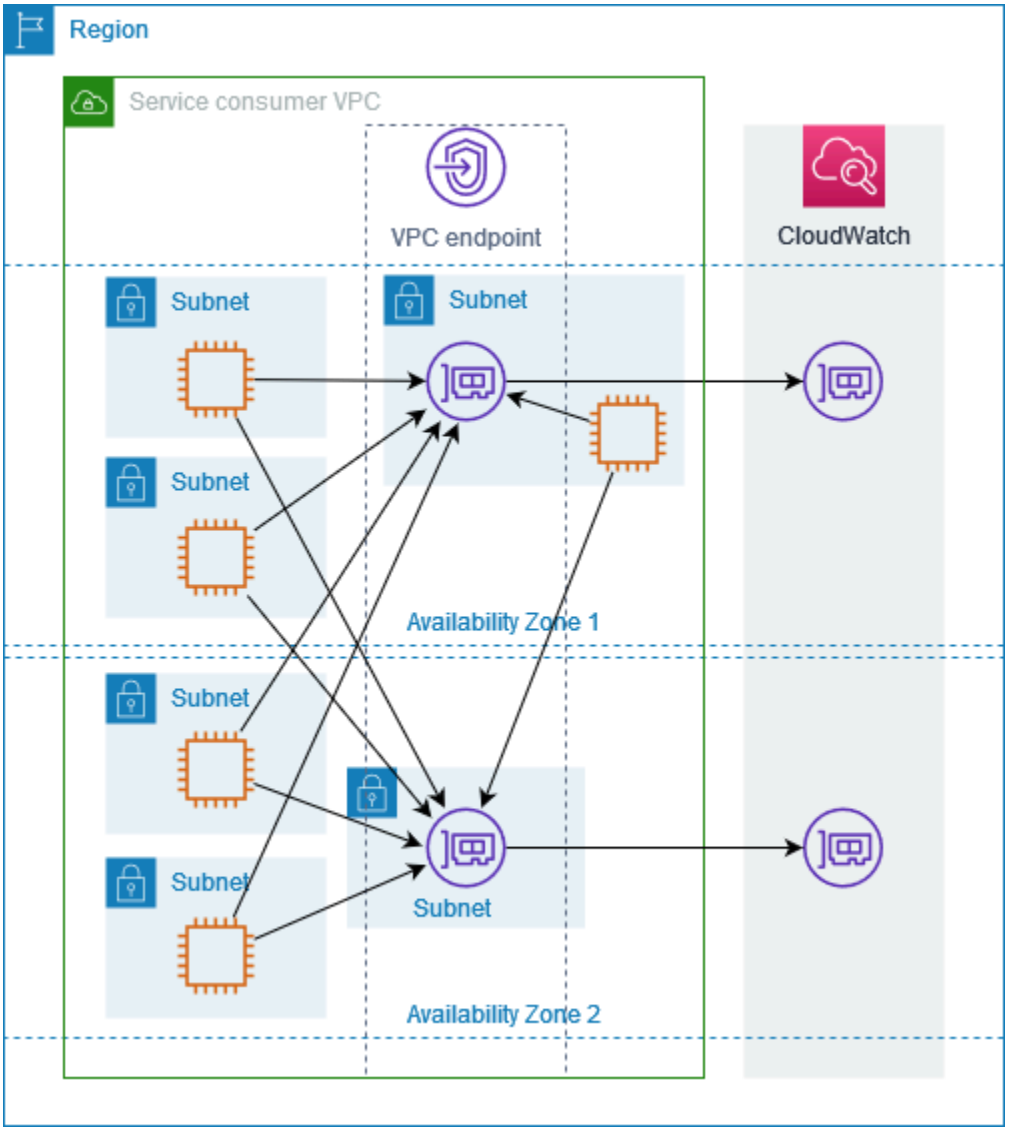
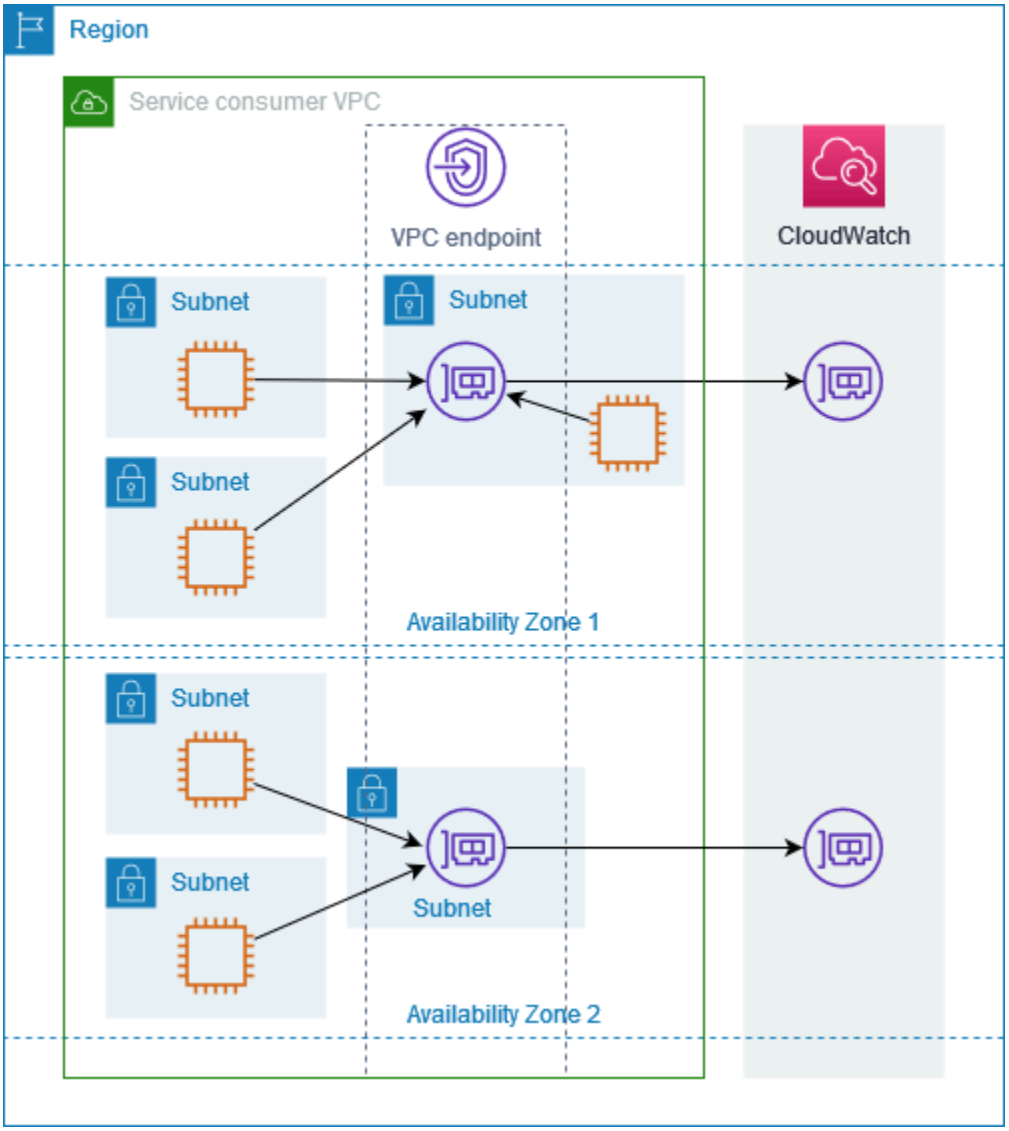


Diagram berikut menunjukkan VPC titik akhir untuk Amazon CloudWatch dengan antarmuka jaringan titik akhir di dua Availability Zones. Ketika sumber daya apa pun di subnet apa pun di VPC mengakses Amazon CloudWatch dengan menggunakan titik akhir publiknya, kami memilih antarmuka jaringan titik akhir yang 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 DNS kueri dengan AAAA catatan.

Persyaratan IPv6 untuk mengaktifkan titik akhir antarmuka

- Layanan AWS Harus membuat titik akhir layanannya tersedia di atasIPv6. Untuk informasi selengkapnya, lihat the section called “Lihat IPv6 dukungan”.
- Jenis alamat IP dari titik akhir antarmuka harus kompatibel dengan subnet untuk titik akhir antarmuka, seperti yang dijelaskan di sini:

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

Jika VPC titik akhir antarmuka mendukungIPv4, antarmuka jaringan titik akhir memiliki alamat. IPv4 Jika VPC titik akhir antarmuka mendukungIPv6, antarmuka jaringan titik akhir memiliki alamat. IPv6 IPv6Alamat untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Jika Anda mendeskripsikan antarmuka jaringan endpoint dengan IPv6 alamat, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Layanan AWS yang terintegrasi dengan AWS PrivateLink

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

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 VPC titik akhir antarmuka, atau ini menunjukkan bahwa layanan mengelola titik akhir.

Layanan AWS	Nama layanan
Penganalisis Akses	com.amazonaws. *region*.akses-penganalisis
AWS Account Management	com.amazonaws. *region*.akun
APIGerbang Amazon	com.amazonaws. *region*.eksekusi api
AWS AppConfig	com.amazonaws. *region*.appconfig
	com.amazonaws. *region*.appconfigdata
AWS App Mesh	com.amazonaws. *region*.appmesh
	com.amazonaws. *region*. appmesh-envoy-management

Layanan AWS	Nama layanan
AWS Pelari Aplikasi	com.amazonaws. *region*.apprunner
AWS Layanan App Runner	com.amazonaws. *region*.apprunner.requests
Penskalaan Otomatis Aplikasi	com.amazonaws. *region*.application-autoscaling
AWS Application Discovery Service	com.amazonaws. *region*.penemuan
	com.amazonaws. *region*.penemuan-arsenal
AWS Layanan Migrasi Aplikasi	com.amazonaws. *region*.mgn
Amazon AppStream 2.0	com.amazonaws. *region*.appstream.api
	com.amazonaws. *region*.appstream.streaming
AWS AppSync	com.amazonaws. *region*.appsync-api
Amazon Athena	com.amazonaws. *region*.athena
AWS Audit Manager	com.amazonaws. *region*.auditmanager
Amazon Aurora	com.amazonaws. *region*.rds
AWS Auto Scaling	com.amazonaws. *region*.rencana penskalaan otomatis
AWS Pertukaran Data B2B	com.amazonaws. *region*.b2bi
AWS Backup	com.amazonaws. *region*.cadangan
	com.amazonaws. *region*.backup-gateway
AWS Batch	com.amazonaws. *region*.batch
Amazon Bedrock	com.amazonaws. *region*.batuan dasar
	com.amazonaws. *region*.bedrock-agen
	com.amazonaws. *region*. bedrock-agent-runtime

Layanan AWS	Nama layanan
	com.amazonaws. *region*.bedrock-runtime
AWS Billing and Cost Management	com.amazonaws. *region*.penagihan
	com.amazonaws. *region*.lebih bebas
	com.amazonaws. *region*.pajak
AWS Billing Conductor	com.amazonaws. *region*.billingkonduktor
Amazon Braket	com.amazonaws. *region*.braket
AWS Kamar Bersih	com.amazonaws. *region*.kamar bersih
AWS Kamar Bersih	com.amazonaws. *region*.cleanrooms-ml
AWS Cloud Control API	com.amazonaws. *region*.cloudcontrolapi
	com.amazonaws. *region*.cloudcontrolapi-fips
Amazon Cloud Directory	com.amazonaws. *region*.clouddirectory
AWS CloudFormation	com.amazonaws. *region*.cloudformasi
AWS CloudHSM	com.amazonaws. *region*.cloudhsmv2
AWS Cloud Map	com.amazonaws. *region*.servicediscovery
	com.amazonaws. *region*.servicediscovery-fips
	com.amazonaws. *region*.data-servicediscovery
	com.amazonaws. *region*. data-servicediscovery-fips
AWS CloudTrail	com.amazonaws. *region*.cloudtrail
Amazon CloudWatch	com.amazonaws. *region*.aplikasi-sinyal
	com.amazonaws. *region*.applicationinsights

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

Layanan AWS	Nama layanan
	com.amazonaws. *region*.git-codecommit
	com.amazonaws. *region*. git-codecommit-fips
AWS CodeConnections	com.amazonaws. *region*.codeconnections.api
	com.amazonaws. *region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws. *region*.codedeploy
	com.amazonaws. *region*. codedeploy-commands-secure
Amazon CodeGuru Profiler	com.amazonaws. *region*.codeguru-profiler
CodeGuru Peninjau Amazon	com.amazonaws. *region*.codeguru-pengulas
AWS CodePipeline	com.amazonaws. *region*.codepipeline
Amazon Comprehend	com.amazonaws. *region*.comprehend
Amazon Comprehend Medical	com.amazonaws. *region*.comprehendmedis
AWS Compute Optimizer	com.amazonaws. *region*.pengoptimal komputasi
AWS Config	com.amazonaws. *region*.config
Amazon Connect	com.amazonaws. *region*.app-integrasi
	com.amazonaws. *region*.kasus
	com.amazonaws. *region*.connect-kampanye
	com.amazonaws. *region*.profil
	com.amazonaws. *region*.voiceid
	com.amazonaws. *region*.kebijaksanaan
AWS Connector Service	com.amazonaws. *region*.awskonektor

Layanan AWS	Nama layanan
AWS Katalog Kontrol	com.amazonaws. *region*.controlcatalog
AWS Cost Explorer	com.amazonaws. *region*.ce
Hub Optimisasi Biaya AWS	com.amazonaws. *region*. cost-optimization-hub
AWS Data Exchange	com.amazonaws. *region*.pertukaran data
Ekspor Data AWS	com.amazonaws. *region*. bcm-data-exports
Amazon Data Firehose	com.amazonaws. *region*.kinesis-firehose
AWS Database Migration Service	com.amazonaws. *region*.dms
	com.amazonaws. *region*.dms-fips
AWS DataSync	com.amazonaws. *region*.datasync
Amazon DataZone	com.amazonaws. *region*.datazone
AWS Deadline Cloud	com.amazonaws. *region*.deadline.management
	com.amazonaws. *region*.deadline.scheduling
DevOpsGuru Amazon	com.amazonaws. *region*.devops-guru
AWS Directory Service	com.amazonaws. *region*.ds
	com.amazonaws. *region*.ds-data
Amazon DocumentDB	com.amazonaws. *region*.rds
Amazon DynamoDB	com.amazonaws. *region*.dynamodb
	com.amazonaws. *region*.dynamodb-fips
Amazon EBS langsung APIs	com.amazonaws. *region*.ebs
Amazon EC2	com.amazonaws. *region*.ec2

Layanan AWS	Nama layanan
EC2Auto Scaling Amazon	com.amazonaws. *region*.penskalaan otomatis
EC2Image Builder	com.amazonaws. *region*.imagebuilder
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
Amazon ECS	com.amazonaws. *region*.ecs
	com.amazonaws. *region*.ecs-agen
	com.amazonaws. *region*.ecs-telemetri
Amazon EKS	com.amazonaws. *region*.eks
	com.amazonaws. *region*.eks-auth
AWS Elastic Beanstalk	com.amazonaws. *region*.elasticbeanstalk
	com.amazonaws. *region*.elasticbeanstalk-kesehatan
AWS Elastic Disaster Recovery	com.amazonaws. *region*.drs
Sistem File Elastis Amazon	com.amazonaws. *region*.elasticfilesystem
	com.amazonaws. *region*.elasticfilesystem-fips
Elastic Load Balancing	com.amazonaws. *region*.elasticloadbalancing
Amazon ElastiCache	com.amazonaws. *region*.elasticache
	com.amazonaws. *region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws. *region*.mediaconnect
Amazon EMR	com.amazonaws. *region*.elasticmapreduce
Amazon EMR di EKS	com.amazonaws. *region*.emr-kontainer

Layanan AWS	Nama layanan
Amazon Tanpa EMR Server	com.amazonaws. *region*.emr-tanpa server
	com.amazonaws. *region*. emr-serverless-services.hidup
Amazon EMR WAL	com.amazonaws. *region*.emrwal.prod
AWS Pesan Pengguna Akhir Sosial	com.amazonaws. *region*.pesan sosial
Resolusi Entitas AWS	com.amazonaws. *region*.entityresolution
Amazon EventBridge	com.amazonaws. *region*.acara
	com.amazonaws. *region*.pipa
	com.amazonaws. *region*.pipa-data
	com.amazonaws. *region*.pipes-fips
	com.amazonaws. *region*.skema
AWS Fault Injection Service	com.amazonaws. *region*.fi
Amazon FinSpace	com.amazonaws. *region*.finspace
	com.amazonaws. *region*.finspace-api
Amazon Forecast	com.amazonaws. *region*.perkiraan
	com.amazonaws. *region*.forecastquery
	com.amazonaws. *region*.forecast-fips
	com.amazonaws. *region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws. *region*.detektor penipuan
Amazon FSx	com.amazonaws. *region*.fsx
	com.amazonaws. *region*.fsx-fips

Layanan AWS	Nama layanan
AWS Glue	com.amazonaws. *region*.lem
	com.amazonaws. *region*.glue.dasbor
AWS Glue DataBrew	com.amazonaws. *region*.databrew
Amazon Managed Grafana	com.amazonaws. *region*.grafana
	com.amazonaws. *region*.grafana-ruang kerja
AWS Ground Station	com.amazonaws. *region*.groundstation
Amazon GuardDuty	com.amazonaws. *region*.guardduty
	com.amazonaws. *region*.guardduty-data
	com.amazonaws. *region*. guardduty-data-fips
	com.amazonaws. *region*.guardduty-fips
AWS HealthImaging	com.amazonaws. *region*. dicom-medical-imaging
	com.amazonaws. *region*.pencitraan medis
	com.amazonaws. *region*. runtime-medical-imaging
AWS HealthLake	com.amazonaws. *region*.healthlake
AWS HealthOmics	com.amazonaws. *region*.analytics-omics
	com.amazonaws. *region*. control-storage-omics
	com.amazonaws. *region*.penyimpanan-omics
	com.amazonaws. *region*.tags-omics
	com.amazonaws. *region*.workflows-omics
AWS Identity and Access Management (IAM)	com.amazonaws.iam

Layanan AWS	Nama layanan
IAMPusat Identitas	com.amazonaws. *region*.identitystore
IAMPeran Di Mana Saja	com.amazonaws. *region*.rolesdi mana saja
Amazon Inspector	com.amazonaws. *region*.inspektor2
	com.amazonaws. *region*.inspektor-pemindaian
AWS IoT Core	com.amazonaws. *region*.iot.data
	com.amazonaws. *region*.iot.credentials
	com.amazonaws. *region*.iot.fleethub.api
AWS IoT Core Device Advisor	com.amazonaws. *region*.deviceadvisor.iot
AWS IoT Core for LoRaWAN	com.amazonaws. *region*.iotwireless.api
	com.amazonaws. *region*.lorawan.cangkir
	com.amazonaws. *region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws. *region*.iotfleetwise
AWS IoT Greengrass	com.amazonaws. *region*.greengrass
AWS IoT RoboRunner	com.amazonaws. *region*.iotroborunner
AWS IoT SiteWise	com.amazonaws. *region*.iotsitewise.api
	com.amazonaws. *region*.iotsitewise.data
AWS IoT TwinMaker	com.amazonaws. *region*.iottwinmaker.api
	com.amazonaws. *region*.iottwinmaker.data
Amazon Kendra	com.amazonaws. *region*.kendra
	aws.api. *region*peringkat.kendra

Layanan AWS	Nama layanan
AWS Key Management Service	com.amazonaws. *region*.kms
	com.amazonaws. *region*.kms-fips
Amazon Keyspaces (untuk Apache Cassandra)	com.amazonaws. *region*.cassandra
	com.amazonaws. *region*.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws. *region*.kinesis-stream
	com.amazonaws. *region*. kinesis-streams-fips
AWS Lake Formation	com.amazonaws. *region*.lakeformasi
AWS Lambda	com.amazonaws. *region*.lambda
AWS Launch Wizard	com.amazonaws. *region*.launchwizard
Amazon Lex	com.amazonaws. *region*.model-v2-lex
	com.amazonaws. *region*.runtime-v2-lex
AWS License Manager	com.amazonaws. *region*.lisensi-manajer
	com.amazonaws. *region*. license-manager-fips
	com.amazonaws. *region*. license-manager-linux-subscriptions
	com.amazonaws. *region*. license-manager-linux-subscriptions-fips
	com.amazonaws. *region*. license-manager-user-subscriptions
Amazon Lookout for Equipment	com.amazonaws. *region*.lookoutequipment
Amazon Lookout for Metrics	com.amazonaws. *region*.lookoutmetrics

Layanan AWS	Nama layanan
Amazon Lookout for Vision	com.amazonaws. *region*.lookoutvision
Amazon Macie	com.amazonaws. *region*.macie2
AWS Mainframe Modernization	com.amazonaws. *region*.apptest
	com.amazonaws. *region*.m2
Amazon Managed Blockchain	com.amazonaws. *region*.managedblockchain-query
	com.amazonaws. *region*.managedblockchain.bitcoin.mainnet
	com.amazonaws. *region*.managedblockchain.bitcoin.testnet
Layanan Terkelola Amazon untuk Prometheus	com.amazonaws. *region*.aps
	com.amazonaws. *region*.aps-ruang kerja
Amazon Managed Streaming for Apache Kafka	com.amazonaws. *region*.kafka
	com.amazonaws. *region*.kafka-fips
Alur Kerja Terkelola Amazon untuk Apache Airflow	com.amazonaws. *region*.airflow.api
	com.amazonaws. *region*.airflow.api-fips
	com.amazonaws. *region*.airflow.env
	com.amazonaws. *region*.airflow.env-fips
	com.amazonaws. *region*.airflow.ops
AWS Management Console	com.amazonaws. *region*.konsol
	com.amazonaws. *region*.masuk
Amazon MemoryDB	com.amazonaws. *region*.memori-db

Layanan AWS	Nama layanan
	com.amazonaws. *region*.memorydb-fips
Orkestrator AWS Migration Hub	com.amazonaws. *region*.migrationhub-orkestrator
AWS Migration Hub Refactor Spaces	com.amazonaws. *region*.refactor-spasi
Rekomendasi Strategi Migrasi Hub	com.amazonaws. *region*.migrationhub-strategi
Amazon MQ	com.amazonaws. *region*.mq
Analisis Amazon Neptunus	com.amazonaws. *region*.neptunus grafik
	com.amazonaws. *region*. neptune-graph-data
	com.amazonaws. *region*. neptune-graph-fips
AWS Network Firewall	com.amazonaws. *region*.jaringan-firewall
	com.amazonaws. *region*. network-firewall-fips
OpenSearch Layanan Amazon	Titik akhir ini dikelola layanan
AWS Organizations	com.amazonaws. *region*.organisasi
	com.amazonaws. *region*.organisasi-fips
AWS Outposts	com.amazonaws. *region*.pos terdepan
AWS Panorama	com.amazonaws. *region*.panorama
AWS Kriptografi Pembayaran	com.amazonaws. *region*.pembayaran-cryptography.controlplane
	com.amazonaws. *region*.pembayaran-cryptography.dataplane
AWS PCS	com.amazonaws. *region*.pcs
	com.amazonaws. *region*.pcs-fips

Layanan AWS	Nama layanan
Amazon Personalisasi	com.amazonaws. *region*.personalisasi
	com.amazonaws. *region*.personalisasi-acara
	com.amazonaws. *region*.personalisasi-runtime
Amazon Pinpoint	com.amazonaws. *region*.tepat
	com.amazonaws. *region*. pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws. *region*.polly
Daftar Harga AWS	com.amazonaws. *region*.pricing.api
AWS 5G pribadi	com.amazonaws. *region*.jaringan pribadi
AWS Private Certificate Authority	com.amazonaws. *region*.acm-pca
	com.amazonaws. *region*. pca-connector-ad
	com.amazonaws. *region*. pca-connector-scep
AWS Proton	com.amazonaws. *region*.proton
Amazon Q Bisnis	aws.api. *region*.qbisnis
Amazon Q Developer	com.amazonaws. *region*.codewhisperer
	com.amazonaws. *region*.q
	com.amazonaws. *region*.qapps
Langganan Pengguna Amazon Q	com.amazonaws. *region*.service.user-langganan
Amazon QLDB	com.amazonaws. *region*.qldb.sesi
Amazon QuickSight	com.amazonaws. *region*.situs web quicksight-
Amazon RDS	com.amazonaws. *region*.rds

Layanan AWS	Nama layanan
RDSData Amazon API	com.amazonaws. *region*.rds-data
RDSPerformance Insights Amazon	com.amazonaws. *region*.pi
	com.amazonaws. *region*.pi-fips
AWS Re: Post Pribadi	com.amazonaws. *region*.repostspace
Tempat Sampah Daur Ulang	com.amazonaws. *region*.rbin
Amazon Redshift	com.amazonaws. *region*.pergeseran merah
	com.amazonaws. *region*.redshift-fips
	com.amazonaws. *region*.redshift-tanpa server
	com.amazonaws. *region*. redshift-serverless-fips
Data Pergeseran Merah Amazon API	com.amazonaws. *region*.redshift-data
	com.amazonaws. *region*. redshift-data-fips
Amazon Rekognition	com.amazonaws. *region*.rekognisi
	com.amazonaws. *region*.rekognition-fips
	com.amazonaws. *region*.streaming-rekognisi
	com.amazonaws. *region*. streaming-rekognition-fips
AWS Resource Access Manager	com.amazonaws. *region*.ram
AWS Resource Groups	com.amazonaws. *region*.resource-group
	com.amazonaws. *region*. resource-groups-fips
AWS RoboMaker	com.amazonaws. *region*.robomaker
Amazon S3	com.amazonaws. *region*.s3

Layanan AWS	Nama layanan
	com.amazonaws. *region*.s3tabel
Titik Akses Multi-Wilayah Amazon S3	com.amazonaws.s3-global.accesspoint
Amazon S3 di Outposts	com.amazonaws. *region*.s3-pos terdepan
Amazon SageMaker AI	aws.sagemaker. *region*.eksperimen
	aws.sagemaker. *region*.buku catatan
	aws.sagemaker. *region*.partner-aplikasi
	aws.sagemaker. *region*.studio
	com.amazonaws. *region*. sagemaker-data-science-assistant
	com.amazonaws. *region*.sagemaker.api
	com.amazonaws. *region*.sagemaker.api-fips
	com.amazonaws. *region*.sagemaker.featurestore-runtime
	com.amazonaws. *region*.sagemaker.metrics
	com.amazonaws. *region*.sagemaker.runtime
	com.amazonaws. *region*.sagemaker.runtime-fips
Savings Plans	com.amazonaws. *region*.savingsplans
AWS Secrets Manager	com.amazonaws. *region*.secretsmanager
AWS Security Hub	com.amazonaws. *region*.securityhub
AWS Security Token Service	com.amazonaws. *region*.sts

Layanan AWS	Nama layanan
AWS Serverless Application Repository	com.amazonaws. *region*.serverlessrepo
Katalog Layanan	com.amazonaws. *region*.servicecatalog
	com.amazonaws. *region*.servicecatalog-appregistry
Amazon SES	com.amazonaws. *region*.email-smtp
AWS SimSpace Weaver	com.amazonaws. *region*.simspaceweaver
AWS Snow Device Management	com.amazonaws. *region*. snow-device-management
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
Amazon SWF	com.amazonaws. *region*.swf
	com.amazonaws. *region*.swf-fips
AWS Step Functions	com.amazonaws. *region*.negara
	com.amazonaws. *region*.sync-status
AWS Storage Gateway	com.amazonaws. *region*.storagegateway
Rantai Pasokan AWS	com.amazonaws. *region*.scn
AWS Systems Manager	com.amazonaws. *region*.ec2pesan
	com.amazonaws. *region*.ssm
	com.amazonaws. *region*.ssm-kontak
	com.amazonaws. *region*.ssm-insiden
	com.amazonaws. *region*.ssm-pengaturan cepat
	com.amazonaws. *region*.ssmmessages

Layanan AWS	Nama layanan
AWS Pembangun Jaringan Telco	com.amazonaws. *region*.tnb
Amazon Texttract	com.amazonaws. *region*.textract
	com.amazonaws. *region*.textract-fips
Amazon Timestream	com.amazonaws. *region*.timestream.ingest- *cell*
	com.amazonaws. *region*.timestream.query- *cell*
Amazon Timestream untuk InfluxDB	com.amazonaws. *region*.timestream-influxdb
	com.amazonaws. *region*. timestream-influxdb-fips
Amazon Transcribe	com.amazonaws. *region*.transkripsikan
	com.amazonaws. *region*.transcribestreaming
Amazon Transcribe Medis	com.amazonaws. *region*.transkripsikan
	com.amazonaws. *region*.transcribestreaming
AWS Transfer for SFTP	com.amazonaws. *region*.transfer
	com.amazonaws. *region*.transfer.server
Amazon Translate	com.amazonaws. *region*.terjemahkan
AWS Trusted Advisor	com.amazonaws. *region*.trustedadvisor
Izin Terverifikasi Amazon	com.amazonaws. *region*.verifiedpermissions
VPCKisi Amazon	com.amazonaws. *region*.vpc-kisi
AWS Well-Architected Tool	com.amazonaws. *region*.wellarchitected
Amazon WorkMail	com.amazonaws. *region*.workmail
Amazon WorkSpaces	com.amazonaws. *region*.ruang kerja

Layanan AWS	Nama layanan
Browser Aman Amazon Workspaces	com.amazonaws. *region*.workspace-web
	com.amazonaws. *region*. workspaces-web-fips
Klien WorkSpaces Tipis Amazon	com.amazonaws. *region*.thinclient.api
AWS X-Ray	com.amazonaws. *region*.xray

Lihat Layanan AWS nama yang tersedia

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

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 describe-vpc-endpoint-servicesperintah 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 describe-vpc-endpoint-servicesperintah 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 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==`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-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.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.email-smtp",
    "com.amazonaws.us-east-1.glue.dashboard",
```

```
    "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.neptune-graph-fips",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.q",
    "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 IPv6 dukungan

Anda dapat menggunakan describe-vpc-endpoint-servicesperintah berikut untuk melihat Layanan AWS yang dapat Anda akses IPv6 di Wilayah 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.account",
    "com.amazonaws.us-east-1.applicationinsights",
    "com.amazonaws.us-east-1.apprunner",
```

```
    "com.amazonaws.us-east-1.aps",
    "com.amazonaws.us-east-1.aps-workspaces",
    "com.amazonaws.us-east-1.arsenal-discovery",
    "com.amazonaws.us-east-1.athena",
    "com.amazonaws.us-east-1.backup",
    "com.amazonaws.us-east-1.braket",
    "com.amazonaws.us-east-1.cloudcontrolapi",
    "com.amazonaws.us-east-1.cloudcontrolapi-fips",
    "com.amazonaws.us-east-1.cloudhsmv2",
    "com.amazonaws.us-east-1.compute-optimizer",
    "com.amazonaws.us-east-1.codeartifact.api",
    "com.amazonaws.us-east-1.codeartifact.repositories",
    "com.amazonaws.us-east-1.cost-optimization-hub",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.discovery",
    "com.amazonaws.us-east-1.drs",
    "com.amazonaws.us-east-1.ebs",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.elasticbeanstalk",
    "com.amazonaws.us-east-1.elasticbeanstalk-health",
    "com.amazonaws.us-east-1.execute-api",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.grafana",
    "com.amazonaws.us-east-1.groundstation",
    "com.amazonaws.us-east-1.internetmonitor".
    "com.amazonaws.us-east-1.internetmonitor-fips".
    "com.amazonaws.us-east-1.iotfleetwise",
    "com.amazonaws.us-east-1.kinesis-firehose",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.m2".
    "com.amazonaws.us-east-1.macie2".
    "com.amazonaws.us-east-1.networkflowmonitor".
    "com.amazonaws.us-east-1.networkflowmonitorreports".
    "com.amazonaws.us-east-1.pca-connector-scep",
    "com.amazonaws.us-east-1.pcs",
    "com.amazonaws.us-east-1.pcs-fips",
    "com.amazonaws.us-east-1.pi",
    "com.amazonaws.us-east-1.pi-fips",
    "com.amazonaws.us-east-1.polly",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.rbin",
```

```
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.sagemaker.api",
    "com.amazonaws.us-east-1.securityhub",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.synthetics".
    "com.amazonaws.us-east-1.synthetics-fips".
    "com.amazonaws.us-east-1.textract",
    "com.amazonaws.us-east-1.textract-fips",
    "com.amazonaws.us-east-1.timestream-influxdb",
    "com.amazonaws.us-east-1.timestream-influxdb-fips",
    "com.amazonaws.us-east-1.trustedadvisor",
    "com.amazonaws.us-east-1.workmail",
    "com.amazonaws.us-east-1.xray"
]
```

Mengakses titik VPC akhir Layanan AWS menggunakan antarmuka

Anda dapat membuat VPC titik akhir 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 AndaVPC, 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 AndaVPC.

- Untuk menggunakan pribadiDNS, Anda harus mengaktifkan DNS nama host dan DNS resolusi untuk AndaVPC. Untuk informasi selengkapnya, lihat Melihat dan memperbarui DNS atribut di Panduan VPC Pengguna Amazon.
- IPv6Untuk mengaktifkan titik akhir antarmuka, Layanan AWS harus mendukung akses melaluiIPv6. 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 AndaVPC. Misalnya, untuk memastikan bahwa AWS CLI dapat mengirim HTTPS permintaan ke Layanan AWS, grup keamanan harus mengizinkan HTTPS lalu lintas masuk.
- Jika sumber daya Anda berada dalam subnet dengan jaringanACL, verifikasi bahwa jaringan ACL memungkinkan lalu lintas antara sumber daya di antarmuka jaringan titik akhir AndaVPC.
- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat AWS PrivateLink kuota.

Buat titik VPC akhir

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

Untuk membuat titik akhir antarmuka untuk Layanan AWS

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Jenis, pilih AWS layanan.
5. 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 Layanan AWS.
7. Jika, pada Langkah 5, Anda memilih nama layanan untuk Amazon S3, dan jika Anda ingin mengonfigurasi DNSdukungan pribadi, pilih Pengaturan tambahan, Aktifkan DNS nama. Ketika Anda membuat pilihan ini, itu juga secara otomatis memilih Aktifkan pribadi DNS hanya untuk titik akhir masuk. Anda dapat mengonfigurasi pribadi DNS 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 hanya DNS pribadi 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 DNS nama 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 VPC akhir Anda.

8. Untuk Subnet, pilih subnet untuk membuat antarmuka jaringan titik akhir. Anda dapat memilih satu subnet per Availability Zone. Anda tidak dapat memilih beberapa subnet dari Availability Zone yang sama. Untuk informasi selengkapnya, lihat the section called “Subnet dan Availability Zone”.

   Secara default, kami memilih alamat IP dari rentang alamat IP subnet dan menetapkannya ke antarmuka jaringan titik akhir. Untuk memilih alamat IP sendiri, pilih Tentukan alamat IP. Perhatikan bahwa empat alamat IP pertama dan alamat IP terakhir di CIDR blok 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 IPv4 alamat ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang IPv4 alamat dan layanan menerima permintaan. IPv4
   - IPv6— Tetapkan IPv6 alamat ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih IPv6 hanya subnet dan layanan menerima IPv6 permintaan.
   - Dualstack — Tetapkan keduanya IPv4 dan IPv6 alamat ke antarmuka jaringan endpoint. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang IPv6 alamat IPv4 dan keduanya dan layanan menerima keduanya IPv4 dan IPv6 permintaan.

10. Untuk grup Keamanan, pilih grup keamanan untuk diasosiasikan dengan antarmuka jaringan titik akhir. Secara default, kami mengaitkan grup keamanan default untukVPC.
11. Untuk Kebijakan, untuk mengizinkan semua operasi oleh semua prinsipal pada semua sumber daya melalui titik akhir antarmuka, pilih Akses penuh. Untuk membatasi akses, pilih Kustom dan masukkan kebijakan. Opsi ini hanya tersedia jika layanan mendukung kebijakan VPC titik akhir. 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

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Subnet bersama

Anda tidak dapat membuat, mendeskripsikan, memodifikasi, atau menghapus VPC titik akhir di subnet yang dibagikan dengan Anda. Namun, Anda dapat menggunakan VPC titik akhir dalam subnet yang dibagikan dengan Anda.

ICMP

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

Konfigurasikan titik akhir antarmuka

Setelah Anda membuat VPC titik akhir antarmuka, Anda dapat memperbarui konfigurasinya.

Tugas

- Menambah atau menghapus subnet
- Grup keamanan asosiasi
- Edit kebijakan VPC titik akhir
- Aktifkan DNS nama 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola subnet.
5. Pilih atau batal pilihan Availability Zones sesuai kebutuhan. Untuk setiap Availability Zone, pilih satu subnet. Secara default, kami memilih alamat IP dari rentang alamat IP subnet dan menetapkannya ke antarmuka jaringan titik akhir. Untuk memilih alamat IP untuk antarmuka jaringan titik akhir, pilih Tentukan alamat IP dan masukkan IPv4 alamat dari rentang alamat subnet. Jika layanan endpoint mendukungIPv6, Anda juga dapat memasukkan IPv6 alamat dari rentang alamat subnet.

   Jika Anda menentukan alamat IP untuk subnet yang sudah memiliki antarmuka jaringan endpoint untuk titik VPC akhir 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

- modify-vpc-endpoint (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 AndaVPC.

Untuk mengubah grup keamanan menggunakan konsol

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

6. Pilih Ubah grup keamanan.

Untuk mengubah grup keamanan menggunakan baris perintah

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Edit kebijakan VPC titik akhir

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

Untuk mengubah kebijakan endpoint menggunakan baris perintah

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Aktifkan DNS nama pribadi

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

Untuk menggunakan DNS nama pribadi, Anda harus mengaktifkan DNSnama host dan DNS resolusi untuk AndaVPC. Setelah Anda mengaktifkan DNS nama pribadi, mungkin perlu beberapa menit agar

alamat IP pribadi tersedia. DNSCatatan yang kami buat saat Anda mengaktifkan DNS nama pribadi bersifat pribadi. Oleh karena itu, DNS nama pribadi tidak dapat diselesaikan secara publik.

Untuk mengubah opsi DNS nama pribadi menggunakan konsol

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Ubah DNS nama 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 pribadi DNS hanya untuk titik akhir masuk. Jika Anda lebih suka DNS fungsionalitas pribadi standar, hapus Aktifkan pribadi DNS 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 hanya DNS pribadi untuk titik akhir masuk, Anda akan menerima kesalahan saat menyimpan perubahan di langkah berikutnya. Untuk informasi selengkapnya, lihat the section called “Pribadi DNS”.
7. Pilih Simpan perubahan.

Untuk mengubah opsi DNS nama pribadi menggunakan baris perintah

- modify-vpc-endpoint (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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola tag.

5. Untuk setiap tag untuk menambahkan pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih Hapus di sebelah kanan kunci tag dan nilai.
7. Pilih Simpan.

Untuk mengelola tag menggunakan baris perintah

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

Menerima peringatan untuk acara titik akhir antarmuka

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

Tugas

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

Buat SNS notifikasi

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

Untuk membuat notifikasi untuk titik akhir antarmuka menggunakan konsol

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Dari tab Notifikasi, pilih Buat notifikasi.
5. Untuk Pemberitahuan ARN, pilih SNS topik yang Anda buat. ARN
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

- create-vpc-endpoint-connection-pemberitahuan ()AWS CLI
- New-EC2VpcEndpointConnectionNotification(Alat untuk Windows PowerShell)

Menambahkan kebijakan akses

Tambahkan kebijakan akses ke SNS topik Amazon yang memungkinkan AWS PrivateLink untuk mempublikasikan pemberitahuan atas nama Anda, seperti berikut ini. Untuk informasi selengkapnya, lihat Bagaimana cara mengedit kebijakan akses SNS topik Amazon 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 SNS topik terenkripsi, kebijakan sumber daya untuk KMS kunci harus dipercaya AWS PrivateLink untuk memanggil AWS KMS API operasi. 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 VPC titik akhir, Anda dapat menghapusnya. Menghapus titik akhir antarmuka juga menghapus antarmuka jaringan titik akhir.

Untuk menghapus titik akhir antarmuka menggunakan konsol

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

Untuk menghapus titik akhir antarmuka menggunakan baris perintah

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Titik akhir Gateway

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

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

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

Harga

Tidak dikenakan biaya tambahan untuk menggunakan titik akhir gateway.

Daftar Isi

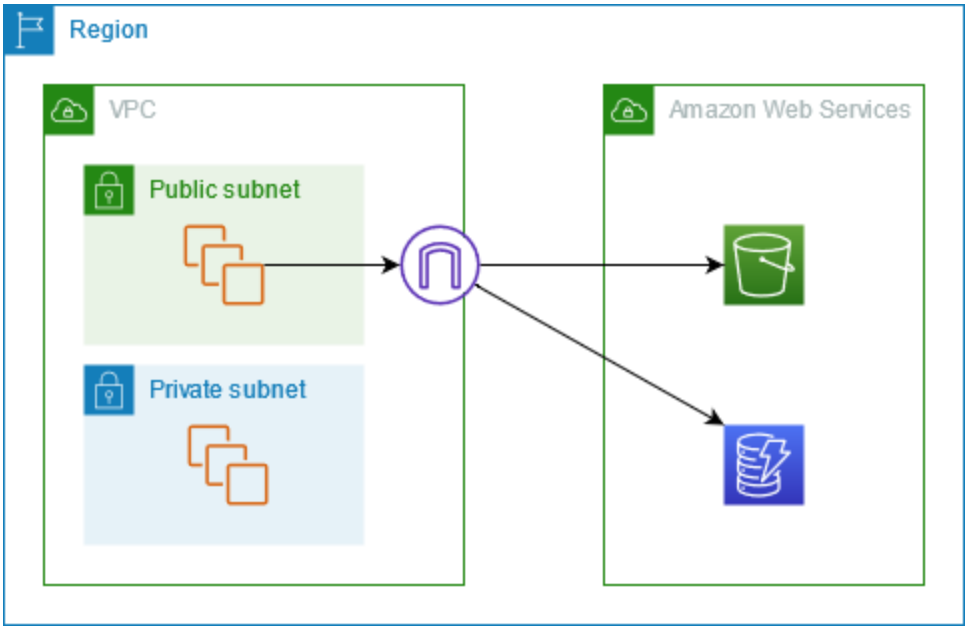
- Titik akhir Gateway untuk Amazon DynamoDB

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.

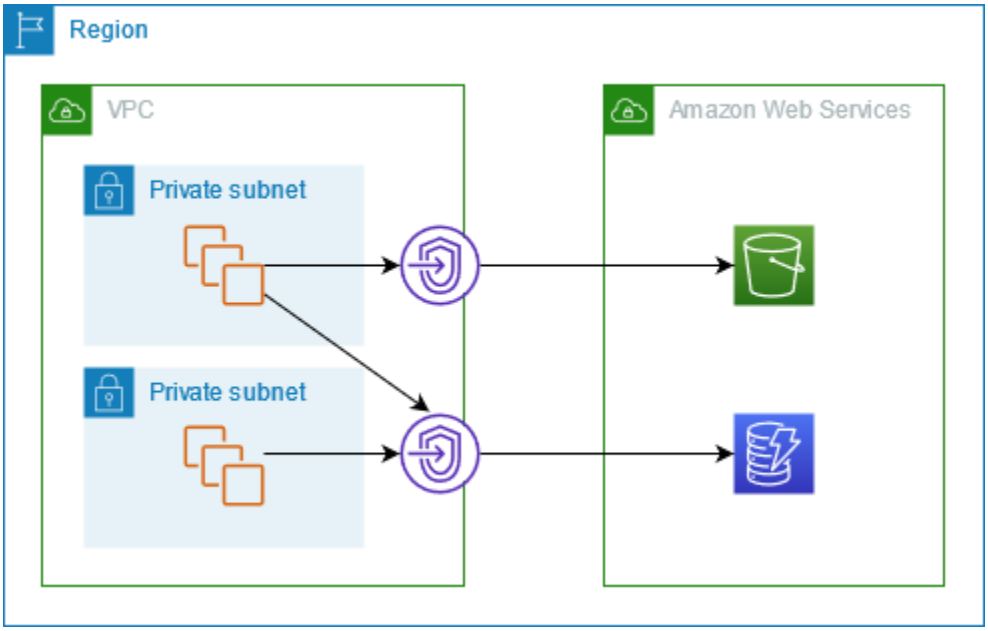
Akses melalui gateway internet

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 dan kemudian ke layanan. VPC 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 NAT menambahkan perangkat 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 Amazon S3 atau DynamoDB Anda VPC 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 VPCPanduan Pengguna Amazon.



Perutean

Saat Anda membuat titik akhir gateway, Anda memilih tabel VPC rute 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

Jaringan ACLs untuk subnet untuk contoh ini juga harus memungkinkan lalu lintas ke dan dari layanan. Berikut ini adalah contoh aturan outbound. Anda tidak dapat mereferensikan daftar awalan dalam ACL aturan 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

Tujuan	Protokol	Rentang port
service_cidr_block_3	TCP	443

Titik akhir gateway untuk Amazon S3

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

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 NAT atau perangkat internet untuk VPC Anda, dan tanpa biaya tambahan. Namun, titik akhir gateway tidak mengizinkan akses dari jaringan lokal, dari peered VPCs 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 VPC titik akhir 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 DNS server Amazon, Anda harus mengaktifkan DNSnama host dan DNS resolusi untuk AndaVPC. Jika Anda menggunakan DNS server 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.
- Jaringan ACL 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 ACL aturan 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 EC2 instans 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 EC2 instance mana yang dapat mengakses Amazon S3 melalui VPC titik akhir.
- Titik akhir Gateway hanya mendukung IPv4 lalu lintas.
- IPv4Alamat sumber dari instans di subnet Anda yang terpengaruh seperti yang diterima oleh Amazon S3 berubah dari alamat IPv4 publik ke alamat IPv4 pribadi di Anda. VPC Titik akhir mengalihkan rute jaringan, dan memutus koneksi terbukaTCP. Koneksi sebelumnya yang menggunakan IPv4 alamat publik tidak dilanjutkan. Kami menyarankan agar Anda tidak menjalankan tugas penting apa pun saat membuat atau memodifikasi titik akhir; atau Anda menguji untuk memastikan bahwa perangkat lunak Anda dapat terhubung kembali secara otomatis ke Amazon S3 setelah koneksi putus.
- Koneksi titik akhir tidak dapat diperpanjang dari aVPC. Sumber daya di sisi lain VPN koneksi, koneksi VPC peering, gateway transit, atau AWS Direct Connect koneksi di Anda VPC 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

Pribadi DNS

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

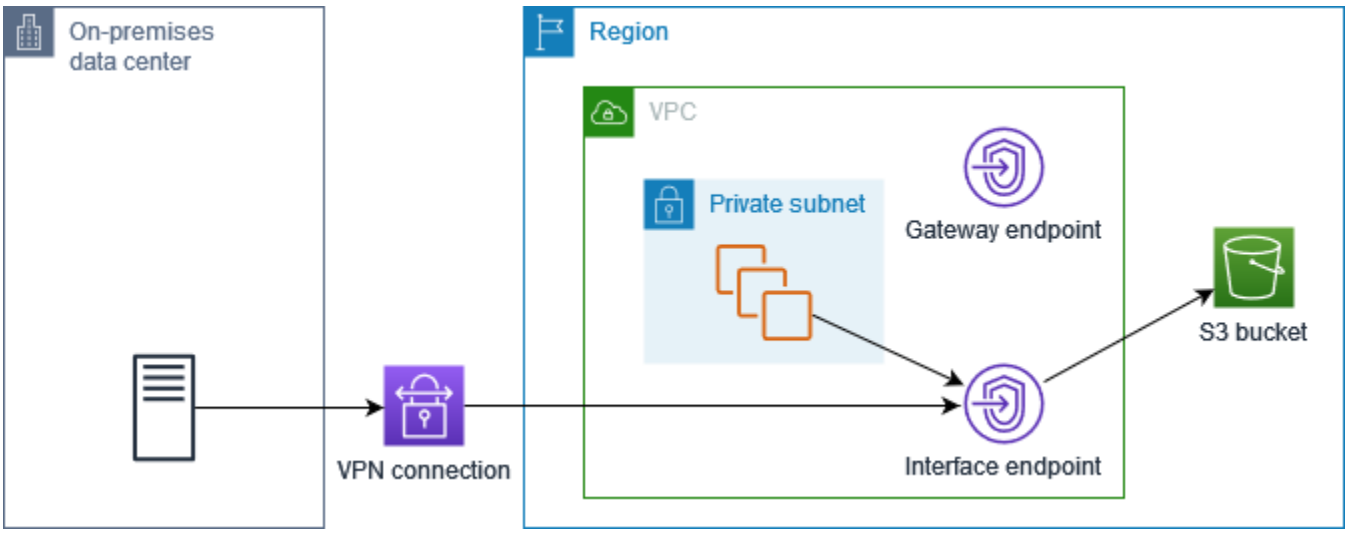
Resolver Rute 53

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

Saat Anda mengonfigurasi titik akhir antarmuka untuk Amazon S3 agar hanya menggunakan DNS private 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 ALIAS catatan untuk Resolver Route 53 ke zona yang dihosting publik untuk Amazon S3, DNS sehingga kueri dari penyelesaian VPC Anda ke alamat IP publik Amazon S3, yang merutekan lalu lintas ke titik akhir gateway.

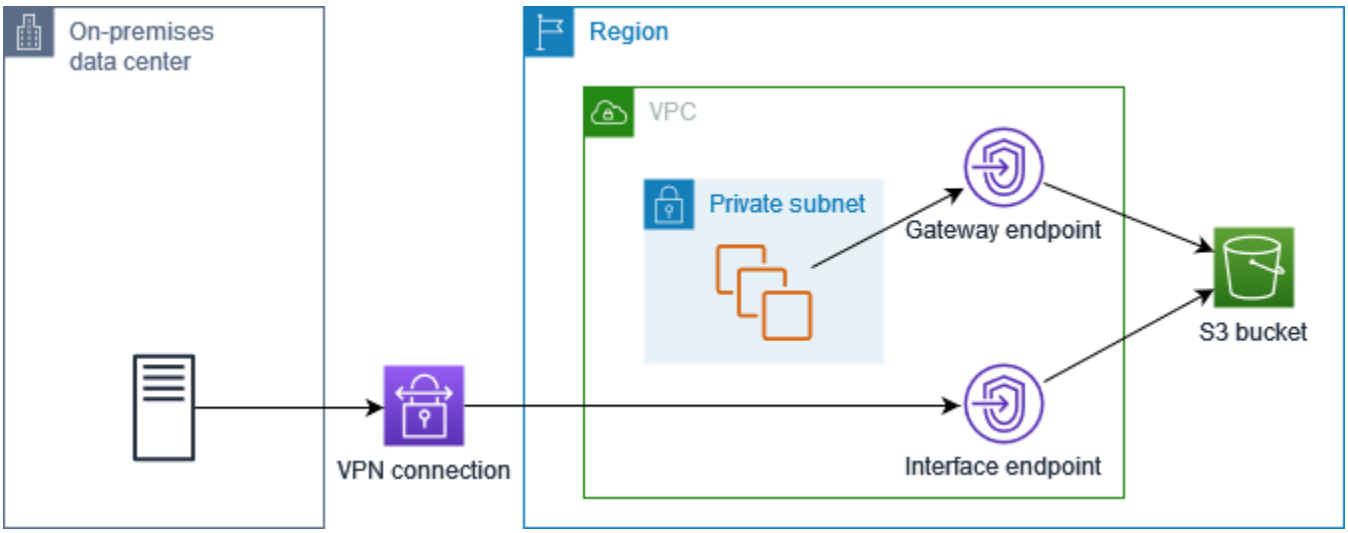
Pribadi DNS

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



Pribadi DNS hanya untuk titik akhir Resolver masuk

Jika Anda mengonfigurasi privat DNS hanya untuk titik akhir Resolver masuk, permintaan dari jaringan lokal menggunakan titik akhir antarmuka untuk mengakses Amazon S3, dan permintaan dari titik akhir gateway 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 pribadi DNS

Anda dapat mengonfigurasi privat DNS untuk titik akhir antarmuka untuk Amazon S3 saat Anda membuatnya atau setelah Anda membuatnya. Untuk informasi selengkapnya, lihat the section called “Buat titik VPC akhir” (konfigurasi selama pembuatan) atau the section called “Aktifkan DNS nama 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Kategori layanan, pilih Layanan AWS.
5. Untuk Layanan, tambahkan filter Type = Gateway dan pilih com.amazonaws. *region*.s3.
6. Untuk VPC, pilih VPC di mana untuk 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 pada semua sumber daya di atas titik akhir. VPC Jika tidak, pilih Kustom untuk melampirkan kebijakan VPC titik akhir yang mengontrol izin yang dimiliki kepala sekolah untuk melakukan tindakan pada sumber daya di 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

- create-vpc-endpoint (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 tertentuVPCs, 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 sourceVpce kondisi aws:. 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 yang spesifik VPC

Anda dapat membuat kebijakan bucket yang membatasi akses ke spesifik VPCs dengan menggunakan aws: sourceVpc condition key. Ini berguna jika Anda memiliki beberapa titik akhir yang dikonfigurasi dalam hal yang samaVPC. Kebijakan berikut menolak akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan kecuali permintaan berasal dari yang ditentukanVPC. 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 VpcSourceIp kondisi aws:. Kebijakan berikut menolak akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan kecuali permintaan berasal dari alamat IP yang ditentukan. Perhatikan bahwa kebijakan ini memblokir akses ke bucket yang ditentukan menggunakan tindakan yang ditentukan melalui 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 VPC konsol Amazon 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

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Edit kebijakan VPC titik akhir

Anda dapat mengedit kebijakan titik akhir untuk titik akhir gateway, yang mengontrol akses ke Amazon S3 dari titik akhir hingga titik VPC akhir. Kebijakan default memungkinkan akses penuh. Untuk informasi selengkapnya, lihat Kebijakan titik akhir.

Untuk mengubah kebijakan titik akhir menggunakan konsol

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

Berikut ini adalah contoh kebijakan endpoint untuk mengakses Amazon S3.

Example Contoh: Batasi akses ke bucket tertentu

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

```
{
  "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 tertentu IAM

Anda dapat membuat kebijakan yang membatasi akses ke IAM peran 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 private DNS diaktifkan.

Untuk menghapus titik akhir gateway menggunakan konsol

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

Untuk menghapus titik akhir gateway menggunakan baris perintah

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Titik akhir Gateway untuk Amazon DynamoDB

Anda dapat mengakses Amazon DynamoDB dari titik akhir gateway VPC Anda menggunakan. VPC Setelah Anda membuat titik akhir gateway, Anda dapat menambahkannya sebagai target dalam tabel rute Anda untuk lalu lintas yang ditujukan dari DynamoDB Anda ke VPC 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 NAT atau perangkat untuk VPC Anda, dan tanpa biaya tambahan. Namun, titik akhir gateway tidak mengizinkan akses dari jaringan lokal, dari peered VPCs 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 VPC titik akhir 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 DNS server Amazon, Anda harus mengaktifkan DNSnama host dan DNS resolusi untuk AndaVPC. Jika Anda menggunakan DNS server 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.
- Jaringan ACL 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 ACL aturan 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 dari instance EC2 di VPC konsumen layanan dan ID titik akhir gateway untuk setiap permintaan yang dilakukan melalui titik akhir.

- Titik akhir Gateway hanya mendukung IPv4 lalu lintas.
- IPv4Alamat sumber dari instance di subnet Anda yang terpengaruh berubah dari IPv4 alamat publik ke IPv4 alamat pribadi dari Anda. VPC Titik akhir mengalihkan rute jaringan dan memutus koneksi terbukaTCP. Koneksi sebelumnya yang menggunakan IPv4 alamat 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 aVPC. Sumber daya di sisi lain VPN koneksi, koneksi VPC peering, gateway transit, atau AWS Direct Connect koneksi di Anda VPC 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Kategori layanan, pilih Layanan AWS.
5. Untuk Layanan, tambahkan filter Type = Gateway dan pilih com.amazonaws. *region*.dinamodb.
6. Untuk VPC, pilih VPC di mana untuk 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 pada semua sumber daya di atas titik akhir. VPC Jika tidak, pilih Kustom untuk melampirkan kebijakan VPC titik akhir yang mengontrol izin yang dimiliki kepala sekolah untuk melakukan tindakan pada sumber daya di 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

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Kontrol akses menggunakan IAM kebijakan

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

Example Contoh: Batasi akses ke titik akhir tertentu

Anda dapat membuat kebijakan yang membatasi akses ke VPC titik akhir tertentu dengan menggunakan kunci sourceVpce kondisi aws:. Kebijakan berikut menolak akses ke tabel DynamoDB di akun kecuali titik akhir yang ditentukan digunakan. VPC 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",
         "Principal": "*",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:region:account-id:table/*",
         "Condition": {
            "StringNotEquals" : {
               "aws:sourceVpce": "vpce-11aa22bb"
            }
         }
      }
   ]
}
```

Example Contoh: Izinkan akses dari IAM peran tertentu

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

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Edit kebijakan VPC titik akhir

Anda dapat mengedit kebijakan titik akhir untuk titik akhir gateway, yang mengontrol akses ke DynamoDB dari titik akhir melalui. VPC Kebijakan default memungkinkan akses penuh. Untuk informasi selengkapnya, lihat Kebijakan titik akhir.

Untuk mengubah kebijakan titik akhir menggunakan konsol

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

Untuk memodifikasi titik akhir gateway menggunakan baris perintah

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

Untuk menghapus titik akhir gateway menggunakan baris perintah

- delete-vpc-endpoints (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 sendiri. VPC

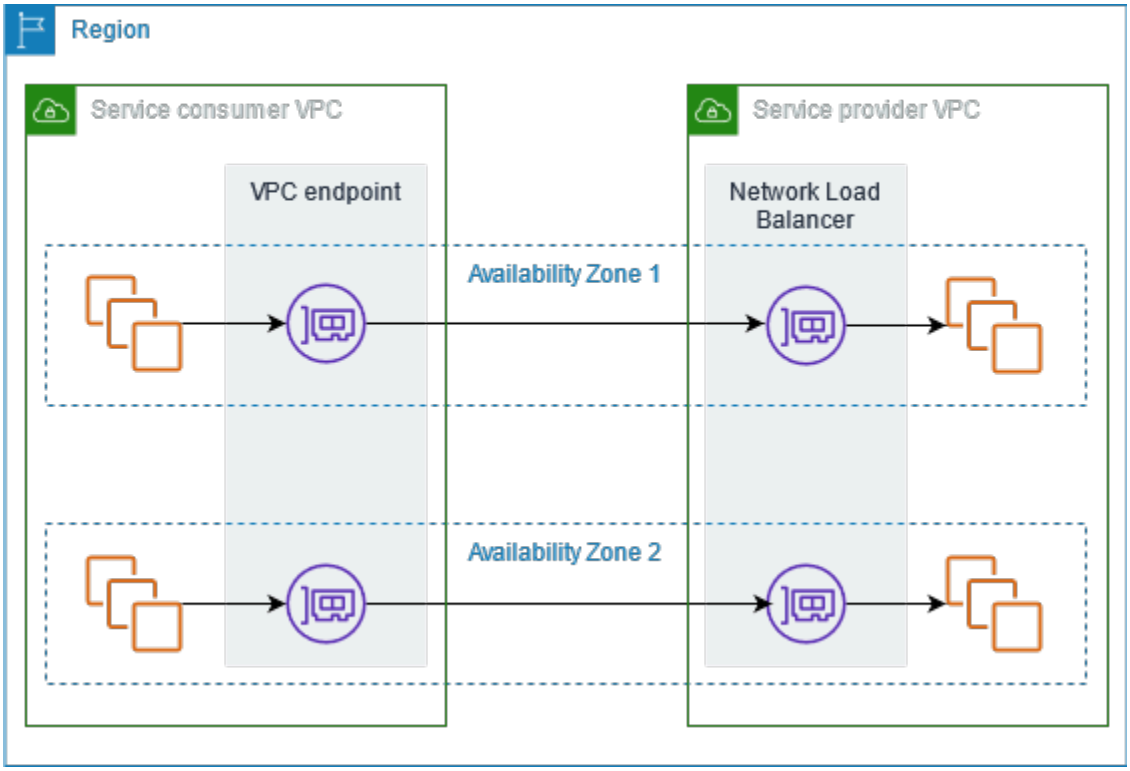
Daftar Isi

Gambaran Umum

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

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

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



Membuat sebuah titik akhir antarmuka

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

Persyaratan

Berlangganan layanan.

Untuk membuat titik akhir antarmuka ke layanan mitra

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

a. Untuk Type, pilih PrivateLink Ready Partner Services.

b. Masukkan nama layanan, lalu pilih Verifikasi layanan.

6. Untuk VPC, pilih VPC dari mana Anda akan mengakses produk.
7. Untuk Subnet, pilih subnet untuk membuat antarmuka jaringan titik akhir.
8. Untuk grup Keamanan, pilih grup keamanan untuk diasosiasikan dengan antarmuka jaringan titik akhir. Aturan grup keamanan harus mengizinkan lalu lintas antara sumber daya di antarmuka jaringan titik akhir VPC dan 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 VPC endpoint. AWS Prinsipal lain mengakses layanan endpoint dengan membuat titik akhir Gateway Load Balancer.

Harga

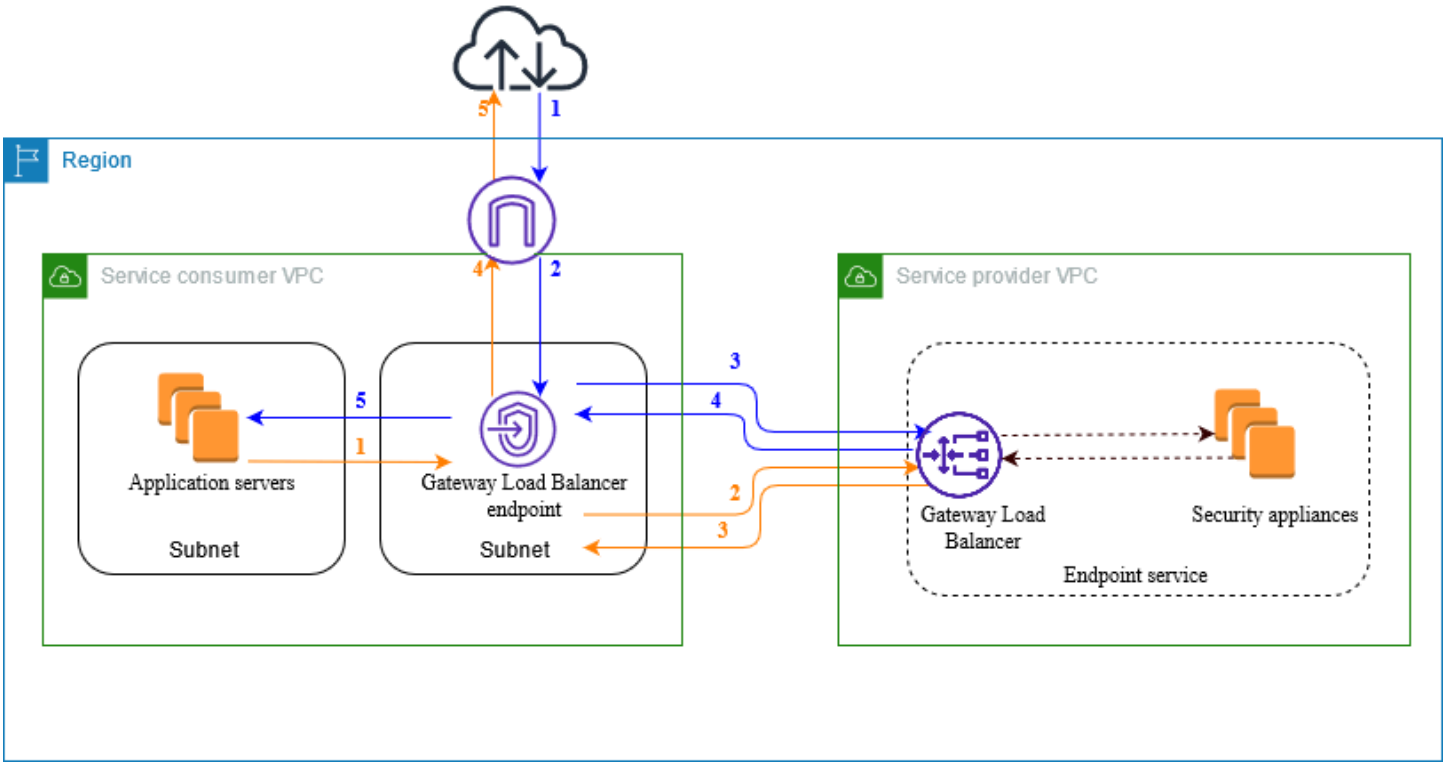
Anda ditagih untuk setiap jam dimana titik akhir Load Balancer Gateway Anda disediakan di setiap Availability Zone. Anda juga ditagih per GB data yang diproses. Untuk informasi selengkapnya, silakan lihat Harga AWS PrivateLink.

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 konsumen VPC layanan. Anda membuat titik akhir Load Balancer Gateway di subnet lain yang sama. VPC Semua lalu lintas yang masuk ke konsumen layanan VPC melalui gateway internet pertama-tama diarahkan ke titik akhir Load Balancer Gateway 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 konsumen layanan VPC 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 bagi konsumen layanan di atasIPv4,IPv6, atau keduanya IPv4 danIPv6, bahkan jika peralatan keamanan mereka hanya IPv4 mendukung. 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 mendukungIPv4, antarmuka jaringan titik akhir memiliki alamat. IPv4 Jika titik akhir Load Balancer Gateway mendukungIPv6, antarmuka jaringan titik akhir memiliki alamat. IPv6 IPv6Alamat untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Jika Anda mendeskripsikan antarmuka jaringan endpoint dengan IPv6 alamat, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Persyaratan IPv6 untuk mengaktifkan layanan endpoint

- Subnet VPC dan untuk layanan endpoint harus memiliki blok terkait IPv6CIDR.
- Load Balancer Gateway untuk layanan endpoint harus menggunakan tipe alamat IP dualstack. Peralatan keamanan tidak perlu mendukung IPv6 lalu lintas.

Persyaratan IPv6 untuk mengaktifkan titik akhir Load Balancer Gateway

- Layanan endpoint harus memiliki jenis alamat IP yang mencakup IPv6 dukungan.
- 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 IPv4 alamat ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang IPv4 alamat.
  - IPv6— Tetapkan IPv6 alamat ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih IPv6 hanya subnet.
  - Dualstack — Tetapkan keduanya IPv4 dan IPv6 alamat ke antarmuka jaringan endpoint Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang keduanya IPv4 dan IPv6 alamat.
- Tabel rute untuk subnet di konsumen layanan VPC harus merutekan IPv6 lalu lintas dan jaringan ACLs untuk subnet ini harus memungkinkan IPv6 lalu lintas.

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 IPv6 rute 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:
Application subnet IPv4 CIDR	*vpc-endpoint-id*
Application subnet IPv6 CIDR	*vpc-endpoint-id*

Tabel rute untuk subnet dengan server aplikasi

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

Tujuan	Target
VPC IPv4 CIDR	Lokal:
VPC IPv6 CIDR	Lokal:
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Tabel rute untuk subnet dengan titik akhir Gateway Load Balancer

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

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 AZ IDs untuk secara konsisten mengidentifikasi Availability Zone untuk layanan Anda. Untuk informasi selengkapnya, lihat AZ IDs di Panduan EC2 Pengguna Amazon.
- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat AWS PrivateLink kuota.

Prasyarat

- Buat penyedia layanan VPC 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 penyedia layanan Anda. VPC Jika Anda berencana untuk mengaktifkan IPv6 dukungan 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 penyedia layanan VPC 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih Buat layanan titik akhir.
4. Untuk jenis Load balancer, pilih Gateway.
5. Untuk penyeimbang beban yang tersedia, pilih Load Balancer Gateway Anda.

6. Untuk Memerlukan penerimaan untuk titik akhir, pilih Penerimaan yang diperlukan untuk mengharuskan permintaan koneksi ke layanan titik akhir Anda diterima secara manual. Kalau tidak, mereka diterima secara otomatis.
7. Untuk jenis alamat IP yang Didukung, lakukan salah satu hal berikut:
   - Pilih IPv4— Aktifkan layanan endpoint untuk menerima IPv4 permintaan.
   - Pilih IPv6— Aktifkan layanan endpoint untuk menerima IPv6 permintaan.
   - Pilih IPv4dan IPv6— Aktifkan layanan endpoint untuk menerima keduanya IPv4 dan IPv6 permintaan.
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

- create-vpc-endpoint-service-konfigurasi ()AWS CLI
- New-EC2VpcEndpointServiceConfiguration(Alat untuk Windows PowerShell)

Jadikan layanan endpoint Anda tersedia

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

- Tambahkan izin yang memungkinkan setiap konsumen layanan terhubung ke layanan endpoint Anda. Untuk informasi selengkapnya, lihat the section called “Kelola izin”.
- Berikan konsumen layanan dengan nama layanan Anda dan Availability Zone yang didukung sehingga mereka dapat membuat titik akhir antarmuka untuk terhubung ke layanan Anda. Untuk informasi lebih lanjut, lihat prosedur di bawah ini.
- Terima permintaan koneksi titik akhir dari konsumen layanan. Untuk 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 AndaVPC, 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 konsumen layananVPC. 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 AZ IDs untuk secara konsisten mengidentifikasi Availability Zone untuk layanan Anda. Untuk informasi selengkapnya, lihat AZ IDs di Panduan EC2 Pengguna Amazon.

- Sebelum Anda dapat menggunakan layanan endpoint, penyedia layanan harus menerima permintaan koneksi. Layanan tidak dapat memulai permintaan ke sumber daya di titik VPC VPC akhir Anda. Titik akhir hanya mengembalikan respons terhadap lalu lintas yang diprakarsai oleh sumber daya di Anda. VPC
- 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 targetnya sama dengan Network VPC Load Balancer.
- Jika server aplikasi dan titik akhir Load Balancer Gateway berada di subnet yang sama, NACL aturan akan dievaluasi untuk lalu lintas dari server aplikasi ke titik akhir Gateway Load Balancer.
- Jika Anda menggunakan Load Balancer Gateway dengan gateway internet khusus egres, lalu lintas akan turun. IPv6 Sebagai gantinya, gunakan gateway internet dan aturan firewall masuk.
- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat AWS PrivateLink kuota.

Prasyarat

- Buat konsumen layanan VPC 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 jaringanACL, verifikasi bahwa jaringan ACL 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Jenis, pilih layanan Endpoint yang menggunakan NLBs dan GWLBs.
5. Untuk nama Layanan, masukkan nama layanan, lalu pilih Verifikasi layanan.
6. Untuk VPC, pilih VPC dari mana Anda akan mengakses layanan endpoint.
7. Untuk Subnet, pilih satu subnet untuk membuat antarmuka jaringan endpoint.
8. Untuk jenis alamat IP, pilih dari opsi berikut:
   - IPv4— Tetapkan IPv4 alamat ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika subnet yang dipilih memiliki rentang IPv4 alamat.
   - IPv6— Tetapkan IPv6 alamat ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika subnet yang dipilih adalah subnet IPv6 satu-satunya.
   - Dualstack — Tetapkan keduanya IPv4 dan IPv6 alamat ke antarmuka jaringan endpoint. Opsi ini didukung hanya jika subnet yang dipilih memiliki rentang keduanya IPv4 dan IPv6 alamat.
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

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Konfigurasikan perutean

Gunakan prosedur berikut untuk mengonfigurasi tabel rute untuk konsumen layananVPC. 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel Rute.
3. Pilih tabel rute untuk gateway internet dan lakukan hal berikut:
   a. Pilih Tindakan, Sunting rute.
   b. Jika Anda mendukungIPv4, pilih Tambahkan rute. Untuk Tujuan, masukkan IPv4 CIDR blok subnet untuk server aplikasi. Untuk Target, pilih VPC titik akhir.
   c. Jika Anda mendukungIPv6, pilih Tambahkan rute. Untuk Tujuan, masukkan IPv6 CIDR blok subnet untuk server aplikasi. Untuk Target, pilih VPC titik akhir.
   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 mendukungIPv4, pilih Tambahkan rute. Untuk Tujuan, masukkan**`0.0.0.0/0`**. Untuk Target, pilih VPC titik akhir.
   c. Jika Anda mendukungIPv6, pilih Tambahkan rute. Untuk Tujuan, masukkan**`::/0`**. Untuk Target, pilih VPC titik akhir.
   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 mendukungIPv4, pilih Tambahkan rute. Untuk Tujuan, masukkan**`0.0.0.0/0`**. Untuk Target, pilih gateway internet.
   c. Jika Anda mendukungIPv6, 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir antarmuka.
4. Pilih Tindakan, Kelola tag.
5. Untuk setiap tag untuk menambahkan pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
6. Untuk menghapus tag, pilih Hapus di sebelah kanan kunci tag dan nilai.
7. Pilih Simpan.

Untuk mengelola tag menggunakan baris perintah

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

Menghapus titik akhir Load Balancer Gateway

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

Untuk menghapus titik akhir Load Balancer Gateway

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

Untuk menghapus titik akhir Load Balancer Gateway

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (AWS Tools for Windows PowerShell)

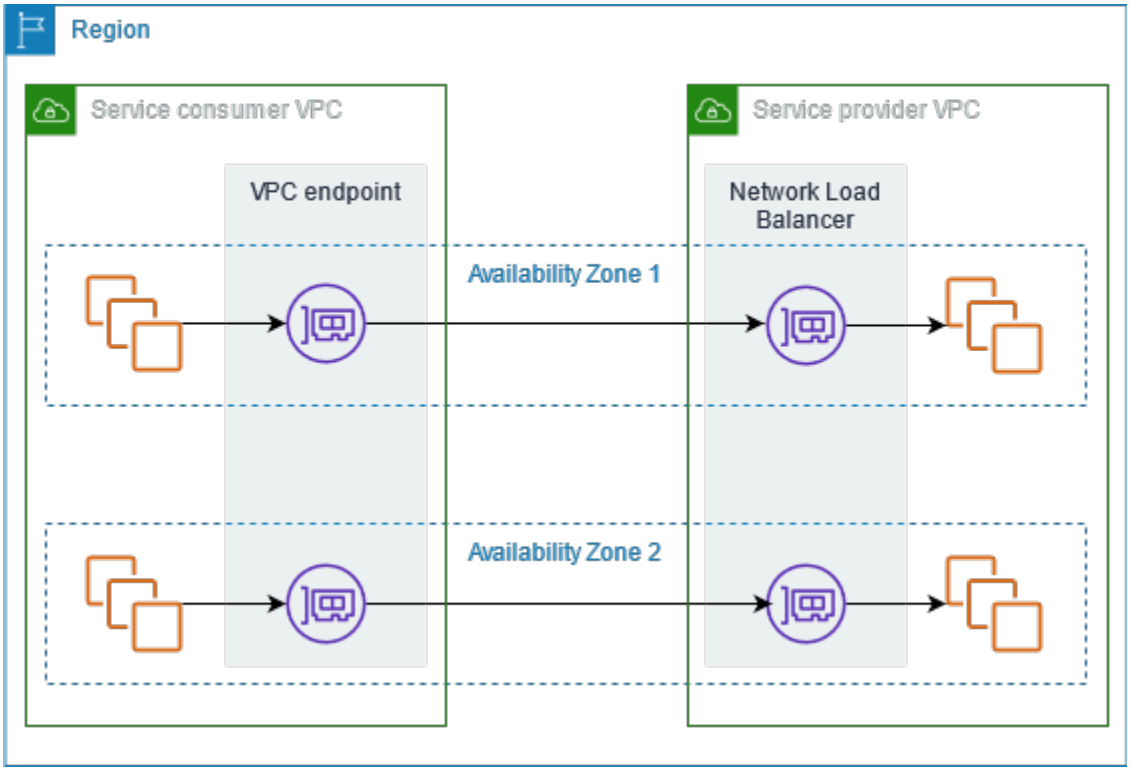
Bagikan layanan Anda melalui AWS PrivateLink

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 bagian depan layanan AndaVPC. Anda kemudian memilih penyeimbang beban ini ketika Anda membuat konfigurasi layanan VPC endpoint. Anda memberikan izin kepada AWS prinsipal tertentu sehingga mereka dapat terhubung ke layanan Anda. Sebagai konsumen layanan, pelanggan membuat VPC titik akhir antarmuka, yang menetapkan koneksi antara subnet yang mereka pilih dari layanan mereka VPC dan endpoint 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.

DNSnama host

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

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

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

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

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

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

Nama zona memiliki sintaks berikut:

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

Pribadi DNS

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

Akses Lintas Wilayah

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

Izin

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

Pertimbangan

- Penyedia layanan harus memilih masuk ke Wilayah keikutsertaan sebelum menambahkannya sebagai Wilayah yang didukung untuk layanan titik akhir.
- Layanan endpoint Anda harus dapat diakses dari Wilayah tuan rumahnya. Anda tidak dapat menghapus Wilayah host dari kumpulan Wilayah yang didukung. Untuk redundansi, Anda dapat menerapkan layanan endpoint Anda di beberapa Wilayah dan mengaktifkan akses lintas wilayah untuk setiap layanan endpoint.

- Konsumen layanan harus memilih masuk ke Wilayah keikutsertaan sebelum memilihnya sebagai Wilayah layanan untuk titik akhir. Jika memungkinkan, kami menyarankan agar konsumen layanan mengakses layanan menggunakan konektivitas intra-wilayah, bukan konektivitas lintas wilayah. Konektivitas Intra-Region memberikan latensi yang lebih rendah dan biaya yang lebih rendah.
- Jika penyedia layanan menghapus Wilayah dari kumpulan Wilayah yang didukung, konsumen layanan tidak dapat memilih Wilayah tersebut sebagai Wilayah layanan saat mereka membuat titik akhir baru. Perhatikan bahwa ini tidak memengaruhi akses ke layanan titik akhir dari titik akhir yang ada yang menggunakan Wilayah ini sebagai Wilayah layanan.
- Untuk ketersediaan tinggi, penyedia dan konsumen harus menggunakan setidaknya dua Availability Zone. Perhatikan bahwa akses lintas wilayah tidak mengharuskan penyedia dan konsumen menggunakan Availability Zone yang sama.
- Dengan akses lintas wilayah, AWS PrivateLink mengelola failover antara Availability Zones. Itu tidak mengelola failover di seluruh Wilayah.
- Akses Lintas Wilayah tidak didukung untuk AWS Marketplace layanan dengan nama yang ramah penggunaDNS.
- Akses Lintas Wilayah tidak didukung untuk Network Load Balancer dengan nilai kustom yang dikonfigurasi untuk batas waktu idle. TCP
- Akses lintas wilayah tidak didukung dengan UDP fragmentasi.

Jenis alamat IP

Penyedia layanan dapat membuat titik akhir layanan mereka tersedia untuk konsumen layanan di atasIPv4,IPv6, atau keduanya IPv4 danIPv6, 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 VPC titik akhir antarmuka mendukungIPv4, antarmuka jaringan titik akhir memiliki alamat. IPv4 Jika VPC titik akhir antarmuka mendukungIPv6, antarmuka jaringan titik akhir memiliki alamat. IPv6 IPv6Alamat untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Jika Anda mendeskripsikan antarmuka jaringan endpoint dengan IPv6 alamat, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Persyaratan IPv6 untuk mengaktifkan layanan endpoint

- Subnet VPC dan untuk layanan endpoint harus memiliki blok terkait IPv6CIDR.

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

Persyaratan IPv6 untuk mengaktifkan titik akhir antarmuka

- Layanan endpoint harus mendukung IPv6 permintaan.
- Jenis alamat IP dari titik akhir antarmuka harus kompatibel dengan subnet untuk titik akhir antarmuka, seperti yang dijelaskan di sini:
  - IPv4— Tetapkan IPv4 alamat ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang IPv4 alamat.
  - IPv6— Tetapkan IPv6 alamat ke antarmuka jaringan titik akhir Anda. Opsi ini didukung hanya jika semua subnet yang dipilih IPv6 hanya subnet.
  - Dualstack — Tetapkan keduanya IPv4 dan IPv6 alamat ke antarmuka jaringan endpoint Anda. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang keduanya IPv4 dan IPv6 alamat.

DNSmerekam jenis alamat IP untuk titik akhir antarmuka

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

- IPv4— Buat catatan A untuk DNS nama pribadi, Regional, dan zona. Jenis alamat IP harus IPv4atau Dualstack.
- IPv6— Buat AAAA catatan untuk DNS nama pribadi, Regional, dan zona. Jenis alamat IP harus IPv6atau Dualstack.
- Dualstack — Buat A dan AAAA catatan untuk nama pribadi, Regional, dan zonaDNS. 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

Pertimbangan

- Layanan endpoint tersedia di Wilayah tempat Anda membuatnya. Konsumen dapat mengakses layanan Anda dari Wilayah lain jika Anda mengaktifkan akses lintas wilayah, atau jika mereka menggunakan VPC peering atau gateway transit.
- Ketika konsumen layanan mengambil informasi tentang layanan endpoint, mereka hanya dapat melihat Availability Zone yang mereka miliki bersama dengan penyedia layanan. Ketika penyedia layanan dan konsumen layanan berada di akun yang berbeda, nama Availability Zone, sepertius-east-1a, mungkin dipetakan ke Availability Zone fisik yang berbeda di masing-masing Akun AWS akun. Anda dapat menggunakan AZ IDs untuk secara konsisten mengidentifikasi Availability Zone untuk layanan Anda. Untuk informasi selengkapnya, lihat AZ IDs di Panduan EC2 Pengguna Amazon.
- 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 titik IDs akhir antarmuka dari header protokol proxy. Untuk informasi selengkapnya, lihat Protokol proxy di Panduan Pengguna untuk Network Load Balancers.
- Network Load Balancer dapat dikaitkan dengan layanan endpoint tunggal, tetapi layanan endpoint dapat dikaitkan dengan beberapa Network Load Balancer.
- Jika layanan endpoint dikaitkan dengan beberapa Network Load Balancer, setiap antarmuka jaringan endpoint dikaitkan dengan satu penyeimbang beban. Ketika koneksi pertama dari

antarmuka jaringan endpoint dimulai, kita memilih salah satu Network Load Balancers di Availability Zone yang sama dengan antarmuka jaringan endpoint secara acak. Semua permintaan koneksi berikutnya dari antarmuka jaringan titik akhir ini menggunakan penyeimbang beban yang dipilih. Kami menyarankan Anda menggunakan konfigurasi listener dan grup target yang sama untuk semua load balancer untuk layanan endpoint, sehingga konsumen dapat menggunakan layanan endpoint dengan sukses terlepas dari load balancer mana yang dipilih.

- Ada kuota pada AWS PrivateLink sumber daya Anda. Untuk informasi selengkapnya, lihat AWS PrivateLink kuota.

Prasyarat

- Buat VPC untuk layanan endpoint Anda dengan setidaknya satu subnet di setiap Availability Zone di mana layanan harus tersedia.
- Untuk memungkinkan konsumen layanan membuat VPC titik akhir IPv6 antarmuka untuk layanan endpoint Anda, subnet VPC dan harus memiliki blok terkait. IPv6 CIDR
- Buat Network Load Balancer di. VPC 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 Balancers.
- Untuk mengaktifkan layanan endpoint Anda menerima IPv6 permintaan, Network Load Balancers harus menggunakan tipe alamat IP dualstack. Target tidak perlu mendukung IPv6 lalu lintas. 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 IPv6 alamat.
- Luncurkan instance di setiap Availability Zone di mana layanan harus tersedia dan daftarkan ke grup target load balancer. Jika Anda tidak meluncurkan instance di semua Availability Zone yang diaktifkan, Anda dapat mengaktifkan penyeimbangan beban lintas zona untuk mendukung konsumen layanan yang menggunakan DNS nama host 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih Buat layanan endpoint.
4. Untuk jenis Load balancer, pilih Network.
5. Untuk penyeimbang beban yang tersedia, pilih Network Load Balancers untuk dikaitkan dengan layanan endpoint. Untuk melihat Availability Zone yang diaktifkan untuk load balancer yang Anda pilih, lihat Detail penyeimbang beban yang dipilih, Termasuk Availability Zone. Layanan endpoint Anda akan tersedia di Availability Zone ini.
6. (Opsional) Untuk membuat layanan endpoint Anda tersedia dari Wilayah selain Wilayah tempat layanan tersebut di-host, pilih Wilayah dari Wilayah Layanan. Untuk informasi selengkapnya, lihat the section called “Akses Lintas Wilayah”.
7. Untuk Memerlukan penerimaan untuk titik akhir, pilih Penerimaan yang diperlukan agar permintaan koneksi ke layanan titik akhir Anda diterima secara manual. Jika tidak, permintaan ini diterima secara otomatis.
8. Untuk Aktifkan DNS nama pribadi, pilih Kaitkan DNS nama pribadi dengan layanan untuk mengaitkan DNS nama pribadi yang dapat digunakan konsumen layanan untuk mengakses layanan Anda, lalu masukkan DNS nama pribadi tersebut. Jika tidak, konsumen layanan dapat menggunakan DNS nama spesifik titik akhir yang disediakan oleh. AWS Sebelum konsumen layanan dapat menggunakan DNS nama pribadi, penyedia layanan harus memverifikasi bahwa mereka memiliki domain. Untuk informasi selengkapnya, lihat Kelola DNS nama.
9. Untuk jenis alamat IP yang Didukung, lakukan salah satu hal berikut:
   - Pilih IPv4— Aktifkan layanan endpoint untuk menerima IPv4 permintaan.
   - Pilih IPv6— Aktifkan layanan endpoint untuk menerima IPv6 permintaan.
   - Pilih IPv4dan IPv6— Aktifkan layanan endpoint untuk menerima keduanya IPv4 dan IPv6 permintaan.

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

Untuk membuat layanan endpoint menggunakan baris perintah

- create-vpc-endpoint-service-konfigurasi ()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 titik akhir antarmuka. VPC Penyedia layanan harus melakukan hal berikut untuk membuat layanan mereka tersedia bagi konsumen layanan.

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

Connect ke layanan endpoint sebagai konsumen layanan

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

Untuk membuat titik akhir antarmuka menggunakan konsol

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Untuk Jenis, pilih layanan Endpoint yang menggunakan NLBs dan GWLBs.

5. Untuk nama Layanan, masukkan nama layanan (misalnya,`com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`), lalu pilih Verifikasi layanan.
6. (Opsional) Untuk terhubung ke layanan titik akhir yang tersedia di Wilayah selain Wilayah titik akhir, pilih Wilayah Layanan, Aktifkan titik akhir Lintas Wilayah, lalu pilih Wilayah. Untuk informasi selengkapnya, lihat the section called “Akses Lintas Wilayah”.
7. Untuk VPC, pilih VPC dari mana Anda akan mengakses layanan endpoint.
8. Untuk Subnet, pilih subnet untuk membuat antarmuka jaringan titik akhir.
9. Untuk jenis alamat IP, pilih dari opsi berikut:

   - IPv4— Tetapkan IPv4 alamat ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki rentang IPv4 alamat dan layanan endpoint menerima IPv4 permintaan.
   - IPv6— Tetapkan IPv6 alamat ke antarmuka jaringan titik akhir. Opsi ini didukung hanya jika semua subnet yang dipilih IPv6 hanya subnet dan layanan endpoint menerima permintaan. IPv6
   - Dualstack — Tetapkan keduanya IPv4 dan IPv6 alamat ke antarmuka jaringan endpoint. Opsi ini didukung hanya jika semua subnet yang dipilih memiliki keduanya IPv4 dan rentang IPv6 alamat dan layanan titik akhir menerima keduanya IPv4 dan permintaan. IPv6
10. Untuk jenis IP DNS rekaman, pilih dari opsi berikut:

    - IPv4— Buat catatan A untuk DNS nama pribadi, Regional, dan zona. Jenis alamat IP harus IPv4atau Dualstack.
    - IPv6— Buat AAAA catatan untuk DNS nama pribadi, Regional, dan zona. Jenis alamat IP harus IPv6atau Dualstack.
    - Dualstack — Buat A dan AAAA catatan untuk nama pribadi, Regional, dan zonaDNS. Jenis alamat IP harus Dualstack.
    - Layanan didefinisikan - Buat catatan untuk nama dan AAAA catatan pribadi, Regional, dan zona untuk DNS nama Regional dan zonaDNS. Jenis alamat IP harus Dualstack.
11. Untuk grup Keamanan, pilih grup keamanan untuk diasosiasikan dengan antarmuka jaringan titik akhir.
12. Pilih Buat Titik Akhir.

Untuk membuat titik akhir antarmuka menggunakan baris perintah

- create-vpc-endpoint (AWS CLI)

- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Konfigurasikan layanan endpoint

Setelah Anda membuat layanan endpoint, Anda dapat memperbarui konfigurasinya.

Tugas

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

Kelola izin

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

Secara default, layanan endpoint Anda tidak tersedia untuk konsumen layanan. Anda harus menambahkan izin yang memungkinkan AWS prinsipal tertentu untuk membuat VPC titik akhir 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 ARNs untuk AWS prinsipal yang didukung.

ARNsuntuk AWS kepala sekolah

Akun AWS (termasuk semua kepala sekolah di akun)

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

Peran

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

Pengguna

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

Semua kepala sekolah di semua Akun AWS

*

Pertimbangan

- 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint dan pilih tab Allow principals.
4. Untuk menambahkan izin, pilih Izinkan prinsipal. Untuk Kepala Sekolah untuk menambahkan, masukkan kepala sekolahARN. 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-izin ()AWS CLI
- Edit-EC2EndpointServicePermission(Alat untuk Windows PowerShell)

Menerima atau menolak permintaan koneksi

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

koneksi, atau Anda dapat memberikan izin kepada kelompok prinsipal yang lebih luas dan secara manual menerima permintaan koneksi tertentu yang Anda percayai.

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

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

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

Untuk mengubah pengaturan penerimaan menggunakan konsol

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

Untuk memodifikasi pengaturan penerimaan menggunakan baris perintah

- modify-vpc-endpoint-service-konfigurasi ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Alat untuk Windows PowerShell)

Untuk menerima atau menolak permintaan koneksi menggunakan konsol

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

6. Untuk menolak permintaan koneksi, pilih Tindakan, Tolak permintaan koneksi titik akhir. Saat diminta konfirmasi, masukkan lalu **`reject`** pilih Tolak.

Untuk menerima atau menolak permintaan koneksi menggunakan baris perintah

- accept-vpc-endpoint-connectionsatau reject-vpc-endpoint-connections(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 antarmuka VPC mereka.

Untuk mengelola penyeimbang beban untuk layanan titik akhir Anda menggunakan konsol

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint.
4. Pilih Actions, Associate, atau disassociate load balancer.
5. Ubah konfigurasi layanan endpoint sesuai kebutuhan. 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

- modify-vpc-endpoint-service-konfigurasi ()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 DNS nama pribadi

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

Untuk mengubah DNS nama pribadi layanan titik akhir menggunakan konsol

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint.
4. Pilih Tindakan, Ubah DNS nama pribadi.
5. Pilih Kaitkan DNS nama pribadi dengan layanan dan masukkan DNS nama pribadi.
   - Nama domain harus menggunakan huruf kecil.
   - Anda dapat menggunakan wildcard dalam nama domain (misalnya,**`*.myexampleservice.com`**).
6. Pilih Simpan perubahan.
7. DNSNama 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 DNS nama pribadi layanan endpoint menggunakan baris perintah

- modify-vpc-endpoint-service-konfigurasi ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Alat untuk Windows PowerShell)

Untuk memulai proses verifikasi domain menggunakan konsol

1. Buka VPC konsol Amazon 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 DNS nama pribadi.
5. Saat diminta konfirmasi, masukkan **`verify`** lalu pilih Verifikasi.

Untuk memulai proses verifikasi domain menggunakan baris perintah

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

Ubah Wilayah yang didukung

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

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

Untuk mengubah Wilayah yang didukung untuk layanan titik akhir Anda

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan endpoint.
4. Pilih Tindakan, Ubah Wilayah yang didukung.
5. Pilih dan batal pilihan Wilayah sesuai kebutuhan.
6. Pilih Simpan perubahan.

Ubah jenis alamat IP yang didukung

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

Pertimbangan

Untuk mengaktifkan layanan endpoint Anda menerima IPv6 permintaan, Network Load Balancers harus menggunakan tipe alamat IP dualstack. Target tidak perlu mendukung IPv6 lalu lintas. 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan VPC endpoint.
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 IPv4 permintaan.
   - Pilih IPv6— Aktifkan layanan endpoint untuk menerima IPv6 permintaan.
   - Pilih IPv4dan IPv6— Aktifkan layanan endpoint untuk menerima keduanya IPv4 dan IPv6 permintaan.
6. Pilih Simpan perubahan.

Untuk memodifikasi jenis alamat IP yang didukung menggunakan baris perintah

- modify-vpc-endpoint-service-konfigurasi ()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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan VPC endpoint.
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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan VPC titik akhir 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Layanan titik akhir.
3. Pilih layanan VPC endpoint dan kemudian pilih tab Allow principals.
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 DNS nama untuk VPC layanan endpoint

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

Sebelum Anda dapat mengonfigurasi DNS nama 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 DNS nama pribadi.
- Saat konsumen membuat titik akhir antarmuka untuk terhubung ke layanan Anda, kami membuat zona host pribadi dan mengaitkannya dengan konsumen VPC layanan. Kami membuat CNAME catatan di zona host pribadi yang memetakan DNS nama pribadi layanan titik akhir ke DNS nama regional titik VPC akhir. Ketika konsumen mengirim permintaan ke DNS nama publik layanan, DNS server pribadi menyelesaikan permintaan ke alamat IP dari antarmuka jaringan endpoint.
- Untuk memverifikasi domain, Anda harus memiliki nama host publik atau DNS penyedia publik.
- Anda dapat memverifikasi domain subdomain. Misalnya, Anda dapat memverifikasi example.com, bukan a.example.com. Setiap DNS label 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 pribadi. DNS Anda harus memverifikasi example.com atau b.example.com sebelum konsumen layanan dapat menggunakan nama tersebut.
- DNSNama pribadi tidak didukung untuk titik akhir Gateway Load Balancer.

Verifikasi kepemilikan domain

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

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

Setelah menambahkan catatan, Anda dapat memeriksa status proses verifikasi domain menggunakan VPC konsol Amazon. 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 DNS nama pribadi.

DNSNama 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 TXT catatan. 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 DNS nama 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 TXT catatan.

```
[
    {
        "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 TXT catatan.

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

Kami menyarankan Anda menggunakan `Name` sebagai subdomain rekaman karena nama domain dasar mungkin sudah digunakan. Namun, jika DNS penyedia Anda tidak mengizinkan nama DNS rekaman 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 TXT catatan ke DNS server domain Anda

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

Amazon Route 53

Buat catatan untuk zona host publik Anda. Gunakan nilai berikut:

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

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

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

Periksa apakah TXT catatan diterbitkan

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

Anda akan menanyakan DNS server 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 DNS server lain.

Untuk memverifikasi bahwa TXT catatan Anda dipublikasikan ke DNS server 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 TXT catatan diterbitkan dengan benar menggunakan perintah berikut, di mana *name_server* 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 TXT nilai.

   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 DNS penyedia Anda mengizinkan garis bawah dalam nama TXT rekaman. Jika DNS penyedia Anda tidak mengizinkan garis bawah, Anda dapat menghilangkan nama verifikasi domain (misalnya, “_6e86v84tqgqubxbwii1m”) dari catatan. TXT
- Periksa apakah DNS penyedia Anda menambahkan nama domain ke akhir TXT catatan. Beberapa DNS penyedia secara otomatis menambahkan nama domain Anda ke nama atribut TXT catatan. Untuk menghindari duplikasi nama domain ini, tambahkan titik ke akhir nama domain saat Anda membuat TXT catatan. Ini memberi tahu DNS penyedia Anda bahwa tidak perlu menambahkan nama domain ke TXT catatan.

- Periksa apakah DNS penyedia Anda memodifikasi nilai DNS rekaman untuk 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 DNS penyedia mengubah nilai TXT rekaman 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 DNS penyedia Anda tidak mengizinkan Anda memiliki lebih dari satu TXT record dengan nama atribut yang sama, periksa apakah DNS penyedia Anda mengizinkan Anda menetapkan beberapa nilai atribut ke TXT rekaman yang sama. Misalnya, jika Anda dikelola DNS oleh Amazon Route 53, Anda dapat menggunakan prosedur berikut.

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

  Jika DNS penyedia Anda tidak mengizinkan Anda menetapkan beberapa nilai ke TXT rekaman yang sama, Anda dapat memverifikasi domain satu kali dengan nilai dalam nama atribut TXT rekaman, 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 SNS notifikasi
- Menambahkan kebijakan akses
- Menambahkan kebijakan kunci

Buat SNS notifikasi

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

Untuk membuat notifikasi untuk layanan endpoint menggunakan konsol

1. Buka VPC konsol Amazon 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 Pemberitahuan ARN, pilih SNS topik yang Anda buat. ARN
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

- create-vpc-endpoint-connection-pemberitahuan ()AWS CLI
- New-EC2VpcEndpointConnectionNotification(Alat untuk Windows PowerShell)

Menambahkan kebijakan akses

Tambahkan kebijakan akses ke SNS topik yang memungkinkan AWS PrivateLink untuk mempublikasikan pemberitahuan atas nama Anda, seperti berikut ini. Untuk informasi selengkapnya, lihat Bagaimana cara mengedit kebijakan akses SNS topik Amazon 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 SNS topik terenkripsi, kebijakan sumber daya untuk KMS kunci harus dipercaya AWS PrivateLink untuk memanggil AWS KMS API operasi. 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 VPC konsol Amazon 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

- delete-vpc-endpoint-service-konfigurasi ()AWS CLI
- Remove-EC2EndpointServiceConfiguration(Alat untuk Windows PowerShell)

Akses VPC sumber daya melalui AWS PrivateLink

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

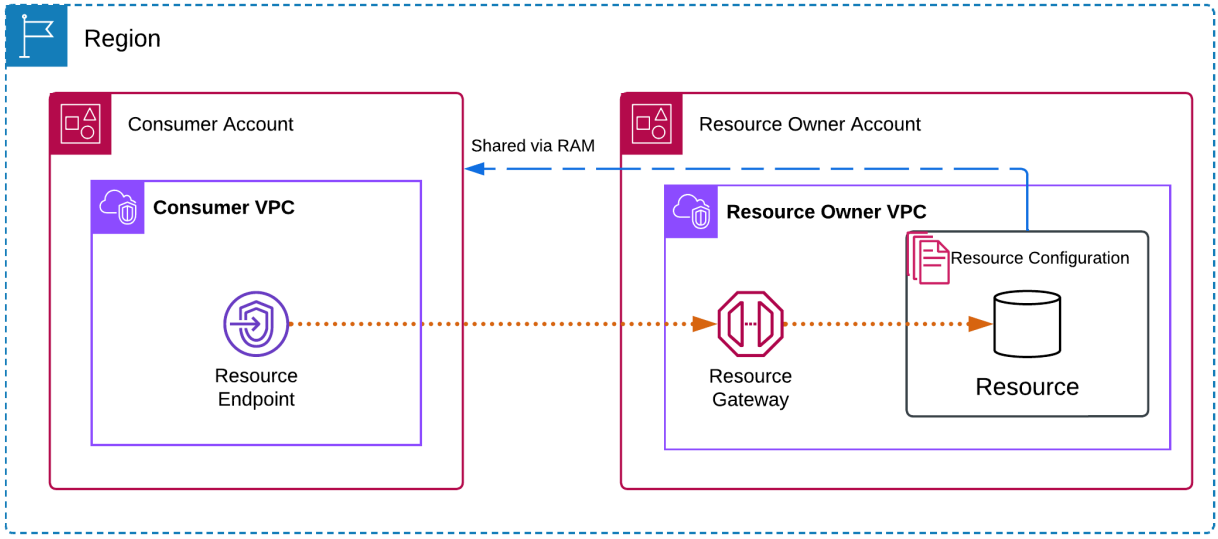
Harga

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

Daftar Isi

Gambaran Umum

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



Pertimbangan

- TCPLalu lintas didukung. UDPLalu lintas tidak didukung.
- Koneksi jaringan harus dimulai dari VPC yang berisi titik akhir sumber daya, dan bukan dari VPC yang memiliki sumber daya. Sumber daya tidak VPC dapat memulai koneksi jaringan ke titik akhirVPC.
- Satu-satunya sumber daya ARN berbasis yang didukung adalah sumber RDS daya Amazon.

DNSnama host

Dengan AWS PrivateLink, Anda mengirim lalu lintas ke sumber daya menggunakan titik akhir pribadi. Saat Anda membuat VPC titik akhir sumber daya, kami membuat DNS nama Regional (disebut DNS nama default) yang dapat Anda gunakan untuk berkomunikasi dengan sumber daya dari Anda VPC

dan dari tempat Anda. DNSNama default untuk VPC titik akhir sumber daya Anda memiliki sintaks berikut:

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

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

describe-vpc-endpoint-associationsPerintah berikut menampilkan DNS entri untuk titik akhir sumber daya.

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

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

```
"DnsEntry": {
                "DnsName": "vpce-1234567890abcdefg-
snra-1234567890abcdefg.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-
east-1.on.aws",
                "HostedZoneId": "ABCDEFGH123456789000"
            },
"PrivateDnsEntry": {
                "DnsName": "database-5-test.cluster-ro-example.us-
east-1.rds.amazonaws.com",
                "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
            }
```

DNSresolusi

DNSCatatan yang kami buat untuk VPC titik akhir sumber daya Anda bersifat publik. Oleh karena itu, DNS nama-nama ini dapat diselesaikan secara publik. Namun, DNS permintaan dari luar VPC

masih mengembalikan alamat IP pribadi dari antarmuka jaringan titik akhir sumber daya. Anda dapat menggunakan DNS nama-nama ini untuk mengakses sumber daya dari lokasi, selama Anda memiliki akses ke titik akhir sumber daya, melalui, VPN atau Direct Connect. VPC

Pribadi DNS

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

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

Subnet dan Availability Zone

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

Jenis alamat IP

Endpoint sumber daya dapat mendukungIPv4,IPv6, atau alamat dualstack. Titik akhir yang mendukung IPv6 dapat merespons DNS kueri dengan AAAA catatan. Jenis alamat IP dari titik akhir sumber daya harus kompatibel dengan subnet untuk titik akhir sumber daya, seperti yang dijelaskan di sini:

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

Jika VPC endpoint sumber daya mendukungIPv4, antarmuka jaringan endpoint memiliki alamat. IPv4 Jika VPC endpoint sumber daya mendukungIPv6, antarmuka jaringan endpoint memiliki alamat. IPv6 IPv6Alamat untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Jika Anda mendeskripsikan antarmuka jaringan endpoint dengan IPv6 alamat, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Mengakses sumber daya melalui titik VPC akhir sumber daya

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

Prasyarat

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

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

Buat titik akhir VPC sumber daya

Gunakan prosedur berikut untuk membuat titik akhir VPC sumber daya.

Untuk membuat titik akhir VPC sumber daya

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Anda dapat menentukan nama untuk membuatnya lebih mudah untuk menemukan dan mengelola endpoint.
5. Untuk Jenis, pilih Sumber Daya.
6. Untuk konfigurasi Sumber Daya, pilih konfigurasi sumber daya yang dibagikan dengan Anda.
7. Untuk pengaturan Jaringan, pilih VPC dari mana Anda akan mengakses sumber daya.
8. Jika, Anda ingin mengkonfigurasi DNS dukungan pribadi, pilih Pengaturan tambahan, Aktifkan DNS nama. Untuk menggunakan fitur ini, pastikan atribut Aktifkan DNS nama host dan DNSdukungan Aktifkan diaktifkan untuk AndaVPC.
9. Pilih Buat Titik Akhir.

Untuk membuat titik akhir sumber daya menggunakan baris perintah

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Kelola titik akhir sumber daya

Setelah Anda membuat titik akhir sumber daya, Anda dapat memperbarui konfigurasinya.

Tugas

- Hapus titik akhir
- Perbarui titik akhir

Hapus titik akhir

Setelah selesai dengan VPC titik akhir, Anda dapat menghapusnya.

Untuk menghapus titik akhir menggunakan konsol

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

2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir.
4. Pilih Tindakan, Hapus VPC titik akhir.
5. Saat diminta mengonfirmasi, pilih **`delete`**.
6. Pilih Hapus.

Untuk menghapus titik akhir menggunakan baris perintah

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Perbarui titik akhir

Anda dapat memperbarui VPC titik akhir.

Untuk memperbarui titik akhir menggunakan konsol

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

Untuk memperbarui titik akhir menggunakan baris perintah

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Konfigurasi sumber daya untuk VPC sumber daya

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

Daftar Isi

Jenis konfigurasi sumber daya

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

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

Gerbang sumber daya

Konfigurasi sumber daya terkait dengan gateway sumber daya. Sebuah gateway sumber daya adalah satu set ENIs yang berfungsi sebagai titik masuknya ke dalam VPC di mana sumber daya berada. Beberapa konfigurasi sumber daya dapat dikaitkan dengan gateway sumber daya yang sama. Ketika klien di akun lain VPCs atau mengakses sumber daya di AndaVPC, sumber daya melihat lalu lintas yang VPC datang secara lokal dari gateway sumber daya di dalamnya.

Definisi sumber daya

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

- Dengan Amazon Resource Name (ARN): Jenis sumber daya yang didukung yang disediakan oleh AWS layanan, dapat diidentifikasi oleh mereka. ARN Misalnya, RDS database Amazon.
- Dengan target nama domain: Nama domain apa pun yang dapat diselesaikan secara publik.
- Dengan alamat IP: Untuk IPv4 danIPv6, hanya IPs di yang VPC didukung.

Protokol

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

Rentang pelabuhan

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

Mengakses sumber daya

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

- Mengakses konfigurasi sumber daya secara langsung

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

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

- Mengakses konfigurasi sumber daya melalui jaringan layanan

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

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

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

Asosiasi dengan jenis jaringan layanan

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

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

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

Jenis jaringan layanan

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

- Menggunakan VPC titik akhir sumber daya tipe (VPCtitik akhir sumber daya).
- Menggunakan VPC titik akhir dari jenis jaringan layanan (VPCtitik akhir jaringan layanan).
- Menggunakan VPC asosiasi jaringan layanan.

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

Berbagi konfigurasi sumber daya melalui AWS RAM

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

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

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

Pemantauan

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

Buat konfigurasi sumber daya di VPC Lattice

Gunakan konsol untuk membuat konfigurasi sumber daya.

Untuk membuat konfigurasi sumber daya menggunakan konsol

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih Konfigurasi sumber daya.
3. Pilih Buat konfigurasi sumber daya.

4. Masukkan nama yang unik di AWS akun Anda. Anda tidak dapat mengubah nama ini setelah konfigurasi sumber daya dibuat.
5. Untuk jenis Konfigurasi, pilih Sumber daya untuk sumber daya tunggal atau anak atau grup Sumber daya untuk grup sumber daya anak.
6. Pilih gateway sumber daya yang sebelumnya Anda buat atau buat sekarang.
7. Pilih pengenal sumber daya yang Anda inginkan untuk diwakili oleh konfigurasi sumber daya ini.
8. Pilih rentang port di mana Anda ingin berbagi sumber daya.
9. Untuk pengaturan Asosiasi, tentukan apakah konfigurasi sumber daya ini dapat dikaitkan dengan jaringan layanan yang dapat dibagikan.
10. Untuk konfigurasi sumber daya Bagikan, pilih pembagian sumber daya yang mengidentifikasi prinsipal yang dapat mengakses sumber daya ini.
11. (Opsional) Untuk Pemantauan, aktifkan log akses Sumber Daya dan tujuan pengiriman jika Anda ingin memantau permintaan dan tanggapan ke dan dari konfigurasi sumber daya.
12. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
13. Pilih Buat konfigurasi sumber daya.

Untuk membuat konfigurasi sumber daya menggunakan AWS CLI

Gunakan perintah create-resource-configuration.

Mengelola asosiasi untuk konfigurasi sumber daya VPC Lattice

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

Kelola asosiasi jaringan layanan

Membuat atau menghapus asosiasi jaringan layanan.

Untuk mengelola asosiasi layanan-jaringan menggunakan konsol

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

2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih Konfigurasi sumber daya.
3. Pilih nama konfigurasi sumber daya untuk membuka halaman detailnya.
4. Pilih tab Asosiasi jaringan layanan.
5. Pilih Buat asosiasi.
6. Pilih jaringan layanan dari jaringan layanan VPC Lattice. Untuk membuat jaringan layanan, pilih Buat jaringan VPC kisi.
7. (Opsional) Untuk menambahkan tag, perluas tag asosiasi layanan, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
8. Pilih Simpan perubahan.
9. Untuk menghapus asosiasi, pilih kotak centang untuk asosiasi, lalu pilih Tindakan, Hapus. Saat diminta konfirmasi, masukkan **`confirm`**, lalu pilih Hapus.

Untuk membuat asosiasi jaringan layanan menggunakan AWS CLI

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

Untuk menghapus asosiasi jaringan layanan menggunakan AWS CLI

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

Kelola VPC asosiasi titik akhir

Kelola asosiasi VPC titik akhir.

Untuk mengelola asosiasi VPC titik akhir menggunakan konsol

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih Konfigurasi sumber daya.
3. Pilih nama konfigurasi sumber daya untuk membuka halaman detailnya.
4. Pilih tab Asosiasi titik akhir.
5. Pilih ID asosiasi untuk membuka halaman detailnya. Dari sini, Anda dapat memodifikasi atau menghapus asosiasi.
6. Untuk membuat asosiasi endpoint baru, buka PrivateLink dan Lattice di panel navigasi kiri dan pilih Endpoints.
7. Pilih Buat titik akhir.

8. Pilih konfigurasi sumber daya untuk terhubung ke AndaVPC.
9. PilihVPC, subnet, dan grup keamanan.
10. (Opsional) Untuk menandai VPC titik akhir Anda, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
11. Pilih Buat Titik Akhir.

Untuk membuat asosiasi VPC titik akhir menggunakan AWS CLI

Gunakan perintah create-vpc-endpoint.

Untuk menghapus asosiasi VPC titik akhir menggunakan AWS CLI

Gunakan perintah delete-vpc-endpoint.

Gerbang sumber daya di VPC Lattice

Gateway sumber daya adalah titik masuknya sumber daya ke VPC tempat sumber daya berada. Ini mencakup beberapa Availability Zone. Agar sumber daya dapat diakses dari semua Availability Zone, Anda harus membuat gateway sumber daya untuk menjangkau sebanyak mungkin Availability Zone.

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

Gateway sumber daya tidak menyediakan kemampuan penyeimbangan beban.

Daftar Isi

Grup keamanan

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

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

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

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

Jenis alamat IP

Gateway sumber daya dapat memilikiIPv4, IPv6 atau alamat dual-stack. Jenis alamat IP dari gateway sumber daya harus kompatibel dengan subnet gateway sumber daya dan jenis alamat IP sumber daya, seperti yang dijelaskan di sini:

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

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

Buat gateway sumber daya di VPC Lattice

Gunakan konsol untuk membuat gateway sumber daya.

Untuk membuat gateway sumber daya menggunakan konsol

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah PrivateLink dan Lattice, pilih gateway sumber daya.
3. Pilih Buat gateway sumber daya.
4. Masukkan nama yang unik di AWS akun Anda.
5. Pilih jenis IP untuk gateway sumber daya.
6. Pilih sumber daya VPC yang ada.
7. Pilih hingga lima grup keamanan untuk mengontrol lalu lintas masuk dari VPC ke jaringan layanan.
8. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
9. Pilih Buat gateway sumber daya.

Untuk membuat gateway sumber daya menggunakan AWS CLI

Gunakan perintah create-resource-gateway.

Hapus gateway sumber daya di VPC Lattice

Gunakan konsol untuk menghapus gateway sumber daya.

Untuk menghapus gateway sumber daya menggunakan konsol

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

Untuk menghapus gateway sumber daya menggunakan AWS CLI

Gunakan perintah delete-resource-gateway.

Akses jaringan layanan melalui AWS PrivateLink

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

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

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

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

Harga

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

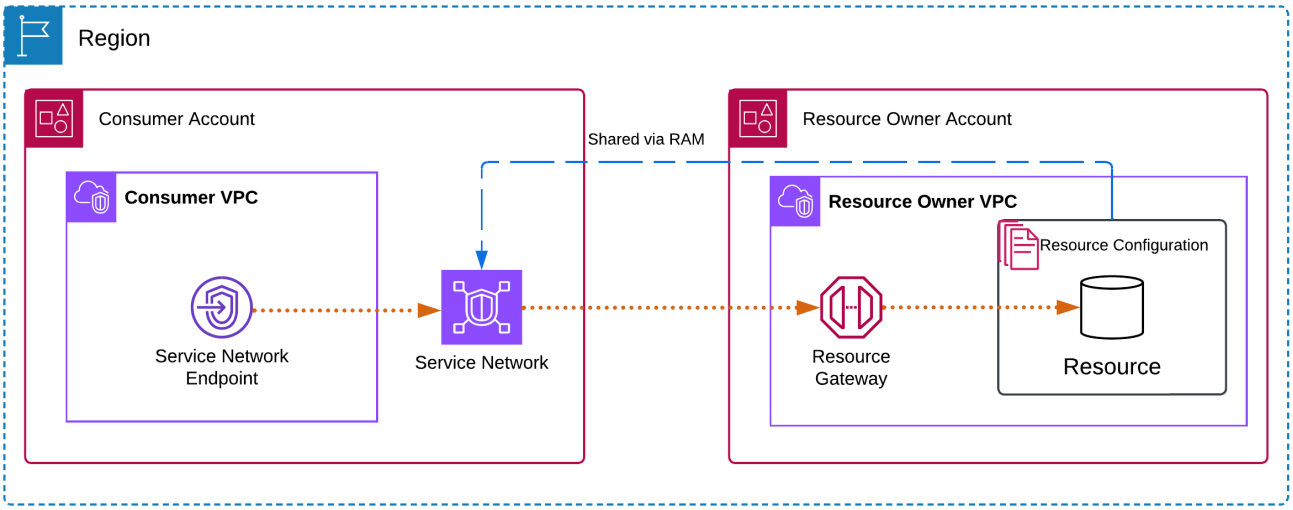
Daftar Isi

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

Gambaran Umum

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

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



Koneksi jaringan hanya dapat dimulai dari VPC yang memiliki endpoint layanan-jaringan ke sumber daya dan layanan dalam jaringan layanan. VPCDengan sumber daya dan layanan tidak dapat memulai koneksi jaringan ke titik akhirVPC.

DNSnama host

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

(disebut DNS nama default) untuk setiap sumber daya dan layanan yang dapat Anda gunakan untuk berkomunikasi dengan sumber daya dan layanan dari Anda VPC dan dari tempat Anda.

DNSNama default untuk sumber daya di jaringan layanan memiliki sintaks berikut:

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

DNSNama default untuk layanan Lattice di jaringan layanan memiliki sintaks berikut:

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

Ketika jaringan layanan Anda memiliki konfigurasi sumber daya yang digunakanARNs, Anda dapat mengaktifkan pribadi DNS. Dengan pribadiDNS, Anda dapat terus membuat permintaan ke sumber daya menggunakan DNS nama yang disediakan untuk sumber daya oleh AWS layanan, sambil memanfaatkan konektivitas pribadi melalui titik akhir jaringan layanan. VPC Untuk informasi selengkapnya, lihat the section called “DNSresolusi”.

DNSresolusi

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

Pribadi DNS

Jika Anda mengaktifkan privat DNS untuk VPC titik akhir jaringan layanan Anda, dan Anda mengaktifkan DNSnama host dan DNS resolusi, kami membuat zona host pribadi AWS terkelola tersembunyi untuk konfigurasi sumber daya yang VPC memiliki nama khusus. DNS Zona yang dihosting berisi kumpulan catatan untuk DNS nama default untuk sumber daya yang menyelesaikannya ke alamat IP pribadi dari antarmuka jaringan titik akhir jaringan layanan di Anda. VPC

Amazon menyediakan DNS server untuk AndaVPC, yang disebut Resolver Route 53. Resolver Route 53 secara otomatis menyelesaikan nama VPC domain lokal dan merekam di zona host

pribadi. Namun, Anda tidak dapat menggunakan Resolver Route 53 dari luar Anda. VPC Jika Anda ingin mengakses VPC titik akhir dari jaringan lokal, Anda dapat menggunakan DNS nama default atau Anda dapat menggunakan titik akhir Route 53 Resolver dan aturan Resolver. Untuk informasi selengkapnya, lihat Mengintegrasikan AWS Transit Gateway dengan AWS PrivateLink dan Amazon Route 53 Resolver.

Subnet dan Availability Zone

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

Jenis alamat IP

Endpoint jaringan layanan dapat mendukungIPv4,IPv6, atau alamat dual-stack. Titik akhir yang mendukung IPv6 dapat merespons DNS kueri dengan AAAA catatan. Jenis alamat IP dari titik akhir jaringan layanan harus kompatibel dengan subnet untuk titik akhir sumber daya, seperti yang dijelaskan di sini:

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

Jika VPC endpoint jaringan layanan mendukungIPv4, antarmuka jaringan endpoint memiliki alamat. IPv4 Jika VPC endpoint jaringan layanan mendukungIPv6, antarmuka jaringan endpoint memiliki alamat. IPv6 IPv6Alamat untuk antarmuka jaringan endpoint tidak dapat dijangkau dari internet. Jika Anda mendeskripsikan antarmuka jaringan endpoint dengan IPv6 alamat, perhatikan bahwa itu `denyAllIgwTraffic` diaktifkan.

Mengakses jaringan layanan melalui titik akhir jaringan layanan

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

Prasyarat

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

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

Buat titik akhir jaringan layanan

Buat titik akhir jaringan layanan untuk mengakses jaringan layanan yang dibagikan dengan Anda.

Untuk membuat titik akhir jaringan layanan

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih Buat Titik Akhir.
4. Anda dapat menentukan nama untuk membuatnya lebih mudah untuk menemukan dan mengelola endpoint.
5. Untuk Jenis, pilih Jaringan layanan.
6. Untuk jaringan Layanan, pilih jaringan layanan yang dibagikan dengan Anda.
7. Untuk pengaturan Jaringan, pilih VPC dari mana Anda akan mengakses jaringan layanan.
8. Jika, Anda ingin mengkonfigurasi DNS dukungan pribadi, pilih Pengaturan tambahan, Aktifkan DNS nama. Untuk menggunakan fitur ini, pastikan atribut Aktifkan DNS nama host dan DNSdukungan Aktifkan diaktifkan untuk AndaVPC.
9. Pilih Buat Titik Akhir.

Untuk membuat endpoint jaringan layanan menggunakan baris perintah

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Kelola titik akhir jaringan layanan

Setelah Anda membuat titik akhir jaringan layanan, Anda dapat memperbarui konfigurasinya.

Tugas

- Hapus titik akhir
- Memperbarui titik akhir jaringan layanan

Hapus titik akhir

Setelah selesai dengan VPC titik akhir, Anda dapat menghapusnya.

Untuk menghapus titik akhir menggunakan konsol

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

Untuk menghapus titik akhir menggunakan baris perintah

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Memperbarui titik akhir jaringan layanan

Anda dapat memperbarui VPC titik akhir.

Untuk memperbarui titik akhir menggunakan konsol

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

Untuk memperbarui titik akhir menggunakan baris perintah

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

Identitas dan manajemen akses untuk AWS PrivateLink

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

Daftar Isi

Audiens

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

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

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

IAMadministrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses AWS PrivateLink.

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peranIAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. 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 menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Versi AWS Tanda Tangan 4 untuk API permintaan di Panduan IAM Pengguna.

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 di Panduan AWS IAM Identity Center Pengguna dan Autentikasi AWS multi-faktor IAM di 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 kredensi pengguna root di IAMPanduan Pengguna.

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 kredensil 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 IAM Identitas, 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 IAM Identitas, lihat Apa itu Pusat IAM Identitas? dalam AWS IAM Identity Center User Guide.

Pengguna dan grup IAM

IAMPengguna adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensi jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang di IAMPanduan Pengguna.

IAMGrup adalah identitas yang menentukan kumpulan IAM pengguna. 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 bernama IAMAdminsdan memberikan izin grup tersebut untuk mengelola sumber dayaIAM.

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 Kasus penggunaan untuk IAM pengguna di Panduan IAM Pengguna.

Peran IAM

IAMPeran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Untuk mengambil IAM peran sementara di dalam AWS Management Console, Anda dapat beralih dari pengguna ke IAM peran (konsol). Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Metode untuk mengambil peran dalam Panduan IAM Pengguna.

IAMperan dengan kredensi 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 (federasi) di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas mengkorelasikan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain 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 Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam 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 IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan

beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan 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 saat membuat FAS permintaan, lihat Meneruskan sesi akses.

- Peran layanan — Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.
- 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. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

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

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 JSON dokumen. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat Ringkasan JSON kebijakan di Panduan IAM Pengguna.

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

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

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

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Menentukan IAM izin khusus dengan kebijakan yang dikelola pelanggan di 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 terkelola atau kebijakan sebaris, lihat Memilih antara kebijakan terkelola dan kebijakan sebaris di IAMPanduan Pengguna.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran 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 IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnyaACLs, lihat Ikhtisar daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

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.

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM 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 batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan 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 dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah JSON kebijakan yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui IAM kebijakan yang dilampirkan ke setiap sumber daya yang Anda miliki. RCPMembatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif

untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations danRCPs, termasuk daftar dukungan Layanan AWS tersebutRCPs, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.

- 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 secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

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 IAM Pengguna.

Bagaimana AWS PrivateLink bekerja dengan IAM

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

IAMfitur	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
ACLs	Tidak
ABAC(tag dalam kebijakan)	Ya

IAMfitur	AWS PrivateLink dukungan
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Peran terkait layanan	Tidak

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

Kebijakan berbasis identitas untuk AWS PrivateLink

Mendukung kebijakan berbasis identitas: Ya

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

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. 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 JSON kebijakan, lihat referensi elemen IAM JSON kebijakan di Panduan IAM Pengguna.

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 JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran 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 seluruh akun atau entitas IAM di akun lain sebagai penanggung jawab 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, IAM administrator 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 principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun IAM di Panduan IAM Pengguna.

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

`Action`Elemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

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

Tindakan di namespace ec2

Beberapa tindakan untuk AWS PrivateLink adalah bagian dari Amazon EC2API. Tindakan kebijakan ini menggunakan `ec2` awalan. Untuk informasi selengkapnya, lihat AWS PrivateLink tindakan di EC2APIReferensi Amazon.

Tindakan di namespace vpce

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

Sumber daya kebijakan untuk AWS PrivateLink

Mendukung sumber daya kebijakan: Ya

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

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, 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: Yes

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam 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. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan IAM Pengguna.

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 IAM Pengguna.

Kunci kondisi berikut khusus untuk AWS PrivateLink:

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

Untuk informasi selengkapnya, lihat Kunci kondisi untuk Amazon EC2.

ACLsdi AWS PrivateLink

MendukungACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

ABACdengan AWS PrivateLink

Mendukung ABAC (tag dalam kebijakan): Ya

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari. ABAC Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABACmembantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

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

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

Untuk informasi selengkapnyaABAC, lihat Menentukan izin dengan ABAC otorisasi di IAMPanduan Pengguna. Untuk melihat tutorial dengan langkah-langkah penyiapanABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di IAMPanduan Pengguna.

Menggunakan kredensi sementara dengan AWS PrivateLink

Mendukung kredensial sementara: Ya

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

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 link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat Beralih dari pengguna ke IAM peran (konsol) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensi sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensi 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 Kredensi keamanan sementara di. IAM

Izin utama lintas layanan untuk AWS PrivateLink

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan 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 saat membuat FAS permintaan, lihat Meneruskan sesi akses.

Peran layanan untuk AWS PrivateLink

Mendukung peran layanan: Tidak

Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.

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. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Contoh kebijakan berbasis identitas untuk AWS PrivateLink

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau mengubah sumber daya AWS PrivateLink . 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 pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

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

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

Contoh

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

Kontrol penggunaan titik VPC akhir

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 VPC titik akhir, lihatthe section called “Kebijakan titik akhir”.

Kontrol pembuatan VPC titik akhir berdasarkan pemilik layanan

Anda dapat menggunakan tombol `ec2:VpceServiceOwner` kondisi untuk mengontrol VPC titik akhir apa yang dapat dibuat berdasarkan siapa yang memiliki layanan (`amazon`,`aws-marketplace`, atau ID akun). Contoh berikut memberikan izin untuk membuat VPC titik akhir dengan pemilik layanan tertentu. 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 DNS nama pribadi yang dapat ditentukan untuk layanan VPC endpoint

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

Mengontrol nama layanan yang dapat ditentukan untuk layanan VPC endpoint

Anda dapat menggunakan tombol `ec2:VpceServiceName` kondisi untuk mengontrol VPC titik akhir apa yang dapat dibuat berdasarkan nama layanan VPC endpoint. Contoh berikut memberikan izin untuk membuat VPC titik akhir 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 VPC titik akhir menggunakan kebijakan titik akhir

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

Daftar Isi

Pertimbangan

- Kebijakan endpoint adalah dokumen JSON kebijakan yang menggunakan bahasa IAM kebijakan. Itu harus mengandung elemen Utama. 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 VPC titik akhir untuk layanan endpoint selain Layanan AWS, kami mengizinkan akses penuh ke titik akhir.
- Anda tidak dapat menggunakan karakter wildcard (* atau?) atau operator kondisi numerik dengan kunci konteks global yang mereferensikan pengidentifikasi yang dihasilkan sistem (misalnya, atau). `aws:PrincipalAccount` `aws:SourceVpc`
- Bila Anda menggunakan operator kondisi string, Anda harus menggunakan setidaknya enam karakter berturut-turut sebelum atau setelah setiap karakter wildcard.
- Saat Anda menentukan elemen ARN sumber daya atau kondisi, bagian akun ARN dapat menyertakan ID akun atau karakter wildcard, tetapi tidak keduanya.

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 VPC titik akhir

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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih VPC titik akhir.
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 memperbarui kebijakan titik akhir menggunakan baris perintah

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Alat untuk Windows PowerShell)

AWS kebijakan terkelola untuk AWS PrivateLink

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

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

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

Untuk informasi selengkapnya, lihat kebijakan AWS terkelola di Panduan IAM Pengguna.

AWS PrivateLink pembaruan kebijakan AWS terkelola

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

Perubahan	Deskripsi	Tanggal
AWS PrivateLink mulai melacak perubahan	AWS PrivateLink mulai melacak perubahan untuk kebijakan yang AWS dikelola.	1 Maret 2021

CloudWatch metrik untuk AWS PrivateLink

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

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

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

Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Daftar Isi

Metrik dan dimensi titik akhir

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

Metrik	Deskripsi
`ActiveConnections`	Jumlah koneksi aktif bersamaan. Ini termasuk koneksi di SYN _ SENT dan ESTABLISHED status.

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

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

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

Untuk memfilter metrik ini, gunakan dimensi berikut.

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

Metrik dan dimensi layanan titik akhir

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

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

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

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

Untuk memfilter metrik ini, gunakan dimensi berikut.

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

Lihat CloudWatch metrik

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

Untuk melihat metrik menggunakan konsol Amazon VPC

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

Untuk melihat metrik menggunakan konsol CloudWatch

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

Untuk melihat metrik menggunakan AWS CLI

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

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

Gunakan perintah list-metrics berikut untuk mencantumkan metrik yang tersedia untuk layanan endpoint:

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

Gunakan aturan Wawasan Kontributor bawaan

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

AWS PrivateLink memberikan aturan berikut:

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1`— Memberi peringkat titik akhir berdasarkan jumlah koneksi aktif.

- `VpcEndpointService-BytesByEndpointId-v1`— Peringkat titik akhir dengan jumlah byte yang diproses.
- `VpcEndpointService-NewConnectionsByEndpointId-v1`— Peringkat titik akhir dengan jumlah koneksi baru.
- `VpcEndpointService-RstPacketsByEndpointId-v1`— Peringkat titik akhir dengan jumlah RST paket yang dikirim ke titik akhir.

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

Anda harus memiliki izin berikut untuk menggunakan Contributor Insights:

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

Tugas

- Aktifkan aturan Contributor Insights
- Nonaktifkan aturan Wawasan Kontributor
- Hapus aturan Wawasan Kontributor

Aktifkan aturan Contributor Insights

Gunakan prosedur berikut untuk mengaktifkan aturan bawaan untuk AWS PrivateLink menggunakan salah satu AWS Management Console atau AWS CLI.

Untuk mengaktifkan aturan Contributor Insights untuk AWS PrivateLink menggunakan konsol

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

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

Untuk mengaktifkan aturan Contributor Insights untuk menggunakan AWS PrivateLinkAWS CLI

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

```
aws cloudwatch list-managed-insight-rules --resource-arn
 arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. Dalam output `list-managed-insight-rules` perintah, salin nama template dari `TemplateName` bidang. Berikut ini adalah contoh dari bidang ini.

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

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

```
aws cloudwatch put-managed-insight-rules --managed-rules
 TemplateName=VpcEndpointService-NewConnectionsByEndpointId-
v1,ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

Nonaktifkan aturan Wawasan Kontributor

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

Untuk menonaktifkan aturan Contributor Insights untuk AWS PrivateLink menggunakan konsol

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

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

Untuk menonaktifkan aturan Contributor Insights untuk menggunakan AWS PrivateLinkAWS CLI

Gunakan disable-insight-rulesperintah untuk menonaktifkan aturan.

Hapus aturan Wawasan Kontributor

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

Untuk menghapus aturan Contributor Insights untuk AWS PrivateLink menggunakan konsol

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

Untuk menghapus aturan Contributor Insights untuk menggunakan AWS PrivateLinkAWS CLI

Gunakan delete-insight-rulesperintah untuk menghapus aturan.

AWS PrivateLink kuota

AWS Akun Anda memiliki kuota default, sebelumnya disebut sebagai batas, untuk setiap layanan. AWS Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan. Jika Anda meminta penambahan kuota yang berlaku per sumber daya, kami meningkatkan kuota untuk semua sumber daya di Wilayah.

Untuk meminta penambahan kuota, lihat Meminta penambahan kuota di Panduan Pengguna Service Quotas.

Permintaan throttling

APITindakan untuk AWS PrivateLink adalah bagian dari Amazon EC2API. Amazon EC2 membatasi API permintaannya di level tersebut. Akun AWS Untuk informasi selengkapnya, lihat Meminta pembatasan di Panduan EC2Pengembang Amazon. Selain itu, API permintaan juga dibatasi di tingkat organisasi untuk membantu kinerja. AWS PrivateLink Jika Anda menggunakan AWS Organizations dan menerima kode `RequestLimitExceeded` kesalahan saat Anda masih dalam API batas tingkat akun, lihat Cara mengidentifikasi AWS akun yang melakukan banyak API panggilan. Jika Anda memerlukan bantuan, hubungi tim akun Anda atau buka kasus dukungan teknis menggunakan VPClayanan dan kategori VPCTitik Akhir. Pastikan untuk melampirkan gambar kode `RequestLimitExceeded` kesalahan.

VPCkuota titik akhir

AWS Akun Anda memiliki kuota berikut yang terkait dengan titik VPC akhir.

Nama	Default	Dapat disesuaikan	Komentar
Antarmuka dan titik akhir Load Balancer Gateway per VPC	50	Ya	Ini adalah kuota gabungan untuk titik akhir antarmuka dan titik akhir Load Balancer Gateway
VPCTitik akhir Gateway per Wilayah	20	Ya	Anda dapat membuat hingga 255 titik akhir gateway per VPC

Nama	Default	Dapat disesuaikan	Komentar
Karakter per VPC kebijakan titik akhir	20,480	Tidak	Ukuran maksimum kebijakan VPC titik akhir, termasuk spasi putih

Pertimbangan berikut berlaku untuk lalu lintas yang melewati titik VPC akhir:

- Secara default, setiap VPC titik akhir dapat mendukung bandwidth hingga 10 Gbps per Availability Zone, dan secara otomatis menskalakan hingga 100 Gbps. Bandwidth maksimum untuk VPC titik akhir, 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 besarMTU, semakin banyak data yang dapat dilewatkan dalam satu paket. VPCEndpoint mendukung MTU 8500 byte. Paket dengan ukuran lebih besar dari 8500 byte yang tiba di titik VPC akhir dijatuhkan.
- Path MTU Discovery (PMTUD) tidak didukung. VPCtitik akhir tidak menghasilkan ICMP pesan berikut: `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (Tipe 3, Kode 4).
- VPCendpoint memberlakukan penjepitan Ukuran Segmen Maksimum (MSS) untuk semua paket. Untuk informasi lebih lanjut, lihat RFC879.

Riwayat dokumen untuk AWS PrivateLink

Tabel berikut menjelaskan rilis untuk AWS PrivateLink.

Perubahan	Deskripsi	Tanggal
Akses sumber daya dan jaringan layanan	AWS PrivateLink mendukung akses sumber daya dan jaringan layanan di seluruh VPC dan batas akun.	Desember 1, 2024
Akses Lintas Wilayah	Penyedia layanan dapat meng-host layanan di satu Wilayah dan membuatnya tersedia dalam satu set AWS Wilayah. Konsumen layanan memilih Wilayah layanan saat membuat titik akhir.	November 26, 2024
Alamat IP yang ditunjuk	Anda dapat menentukan alamat IP untuk antarmuka jaringan titik akhir Anda ketika Anda membuat atau memodifikasi titik akhir AndaVPC.	17 Agustus 2023
IPv6dukungan	Anda dapat mengonfigurasi layanan titik akhir Load Balancer Gateway dan titik akhir Load Balancer Gateway untuk mendukung keduanya IPv4 dan alamat atau hanya alamat. IPv6 IPv6	12 Desember 2022
Wawasan Kontributor	Anda dapat menggunakan aturan Contributor Insights bawaan untuk mengident	18 Agustus 2022

	ifikasi titik akhir tertentu yang merupakan kontributor teratas untuk metrik tersebut. CloudWatch AWS PrivateLink	
IPv6dukungan	Penyedia layanan dapat mengaktifkan layanan endpoint mereka untuk menerima IPv6 permintaan, bahkan jika layanan backend mereka hanya mendukung . IPv4 Jika layanan endpoint menerima IPv6 permintaa n, konsumen layanan dapat mengaktifkan IPv6 dukungan untuk titik akhir antarmuka mereka sehingga mereka dapat mengakses layanan titik akhir. IPv6	Mei 11, 2022
CloudWatch metrik	AWS PrivateLink menerbitk an CloudWatch metrik untuk titik akhir antarmuka Anda, titik akhir Load Balancer Gateway, dan layanan titik akhir.	27 Januari 2022
Titik akhir Load Balancer Gateway	Anda dapat membuat titik akhir Load Balancer Gateway untuk merutekan lalu lintas VPC ke layanan VPC endpoint yang telah dikonfigurasi menggunakan Load Balancer Gateway.	10 November 2020

VPCkebijakan titik akhir	Anda dapat melampirkan IAM kebijakan ke VPC titik akhir antarmuka untuk AWS layan an untuk mengontrol akses ke layanan.	23 Maret 2020
Kunci kondisi untuk layanan VPC endpoint dan endpoint	Anda dapat menggunakan tombol EC2 kondisi untuk mengontrol akses ke VPC titik akhir dan layanan titik akhir.	6 Maret 2020
Menandai VPC titik akhir dan layanan titik akhir pada pembuatan	Anda dapat menambahkan tag saat membuat layanan VPC endpoint dan endpoint.	5 Februari 2020
DNSNama pribadi	Anda dapat mengakses layanan AWS PrivateLink berbasis dari dalam VPC menggunakan DNS nama pribadi Anda.	6 Januari 2020
VPClayanan endpoint	Anda dapat membuat layanan endpoint Anda sendiri dan memungkinkan orang lain Akun AWS dan pengguna untuk terhubung ke layanan Anda melalui titik VPC akhir antarmuka. Anda dapat menawarkan layanan endpoint Anda untuk berlangganan di. AWS Marketplace	28 November 2017

VPCTitik akhir antarmuka untuk Layanan AWS	Anda dapat membuat titik akhir antarmuka untuk terhubung ke Layanan AWS yang terintegrasi dengan AWS PrivateLink tanpa menggunakan gateway atau NAT perangkat internet.	8 November 2017
VPCtitik akhir untuk DynamoDB	Anda dapat membuat VPC titik akhir gateway untuk mengakses Amazon DynamoDB VPC dari Anda tanpa menggunakan gateway atau perangkat internet. NAT	16 Agustus 2017
VPCtitik akhir untuk Amazon S3	Anda dapat membuat VPC titik akhir gateway untuk mengakses Amazon S3 dari VPC Anda tanpa menggunak an gateway NAT atau perangkat internet.	11 Mei 2015

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