Panduan Pengguna

AWS Direct Connect

AWS Direct Connect: Panduan Pengguna

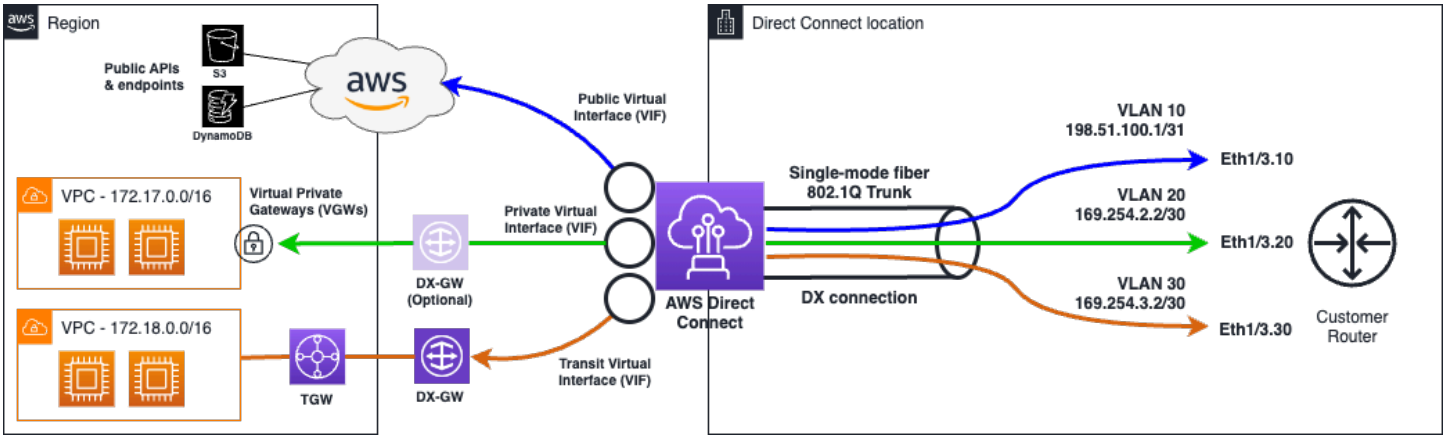
Table of Contents

Apa itu AWS Direct Connect?

AWS Direct Connect menghubungkan jaringan internal Anda ke AWS Direct Connect lokasi melalui kabel serat optik Ethernet standar. Salah satu ujung kabel terhubung ke router Anda, yang lainnya ke router AWS Direct Connect . Dengan koneksi ini, Anda dapat membuat antarmuka virtual langsung ke AWS layanan publik (misalnya, ke Amazon S3) atau ke Amazon VPC, melewati penyedia layanan internet di jalur jaringan Anda. AWS Direct Connect Lokasi menyediakan akses ke AWS Wilayah yang terkait dengannya. Anda dapat menggunakan satu koneksi di Wilayah publik atau AWS GovCloud (US) untuk mengakses AWS layanan publik di semua Wilayah publik lainnya.

- Untuk daftar lokasi Direct Connect yang dapat Anda sambungkan, lihat Lokasi AWS Direct Connect.
- Untuk jawaban atas pertanyaan tentang Direct Connect, lihat FAQ Direct Connect.

Diagram berikut menunjukkan gambaran tingkat tinggi tentang bagaimana AWS Direct Connect antarmuka dengan jaringan Anda.



Daftar Isi

AWS Direct Connect komponen

Berikut ini adalah komponen kunci yang Anda gunakan untuk Direct Connect:

Koneksi

Buat koneksi di AWS Direct Connect lokasi untuk membuat koneksi jaringan dari tempat Anda ke AWS Wilayah. Untuk informasi selengkapnya, lihat AWS Direct Connect koneksi khusus dan host.

Antarmuka virtual

Buat antarmuka virtual untuk mengaktifkan akses ke AWS layanan. Sebuah antarmuka virtual publik memungkinkan akses ke layanan publik, seperti Amazon S3. Antarmuka virtual privat memungkinkan akses ke VPC Anda. Jenis antarmuka yang didukung dijelaskan di bawah ini dithe section called “Jenis antarmuka virtual Direct Connect yang didukung”. Untuk detail selengkapnya tentang antarmuka yang didukung, lihat AWS Direct Connect antarmuka virtual dan antarmuka virtual yang dihosting danPrasyarat untuk antarmuka virtual.

Persyaratan jaringan

Untuk digunakan AWS Direct Connect di suatu AWS Direct Connect lokasi, jaringan Anda harus memenuhi salah satu ketentuan berikut:

- Jaringan Anda ditempatkan dengan lokasi yang ada AWS Direct Connect . Untuk informasi selengkapnya tentang AWS Direct Connect lokasi yang tersedia, lihat Detail Produk AWS Direct Connect.
- Anda bekerja dengan AWS Direct Connect mitra yang merupakan anggota Jaringan AWS Mitra (APN). Untuk informasi, lihat Partner APN Mendukung Direct Connect AWS.
- Anda bekerja dengan penyedia layanan independen untuk terhubung ke AWS Direct Connect.

Di samping itu, Jaringan Anda harus memenuhi syarat-syarat berikut:

- Jaringan Anda harus menggunakan serat mode tunggal dengan transceiver 1000BASE-LX (1310 nm) untuk 1 gigabit Ethernet, transceiver 10GBASE-LR (1310 nm) untuk 10 gigabit, 100GBASE- untuk 100 gigabit Ethernet, atau 400GBASE- untuk 400 Gbps Ethernet. LR4 LR4
- Bergantung pada titik akhir AWS Direct Connect yang melayani koneksi Anda, negosiasi otomatis perangkat lokal mungkin perlu diaktifkan atau dinonaktifkan untuk koneksi khusus apa pun. Jika

antarmuka virtual tetap down saat koneksi Direct Connect aktif, lihatPemecahan masalah lapisan 2 (tautan data).

- Enkapsulasi VLAN 802.1Q harus didukung di seluruh koneksi, termasuk perangkat perantara.
- Perangkat Anda harus mendukung Border Gateway Protocol (BGP) dan otentikasi MD5 BGP.
- (Opsional) Anda dapat mengonfigurasi Deteksi Penerusan Dua Arah (BFD) pada jaringan Anda. BFD asinkron secara otomatis diaktifkan untuk setiap antarmuka virtual. AWS Direct Connect Ini secara otomatis diaktifkan untuk antarmuka virtual Direct Connect, tetapi tidak berlaku sampai Anda mengkonfigurasinya di router Anda. Untuk informasi selengkapnya, lihat Mengaktifkan BFD untuk koneksi Direct Connect.

AWS Direct Connect mendukung protokol IPv6 komunikasi IPv4 dan komunikasi. IPv6 alamat yang disediakan oleh AWS layanan publik dapat diakses melalui antarmuka virtual AWS Direct Connect publik.

AWS Direct Connect mendukung ukuran bingkai Ethernet 1522 atau 9023 byte (14 byte header Ethernet + 4 byte tanda VLAN + byte untuk datagram IP + 4 byte FCS) pada lapisan tautan. Anda dapat mengatur MTU antarmuka virtual privat. Untuk informasi selengkapnya, lihat MTUs untuk antarmuka virtual pribadi atau antarmuka virtual transit.

Jenis antarmuka virtual Direct Connect yang didukung

AWS Direct Connect mendukung tiga jenis antarmuka virtual (VIF) berikut:

- Antarmuka virtual pribadi

  Jenis antarmuka ini digunakan untuk mengakses Amazon Virtual Private Cloud (VPC) menggunakan alamat IP pribadi. Dengan antarmuka virtual pribadi Anda dapat

  - Hubungkan langsung ke satu VPC per antarmuka virtual pribadi untuk mengakses sumber daya tersebut menggunakan pribadi IPs di Wilayah yang sama.
  - Hubungkan antarmuka virtual pribadi ke gateway Direct Connect untuk mengakses beberapa gateway pribadi virtual di seluruh akun dan AWS Wilayah mana pun (kecuali Wilayah AWS Tiongkok).
- Antarmuka virtual publik

  Jenis antarmuka virtual ini digunakan untuk mengakses semua layanan AWS publik menggunakan alamat IP publik. Dengan antarmuka virtual publik, Anda dapat terhubung ke semua alamat dan layanan IP AWS publik secara global.

- Antarmuka virtual transit

  Jenis antarmuka ini digunakan untuk mengakses satu atau lebih Gateway Transit VPC Amazon yang terkait dengan gateway Direct Connect. Dengan antarmuka virtual transit, Anda menghubungkan beberapa Gateway Transit VPC Amazon di beberapa akun dan Wilayah AWS (kecuali Wilayah Tiongkok AWS).

  > **Note**
  >
  > Ada batasan jumlah jenis asosiasi yang berbeda antara gateway Direct Connect dan antarmuka virtual. Untuk informasi selengkapnya tentang batasan tertentu, lihat Kuota Direct Connect halaman.

Untuk informasi selengkapnya tentang antarmuka virtual, lihatAntarmuka virtual dan antarmuka virtual yang dihosting.

Harga untuk Direct Connect

AWS Direct Connect memiliki dua elemen penagihan: jam port dan transfer data keluar. Harga jam port ditentukan oleh kapasitas dan jenis koneksi (koneksi khusus atau koneksi host).

Biaya Transfer Data Keluar untuk antarmuka pribadi dan antarmuka virtual transit dialokasikan ke AWS akun yang bertanggung jawab atas Transfer Data. Tidak ada biaya tambahan untuk penggunaan gateway AWS Direct Connect multiakun.

Untuk AWS sumber daya yang dapat dialamatkan secara publik (misalnya, bucket Amazon S3, EC2 instans Klasik, atau EC2 lalu lintas yang melewati gateway internet), jika lalu lintas keluar ditujukan untuk awalan publik yang dimiliki oleh akun AWS pembayar yang sama dan secara aktif diiklankan AWS melalui Antarmuka virtual AWS Direct Connect publik, penggunaan Data Transfer Out (DTO) diukur ke pemilik sumber daya dengan kecepatan transfer data. AWS Direct Connect

Untuk informasi selengkapnya, lihat Harga AWS Direct Connect.

Akses ke AWS Direct Connect Daerah Terpencil

AWS Direct Connect lokasi di Wilayah publik atau AWS GovCloud (US) dapat mengakses layanan publik di Wilayah publik lainnya (tidak termasuk Tiongkok (Beijing dan Ningxia)). Selain itu, AWS

Direct Connect koneksi di Wilayah publik atau AWS GovCloud (US) dapat dikonfigurasi untuk mengakses VPC di akun Anda di Wilayah publik lainnya (tidak termasuk Tiongkok (Beijing dan Ningxia). Oleh karena itu Anda dapat menggunakan satu koneksi AWS Direct Connect untuk membangun layanan multi-Wilayah. Semua lalu lintas jaringan tetap berada di tulang punggung jaringan AWS global, terlepas dari apakah Anda mengakses AWS layanan publik atau VPC di Wilayah lain.

Setiap transfer data keluar dari Wilayah jarak jauh ditagihkan dengan laju transfer data Wilayah jarak jauh. Untuk informasi selengkapnya tentang harga transfer data, lihat bagian Harga di halaman detail AWS Direct Connect.

Untuk informasi selengkapnya tentang kebijakan perutean dan komunitas BGP yang didukung untuk koneksi AWS Direct Connect , lihat Kebijakan Perutean dan Komunitas BGP.

Akses ke layanan publik di Wilayah terpencil

Untuk mengakses sumber daya publik di Wilayah jarak jauh, Anda harus menyiapkan antarmuka virtual publik dan membuat sesi Border Gateway Protocol (BGP). Untuk informasi selengkapnya, lihat Antarmuka virtual dan antarmuka virtual yang dihosting.

Setelah Anda membuat antarmuka virtual publik dan membuat sesi BGP untuk itu, router Anda mempelajari rute Wilayah publik lainnya. AWS Untuk informasi selengkapnya tentang awalan yang saat ini diiklankan oleh AWS, lihat Rentang Alamat AWS IP di. Referensi Umum Amazon Web Services

Akses ke VPCs wilayah terpencil

Anda dapat membuat gateway Direct Connect di Wilayah publik mana saja. Gunakan untuk menghubungkan AWS Direct Connect koneksi Anda melalui antarmuka virtual pribadi ke VPCs akun Anda yang terletak di Wilayah yang berbeda atau ke gateway transit. Untuk informasi selengkapnya, lihat AWS Direct Connect gerbang.

Atau, Anda dapat membuat antarmuka virtual publik untuk AWS Direct Connect koneksi Anda dan kemudian membuat koneksi VPN ke VPC Anda di Wilayah terpencil. Untuk informasi selengkapnya tentang mengonfigurasi konektivitas VPN ke VPC, lihat Skenario untuk Menggunakan Amazon Virtual Private Cloud dalam Panduan Pengguna Amazon VPC.

Network-to-Amazon Opsi Konektivitas VPC

Konfigurasi berikut dapat digunakan untuk menghubungkan jaringan jarak jauh dengan lingkungan Amazon VPC Anda. Opsi ini berguna untuk mengintegrasikan AWS sumber daya dengan layanan di tempat Anda yang ada:

- Pilihan Konektivitas Amazon Virtual Private Cloud

AWS Direct Connect kebijakan routing dan komunitas BGP

AWS Direct Connect menerapkan kebijakan perutean masuk (dari pusat data lokal) dan keluar (dari AWS Wilayah Anda) untuk koneksi publik. AWS Direct Connect Anda juga dapat menggunakan tanda komunitas Border Gateway Protocol (BGP) pada rute yang diiklankan oleh Amazon dan menerapkan tanda komunitas BGP pada rute yang Anda iklankan ke Amazon.

Kebijakan perutean antarmuka virtual publik

Jika Anda menggunakan AWS Direct Connect untuk mengakses AWS layanan publik, Anda harus menentukan awalan atau IPv4 IPv6 awalan publik untuk beriklan melalui BGP.

Kebijakan perutean masuk berikut berlaku:

- Anda harus memiliki prefiks publik dan prefiks tersebut harus terdaftar di registri internet regional yang sesuai.
- Lalu lintas harus ditujukan ke prefiks publik Amazon. Perutean transitif antarkoneksi tidak didukung.
- AWS Direct Connect melakukan penyaringan paket masuk untuk memvalidasi bahwa sumber lalu lintas berasal dari awalan yang diiklankan.

Kebijakan perutean masuk berikut berlaku:

- AS_PATH dan Longest Prefix Match digunakan untuk menentukan jalur routing. AWS merekomendasikan iklan rute yang lebih spesifik menggunakan AWS Direct Connect jika awalan yang sama diiklankan ke Internet dan ke antarmuka virtual publik.
- AWS Direct Connect mengiklankan semua awalan AWS Wilayah lokal dan terpencil jika tersedia dan menyertakan awalan on-net dari titik kehadiran AWS non-Region (PoP) lainnya jika tersedia; misalnya, dan Rute 53. CloudFront

> **Note**
>
> - Awalan yang tercantum dalam file JSON rentang alamat AWS IP, ip-ranges.json, untuk Wilayah Tiongkok hanya diiklankan di Wilayah AWS Tiongkok. AWS
> - Awalan yang tercantum dalam alamat AWS IP berkisar file JSON, ip-ranges.json, untuk Wilayah Komersil hanya diiklankan di Kawasan AWS Komersil. AWS
>
> Untuk informasi selengkapnya tentang file ip-ranges.json, lihat rentang AWS alamat IP di file. Referensi Umum AWS

- AWS Direct Connect mengiklankan awalan dengan panjang jalur minimum 3.
- AWS Direct Connect mengiklankan semua awalan publik dengan komunitas BGP yang terkenal`NO_EXPORT`.
- Jika Anda mengiklankan awalan yang sama dari dua Wilayah berbeda menggunakan dua antarmuka virtual publik yang berbeda, dan keduanya memiliki atribut BGP yang sama dan panjang awalan terpanjang, AWS akan memprioritaskan Wilayah asal untuk lalu lintas keluar.
- Jika Anda memiliki beberapa AWS Direct Connect koneksi, Anda dapat menyesuaikan pembagian beban lalu lintas masuk dengan awalan iklan dengan atribut jalur yang sama.
- Awalan yang diiklankan oleh tidak AWS Direct Connect boleh diiklankan di luar batas jaringan koneksi Anda. Sebagai contoh, prefiks ini tidak boleh disertakan dalam tabel perutean internet publik.
- AWS Direct Connect menyimpan awalan yang diiklankan oleh pelanggan dalam jaringan Amazon. Kami tidak mengiklankan kembali prefiks pelanggan yang dipelajari dari VIF publik ke salah satu dari berikut ini:
  - AWS Direct Connect Pelanggan lain
  - Jaringan yang sejajar dengan Jaringan AWS Global
  - Penyedia transit Amazon
- Saat menggunakan antarmuka publik, Anda dapat menggunakan ASN publik atau pribadi. Namun, ada pertimbangan penting:
  - Publik ASNs: Anda harus memiliki ASN dan memiliki hak untuk mengumumkannya. AWS akan memverifikasi kepemilikan Anda atas ASN.
  - Pribadi ASNs: Anda dapat menggunakan pribadi ASNs (64512-65534, 4200000000-4294967294). Namun, AWS Direct Connect akan mengganti ASN pribadi dengan AWS ASN (7224) saat mengiklankan awalan Anda ke pelanggan lain atau internet. AWS

- ASN mendahului:
  - Dengan ASN publik, prepending akan berfungsi seperti yang diharapkan, dan ASN prepended Anda akan terlihat oleh jaringan lain.
  - Dengan ASN pribadi, prepending apa pun yang Anda lakukan akan dilucuti saat AWS mengganti ASN pribadi Anda dengan 7224. Ini berarti ASN prepending tidak efektif untuk mempengaruhi keputusan routing di luar AWS saat menggunakan ASN pribadi pada antarmuka virtual publik.
- Saat membuat sesi peering BGP dengan AWS melalui antarmuka virtual publik, gunakan 7224 untuk nomor sistem otonom (ASN) untuk menetapkan sesi BGP di samping. AWS ASN pada router atau perangkat gateway pelanggan Anda harus berbeda dari ASN itu.

Komunitas BGP antarmuka virtual publik

AWS Direct Connect mendukung lingkup tag komunitas BGP untuk membantu mengontrol ruang lingkup (Regional atau global) dan preferensi rute lalu lintas pada antarmuka virtual publik. AWS memperlakukan semua rute yang diterima dari VIF publik seolah-olah mereka ditandai dengan tag komunitas NO_EXPORT BGP, yang berarti hanya AWS jaringan yang akan menggunakan informasi perutean itu.

Cakupan Komunitas BGP

Anda dapat menerapkan tanda komunitas BGP pada prefiks publik yang Anda beriklan ke Amazon untuk menunjukkan seberapa jauh untuk menyebarkan prefiks Anda di jaringan Amazon, untuk Wilayah AWS lokal saja, semua Wilayah dalam benua, atau semua Wilayah publik.

Wilayah AWS komunitas

Untuk kebijakan perutean masuk, Anda dapat menggunakan komunitas BGP berikut untuk awalan Anda:

- `7224:9100`—Lokal Wilayah AWS
- `7224:9200`—Semua Wilayah AWS untuk benua:
  - Seluruh Amerika Utara
  - Asia Pasifik
  - Eropa, Timur Tengah, dan Afrika
- `7224:9300`—Global (semua AWS Wilayah publik)

> **Note**
>
> Jika Anda tidak menerapkan tag komunitas apa pun, awalan diiklankan ke semua AWS Wilayah publik (global) secara default.
> Prefiks yang ditandai dengan komunitas yang sama, dan memiliki atribut AS_PATH identik adalah kandidat untuk multi-pathing.

Komunitas `7224:1` — `7224:65535` dicadangkan oleh AWS Direct Connect.

Untuk kebijakan perutean keluar, AWS Direct Connect terapkan komunitas BGP berikut ke rute yang diiklankan:

- `7224:8100`—Rute yang berasal dari AWS Wilayah yang sama di mana AWS Direct Connect titik keberadaan dikaitkan.
- `7224:8200`—Rute yang berasal dari benua yang sama dengan AWS Direct Connect titik keberadaan yang terkait.
- Tidak ada tag — rute yang berasal dari benua lain.

> **Note**
>
> Untuk menerima semua awalan AWS publik, jangan gunakan filter apa pun.

Komunitas yang tidak didukung untuk koneksi AWS Direct Connect publik akan dihapus.

`NO_EXPORT` Komunitas BGP

Untuk kebijakan perutean keluar, tag komunitas `NO_EXPORT` BGP didukung untuk antarmuka virtual publik.

AWS Direct Connect juga menyediakan tag komunitas BGP pada rute Amazon yang diiklankan. Jika Anda menggunakan AWS Direct Connect untuk mengakses AWS layanan publik, Anda dapat membuat filter berdasarkan tag komunitas ini.

Untuk antarmuka virtual publik, semua rute yang AWS Direct Connect mengiklankan ke pelanggan ditandai dengan tag komunitas NO_EXPORT.

Kebijakan perutean antarmuka virtual privat dan antarmuka virtual transit

Jika Anda menggunakan AWS Direct Connect untuk mengakses AWS sumber daya pribadi Anda, Anda harus menentukan IPv4 atau IPv6 awalan untuk beriklan melalui BGP. Awalan ini bisa bersifat publik atau pribadi.

Aturan perutean keluar berikut berlaku berdasarkan awalan yang diiklankan:

- AWS mengevaluasi panjang awalan terpanjang terlebih dahulu. AWS merekomendasikan iklan rute yang lebih spesifik menggunakan beberapa antarmuka virtual Direct Connect jika jalur perutean yang diinginkan dimaksudkan untuk koneksi aktif/pasif. Lihat Mempengaruhi Lalu Lintas melalui Jaringan Hybrid menggunakan Pencocokan Awalan Terpanjang untuk informasi selengkapnya.
- Preferensi lokal adalah atribut BGP yang direkomendasikan untuk digunakan ketika jalur perutean yang diinginkan dimaksudkan untuk koneksi aktif/pasif dan panjang awalan yang diiklankan adalah sama. Nilai ini ditetapkan per Wilayah untuk memilih AWS Direct Connect Lokasi yang memiliki hubungan yang sama Wilayah AWS menggunakan nilai komunitas preferensi lokal `7224:7200` — Medium. Jika Wilayah lokal tidak terkait dengan lokasi Direct Connect, itu diatur ke nilai yang lebih rendah. Ini hanya berlaku jika tidak ada tag komunitas preferensi lokal yang ditetapkan.
- Panjang AS_PATH dapat digunakan untuk menentukan jalur perutean ketika panjang awalan dan preferensi lokal sama.
- Multi-Exit Discriminator (MED) dapat digunakan untuk menentukan jalur perutean ketika panjang awalan, preferensi lokal, dan AS_PATH sama. AWS tidak merekomendasikan penggunaan nilai MED mengingat prioritas yang lebih rendah dalam evaluasi.
- AWS menggunakan perutean multi-jalur (ECMP) biaya sama di beberapa transit atau antarmuka virtual pribadi ketika awalan memiliki panjang AS_PATH dan atribut BGP yang sama. ASNs Dalam AS_PATH awalan tidak perlu cocok.

Antarmuka virtual privat dan transit komunitas BGP antarmuka virtual

Saat Wilayah AWS merutekan lalu lintas ke lokasi lokal melalui antarmuka virtual pribadi atau transit Direct Connect, lokasi Direct Connect yang terkait Wilayah AWS memengaruhi kemampuan untuk menggunakan ECMP. Wilayah AWS lebih suka lokasi Direct Connect di lokasi yang sama terkait secara Wilayah AWS default. Lihat AWS Direct Connect Lokasi untuk mengidentifikasi lokasi yang terkait Wilayah AWS dari setiap lokasi Direct Connect.

Jika tidak ada tag komunitas preferensi lokal yang diterapkan, Direct Connect mendukung ECMP melalui antarmuka virtual pribadi atau transit untuk awalan dengan panjang AS_PATH, dan nilai MED yang sama pada dua jalur atau lebih dalam skenario berikut:

- Lalu lintas Wilayah AWS pengirim memiliki dua atau lebih jalur antarmuka virtual dari lokasi yang terkait Wilayah AWS, baik di fasilitas kolokasi yang sama atau berbeda.
- Lalu lintas Wilayah AWS pengirim memiliki dua atau lebih jalur antarmuka virtual dari lokasi yang tidak berada di Wilayah yang sama.

Untuk informasi selengkapnya, lihat Bagaimana cara mengatur koneksi Active/Active or Active/Passive Direct Connect AWS dari antarmuka virtual pribadi atau transit?

> **Note**
>
> Ini tidak berpengaruh pada ECMP ke Wilayah AWS dari lokasi lokal.

Untuk mengontrol preferensi rute, Direct Connect mendukung tag komunitas BGP preferensi lokal untuk antarmuka virtual pribadi dan antarmuka virtual transit.

Komunitas BGP preferensi lokal

Anda dapat menggunakan tanda komunitas BGP preferensi lokal untuk mencapai penyeimbangan beban dan preferensi rute untuk lalu lintas masuk ke jaringan Anda. Untuk setiap prefiks yang Anda iklankan melalui sesi BGP, Anda dapat menerapkan tanda komunitas untuk menunjukkan prioritas jalur terkait untuk menghasilkan lalu lintas.

Tanda komunitas BGP preferensi lokal berikut didukung:

- `7224:7100`—Preferensi rendah
- `7224:7200`—Preferensi sedang
- `7224:7300`—Preferensi tinggi

Tanda komunitas BGP preferensi lokal saling eksklusif. Untuk memuat lalu lintas keseimbangan di beberapa AWS Direct Connect koneksi (aktif/aktif) yang di-homed ke AWS Wilayah yang sama atau berbeda, terapkan tag komunitas yang sama; misalnya, `7224:7200` (preferensi sedang) di seluruh awalan untuk koneksi. Jika salah satu koneksi gagal, lalu lintas akan menjadi keseimbangan beban menggunakan ECMP di seluruh koneksi aktif yang tersisa terlepas dari asosiasi Wilayah asal

mereka. Untuk mendukung failover di beberapa AWS Direct Connect koneksi (aktif/pasif), terapkan tag komunitas dengan preferensi yang lebih tinggi ke awalan untuk antarmuka virtual primer atau aktif dan preferensi yang lebih rendah ke awalan untuk cadangan atau antarmuka virtual pasif. Misalnya, atur tag komunitas BGP untuk antarmuka virtual primer atau aktif Anda ke `7224:7300` (preferensi tinggi) dan `7224:7100` (preferensi rendah) untuk antarmuka virtual pasif Anda.

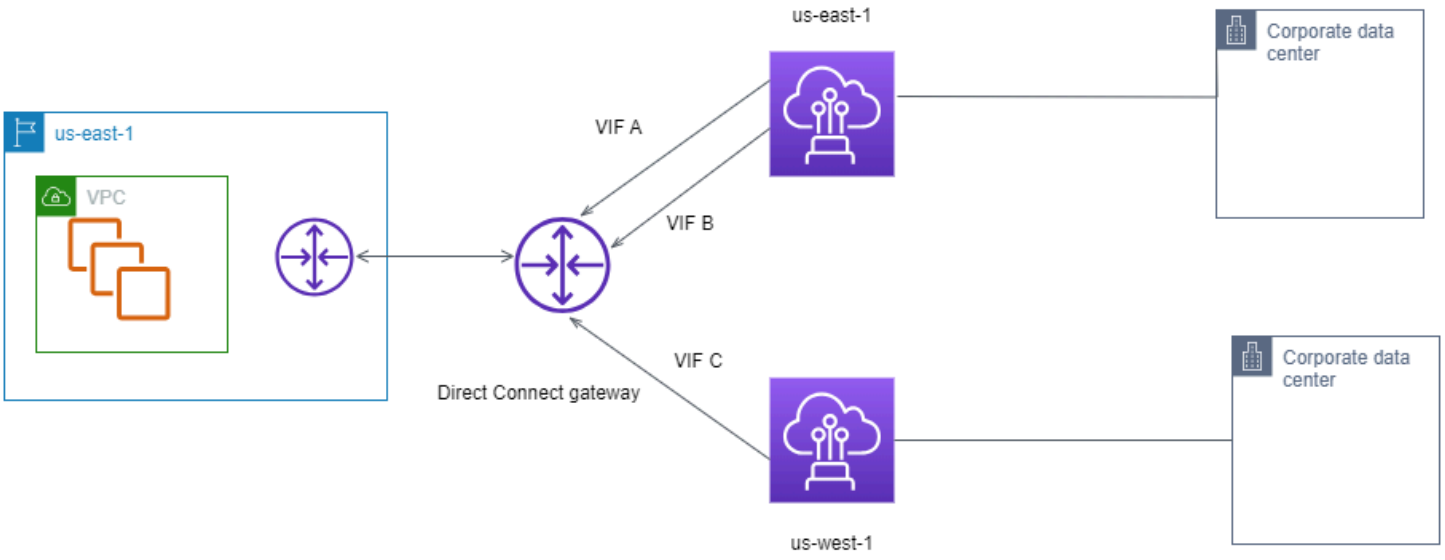
Preferensi lokal tanda komunitas BGP dievaluasi sebelum atribut AS_PATH, dan dievaluasi dalam urutan dari terendah ke preferensi tertinggi (di mana preferensi tertinggi lebih disukai).

AWS Direct Connect contoh perutean antarmuka virtual pribadi

Pertimbangkan konfigurasi di mana AWS Direct Connect lokasi 1 rumah Wilayah sama dengan Wilayah rumah VPC. Ada AWS Direct Connect lokasi redundan di Wilayah yang berbeda Ada dua pribadi VIFs (VIF A dan VIF B) dari lokasi AWS Direct Connect 1 (us-east-1) ke gateway Direct Connect. Ada satu VIF pribadi (VIF C) dari AWS Direct Connect lokasi (us-west-1) ke gateway Direct Connect. Untuk memiliki lalu lintas AWS rute melalui VIF B sebelum VIF A, atur atribut AS_PATH VIF B menjadi lebih pendek dari atribut VIF A AS_PATH.

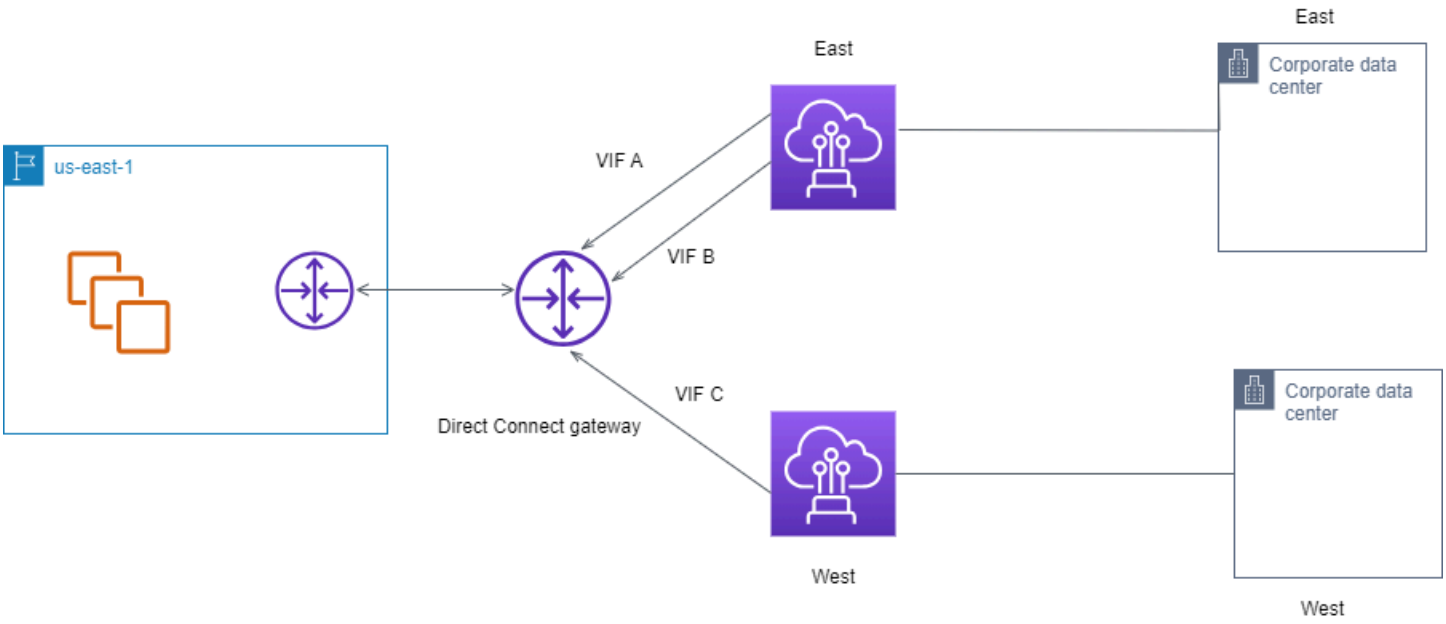
VIFs Memiliki konfigurasi berikut:

- VIF A (di us-east-1) mengiklankan 172.16.0.0/16 dan memiliki atribut AS_PATH 65001, 65001, 65001
- VIF B (in us-east-1) mengiklankan 172.16.0.0/16 dan memiliki atribut AS_PATH 65001, 65001
- VIF C (di us-west-1) mengiklankan 172.16.0.0/16 dan memiliki atribut AS_PATH 65001



Jika Anda mengubah konfigurasi rentang CIDR VIF C, rute yang termasuk dalam rentang VIF C CIDR menggunakan VIF C karena memiliki panjang awalan terpanjang.

- VIF C (di us-west-1) mengiklankan 172.16.0.0/24 dan memiliki atribut AS_PATH 65001



AWS Direct Connect Toolkit Ketahanan

AWS menawarkan pelanggan kemampuan untuk mencapai koneksi jaringan yang sangat tangguh antara Amazon Virtual Private Cloud (Amazon VPC) dan infrastruktur lokal mereka. The AWS Direct Connect Resiliency Toolkit menyediakan wizard koneksi dengan beberapa model ketahanan. Model ini membantu Anda menentukan, lalu menempatkan pesanan untuk jumlah koneksi khusus guna mencapai tujuan SLA Anda. Anda memilih model ketahanan, dan kemudian AWS Direct Connect Resiliency Toolkit memandu Anda melalui proses pemesanan koneksi khusus. Model ketahanan didesain untuk memastikan Anda memiliki jumlah koneksi khusus yang sesuai di beberapa lokasi.

The AWS Direct Connect Resiliency Toolkit memiliki manfaat sebagai berikut:

- Memberikan panduan tentang cara menentukan lalu memesan koneksi khusus AWS Direct Connect redundan yang sesuai.
- Memastikan bahwa koneksi khusus redundan memiliki kecepatan yang sama.
- Mengonfigurasi nama koneksi khusus secara otomatis.
- Secara otomatis menyetujui koneksi khusus Anda ketika Anda memiliki AWS akun yang sudah ada dan Anda memilih AWS Direct Connect Mitra yang dikenal. Letter of Authority (LOA) tersedia untuk pengunduhan segera.
- Secara otomatis membuat tiket dukungan untuk persetujuan koneksi khusus saat Anda adalah AWS pelanggan baru, atau Anda memilih mitra (Lainnya) yang tidak dikenal.
- Menyediakan ringkasan pesanan untuk koneksi khusus Anda, dengan SLA yang dapat Anda capai dan biaya port-jam untuk koneksi khusus yang dipesan.
- Membuat grup agregasi tautan (LAGs), dan menambahkan jumlah koneksi khusus yang sesuai ke LAGs saat Anda memilih kecepatan selain 1 Gbps, 10 Gbps, 100 Gbps, atau 400 Gbps.
- Menyediakan ringkasan LAG dengan SLA koneksi khusus yang dapat Anda capai, dan biaya port-jam total untuk setiap koneksi khusus yang dipesan sebagai bagian dari LAG.
- Mencegah Anda mengakhiri koneksi khusus pada perangkat AWS Direct Connect yang sama.
- Menyediakan cara bagi Anda guna menguji konfigurasi untuk ketahanan. Anda bekerja dengan AWS untuk menurunkan sesi peering BGP guna memverifikasi bahwa lalu lintas tersebut dirutekan ke salah satu antarmuka virtual redundan. Untuk informasi selengkapnya, lihat the section called “Tes failover Direct Connect”.
- Menyediakan CloudWatch metrik Amazon untuk koneksi dan antarmuka virtual. Untuk informasi selengkapnya, lihat Memantau sumber daya Direct Connect.

Model ketahanan berikut tersedia di Resiliency Toolkit AWS Direct Connect :

- Ketahanan Maksimum: Model ini menyediakan cara untuk memesan koneksi khusus guna mencapai SLA 99,99%. Model ini mengharuskan Anda memenuhi semua persyaratan untuk mencapai SLA yang ditentukan dalam Perjanjian Tingkat Layanan AWS Direct Connect.
- Ketahanan Tinggi: Model ini menyediakan cara untuk memesan koneksi khusus guna mencapai SLA 99,9%. Model ini mengharuskan Anda memenuhi semua persyaratan untuk mencapai SLA yang ditentukan dalam Perjanjian Tingkat Layanan AWS Direct Connect.
- Pengembangan dan Pengujian: Model ini menyediakan Anda cara untuk mencapai ketahanan pengembangan dan pengujian untuk beban kerja nonkritis, dengan menggunakan koneksi terpisah yang berakhir pada perangkat terpisah di satu lokasi.
- Klasik. Model ini ditujukan untuk pengguna yang memiliki koneksi dan ingin menambahkan koneksi tambahan. Model ini tidak menyediakan SLA.

Praktik terbaik adalah menggunakan wizard Koneksi di AWS Direct Connect Resiliency Toolkit untuk memesan koneksi khusus untuk mencapai tujuan SLA Anda.

Setelah Anda memilih model resiliency, AWS Direct Connect Resiliency Toolkit akan memandu Anda melalui prosedur berikut:

- Memilih jumlah koneksi khusus
- Memilih kapasitas koneksi, dan lokasi koneksi khusus
- Memesan koneksi khusus
- Memverifikasi bahwa koneksi khusus siap digunakan
- Mengunduh Letter of Authority (LOA-CFA) Anda untuk setiap koneksi khusus
- Memverifikasi bahwa konfigurasi Anda memenuhi persyaratan ketahanan

Prasyarat

AWS Direct Connect mendukung kecepatan port berikut melalui serat mode tunggal: transceiver 1000BASE-LX (1310 nm) untuk 1 gigabit Ethernet, transceiver 10GBASE-LR (1310 nm) untuk 10 gigabit, 100GBASE- untuk 100 gigabit Ethernet, atau 400GBASE- untuk 400 Gbps Ethernet. LR4 LR4

Anda dapat mengatur AWS Direct Connect koneksi dengan salah satu cara berikut:

Model	Bandwidth	Metode
Koneksi khusus	1 Gbps, 10 Gbps, 100 Gbps, dan 400 Gbps	Bekerja dengan AWS Direct Connect Mitra atau penyedia jaringan untuk menghubungkan router dari pusat data, kantor, atau lingkungan colocation Anda ke suatu AWS Direct Connect lokasi. Penyedia jaringan tidak harus menjadi AWS Direct Connect Mitra untuk menghubungkan Anda ke koneksi khusus. AWS Direct Connect koneksi khusus mendukung kecepatan port ini melalui serat mode tunggal: 1 Gbps: 1000BASE-LX (1310 nm), 10 Gbps: 10GBASE-LR (1310 nm), 100Gbps: 100GBASE-, atau 400GBASE- untuk 400 Gbps Ethernet. LR4 LR4
Koneksi yang di-host	50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps, dan 25 Gbps.	Bekerja dengan mitra dalam Program AWS Direct Connect Mitra untuk menghubungkan router dari pusat data, kantor, atau lingkungan colocation Anda ke suatu AWS Direct Connect lokasi. Hanya partner tertentu yang menyediakan koneksi dengan kapasitas lebih tinggi.

Untuk koneksi AWS Direct Connect dengan bandwidth 1 Gbps atau lebih tinggi, pastikan jaringan Anda memenuhi persyaratan berikut:

- Jaringan Anda harus menggunakan serat mode tunggal dengan transceiver 1000BASE-LX (1310 nm) untuk 1 gigabit Ethernet, transceiver 10GBASE-LR (1310 nm) untuk 10 gigabit, 100GBASE- untuk 100 gigabit Ethernet, atau 400GBASE- untuk 400 Gbps Ethernet. LR4 LR4
- Bergantung pada titik akhir AWS Direct Connect yang melayani koneksi Anda, negosiasi otomatis perangkat lokal mungkin perlu diaktifkan atau dinonaktifkan untuk koneksi khusus apa pun. Jika antarmuka virtual tetap down saat koneksi Direct Connect aktif, lihatPemecahan masalah lapisan 2 (tautan data).
- Enkapsulasi VLAN 802.1Q harus didukung di seluruh koneksi, termasuk perangkat perantara.
- Perangkat Anda harus mendukung Border Gateway Protocol (BGP) dan otentikasi MD5 BGP.
- (Opsional) Anda dapat mengonfigurasi Deteksi Penerusan Dua Arah (BFD) pada jaringan Anda. BFD asinkron secara otomatis diaktifkan untuk setiap antarmuka virtual. AWS Direct Connect Ini secara otomatis diaktifkan untuk antarmuka virtual Direct Connect, tetapi tidak berlaku sampai Anda mengkonfigurasinya di router Anda. Untuk informasi selengkapnya, lihat Mengaktifkan BFD untuk koneksi Direct Connect.

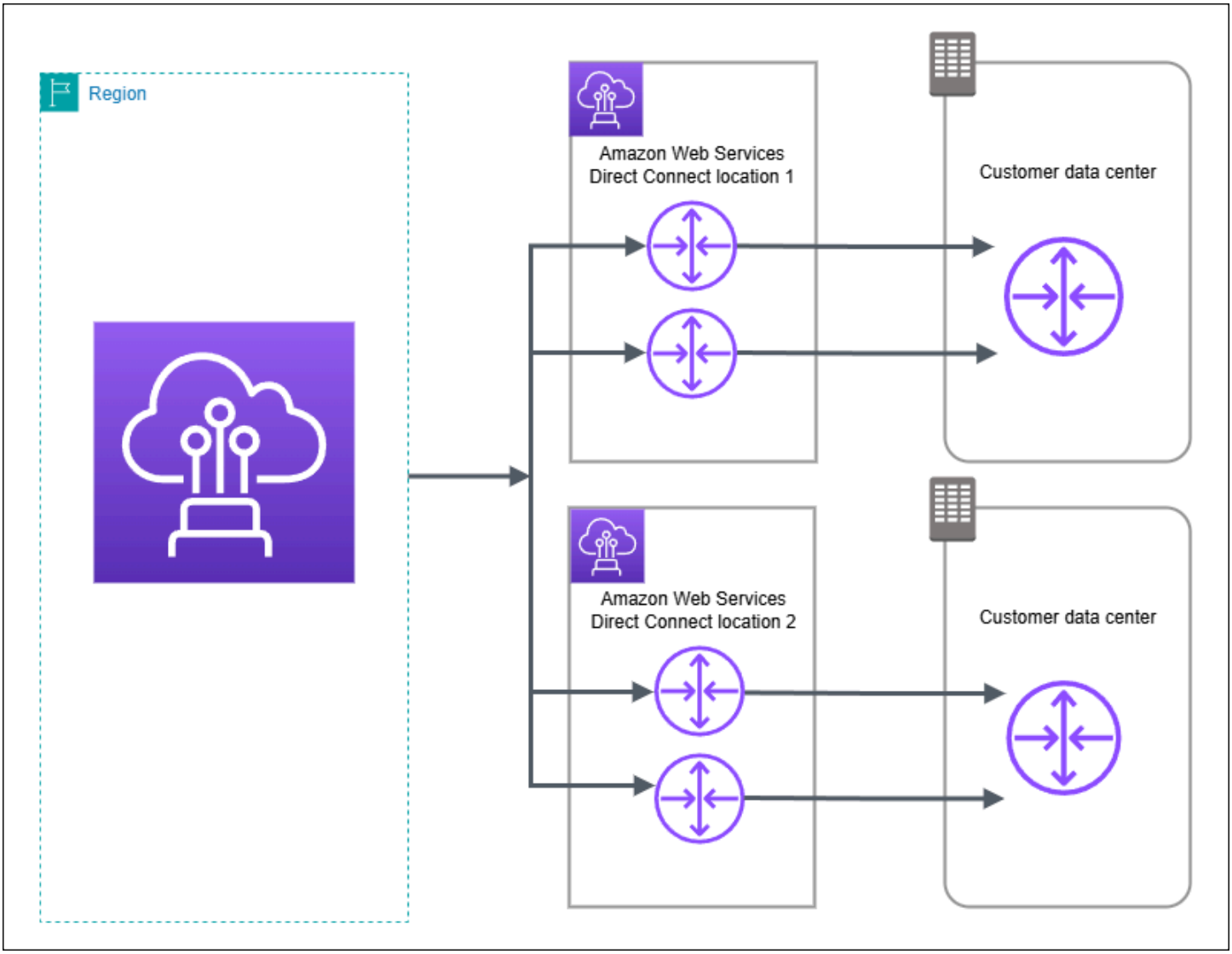
Pastikan Anda memiliki informasi berikut sebelum memulai konfigurasi:

- Model ketahanan yang ingin Anda gunakan.
- Kecepatan, lokasi, dan partner untuk semua koneksi Anda.

  Anda hanya membutuhkan kecepatan untuk satu koneksi.

Ketahanan maksimum

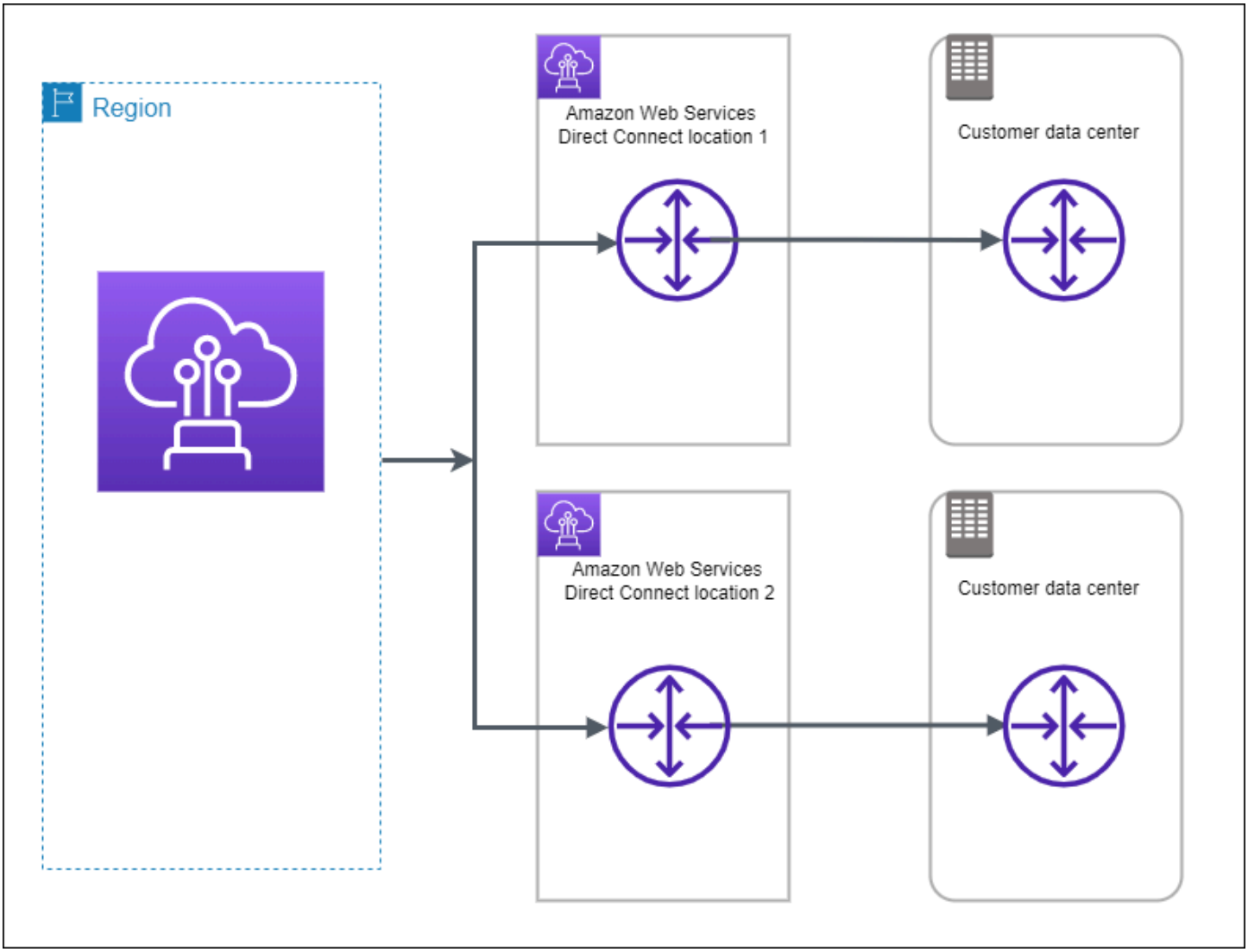
Anda dapat mencapai ketahanan maksimum untuk beban kerja kritis dengan menggunakan koneksi terpisah yang berakhir pada perangkat terpisah di lebih dari satu lokasi (seperti yang ditampilkan pda gambar berikut). Model ini memberikan ketahanan pada perangkat, konektivitas, dan kegagalan lokasi lengkap. Gambar berikut menunjukkan kedua koneksi dari setiap pusat data pelanggan menuju ke AWS Direct Connect lokasi yang sama. Secara opsionla, Anda dapat membuat setiap koneksi dari pusat data pelanggan mengarah ke lokasi yang berbeda.



Untuk prosedur penggunaan AWS Direct Connect Resiliency Toolkit untuk mengonfigurasi model ketahanan maksimum, lihat. Konfigurasikan ketahanan maksimum

Ketahanan tinggi

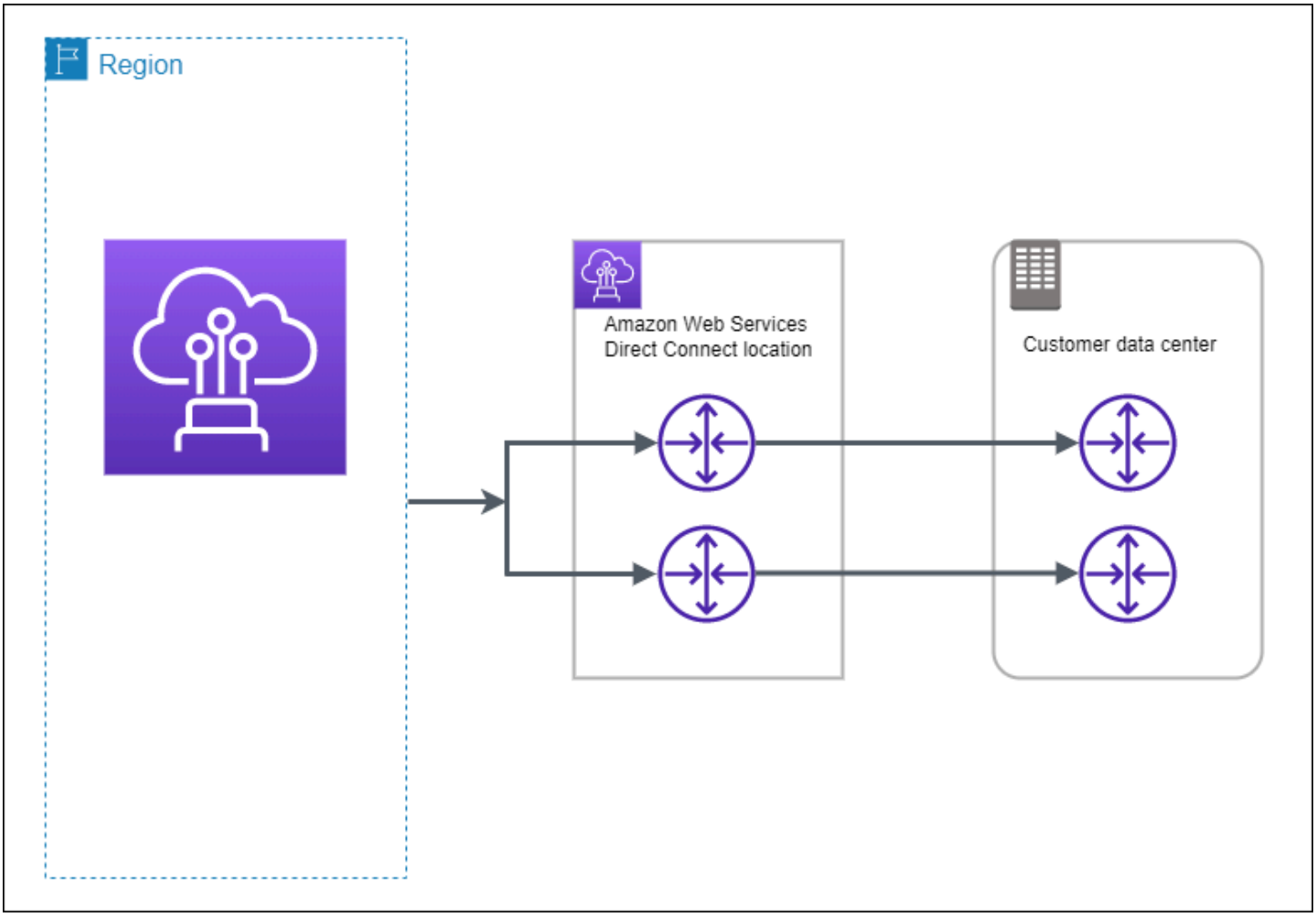
Anda dapat mencapai ketahanan tinggi untuk beban kerja kritis dengan menggunakan dua koneksi tunggal ke beberapa lokasi (seperti yang ditampilkan pada gambar berikut). Model ini memberikan ketahanan terhadap kegagalan konektivitas yang disebabkan oleh pemotongan serat atau kegagalan perangkat. Ini juga membantu mencegah kegagalan lokasi lengkap.



Untuk prosedur penggunaan AWS Direct Connect Resiliency Toolkit untuk mengonfigurasi model ketahanan tinggi, lihat. Konfigurasikan ketahanan tinggi

Pengembangan dan pengujian

Anda dapat mencapai ketahanan pengembangan dan pengujian untuk beban kerja kritis dengan menggunakan koneksi terpisah yang berakhir pada perangkat terpisah di satu lokasi (seperti yang ditampilkan pda gambar berikut). Model ini memberikan ketahanan terhadap kegagalan perangkat, tetapi tidak memberikan ketahanan terhadap kegagalan lokasi.



Untuk prosedur penggunaan AWS Direct Connect Resiliency Toolkit untuk mengonfigurasi model ketahanan maksimum, lihat. Konfigurasikan pengembangan dan uji ketahanan

Klasik

Pilih Klasik jika Anda memiliki koneksi yang ada.

Prosedur berikut menunjukkan skenario umum untuk menyiapkan dengan koneksi AWS Direct Connect .

Prasyarat

Untuk koneksi AWS Direct Connect dengan kecepatan port 1 Gbps atau lebih tinggi, pastikan jaringan Anda memenuhi persyaratan berikut:

- Jaringan Anda harus menggunakan serat mode tunggal dengan transceiver 1000BASE-LX (1310 nm) untuk 1 gigabit Ethernet, transceiver 10GBASE-LR (1310 nm) untuk 10 gigabit, 100GBASE- untuk 100 gigabit Ethernet, atau 400GBASE- untuk 400 Gbps Ethernet. LR4 LR4
- Bergantung pada titik akhir AWS Direct Connect yang melayani koneksi Anda, negosiasi otomatis perangkat lokal mungkin perlu diaktifkan atau dinonaktifkan untuk koneksi khusus apa pun. Jika antarmuka virtual tetap down saat koneksi Direct Connect aktif, lihatPemecahan masalah lapisan 2 (tautan data).
- Enkapsulasi VLAN 802.1Q harus didukung di seluruh koneksi, termasuk perangkat perantara.
- Perangkat Anda harus mendukung Border Gateway Protocol (BGP) dan otentikasi MD5 BGP.
- (Opsional) Anda dapat mengonfigurasi Deteksi Penerusan Dua Arah (BFD) pada jaringan Anda. BFD asinkron secara otomatis diaktifkan untuk setiap antarmuka virtual. AWS Direct Connect Ini secara otomatis diaktifkan untuk antarmuka virtual Direct Connect, tetapi tidak berlaku sampai Anda mengkonfigurasinya di router Anda. Untuk informasi selengkapnya, lihat Mengaktifkan BFD untuk koneksi Direct Connect.

Untuk prosedur menggunakan AWS Direct Connect Resiliency Toolkit untuk mengkonfigurasi koneksi Klasik, lihat. Konfigurasikan koneksi Klasik

AWS Direct Connect FailoverTest

Gunakan AWS Direct Connect Resiliency Toolkit untuk memverifikasi rute lalu lintas dan rute tersebut memenuhi persyaratan ketahanan Anda.

Untuk prosedur penggunaan AWS Direct Connect Resiliency Toolkit untuk melakukan pengujian failover, lihat. Tes failover Direct Connect

Gunakan AWS Direct Connect Resiliency Toolkit untuk mengonfigurasi AWS Direct Connect ketahanan maksimum

Dalam contoh ini, AWS Direct Connect Resiliency Toolkit digunakan untuk mengonfigurasi model ketahanan maksimum

Tugas

- Langkah 1: Mendaftar untuk AWS
- Langkah 2: Mengonfigurasi model ketahanan

Langkah 1: Mendaftar untuk AWS

Untuk menggunakannya AWS Direct Connect, Anda memerlukan AWS akun jika Anda belum memilikinya.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimkan email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Langkah 2: Mengonfigurasi model ketahanan

Untuk mengonfigurasi model ketahanan maksimum

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Koneksi, lalu pilih Buat koneksi.
3. Di bawah Jenis pemesanan koneksi, pilih Wizard koneksi.
4. Di bawah Tingkat ketahanan, pilih Ketahanan Maksimum, lalu pilih Selanjutnya.
5. Pada panel Konfigurasi koneksi, di bawah Pengaturan koneksi, lakukan hal berikut:

   a. Untuk Bandwidth, pilih bandwidth koneksi khusus.

      Bandwidth ini berlaku untuk semua koneksi yang dibuat.

   b. Untuk penyedia layanan lokasi pertama, pilih AWS Direct Connect lokasi yang sesuai untuk koneksi khusus.

   c. Jika berlaku, untuk Sub lokasi pertama, pilih lantai yang paling dekat dengan Anda atau penyedia jaringan Anda. Opsi ini hanya tersedia jika lokasi memiliki ruang meet-me (MMRs) di beberapa lantai gedung.

   d. Jika Anda memilih Lainnya untuk Penyedia location service pertama, untuk Nama penyedia lain, masukkan nama partner yang Anda gunakan.

   e. Untuk penyedia layanan lokasi kedua, pilih AWS Direct Connect lokasi yang sesuai.

   f. Jika berlaku, untuk Sub lokasi kedua, pilih lantai yang paling dekat dengan Anda atau penyedia jaringan Anda. Opsi ini hanya tersedia jika lokasi memiliki ruang meet-me (MMRs) di beberapa lantai gedung.

   g. Jika Anda memilih Lainnya untuk Penyedia location service kedua, untuk Nama penyedia lain, masukkan nama partner yang Anda gunakan.

   h. (Opsional) Tambahkan atau hapus tanda.

      [Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

      - Untuk Kunci, masukkan nama kunci.
      - Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

6. Pilih Selanjutnya.
7. Periksa koneksi Anda, lalu pilih Lanjutkan.

   Jika Anda LOAs siap, Anda dapat memilih Unduh LOA, dan kemudian klik Lanjutkan.

   Diperlukan waktu hingga 72 jam AWS untuk meninjau permintaan Anda dan menyediakan port untuk koneksi Anda. Selama waktu ini, Anda mungkin menerima email berisi permintaan untuk informasi lebih lanjut tentang kasus penggunaan atau lokasi yang ditentukan. Email dikirim ke alamat email yang Anda gunakan saat mendaftar AWS. Anda harus merespons dalam waktu 7 hari atau koneksi dihapus.

Langkah 3: Membuat antarmuka virtual

Anda dapat membuat antarmuka virtual privat untuk terhubung ke VPC. Atau, Anda dapat membuat antarmuka virtual publik untuk terhubung ke AWS layanan publik yang tidak ada dalam VPC. Ketika membuat antarmuka virtual privat untuk VPC, Anda memerlukan antarmuka virtual privat untuk setiap VPC yang terhubung dengan Anda. Misalnya, Anda memerlukan tiga antarmuka virtual pribadi untuk terhubung ke tiga VPCs.

Sebelum memulai, pastikan Anda memiliki informasi berikut:

Sumber Daya	Informasi yang diperlukan
Koneksi	Grup agregasi AWS Direct Connect koneksi atau tautan (LAG) tempat Anda membuat antarmuka virtual.
Nama antarmuka virtual	Nama untuk antarmuka virtual.
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID AWS akun dari akun lain.
(Antarmuka virtual privat saja) Koneksi	Untuk menghubungkan ke VPC di AWS Wilayah yang sama, Anda memerlukan gateway pribadi virtual untuk VPC Anda. ASN untuk sisi Amazon sesi BGP diwarisi dari virtual private gateway. Bila Anda membuat virtual private gateway, Anda dapat menentukan ASN privat Anda sendiri. Jika

Sumber Daya	Informasi yang diperlukan
	tidak, Amazon menyediakan ASN default. Untuk informasi selengkapnya, lihat Membuat Virtual Private Gateway di Panduan Pengguna Amazon VPC. Untuk terhubung ke VPC melalui gateway Direct Connect, Anda memerlukan gateway Direct Connect. Untuk informasi selengkapnya, lihat Gateway Direct Connect.
VLAN	Tanda virtual local area network (VLAN) unik yang belum digunakan pada koneksi Anda. Nilai harus antara 1 hingga 4094 dan harus sesuai dengan standar Ethernet 802.1Q. Tanda ini diperlukan untuk lalu lintas yang melintasi koneksi AWS Direct Connect . Jika Anda memiliki koneksi yang di-host, AWS Direct Connect Mitra Anda memberikan nilai ini. Anda tidak dapat mengubah nilai setelah Anda membuat antarmuka virtual.

Sumber Daya	Informasi yang diperlukan

Alamat IP rekan	Antarmuka virtual dapat mendukung sesi peering BGP untuk IPv4, IPv6, atau salah satu dari masing-masing (dual-stack). Jangan gunakan Elastic IPs (EIPs) atau Bawa alamat IP Anda sendiri (BYOIP) dari Amazon Pool untuk membuat antarmuka virtual publik. Anda tidak dapat membuat beberapa sesi BGP untuk keluarga pengalamatan IP yang sama pada antarmuka virtual yang sama. Cakupan alamat IP ditetapkan untuk setiap akhir antarmuka virtual untuk sesi peering BGP.
	
	• IPv4:
	  • (Hanya antarmuka virtual publik) Anda harus menentukan IPv4 alamat publik unik yang Anda miliki. Nilai dapat menjadi salah satu dari yang berikut:
	  • CIDR milik pelanggan IPv4
	
	Ini dapat berupa publik IPs (milik pelanggan atau disediakan oleh AWS), tetapi subnet mask yang sama harus digunakan untuk IP rekan Anda dan IP peer router. AWS Misalnya, jika Anda mengalokasikan `/31` rentang, seperti`203.0.113.0/31` , Anda dapat menggunakan `203.0.113.0` untuk IP rekan Anda dan `203.0.113.1` untuk IP AWS rekan. Atau, jika Anda mengalokasikan `/24` rentang, seperti`198.51.100.0/24` , Anda dapat menggunakan `198.51.100.0` untuk IP rekan Anda dan `198.51.100.20` untuk IP AWS rekan.
	  • Rentang IP yang dimiliki oleh AWS Direct Connect Mitra atau ISP Anda, bersama dengan otorisasi LOA-CFA
	  • AWS-Disediakan /31 CIDR. Hubungi AWS Support untuk meminta IPv4 CIDR publik (dan memberikan kasus penggunaan dalam permintaan Anda)
	
	Note
	Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk IPv4 alamat publik AWS yang disediakan.

Sumber Daya	Informasi yang diperlukan
	• (Hanya antarmuka virtual pribadi) Amazon dapat menghasilkan IPv4 alamat pribadi untuk Anda. Jika Anda menentukan sendiri, pastikan bahwa Anda menentukan pribadi CIDRs untuk antarmuka router Anda dan antarmuka AWS Direct Connect saja. Misalnya, jangan tentukan alamat IP lain dari jaringan lokal Anda. Mirip dengan antarmuka virtual publik, subnet mask yang sama harus digunakan untuk IP peer Anda dan IP peer AWS router. Misalnya, jika Anda mengalokasikan `/30` rentang, seperti`192.168.0.0/30` , Anda dapat menggunakan `192.168.0.1` untuk IP rekan Anda dan `192.168.0.2` untuk IP AWS rekan. • IPv6: Amazon secara otomatis mengalokasikan Anda IPv6 /125 CIDR. Anda tidak dapat menentukan IPv6 alamat rekan Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan berakhir atau. IPv4 IPv6
Informasi BGP	• Border Gateway Protocol (BGP) Autonomous System Number (ASN) publik atau privat untuk sisi sesi BGP Anda. Jika Anda menggunakan ASN publik, Anda harus memilikinya. Jika Anda menggunakan ASN pribadi, Anda dapat mengatur nilai ASN kustom. Untuk ASN 16-bit, nilainya harus berada dalam rentang 64512 hingga 65534. Untuk ASN 32-bit, nilainya harus dalam kisaran 1 hingga 2147483647. Penambahan Autonomous System (AS) tidak bekerja jika Anda menggunakan ASN privat untuk antarmuka virtual publik. • AWS memungkinkan secara MD5 default. Anda tidak dapat mengubah opsi ini. • Kunci otentikasi MD5 BGP. Anda dapat memberikan kunci milik Anda sendiri, atau Anda dapat membiarkan Amazon menghasilkannya untuk Anda.

Sumber Daya	Informasi yang diperlukan

(Antarmuka virtual publik saja) Prefiks yang ingin Anda iklankan	IPv4 Rute umum atau IPv6 rute untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: IPv4 CIDR dapat tumpang tindih dengan IPv4 CIDR publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari berikut ini benar:
	  • CIDRs Mereka berasal dari berbagai AWS daerah. Pastikan bahwa Anda menerapkan tanda komunitas BGP pada prefiks publik.
	  • Anda menggunakan AS_PATH ketika Anda memiliki ASN publik dalam konfigurasi. active/passive
	  Untuk informasi selengkapnya, lihat Kebijakan perutean dan komunitas BGP.
	• Melalui antarmuka virtual publik Direct Connect, Anda dapat menentukan panjang awalan dari /1 hingga /32 untuk IPv4 dan dari /1 hingga /64 untuk. IPv6
	• Anda dapat menambahkan awalan tambahan ke VIF publik yang ada dan mengiklankannya dengan menghubungi dukungan.AWS Dalam kasus dukungan Anda, berikan daftar awalan CIDR tambahan yang ingin Anda tambahkan ke VIF publik dan beriklan.

(Hanya antarmuka virtual pribadi dan transit) Jumbo frame	Unit transmisi maksimum (MTU) paket over. AWS Direct Connect Default-n ya adalah 1500. Mengatur MTU antarmuka virtual ke 9001 (bingkai jumbo) dapat menyebabkan pembaruan untuk koneksi fisik yang mendasari jika itu tidak diperbarui untuk mendukung bingkai jumbo. Memperbarui koneksi mengganggu konektivitas jaringan untuk semua antarmuka virtual yang terkait dengan koneksi hingga 30 detik. Bingkai jumbo hanya berlaku untuk rute yang disebarkan dari. AWS Direct Connect Jika Anda menambahkan rute statis ke tabel rute yang mengarah ke virtual private gateway, lalu lintas diarahkan melalui rute statis dikirim menggunakan 1500 MTU. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di AWS Direct Connect konsol dan temukan bingkai Jumbo yang mampu pada antarmuka virtual Halaman konfigurasi umum.

Jika awalan publik Anda atau ASNs milik ISP atau operator jaringan, kami meminta informasi tambahan dari Anda. Ini bisa berupa dokumen menggunakan kop surat resmi perusahaan, atau email dari nama domain perusahaan yang memverifikasi bahwa jaringan prefix/ASN dapat digunakan oleh Anda.

Saat Anda membuat antarmuka virtual publik, diperlukan waktu hingga 72 jam AWS untuk meninjau dan menyetujui permintaan Anda.

Untuk menyediakan antarmuka virtual publik ke layanan non-VPC

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Publik.
5. Di bawah Pengaturan antarmuka virtual publik, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.
   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.
   c. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).
   d. Untuk BGP ASN, masukkan Autonomous System Number (ASN) Border Gateway Protocol (BGP) dari gateway Anda.

      Nilai yang valid adalah 1-2147483647.
6. Di bawah Pengaturan tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

      - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

      [IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

   b. Untuk memberikan kunci BGP Anda sendiri, masukkan kunci MD5 BGP Anda.

Jika Anda tidak memasukkan nilai, kami menghasilkan kunci BGP.

c. Untuk mengiklankan awalan ke Amazon, untuk Awalan yang ingin Anda iklankan, masukkan alamat tujuan IPv4 CIDR (dipisahkan dengan koma) ke mana lalu lintas harus diarahkan melalui antarmuka virtual.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.

Untuk menyediakan antarmuka virtual privat bagi VPC

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Privat.
5. Di bawah Pengaturan antarmuka virtual privat, lakukan hal berikut:

a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.

b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.

c. Untuk Jenis gateway, pilih Virtual private gateway, atau Gateway Direct Connect.

d. Untuk pemilik antarmuka virtual, pilih AWS Akun lain, lalu masukkan AWS akun.

e. Untuk Virtual private gateway, pilih virtual private gateway yang akan digunakan untuk antarmuka ini.

f. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).

g. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

Nilai yang valid adalah 1 hingga 2147483647.

6. Di bawah Pengaturan Tambahan, lakukan hal berikut:

a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

   [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

   - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
   - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

   > **Important**
   >
   > Saat mengonfigurasi antarmuka virtual AWS Direct Connect, Anda dapat menentukan alamat IP Anda sendiri menggunakan RFC 1918, menggunakan skema pengalamatan lain, atau memilih alamat IPv4 /29 CIDR yang AWS ditetapkan yang dialokasikan dari rentang RFC 3927 169.254.0.0/16 Link-Local untuk konektivitas. IPv4 point-to-point point-to-pointKoneksi ini harus digunakan secara eksklusif untuk mengintip eBGP antara router gateway pelanggan Anda dan titik akhir Direct Connect. Untuk tujuan lalu lintas atau tunneling VPC, seperti AWS Site-to-Site Private IP VPN, atau Transit Gateway Connect, AWS merekomendasikan penggunaan antarmuka loopback atau LAN pada router gateway pelanggan Anda sebagai alamat sumber atau tujuan alih-alih koneksi. point-to-point
   >
   > - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
   > - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat IPv4 Lokal-Tautan.

   [IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk mengubah maximum transmission unit (MTU) dari 1500 (default) menjadi 9001 (bingkai jumbo), pilih MTU Jumbo (MTU ukuran 9001).

c. (Opsional) Di bawah Aktifkan SiteLink, pilih Diaktifkan untuk mengaktifkan konektivitas langsung antara titik kehadiran Direct Connect.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.

Langkah 4: Memverifikasi konfigurasi ketahanan antarmuka virtual

Setelah Anda membuat antarmuka virtual ke AWS Cloud atau ke Amazon VPC, lakukan pengujian failover antarmuka virtual untuk memverifikasi bahwa konfigurasi Anda memenuhi persyaratan ketahanan Anda. Untuk informasi selengkapnya, lihat the section called “Tes failover Direct Connect”.

Langkah 5: Memverifikasi konektivitas antarmuka virtual

Setelah Anda membuat antarmuka virtual ke AWS Cloud atau ke Amazon VPC, Anda dapat memverifikasi koneksi AWS Direct Connect Anda menggunakan prosedur berikut.

Untuk memverifikasi koneksi antarmuka virtual Anda ke AWS Cloud

- Jalankan `traceroute` dan verifikasi bahwa AWS Direct Connect pengenal ada di jejak jaringan.

Untuk memverifikasi koneksi antarmuka virtual Anda ke Amazon VPC

1. Menggunakan AMI yang dapat di-ping, seperti AMI Amazon Linux, luncurkan EC2 instance ke VPC yang dilampirkan ke gateway pribadi virtual Anda. Amazon Linux AMIs tersedia di tab Mulai Cepat saat Anda menggunakan wizard peluncuran instans di EC2 konsol Amazon. Untuk informasi selengkapnya, lihat Meluncurkan Instance di Panduan EC2 Pengguna Amazon. Pastikan bahwa grup keamanan yang terkait dengan instans mencakup aturan yang mengizinkan lalu lintas ICMP masuk (untuk permintaan ping).
2. Setelah instance berjalan, dapatkan IPv4 alamat pribadinya (misalnya, 10.0.0.4). EC2 Konsol Amazon menampilkan alamat sebagai bagian dari detail instance.
3. Ping IPv4 alamat pribadi dan dapatkan tanggapan.

Gunakan AWS Direct Connect Resiliency Toolkit untuk mengonfigurasi AWS Direct Connect ketahanan tinggi

Dalam contoh ini, AWS Direct Connect Resiliency Toolkit digunakan untuk mengonfigurasi model ketahanan tinggi

Tugas

- Langkah 1: Mendaftar untuk AWS
- Langkah 2: Mengonfigurasi model ketahanan
- Langkah 3: Membuat antarmuka virtual
- Langkah 4: Memverifikasi konfigurasi ketahanan antarmuka virtual
- Langkah 5: Memverifikasi konektivitas antarmuka virtual

Langkah 1: Mendaftar untuk AWS

Untuk menggunakannya AWS Direct Connect, Anda memerlukan AWS akun jika Anda belum memilikinya.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Langkah 2: Mengonfigurasi model ketahanan

Untuk mengonfigurasi model ketahanan tinggi

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Koneksi, lalu pilih Buat koneksi.
3. Di bawah Jenis pemesanan koneksi, pilih Wizard koneksi.
4. Di bawah Tingkat ketahanan, pilih Ketahanan Tinggi, lalu pilih Selanjutnya.
5. Pada panel Konfigurasi koneksi, di bawah Pengaturan koneksi, lakukan hal berikut:

   a. Untuk Bandwidth, pilih bandwidth koneksi.

      Bandwidth ini berlaku untuk semua koneksi yang dibuat.

   b. Untuk penyedia layanan lokasi pertama, pilih AWS Direct Connect lokasi yang sesuai.

   c. Jika berlaku, untuk Sub lokasi pertama, pilih lantai yang paling dekat dengan Anda atau penyedia jaringan Anda. Opsi ini hanya tersedia jika lokasi memiliki ruang meet-me (MMRs) di beberapa lantai gedung.

   d. Jika Anda memilih Lainnya untuk Penyedia location service pertama, untuk Nama penyedia lain, masukkan nama partner yang Anda gunakan.

   e. Untuk penyedia layanan lokasi kedua, pilih AWS Direct Connect lokasi yang sesuai.

f. Jika berlaku, untuk Sub lokasi kedua, pilih lantai yang paling dekat dengan Anda atau penyedia jaringan Anda. Opsi ini hanya tersedia jika lokasi memiliki ruang meet-me (MMRs) di beberapa lantai gedung.

g. Jika Anda memilih Lainnya untuk Penyedia location service kedua, untuk Nama penyedia lain, masukkan nama partner yang Anda gunakan.

h. (Opsional) Tambahkan atau hapus tanda.

   [Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

   - Untuk Kunci, masukkan nama kunci.
   - Untuk Nilai, masukkan nilai kunci.

   [Menghapus tanda] Di samping tanda, pilih Hapus tanda.

6. Pilih Selanjutnya.
7. Periksa koneksi Anda, lalu pilih Lanjutkan.

   Jika Anda LOAs siap, Anda dapat memilih Unduh LOA, dan kemudian klik Lanjutkan.

   Diperlukan waktu hingga 72 jam AWS untuk meninjau permintaan Anda dan menyediakan port untuk koneksi Anda. Selama waktu ini, Anda mungkin menerima email berisi permintaan untuk informasi lebih lanjut tentang kasus penggunaan atau lokasi yang ditentukan. Email dikirim ke alamat email yang Anda gunakan saat mendaftar AWS. Anda harus merespons dalam waktu 7 hari atau koneksi dihapus.

Langkah 3: Membuat antarmuka virtual

Anda dapat membuat antarmuka virtual privat untuk terhubung ke VPC. Atau, Anda dapat membuat antarmuka virtual publik untuk terhubung ke AWS layanan publik yang tidak ada dalam VPC. Ketika membuat antarmuka virtual privat untuk VPC, Anda memerlukan antarmuka virtual privat untuk setiap VPC yang terhubung dengan Anda. Misalnya, Anda memerlukan tiga antarmuka virtual pribadi untuk terhubung ke tiga VPCs.

Sebelum memulai, pastikan Anda memiliki informasi berikut:

Sumber Daya	Informasi yang diperlukan
Koneksi	Grup agregasi AWS Direct Connect koneksi atau tautan (LAG) tempat Anda membuat antarmuka virtual.
Nama antarmuka virtual	Nama untuk antarmuka virtual.
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID AWS akun dari akun lain.
(Antarmuka virtual privat saja) Koneksi	Untuk menghubungkan ke VPC di AWS Wilayah yang sama, Anda memerlukan gateway pribadi virtual untuk VPC Anda. ASN untuk sisi Amazon sesi BGP diwarisi dari virtual private gateway. Bila Anda membuat virtual private gateway, Anda dapat menentukan ASN privat Anda sendiri. Jika tidak, Amazon menyediakan ASN default. Untuk informasi selengkapnya, lihat Membuat Virtual Private Gateway di Panduan Pengguna Amazon VPC. Untuk terhubung ke VPC melalui gateway Direct Connect, Anda memerlukan gateway Direct Connect. Untuk informasi selengkapnya, lihat Gateway Direct Connect.
VLAN	Tanda virtual local area network (VLAN) unik yang belum digunakan pada koneksi Anda. Nilai harus antara 1 hingga 4094 dan harus sesuai dengan standar Ethernet 802.1Q. Tanda ini diperlukan untuk lalu lintas yang melintasi koneksi AWS Direct Connect . Jika Anda memiliki koneksi yang di-host, AWS Direct Connect Mitra Anda memberikan nilai ini. Anda tidak dapat mengubah nilai setelah Anda membuat antarmuka virtual.
Alamat IP rekan	Antarmuka virtual dapat mendukung sesi peering BGP untuk IPv4, IPv6, atau salah satu dari masing-masing (dual-stack). Jangan gunakan Elastic IPs (EIPs) atau Bawa alamat IP Anda sendiri (BYOIP) dari Amazon Pool untuk membuat antarmuka virtual publik. Anda tidak dapat membuat beberapa sesi BGP untuk keluarga pengalamatan IP yang sama pada antarmuka virtual yang sama. Cakupan alamat IP ditetapkan untuk setiap akhir antarmuka virtual untuk sesi peering BGP.

Sumber Daya	Informasi yang diperlukan
	• IPv4: • (Hanya antarmuka virtual publik) Anda harus menentukan IPv4 alamat publik unik yang Anda miliki. Nilai dapat menjadi salah satu dari yang berikut: • CIDR milik pelanggan IPv4 Ini dapat berupa publik IPs (milik pelanggan atau disediakan oleh AWS), tetapi subnet mask yang sama harus digunakan untuk IP rekan Anda dan IP peer router. AWS Misalnya, jika Anda mengalokasikan `/31` rentang, seperti`203.0.113.0/31` , Anda dapat menggunak an `203.0.113.0` untuk IP rekan Anda dan `203.0.113.1` untuk IP AWS rekan. Atau, jika Anda mengalokasikan `/24` rentang, seperti`198.51.100.0/24` , Anda dapat menggunakan `198.51.10 0.10` untuk IP rekan Anda dan `198.51.100.20` untuk IP AWS rekan. • Rentang IP yang dimiliki oleh AWS Direct Connect Mitra atau ISP Anda, bersama dengan otorisasi LOA-CFA • AWS-Disediakan /31 CIDR. Hubungi AWS Support untuk meminta IPv4 CIDR publik (dan memberikan kasus penggunaan dalam permintaan Anda) **Note** Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk IPv4 alamat publik AWS yang disediakan. • (Hanya antarmuka virtual pribadi) Amazon dapat menghasilkan IPv4 alamat pribadi untuk Anda. Jika Anda menentukan sendiri, pastikan bahwa Anda menentukan pribadi CIDRs untuk antarmuka router Anda dan antarmuka AWS Direct Connect saja. Misalnya, jangan tentukan alamat IP lain dari jaringan lokal Anda. Mirip dengan antarmuka virtual publik, subnet mask yang sama harus digunakan untuk IP peer Anda dan IP peer AWS router. Misalnya, jika Anda mengalokasikan `/30` rentang,

Sumber Daya	Informasi yang diperlukan
	seperti`192.168.0.0/30` , Anda dapat menggunakan `192.168.0.1` untuk IP rekan Anda dan `192.168.0.2` untuk IP AWS rekan. • IPv6: Amazon secara otomatis mengalokasikan Anda IPv6 /125 CIDR. Anda tidak dapat menentukan IPv6 alamat rekan Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan berakhir atau. IPv4 IPv6
Informasi BGP	• Border Gateway Protocol (BGP) Autonomous System Number (ASN) publik atau privat untuk sisi sesi BGP Anda. Jika Anda menggunakan ASN publik, Anda harus memilikinya. Jika Anda menggunakan ASN pribadi, Anda dapat mengatur nilai ASN kustom. Untuk ASN 16-bit, nilainya harus berada dalam rentang 64512 hingga 65534. Untuk ASN 32-bit, nilainya harus dalam kisaran 1 hingga 2147483647. Penambahan Autonomous System (AS) tidak bekerja jika Anda menggunakan ASN privat untuk antarmuka virtual publik. • AWS memungkinkan secara MD5 default. Anda tidak dapat mengubah opsi ini. • Kunci otentikasi MD5 BGP. Anda dapat memberikan kunci milik Anda sendiri, atau Anda dapat membiarkan Amazon menghasilkannya untuk Anda.

Sumber Daya	Informasi yang diperlukan

(Antarmuka virtual publik saja) Prefiks yang ingin Anda iklankan	IPv4 Rute umum atau IPv6 rute untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: IPv4 CIDR dapat tumpang tindih dengan IPv4 CIDR publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari berikut ini benar:
	  • CIDRs Mereka berasal dari berbagai AWS daerah. Pastikan bahwa Anda menerapkan tanda komunitas BGP pada prefiks publik.
	  • Anda menggunakan AS_PATH ketika Anda memiliki ASN publik dalam konfigurasi. active/passive
	  Untuk informasi selengkapnya, lihat Kebijakan perutean dan komunitas BGP.
	• Melalui antarmuka virtual publik Direct Connect, Anda dapat menentukan panjang awalan dari /1 hingga /32 untuk IPv4 dan dari /1 hingga /64 untuk. IPv6
	• Anda dapat menambahkan awalan tambahan ke VIF publik yang ada dan mengiklankannya dengan menghubungi dukungan.AWS Dalam kasus dukungan Anda, berikan daftar awalan CIDR tambahan yang ingin Anda tambahkan ke VIF publik dan beriklan.

(Hanya antarmuka virtual pribadi dan transit) Frame jumbo	Unit transmisi maksimum (MTU) paket over. AWS Direct Connect Default-n ya adalah 1500. Mengatur MTU antarmuka virtual ke 9001 (bingkai jumbo) dapat menyebabkan pembaruan untuk koneksi fisik yang mendasari jika itu tidak diperbarui untuk mendukung bingkai jumbo. Memperbarui koneksi mengganggu konektivitas jaringan untuk semua antarmuka virtual yang terkait dengan koneksi hingga 30 detik. Bingkai jumbo hanya berlaku untuk rute yang disebarkan dari. AWS Direct Connect Jika Anda menambahkan rute statis ke tabel rute yang mengarah ke virtual private gateway, lalu lintas diarahkan melalui rute statis dikirim menggunakan 1500 MTU. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di AWS Direct Connect konsol dan temukan bingkai Jumbo yang mampu pada antarmuka virtual Halaman konfigurasi umum.

Jika awalan publik Anda atau ASNs milik ISP atau operator jaringan, AWS mintalah informasi tambahan dari Anda. Ini bisa berupa dokumen menggunakan kop surat resmi perusahaan, atau email dari nama domain perusahaan yang memverifikasi bahwa jaringan prefix/ASN dapat digunakan oleh Anda.

Saat Anda membuat antarmuka virtual publik, diperlukan waktu hingga 72 jam AWS untuk meninjau dan menyetujui permintaan Anda.

Untuk menyediakan antarmuka virtual publik ke layanan non-VPC

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Publik.
5. Di bawah Pengaturan antarmuka virtual publik, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.
   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.
   c. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).
   d. Untuk BGP ASN, masukkan Autonomous System Number (ASN) Border Gateway Protocol (BGP) dari gateway Anda.

      Nilai yang valid adalah 1-2147483647.
6. Di bawah Pengaturan tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

      - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

      [IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

   b. Untuk memberikan kunci BGP Anda sendiri, masukkan kunci MD5 BGP Anda.

Jika Anda tidak memasukkan nilai, kami menghasilkan kunci BGP.

c. Untuk mengiklankan awalan ke Amazon, untuk Awalan yang ingin Anda iklankan, masukkan alamat tujuan IPv4 CIDR (dipisahkan dengan koma) ke mana lalu lintas harus diarahkan melalui antarmuka virtual.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.

Untuk menyediakan antarmuka virtual privat bagi VPC

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Privat.
5. Di bawah Pengaturan antarmuka virtual privat, lakukan hal berikut:

a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.

b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.

c. Untuk Jenis gateway, pilih Virtual private gateway, atau Gateway Direct Connect.

d. Untuk pemilik antarmuka virtual, pilih AWS Akun lain, lalu masukkan AWS akun.

e. Untuk Virtual private gateway, pilih virtual private gateway yang akan digunakan untuk antarmuka ini.

f. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).

g. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

Nilai yang valid adalah 1 hingga 2147483647.

6. Di bawah Pengaturan Tambahan, lakukan hal berikut:

a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

   [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

   - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
   - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

   > **Important**
   >
   > Saat mengonfigurasi antarmuka virtual AWS Direct Connect, Anda dapat menentukan alamat IP Anda sendiri menggunakan RFC 1918, menggunakan skema pengalamatan lain, atau memilih alamat IPv4 /29 CIDR yang AWS ditetapkan yang dialokasikan dari rentang RFC 3927 169.254.0.0/16 Link-Local untuk konektivitas. IPv4 point-to-point point-to-pointKoneksi ini harus digunakan secara eksklusif untuk mengintip eBGP antara router gateway pelanggan Anda dan titik akhir Direct Connect. Untuk tujuan lalu lintas atau tunneling VPC, seperti AWS Site-to-Site Private IP VPN, atau Transit Gateway Connect, AWS merekomendasikan penggunaan antarmuka loopback atau LAN pada router gateway pelanggan Anda sebagai alamat sumber atau tujuan alih-alih koneksi. point-to-point
   >
   > - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
   > - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat IPv4 Lokal-Tautan.

   [IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk mengubah maximum transmission unit (MTU) dari 1500 (default) menjadi 9001 (bingkai jumbo), pilih MTU Jumbo (MTU ukuran 9001).

c. (Opsional) Di bawah Aktifkan SiteLink, pilih Diaktifkan untuk mengaktifkan konektivitas langsung antara titik kehadiran Direct Connect.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.

Langkah 4: Memverifikasi konfigurasi ketahanan antarmuka virtual

Setelah Anda membuat antarmuka virtual ke AWS Cloud atau ke Amazon VPC, lakukan pengujian failover antarmuka virtual untuk memverifikasi bahwa konfigurasi Anda memenuhi persyaratan ketahanan Anda. Untuk informasi selengkapnya, lihat the section called “Tes failover Direct Connect”.

Langkah 5: Memverifikasi konektivitas antarmuka virtual

Setelah Anda membuat antarmuka virtual ke AWS Cloud atau ke Amazon VPC, Anda dapat memverifikasi koneksi AWS Direct Connect Anda menggunakan prosedur berikut.

Untuk memverifikasi koneksi antarmuka virtual Anda ke AWS Cloud

- Jalankan `traceroute` dan verifikasi bahwa AWS Direct Connect pengenal ada di jejak jaringan.

Untuk memverifikasi koneksi antarmuka virtual Anda ke Amazon VPC

1. Menggunakan AMI yang dapat di-ping, seperti AMI Amazon Linux, luncurkan EC2 instance ke VPC yang dilampirkan ke gateway pribadi virtual Anda. Amazon Linux AMIs tersedia di tab Mulai Cepat saat Anda menggunakan wizard peluncuran instans di EC2 konsol Amazon. Untuk informasi selengkapnya, lihat Meluncurkan Instance di Panduan EC2 Pengguna Amazon. Pastikan bahwa grup keamanan yang terkait dengan instans mencakup aturan yang mengizinkan lalu lintas ICMP masuk (untuk permintaan ping).
2. Setelah instance berjalan, dapatkan IPv4 alamat pribadinya (misalnya, 10.0.0.4). EC2 Konsol Amazon menampilkan alamat sebagai bagian dari detail instance.
3. Ping IPv4 alamat pribadi dan dapatkan tanggapan.

Gunakan AWS Direct Connect Resiliency Toolkit AWS Direct Connect untuk mengonfigurasi pengembangan dan pengujian ketahanan

Dalam contoh ini, AWS Direct Connect Resiliency Toolkit digunakan untuk mengonfigurasi model pengembangan dan pengujian ketahanan

Tugas

- Langkah 1: Mendaftar AWS
- Langkah 2: Mengonfigurasi model ketahanan
- Langkah 3: Membuat antarmuka virtual
- Langkah 4: Memverifikasi konfigurasi ketahanan antarmuka virtual
- Langkah 5: Memverifikasi antarmuka virtual

Langkah 1: Mendaftar AWS

Untuk menggunakannya AWS Direct Connect, Anda memerlukan AWS akun jika Anda belum memilikinya.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Langkah 2: Mengonfigurasi model ketahanan

Untuk mengonfigurasi model ketahanan

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Koneksi, lalu pilih Buat koneksi.
3. Di bawah Jenis pemesanan koneksi, pilih Wizard koneksi.
4. Di bawah Tingkat ketahanan, pilih Pengembangan dan pengujian, lalu pilih Selanjutnya.
5. Pada panel Konfigurasi koneksi, di bawah Pengaturan koneksi, lakukan hal berikut:

   a. Untuk Bandwidth, pilih bandwidth koneksi.

      Bandwidth ini berlaku untuk semua koneksi yang dibuat.

   b. Untuk penyedia layanan lokasi pertama, pilih AWS Direct Connect lokasi yang sesuai.

   c. Jika berlaku, untuk Sub lokasi pertama, pilih lantai yang paling dekat dengan Anda atau penyedia jaringan Anda. Opsi ini hanya tersedia jika lokasi memiliki ruang meet-me (MMRs) di beberapa lantai gedung.

   d. Jika Anda memilih Lainnya untuk Penyedia location service pertama, untuk Nama penyedia lain, masukkan nama partner yang Anda gunakan.

   e. (Opsional) Tambahkan atau hapus tanda.

      [Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

6. Pilih Selanjutnya.
7. Periksa koneksi Anda, lalu pilih Lanjutkan.

   Jika Anda LOAs siap, Anda dapat memilih Unduh LOA, dan kemudian klik Lanjutkan.

   Diperlukan waktu hingga 72 jam AWS untuk meninjau permintaan Anda dan menyediakan port untuk koneksi Anda. Selama waktu ini, Anda mungkin menerima email berisi permintaan untuk informasi lebih lanjut tentang kasus penggunaan atau lokasi yang ditentukan. Email dikirim ke alamat email yang Anda gunakan saat mendaftar AWS. Anda harus merespons dalam waktu 7 hari atau koneksi akan dihapus.

Langkah 3: Membuat antarmuka virtual

Untuk mulai menggunakan AWS Direct Connect koneksi Anda, Anda harus membuat antarmuka virtual. Anda dapat membuat antarmuka virtual privat untuk terhubung ke VPC Anda. Atau, Anda dapat membuat antarmuka virtual publik untuk terhubung ke AWS layanan publik yang tidak ada dalam VPC. Ketika membuat antarmuka virtual privat untuk VPC, Anda memerlukan antarmuka virtual privat untuk setiap VPC yang terhubung dengan Anda. Misalnya, Anda memerlukan tiga antarmuka virtual pribadi untuk terhubung ke tiga VPCs.

Sebelum memulai, pastikan Anda memiliki informasi berikut:

Sumber Daya	Informasi yang diperlukan
Koneksi	Grup agregasi AWS Direct Connect koneksi atau tautan (LAG) tempat Anda membuat antarmuka virtual.
Nama antarmuka virtual	Nama untuk antarmuka virtual.
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID AWS akun dari akun lain.

Sumber Daya	Informasi yang diperlukan
(Antarmuka virtual privat saja) Koneksi	Untuk menghubungkan ke VPC di AWS Wilayah yang sama, Anda memerlukan gateway pribadi virtual untuk VPC Anda. ASN untuk sisi Amazon sesi BGP diwarisi dari virtual private gateway. Bila Anda membuat virtual private gateway, Anda dapat menentukan ASN privat Anda sendiri. Jika tidak, Amazon menyediakan ASN default. Untuk informasi selengkapnya, lihat Membuat Virtual Private Gateway di Panduan Pengguna Amazon VPC. Untuk terhubung ke VPC melalui gateway Direct Connect, Anda memerlukan gateway Direct Connect. Untuk informasi selengkapnya, lihat Gateway Direct Connect.
VLAN	Tanda virtual local area network (VLAN) unik yang belum digunakan pada koneksi Anda. Nilai harus antara 1 hingga 4094 dan harus sesuai dengan standar Ethernet 802.1Q. Tanda ini diperlukan untuk lalu lintas yang melintasi koneksi AWS Direct Connect . Jika Anda memiliki koneksi yang di-host, AWS Direct Connect Mitra Anda memberikan nilai ini. Anda tidak dapat mengubah nilai setelah Anda membuat antarmuka virtual.

Sumber Daya	Informasi yang diperlukan

Alamat IP rekan	Antarmuka virtual dapat mendukung sesi peering BGP untuk IPv4, IPv6, atau salah satu dari masing-masing (dual-stack). Jangan gunakan Elastic IPs (EIPs) atau Bawa alamat IP Anda sendiri (BYOIP) dari Amazon Pool untuk membuat antarmuka virtual publik. Anda tidak dapat membuat beberapa sesi BGP untuk keluarga pengalamatan IP yang sama pada antarmuka virtual yang sama. Cakupan alamat IP ditetapkan untuk setiap akhir antarmuka virtual untuk sesi peering BGP.
	
	• IPv4:
	  • (Hanya antarmuka virtual publik) Anda harus menentukan IPv4 alamat publik unik yang Anda miliki. Nilai dapat menjadi salah satu dari yang berikut:
	  • CIDR milik pelanggan IPv4
	
	Ini dapat berupa publik IPs (milik pelanggan atau disediakan oleh AWS), tetapi subnet mask yang sama harus digunakan untuk IP rekan Anda dan IP peer router. AWS Misalnya, jika Anda mengalokasikan `/31` rentang, seperti`203.0.113.0/31` , Anda dapat menggunakan `203.0.113.0` untuk IP rekan Anda dan `203.0.113.1` untuk IP AWS rekan. Atau, jika Anda mengalokasikan `/24` rentang, seperti`198.51.100.0/24` , Anda dapat menggunakan `198.51.100.0` untuk IP rekan Anda dan `198.51.100.20` untuk IP AWS rekan.
	  • Rentang IP yang dimiliki oleh AWS Direct Connect Mitra atau ISP Anda, bersama dengan otorisasi LOA-CFA
	  • AWS-Disediakan /31 CIDR. Hubungi AWS Support untuk meminta IPv4 CIDR publik (dan memberikan kasus penggunaan dalam permintaan Anda)
	
	Note
	Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk IPv4 alamat publik AWS yang disediakan.

Sumber Daya	Informasi yang diperlukan
	• (Hanya antarmuka virtual pribadi) Amazon dapat menghasilkan IPv4 alamat pribadi untuk Anda. Jika Anda menentukan sendiri, pastikan bahwa Anda menentukan pribadi CIDRs untuk antarmuka router Anda dan antarmuka AWS Direct Connect saja. Misalnya, jangan tentukan alamat IP lain dari jaringan lokal Anda. Mirip dengan antarmuka virtual publik, subnet mask yang sama harus digunakan untuk IP peer Anda dan IP peer AWS router. Misalnya, jika Anda mengalokasikan `/30` rentang, seperti`192.168.0.0/30` , Anda dapat menggunakan `192.168.0.1` untuk IP rekan Anda dan `192.168.0.2` untuk IP AWS rekan. • IPv6: Amazon secara otomatis mengalokasikan Anda IPv6 /125 CIDR. Anda tidak dapat menentukan IPv6 alamat rekan Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan berakhir atau. IPv4 IPv6
Informasi BGP	• Border Gateway Protocol (BGP) Autonomous System Number (ASN) publik atau privat untuk sisi sesi BGP Anda. Jika Anda menggunakan ASN publik, Anda harus memilikinya. Jika Anda menggunakan ASN pribadi, Anda dapat mengatur nilai ASN kustom. Untuk ASN 16-bit, nilainya harus berada dalam rentang 64512 hingga 65534. Untuk ASN 32-bit, nilainya harus dalam kisaran 1 hingga 2147483647. Penambahan Autonomous System (AS) tidak bekerja jika Anda menggunakan ASN privat untuk antarmuka virtual publik. • AWS memungkinkan secara MD5 default. Anda tidak dapat mengubah opsi ini. • Kunci otentikasi MD5 BGP. Anda dapat memberikan kunci milik Anda sendiri, atau Anda dapat membiarkan Amazon menghasilkannya untuk Anda.

Sumber Daya	Informasi yang diperlukan

(Antarmuka virtual publik saja) Prefiks yang ingin Anda iklankan	IPv4 Rute umum atau IPv6 rute untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: IPv4 CIDR dapat tumpang tindih dengan IPv4 CIDR publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari berikut ini benar:
	  • CIDRs Mereka berasal dari berbagai AWS daerah. Pastikan bahwa Anda menerapkan tanda komunitas BGP pada prefiks publik.
	  • Anda menggunakan AS_PATH ketika Anda memiliki ASN publik dalam konfigurasi. active/passive
	  Untuk informasi selengkapnya, lihat Kebijakan perutean dan komunitas BGP.
	• Melalui antarmuka virtual publik Direct Connect, Anda dapat menentukan panjang awalan dari /1 hingga /32 untuk IPv4 dan dari /1 hingga /64 untuk. IPv6
	• Anda dapat menambahkan awalan tambahan ke VIF publik yang ada dan mengiklankannya dengan menghubungi dukungan.AWS Dalam kasus dukungan Anda, berikan daftar awalan CIDR tambahan yang ingin Anda tambahkan ke VIF publik dan beriklan.

(Hanya antarmuka virtual pribadi dan transit) Frame jumbo	Unit transmisi maksimum (MTU) paket over. AWS Direct Connect Default-n ya adalah 1500. Mengatur MTU antarmuka virtual ke 9001 (bingkai jumbo) dapat menyebabkan pembaruan untuk koneksi fisik yang mendasari jika itu tidak diperbarui untuk mendukung bingkai jumbo. Memperbarui koneksi mengganggu konektivitas jaringan untuk semua antarmuka virtual yang terkait dengan koneksi hingga 30 detik. Bingkai jumbo hanya berlaku untuk rute yang disebarkan dari. AWS Direct Connect Jika Anda menambahkan rute statis ke tabel rute yang mengarah ke virtual private gateway, lalu lintas diarahkan melalui rute statis dikirim menggunakan 1500 MTU. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di AWS Direct Connect konsol dan temukan bingkai Jumbo yang mampu pada antarmuka virtual Halaman konfigurasi umum.

Jika awalan publik Anda atau ASNs milik ISP atau operator jaringan, kami meminta informasi tambahan dari Anda. Ini bisa berupa dokumen menggunakan kop surat resmi perusahaan, atau email dari nama domain perusahaan yang memverifikasi bahwa jaringan prefix/ASN dapat digunakan oleh Anda.

Jika Anda membuat antarmuka virtual publik, dibutuhkan waktu hingga 72 jam bagi AWS untuk meninjau dan menyetujui permintaan Anda.

Untuk menyediakan antarmuka virtual publik ke layanan non-VPC

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Publik.
5. Di bawah Pengaturan antarmuka virtual publik, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.
   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.
   c. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).
   d. Untuk BGP ASN, masukkan Autonomous System Number (ASN) Border Gateway Protocol (BGP) dari gateway Anda.

      Nilai yang valid adalah 1-2147483647.
6. Di bawah Pengaturan tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

      - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

      [IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

   b. Untuk memberikan kunci BGP Anda sendiri, masukkan kunci MD5 BGP Anda.

Jika Anda tidak memasukkan nilai, kami menghasilkan kunci BGP.

c. Untuk mengiklankan awalan ke Amazon, untuk Awalan yang ingin Anda iklankan, masukkan alamat tujuan IPv4 CIDR (dipisahkan dengan koma) ke mana lalu lintas harus diarahkan melalui antarmuka virtual.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.

Untuk menyediakan antarmuka virtual privat bagi VPC

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Privat.
5. Di bawah Pengaturan antarmuka virtual privat, lakukan hal berikut:

a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.

b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.

c. Untuk Jenis gateway, pilih Virtual private gateway, atau Gateway Direct Connect.

d. Untuk pemilik antarmuka virtual, pilih AWS Akun lain, lalu masukkan AWS akun.

e. Untuk Virtual private gateway, pilih virtual private gateway yang akan digunakan untuk antarmuka ini.

f. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).

g. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

Nilai yang valid adalah 1 hingga 2147483647.

6. Di bawah Pengaturan Tambahan, lakukan hal berikut:

a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

   [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

   - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
   - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

   > **Important**
   >
   > Saat mengonfigurasi antarmuka virtual AWS Direct Connect, Anda dapat menentukan alamat IP Anda sendiri menggunakan RFC 1918, menggunakan skema pengalamatan lain, atau memilih alamat IPv4 /29 CIDR yang AWS ditetapkan yang dialokasikan dari rentang RFC 3927 169.254.0.0/16 Link-Local untuk konektivitas. IPv4 point-to-point point-to-pointKoneksi ini harus digunakan secara eksklusif untuk mengintip eBGP antara router gateway pelanggan Anda dan titik akhir Direct Connect. Untuk tujuan lalu lintas atau tunneling VPC, seperti AWS Site-to-Site Private IP VPN, atau Transit Gateway Connect, AWS merekomendasikan penggunaan antarmuka loopback atau LAN pada router gateway pelanggan Anda sebagai alamat sumber atau tujuan alih-alih koneksi. point-to-point
   >
   > - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
   > - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat IPv4 Lokal-Tautan.

   [IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk mengubah maximum transmission unit (MTU) dari 1500 (default) menjadi 9001 (bingkai jumbo), pilih MTU Jumbo (MTU ukuran 9001).

c. (Opsional) Di bawah Aktifkan SiteLink, pilih Diaktifkan untuk mengaktifkan konektivitas langsung antara titik kehadiran Direct Connect.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.

Langkah 4: Memverifikasi konfigurasi ketahanan antarmuka virtual

Setelah Anda membuat antarmuka virtual ke AWS Cloud atau ke Amazon VPC, lakukan pengujian failover antarmuka virtual untuk memverifikasi bahwa konfigurasi Anda memenuhi persyaratan ketahanan Anda. Untuk informasi selengkapnya, lihat the section called “Tes failover Direct Connect”.

Langkah 5: Memverifikasi antarmuka virtual

Setelah Anda membuat antarmuka virtual ke AWS Cloud atau ke Amazon VPC, Anda dapat memverifikasi koneksi AWS Direct Connect Anda menggunakan prosedur berikut.

Untuk memverifikasi koneksi antarmuka virtual Anda ke AWS Cloud

- Jalankan `traceroute` dan verifikasi bahwa AWS Direct Connect pengenal ada di jejak jaringan.

Untuk memverifikasi koneksi antarmuka virtual Anda ke Amazon VPC

1. Menggunakan AMI yang dapat di-ping, seperti AMI Amazon Linux, luncurkan EC2 instance ke VPC yang dilampirkan ke gateway pribadi virtual Anda. Amazon Linux AMIs tersedia di tab Mulai Cepat saat Anda menggunakan wizard peluncuran instans di EC2 konsol Amazon. Untuk informasi selengkapnya, lihat Meluncurkan Instance di Panduan EC2 Pengguna Amazon. Pastikan bahwa grup keamanan yang terkait dengan instans mencakup aturan yang mengizinkan lalu lintas ICMP masuk (untuk permintaan ping).
2. Setelah instance berjalan, dapatkan IPv4 alamat pribadinya (misalnya, 10.0.0.4). EC2 Konsol Amazon menampilkan alamat sebagai bagian dari detail instans.
3. Ping IPv4 alamat pribadi dan dapatkan tanggapan.

Konfigurasikan koneksi AWS Direct Connect Klasik

Konfigurasikan koneksi Klasik ketika Anda memiliki koneksi Direct Connect yang ada.

Langkah 1: Mendaftar AWS

Untuk menggunakannya AWS Direct Connect, Anda memerlukan akun jika Anda belum memilikinya.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Langkah 2: Minta koneksi AWS Direct Connect khusus

Untuk koneksi khusus, Anda dapat mengirimkan permintaan koneksi menggunakan AWS Direct Connect konsol. Untuk koneksi yang dihosting, bekerja sama dengan AWS Direct Connect Mitra untuk meminta koneksi yang dihosting. Pastikan bahwa Anda memiliki informasi berikut:

- Kecepatan port yang Anda butuhkan. Anda tidak dapat mengubah kecepatan port setelah Anda membuat permintaan koneksi.
- AWS Direct Connect Lokasi di mana koneksi akan diakhiri.

> **Note**
>
> Anda tidak dapat menggunakan AWS Direct Connect konsol untuk meminta koneksi yang dihosting. Sebagai gantinya, hubungi AWS Direct Connect Mitra, yang dapat membuat koneksi yang dihosting untuk Anda, yang kemudian Anda terima. Lewati prosedur berikut dan pergi ke Terima koneksi yang di-host.

Untuk membuat AWS Direct Connect koneksi baru

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi pilih Koneksi, lalu pilih Buat koneksi.
3. PilihKlasik.
4. Pada panel Buat Koneksi, di bawahPengaturan koneksi, lakukan hal berikut:
   a. Untuk Nama, masukkan nama untuk koneksi.
   b. Untuk Lokasi, pilih lokasi AWS Direct Connect yang sesuai.
   c. Jika berlaku, untuk Sub-lokasi, pilih lantai yang paling dekat dengan Anda atau penyedia jaringan Anda. Opsi ini hanya tersedia jika lokasi memiliki ruang meet-me (MMRs) di beberapa lantai gedung.
   d. Untuk Kecepatan Port, pilih bandwidth koneksi.
   e. Untuk Lokal, pilih Connect through an AWS Direct Connect partner saat Anda menggunakan koneksi ini untuk menyambung ke pusat data Anda.
   f. Untuk penyedia layanan, pilih AWS Direct Connect Partner. Jika Anda menggunakan partner yang tidak ada dalam daftar, pilih Lainnya.

g. Jika Anda memilih Lainnya untuk Penyedia layanan, untuk Nama penyedia lain, masukkan nama partner yang Anda gunakan.

h. (Opsional) Tambahkan atau hapus tanda.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Hapus tanda] Di samping tanda, pilih Hapus tanda.

5. Pilih Buat Koneksi.

Diperlukan waktu hingga 72 jam AWS untuk meninjau permintaan Anda dan menyediakan port untuk koneksi Anda. Selama waktu ini, Anda mungkin menerima email berisi permintaan untuk informasi lebih lanjut tentang kasus penggunaan atau lokasi yang ditentukan. Email dikirim ke alamat email yang Anda gunakan saat mendaftar AWS. Anda harus merespons dalam waktu 7 hari atau koneksi akan dihapus.

Untuk informasi selengkapnya, lihat AWS Direct Connect koneksi khusus dan host.

Terima koneksi yang di-host

Anda harus menerima koneksi yang dihosting di AWS Direct Connect konsol sebelum Anda dapat membuat antarmuka virtual. Langkah ini hanya berlaku untuk koneksi yang di-host.

Untuk menerima antarmuka virtual yang di-host

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Koneksi.
3. Pilih koneksi yang di-host, lalu pilih Terima.

   Pilih Terima.

(Koneksi khusus) Langkah 3: Unduh LOA-CFA

Setelah Anda meminta koneksi, kami membuat Letter of Authorization and Connecting Facility Assignment (LOA-CFA) tersedia bagi Anda untuk diunduh, atau mengirimi Anda email dengan permintaan untuk informasi selengkapnya. LOA-CFA adalah otorisasi untuk terhubung AWS, dan

diperlukan oleh penyedia colocation atau penyedia jaringan Anda untuk membuat koneksi lintas-jaringan (cross-connect).

Untuk mengunduh LOA-CFA

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Koneksi.
3. Pilih koneksi dan pilih Lihat Detail.
4. Pilih Unduh LOA-CFA.

   LOA-CFA diunduh ke komputer anda sebagai file PDF.

   > **Note**
   >
   > Jika tautan tidak diaktifkan, LOA-CFA belum tersedia bagi Anda untuk diunduh. Periksa email Anda untuk permintaan untuk informasi selengkapnya. Jika masih tidak tersedia, atau Anda belum menerima email setelah 72 jam, hubungi AWS Support.

5. Setelah Anda mengunduh LOA-CFA, lakukan salah satu hal berikut:

   - Jika Anda bekerja dengan AWS Direct Connect Mitra atau penyedia jaringan, kirimkan LOA-CFA kepada mereka sehingga mereka dapat memesan koneksi silang untuk Anda di lokasi. AWS Direct Connect Jika mereka tidak dapat memesan koneksi silang untuk Anda, Anda dapat menghubungi penyedia kolokasi secara langsung.
   - Jika Anda memiliki peralatan di AWS Direct Connect lokasi, hubungi penyedia colocation untuk meminta koneksi lintas jaringan. Anda harus menjadi pelanggan penyedia kolokasi. Anda juga harus menyajikannya dengan LOA-CFA yang mengotorisasi koneksi ke AWS router, dan informasi yang diperlukan untuk terhubung ke jaringan Anda.

AWS Direct Connect lokasi yang terdaftar sebagai beberapa situs (misalnya, Equinix DC1 - DC6 & DC1 0-DC11) diatur sebagai kampus. Jika peralatan Anda atau penyedia jaringan Anda berada di salah satu lokasi ini, Anda dapat meminta koneksi silang ke port yang ditetapkan walaupun berada di gedung kampus yang berbeda.

> **Important**
>
> Kampus diperlakukan sebagai satu AWS Direct Connect lokasi. Untuk mencapai ketersediaan tinggi, konfigurasikan koneksi ke berbagai lokasi AWS Direct Connect .

Jika Anda atau penyedia jaringan mengalami masalah saat membuat koneksi fisik, lihat Pemecahan masalah lapisan 1 (fisik).

Langkah 4: Buat antarmuka virtual

Untuk mulai menggunakan AWS Direct Connect koneksi Anda, Anda harus membuat antarmuka virtual. Anda dapat membuat antarmuka virtual privat untuk terhubung ke VPC Anda. Atau, Anda dapat membuat antarmuka virtual publik untuk terhubung ke AWS layanan publik yang tidak ada di VPC. Saat Anda membuat antarmuka virtual privat untuk VPC, Anda memerlukan antarmuka virtual privat untuk setiap VPC yang terhubung. Misalnya, Anda memerlukan tiga antarmuka virtual pribadi untuk terhubung ke tiga VPCs.

Sebelum memulai, pastikan Anda memiliki informasi berikut:

Sumber Daya	Informasi yang diperlukan
Koneksi	Grup agregasi AWS Direct Connect koneksi atau tautan (LAG) tempat Anda membuat antarmuka virtual.
Nama antarmuka virtual	Nama untuk antarmuka virtual.
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID AWS akun dari akun lain.
(Antarmuka virtual privat saja) Koneksi	Untuk menghubungkan ke VPC di AWS Wilayah yang sama, Anda memerlukan gateway pribadi virtual untuk VPC Anda. ASN untuk sisi Amazon sesi BGP diwarisi dari virtual private gateway. Bila Anda membuat virtual private gateway, Anda dapat menentukan ASN privat Anda sendiri. Jika tidak, Amazon menyediakan ASN default. Untuk informasi selengkapnya, lihat Membuat Virtual Private Gateway di Panduan Pengguna Amazon VPC. Untuk terhubung ke VPC melalui gateway Direct Connect, Anda memerlukan

Sumber Daya	Informasi yang diperlukan
	gateway Direct Connect. Untuk informasi selengkapnya, lihat Gateway Direct Connect.
VLAN	Tanda virtual local area network (VLAN) unik yang belum digunakan pada koneksi Anda. Nilai harus antara 1 hingga 4094 dan harus sesuai dengan standar Ethernet 802.1Q. Tanda ini diperlukan untuk lalu lintas yang melintasi koneksi AWS Direct Connect . Jika Anda memiliki koneksi yang di-host, AWS Direct Connect Mitra Anda memberikan nilai ini. Anda tidak dapat mengubah nilai setelah Anda membuat antarmuka virtual.

Sumber Daya	Informasi yang diperlukan

Alamat IP rekan	Antarmuka virtual dapat mendukung sesi peering BGP untuk IPv4, IPv6, atau salah satu dari masing-masing (dual-stack). Jangan gunakan Elastic IPs (EIPs) atau Bawa alamat IP Anda sendiri (BYOIP) dari Amazon Pool untuk membuat antarmuka virtual publik. Anda tidak dapat membuat beberapa sesi BGP untuk keluarga pengalamatan IP yang sama pada antarmuka virtual yang sama. Cakupan alamat IP ditetapkan untuk setiap akhir antarmuka virtual untuk sesi peering BGP.
	
	• IPv4:
	  • (Hanya antarmuka virtual publik) Anda harus menentukan IPv4 alamat publik unik yang Anda miliki. Nilai dapat menjadi salah satu dari yang berikut:
	  • CIDR milik pelanggan IPv4
	
	Ini dapat berupa publik IPs (milik pelanggan atau disediakan oleh AWS), tetapi subnet mask yang sama harus digunakan untuk IP rekan Anda dan IP peer router. AWS Misalnya, jika Anda mengalokasikan `/31` rentang, seperti`203.0.113.0/31` , Anda dapat menggunakan `203.0.113.0` untuk IP rekan Anda dan `203.0.113.1` untuk IP AWS rekan. Atau, jika Anda mengalokasikan `/24` rentang, seperti`198.51.100.0/24` , Anda dapat menggunakan `198.51.100.10` untuk IP rekan Anda dan `198.51.100.20` untuk IP AWS rekan.
	  • Rentang IP yang dimiliki oleh AWS Direct Connect Mitra atau ISP Anda, bersama dengan otorisasi LOA-CFA
	  • AWS-Disediakan /31 CIDR. Hubungi AWS Support untuk meminta IPv4 CIDR publik (dan memberikan kasus penggunaan dalam permintaan Anda)
	
	Note
	Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk IPv4 alamat publik AWS yang disediakan.

Sumber Daya	Informasi yang diperlukan
	• (Hanya antarmuka virtual pribadi) Amazon dapat menghasilkan IPv4 alamat pribadi untuk Anda. Jika Anda menentukan sendiri, pastikan bahwa Anda menentukan pribadi CIDRs untuk antarmuka router Anda dan antarmuka AWS Direct Connect saja. Misalnya, jangan tentukan alamat IP lain dari jaringan lokal Anda. Mirip dengan antarmuka virtual publik, subnet mask yang sama harus digunakan untuk IP peer Anda dan IP peer AWS router. Misalnya, jika Anda mengalokasikan `/30` rentang, seperti`192.168.0.0/30` , Anda dapat menggunakan `192.168.0.1` untuk IP rekan Anda dan `192.168.0.2` untuk IP AWS rekan. • IPv6: Amazon secara otomatis mengalokasikan Anda IPv6 /125 CIDR. Anda tidak dapat menentukan IPv6 alamat rekan Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan berakhir atau. IPv4 IPv6
Informasi BGP	• Border Gateway Protocol (BGP) Autonomous System Number (ASN) publik atau privat untuk sisi sesi BGP Anda. Jika Anda menggunakan ASN publik, Anda harus memilikinya. Jika Anda menggunakan ASN pribadi, Anda dapat mengatur nilai ASN kustom. Untuk ASN 16-bit, nilainya harus berada dalam rentang 64512 hingga 65534. Untuk ASN 32-bit, nilainya harus dalam kisaran 1 hingga 2147483647. Penambahan Autonomous System (AS) tidak bekerja jika Anda menggunakan ASN privat untuk antarmuka virtual publik. • AWS memungkinkan secara MD5 default. Anda tidak dapat mengubah opsi ini. • Kunci otentikasi MD5 BGP. Anda dapat memberikan kunci milik Anda sendiri, atau Anda dapat membiarkan Amazon menghasilkannya untuk Anda.

Sumber Daya	Informasi yang diperlukan

(Antarmuka virtual publik saja) Prefiks yang ingin Anda iklankan	IPv4 Rute umum atau IPv6 rute untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: IPv4 CIDR dapat tumpang tindih dengan IPv4 CIDR publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari berikut ini benar:
	  • CIDRs Mereka berasal dari berbagai AWS daerah. Pastikan bahwa Anda menerapkan tanda komunitas BGP pada prefiks publik.
	  • Anda menggunakan AS_PATH ketika Anda memiliki ASN publik dalam konfigurasi. active/passive
	  Untuk informasi selengkapnya, lihat Kebijakan perutean dan komunitas BGP.
	• Melalui antarmuka virtual publik Direct Connect, Anda dapat menentukan panjang awalan dari /1 hingga /32 untuk IPv4 dan dari /1 hingga /64 untuk. IPv6
	• Anda dapat menambahkan awalan tambahan ke VIF publik yang ada dan mengiklankannya dengan menghubungi dukungan.AWS Dalam kasus dukungan Anda, berikan daftar awalan CIDR tambahan yang ingin Anda tambahkan ke VIF publik dan beriklan.

(Hanya antarmuka virtual pribadi dan transit) Frame jumbo	Unit transmisi maksimum (MTU) paket over. AWS Direct Connect Default-n ya adalah 1500. Mengatur MTU antarmuka virtual ke 9001 (bingkai jumbo) dapat menyebabkan pembaruan untuk koneksi fisik yang mendasari jika itu tidak diperbarui untuk mendukung bingkai jumbo. Memperbarui koneksi mengganggu konektivitas jaringan untuk semua antarmuka virtual yang terkait dengan koneksi hingga 30 detik. Bingkai jumbo hanya berlaku untuk rute yang disebarkan dari. AWS Direct Connect Jika Anda menambahkan rute statis ke tabel rute yang mengarah ke virtual private gateway, lalu lintas diarahkan melalui rute statis dikirim menggunakan 1500 MTU. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di AWS Direct Connect konsol dan temukan bingkai Jumbo yang mampu pada antarmuka virtual Halaman konfigurasi umum.

Kami meminta informasi tambahan dari Anda jika awalan publik Anda atau ASNs milik ISP atau operator jaringan. Ini bisa berupa dokumen menggunakan kop surat resmi perusahaan atau email dari nama domain perusahaan yang memverifikasi bahwa jaringan tersebut prefix/ASN dapat digunakan oleh Anda.

Maximum transmission unit (MTU) dari koneksi jaringan adalah ukuran, dalam bita, dari paket terbesar yang dapat diizinkan yang dapat dilewatkan melalui koneksi. MTU antarmuka virtual pribadi dapat berupa 1500 atau 9001 (bingkai jumbo). MTU antarmuka virtual transit dapat sebesar 1500 atau 8500 (bingkai jumbo). Anda dapat menentukan MTU saat membuat antarmuka atau memperbaruinya setelah Anda membuatnya. Mengatur MTU antarmuka virtual ke 8500 (bingkai jumbo) atau 9001 (bingkai jumbo) dapat menyebabkan pembaruan untuk koneksi fisik yang mendasari jika itu tidak diperbarui untuk mendukung bingkai jumbo. Memperbarui koneksi mengganggu konektivitas jaringan untuk semua antarmuka virtual yang terkait dengan koneksi hingga 30 detik. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di AWS Direct Connect konsol dan temukan Jumbo Frame Mampu pada tab Ringkasan.

Saat Anda membuat antarmuka virtual publik, diperlukan waktu hingga 72 jam AWS untuk meninjau dan menyetujui permintaan Anda.

Untuk menyediakan antarmuka virtual publik ke layanan non-VPC

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Publik.
5. Di bawah Pengaturan antarmuka virtual publik, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.

   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.

   c. Untuk VLAN, masukkan nomor ID untuk jaringan virtual local area network (VLAN).

   d. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number router peer on-premise untuk antarmuka virtual baru.

      Nilai yang valid adalah 1-2147483647.
6. Di bawah Pengaturan tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

[IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

- Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
- Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

[IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk memberikan kunci BGP Anda sendiri, masukkan kunci MD5 BGP Anda.

Jika Anda tidak memasukkan nilai, kami menghasilkan kunci BGP.

c. Untuk mengiklankan awalan ke Amazon, untuk Awalan yang ingin Anda iklankan, masukkan alamat tujuan IPv4 CIDR (dipisahkan dengan koma) ke mana lalu lintas harus diarahkan melalui antarmuka virtual.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.

Untuk menyediakan antarmuka virtual privat bagi VPC

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Privat.
5. Di bawah Pengaturan antarmuka virtual privat, lakukan hal berikut:

a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.

b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.

c. Untuk Jenis gateway, pilih Virtual private gateway, atau Gateway Direct Connect.

d. Untuk pemilik antarmuka virtual, pilih AWS Akun lain, lalu masukkan AWS akun.

e. Untuk Virtual private gateway, pilih virtual private gateway yang akan digunakan untuk antarmuka ini.

f. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).

g. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

   Nilai yang valid adalah 1 hingga 2147483647.

6. Di bawah Pengaturan Tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

      - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

      > **Important**
      >
      > Saat mengonfigurasi antarmuka virtual AWS Direct Connect, Anda dapat menentukan alamat IP Anda sendiri menggunakan RFC 1918, menggunakan skema pengalamatan lain, atau memilih alamat IPv4 /29 CIDR yang AWS ditetapkan yang dialokasikan dari rentang RFC 3927 169.254.0.0/16 Link-Local untuk konektivitas. IPv4 point-to-point point-to-pointKoneksi ini harus digunakan secara eksklusif untuk mengintip eBGP antara router gateway pelanggan Anda dan titik akhir Direct Connect. Untuk tujuan lalu lintas atau tunneling VPC, seperti AWS Site-to-Site Private IP VPN, atau Transit Gateway Connect, AWS merekomendasikan penggunaan antarmuka loopback atau LAN pada router gateway pelanggan Anda sebagai alamat sumber atau tujuan alih-alih koneksi. point-to-point
      >
      > - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
      > - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat IPv4 Lokal-Tautan.

[IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk mengubah maximum transmission unit (MTU) dari 1500 (default) menjadi 9001 (bingkai jumbo), pilih MTU Jumbo (MTU ukuran 9001).

c. (Opsional) Di bawah Aktifkan SiteLink, pilih Diaktifkan untuk mengaktifkan konektivitas langsung antara titik kehadiran Direct Connect.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.
8. Anda perlu menggunakan perangkat BGP Anda untuk mengiklankan jaringan yang Anda gunakan untuk koneksi VIF publik.

Langkah 5: Unduh konfigurasi router

Setelah Anda membuat antarmuka virtual untuk AWS Direct Connect koneksi Anda, Anda dapat mengunduh file konfigurasi router. File berisi perintah yang diperlukan untuk mengonfigurasi router Anda untuk digunakan dengan antarmuka virtual privat atau publik Anda.

Untuk mengunduh konfigurasi router

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih koneksi dan pilih Lihat Detail.
4. Pilih Unduh konfigurasi router.
5. Untuk Unduh konfigurasi router, lakukan hal berikut:

   a. Untuk Vendor, pilih produsen router Anda.

   b. Untuk Platform, pilih model router Anda.

   c. Untuk Perangkat Lunak, pilih versi perangkat lunak untuk router Anda.

6. Pilih Unduh, lalu gunakan konfigurasi yang sesuai untuk router Anda guna memastikan bahwa Anda dapat terhubung ke AWS Direct Connect.

Untuk informasi selengkapnya tentang mengonfigurasi router secara manual, lihatMengunduh file konfigurasi router.

Setelah Anda mengonfigurasi router, status antarmuka virtual akan berubah menjadi UP. Jika antarmuka virtual tetap down dan Anda tidak dapat melakukan ping ke alamat IP rekan AWS Direct Connect perangkat, lihatPemecahan masalah lapisan 2 (tautan data). Jika Anda dapatmenge-ping alamat IP peer, lihat Pemecahan masalah lapisan 3/4 (Jaringan/Transportasi). Jika sesi peering BGP dibuat tetapi Anda tidak dapat merutekan lalu lintas, lihat Masalah perutean pemecahan masalah.

Langkah 6: Verifikasi antarmuka virtual

Setelah Anda membuat antarmuka virtual ke AWS Cloud atau ke Amazon VPC, Anda dapat memverifikasi koneksi AWS Direct Connect Anda menggunakan prosedur berikut.

Untuk memverifikasi koneksi antarmuka virtual Anda ke AWS Cloud

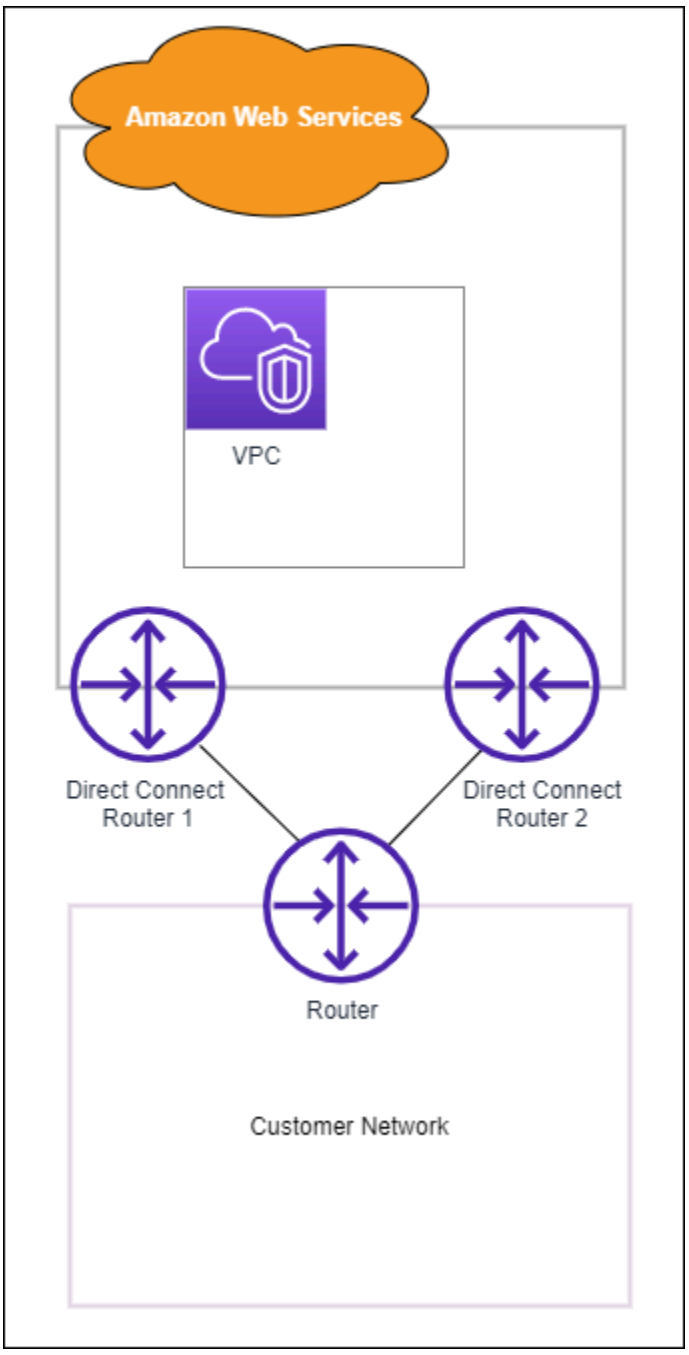
- Jalankan `traceroute` dan verifikasi bahwa AWS Direct Connect pengenal ada di jejak jaringan.

Untuk memverifikasi koneksi int+erface virtual Anda ke Amazon VPC

1. Menggunakan AMI yang dapat di-ping, seperti AMI Amazon Linux, luncurkan EC2 instance ke VPC yang dilampirkan ke gateway pribadi virtual Anda. Amazon Linux AMIs tersedia di tab Mulai Cepat saat Anda menggunakan wizard peluncuran instans di EC2 konsol Amazon. Untuk informasi selengkapnya, lihat Meluncurkan Instance di Panduan EC2 Pengguna Amazon. Pastikan bahwa grup keamanan yang terkait dengan instans mencakup aturan yang mengizinkan lalu lintas ICMP masuk (untuk permintaan ping).
2. Setelah instance berjalan, dapatkan IPv4 alamat pribadinya (misalnya, 10.0.0.4). EC2 Konsol Amazon menampilkan alamat sebagai bagian dari detail instans.
3. Ping IPv4 alamat pribadi dan dapatkan tanggapan.

(Direkomendasikan) Langkah 7: Konfigurasikan koneksi redundan

Untuk menyediakan failover, kami sarankan Anda meminta dan mengonfigurasi dua koneksi khusus ke AWS, seperti yang ditunjukkan pada gambar berikut. Koneksi ini dapat diakhiri pada satu atau dua router di jaringan Anda.



Ada beberapa pilihan konfigurasi yang tersedia saat Anda menyediakan dua koneksi khusus:

- Aktif/Aktif (BGP multijalur). Ini adalah konfigurasi default, di mana kedua koneksi aktif. AWS Direct Connect mendukung multipathing ke beberapa antarmuka virtual dalam lokasi yang sama, dan lalu lintas dibagikan beban antar antarmuka berdasarkan aliran. Jika satu koneksi menjadi tidak tersedia, semua lalu lintas akan dirutekan melalui koneksi lain.
- Aktif/Pasif (failover). Satu koneksi menangani lalu lintas, dan yang lainnya siaga. Jika koneksi aktif menjadi tidak tersedia, semua lalu lintas akan dirutekan melalui koneksi pasif. Anda perlu menambahkan jalur AS ke rute pada salah satu tautan Anda agar itu menjadi tautan pasif.

Cara Anda mengonfigurasi koneksi tidak memengaruhi redundansi, tetapi memengaruhi kebijakan yang menentukan bagaimana data Anda dirutekan melalui kedua koneksi. Kami sarankan Anda mengonfigurasi kedua koneksi sebagai aktif.

Jika Anda menggunakan koneksi VPN untuk redundansi, pastikan bahwa Anda mengimplementasikan pemeriksaan kondisi dan mekanisme failover. Jika Anda menggunakan salah satu dari konfigurasi berikut, Anda perlu memeriksa perutean tabel rute untuk merutekan ke antarmuka jaringan baru.

- Anda menggunakan instans Anda sendiri untuk perutean, misalnya instans adalah firewall.
- Anda menggunakan instans Anda sendiri yang mengakhiri koneksi VPN.

Untuk mencapai ketersediaan tinggi, kami sangat menyarankan Anda mengonfigurasi koneksi ke AWS Direct Connect lokasi yang berbeda.

Untuk informasi lebih lanjut tentang AWS Direct Connect ketahanan, lihat Rekomendasi AWS Direct Connect Ketahanan.

AWS Direct Connect Tes Failover

Model AWS Direct Connect ketahanan Resiliency Toolkit dirancang untuk memastikan bahwa Anda memiliki jumlah koneksi antarmuka virtual yang sesuai di beberapa lokasi. Setelah Anda menyelesaikan wizard, gunakan tes failover AWS Direct Connect Resiliency Toolkit untuk menurunkan sesi peering BGP untuk memverifikasi rute lalu lintas ke salah satu antarmuka virtual Anda yang berlebihan, dan memenuhi persyaratan ketahanan Anda.

Gunakan pengujian untuk memastikan bahwa lalu lintas dirutekan melalui antarmuka virtual redundan ketika antarmuka virtual tidak berjalan. Anda memulai tes dengan memilih antarmuka virtual, sesi peering BGP, dan berapa lama untuk menjalankan tes. AWS menempatkan sesi peering

BGP antarmuka virtual yang dipilih dalam keadaan turun. Ketika antarmuka dalam status ini, lalu lintas harus melalui antarmuka virtual redundan. Jika konfigurasi Anda tidak berisi koneksi redundan yang sesuai, sesi peering BGP gagal, dan lalu lintas tidak dirutekan. Ketika tes selesai, atau Anda menghentikan tes secara manual, AWS mengembalikan sesi BGP. Setelah pengujian selesai, Anda dapat menggunakan AWS Direct Connect Resiliency Toolkit untuk menyesuaikan konfigurasi Anda.

> **Note**
>
> Jangan gunakan fitur ini selama periode pemeliharaan Direct Connect karena sesi BGP mungkin dipulihkan sebelum waktunya baik selama atau setelah pemeliharaan.

Riwayat tes

AWS menghapus riwayat pengujian setelah 365 hari. Riwayat pengujian mencakup status untuk pengujian yang dijalankan pada semua peer BGP. Riwayat mencakup sesi peering BGP yang diuji, waktu mulai dan berakhir, dan status pengujian, yang dapat menjadi salah satu dari nilai berikut:

- Sedang berlangsung - Pengujian sedang berjalan.
- Selesai - Pengujian berjalan dalam waktu yang Anda tentukan.
- Dibatalkan - Pengujian dibatalkan sebelum waktu yang ditentukan.
- Gagal - Pengujian tidak berjalan dalam waktu yang Anda tentukan. Hal ini bisa terjadi ketika ada masalah dengan router.

Untuk informasi selengkapnya, lihat the section called “Melihat riwayat pengujian failover antarmuka virtual”.

Izin validasi

Satu-satunya account yang memiliki izin untuk menjalankan pengujian failover adalah akun yang memiliki antarmuka virtual. Pemilik akun menerima indikasi melalui pengujian AWS CloudTrail yang dijalankan pada antarmuka virtual.

Topik

Mulai uji AWS Direct Connect failover antarmuka virtual Resiliency Toolkit

Anda dapat memulai uji failover antarmuka virtual menggunakan AWS Direct Connect konsol, atau file. AWS CLI

Untuk memulai pengujian failover antarmuka virtual dari konsol AWS Direct Connect

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Pilih Antarmuka virtual.
3. Pilih antarmuka virtual lalu pilih Tindakan, Turunkan BGP.

   Anda dapat menjalankan pengujian di antarmuka virtual publik, privat, atau transit.
4. Di kotak dialog Mulai pengujian kegagalan, lakukan hal berikut:

   a. Agar Peerings dapat diuji, pilih sesi peering mana yang akan diuji, misalnya. IPv4

   b. Untuk Uji waktu maksimum, masukkan jumlah menit untuk melangsungkan pengujian.

      Nilai maksimumnya adalah 4.320 menit (72 jam).

      Nilai default adalah 180 menit (3 jam).

   c. Untuk Untuk mengonfirmasi pengujian, masukkan Konfirmasi.

   d. Pilih Konfirmasi.

   Sesi peering BGP ditempatkan dalam status TURUN. Anda dapat mengirim lalu lintas untuk memverifikasi bahwa tidak ada pemadaman. Jika perlu, Anda dapat segera menghentikan pengujian.

Untuk memulai uji failover antarmuka virtual menggunakan AWS CLI

Gunakan StartBgpFailoverTest.

Lihat riwayat AWS Direct Connect pengujian failover antarmuka virtual Resiliency Toolkit

Anda dapat melihat riwayat pengujian failover antarmuka virtual menggunakan AWS Direct Connect konsol, atau file. AWS CLI

Untuk melihat riwayat pengujian failover antarmuka virtual dari konsol AWS Direct Connect

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Pilih Antarmuka virtual.
3. Pilih antarmuka virtual lalu pilih Lihat detail.
4. Pilih Riwayat pengujian.

   Konsol menampilkan pengujian antarmuka virtual yang Anda lakukan untuk antarmuka virtual.
5. Untuk melihat detail bagi pengujian tertentu, pilih id pengujian.

Untuk melihat riwayat pengujian failover antarmuka virtual menggunakan AWS CLI

Gunakan ListVirtualInterfaceTestHistory.

Hentikan pengujian AWS Direct Connect failover antarmuka virtual Resiliency Toolkit

Anda dapat menghentikan uji failover antarmuka virtual menggunakan AWS Direct Connect konsol, atau file. AWS CLI

Untuk menghentikan pengujian failover antarmuka virtual dari konsol AWS Direct Connect

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Pilih Antarmuka virtual.
3. Pilih antarmuka virtual, lalu pilih Tindakan, Batalkan pengujian.
4. Pilih Konfirmasi.

AWS mengembalikan sesi peering BGP. Riwayat pengujian menampilkan "dibatalkan" untuk pengujian.

Untuk menghentikan uji failover antarmuka virtual menggunakan AWS CLI

Gunakan StopBgpFailoverTest.

AWS Direct Connect pemeliharaan

AWS Direct Connect berkomitmen untuk memastikan keamanan layanan, ketersediaan, dan skalabilitas. Untuk mempertahankan standar ini, pemeliharaan berkala diperlukan pada perangkat jaringan perangkat keras. Perawatan Direct Connect dibagi menjadi dua jenis - direncanakan dan darurat.

Peristiwa pemeliharaan ini termasuk mengatasi kerentanan keamanan, masalah perangkat keras, melakukan migrasi perangkat untuk mematuhi standar, memperbaiki cacat, dan memberikan fitur baru. Dengan mengikuti praktik yang dijelaskan dalamPersiapan acara pemeliharaan, Anda dapat mempersiapkan lingkungan Direct Connect dengan lebih baik untuk menghindari gangguan selama acara pemeliharaan. Jika Anda memiliki pengaturan jaringan yang tidak tangguh atau satu koneksi, Anda akan mengalami gangguan konektivitas antara jaringan lokal dan sumber daya. AWS

Direct Connect mengirimkan pemberitahuan email tentang peristiwa pemeliharaan yang direncanakan dan darurat ke alamat email yang terkait dengan AWS akun yang memiliki koneksi Direct Connect atau sumber daya antarmuka virtual. Jika Anda menggunakan koneksi yang dihosting Direct Connect dengan salah satu Mitra Pengiriman Direct Connect, pemberitahuan email akan dikirimkan kepada Anda dan akun mitra tentang acara pemeliharaan. Anda juga dapat menambahkan alamat email atau daftar distribusi tambahan untuk menerima pemberitahuan. Lihat Memperbarui kontak alternatif untuk AWS akun Anda untuk informasi selengkapnya.

Acara pemeliharaan

- Perawatan terencana Direct Connect
- Perawatan darurat Direct Connect
- Pemeliharaan pihak ketiga
- Persiapan acara pemeliharaan
- Permintaan untuk penundaan atau pembatalan acara pemeliharaan

Perawatan terencana Direct Connect

Acara pemeliharaan yang direncanakan melibatkan peningkatan jaringan seperti penambalan sistem operasi dan pembaruan konfigurasi pada titik akhir perangkat keras yang diperlukan untuk meningkatkan ketersediaan dan menghadirkan fitur baru.

Acara pemeliharaan ini dijadwalkan 14 hari sebelumnya dan biasanya terjadi selama jendela empat jam dalam jam lalu lintas rendah di lokasi Direct Connect tempat titik akhir perangkat berada. Kegiatan pemeliharaan biasanya selesai sebelum jendela empat jam penuh berakhir dan Anda akan menerima pemberitahuan setelah pekerjaan selesai. Dalam kasus yang jarang terjadi di mana keadaan yang tidak terduga memerlukan perpanjangan jendela pemeliharaan, kami akan mengirimkan pemberitahuan terpisah dengan perkiraan penyelesaian yang direvisi.

Menggunakan jadwal berikut, pemberitahuan awal dan pemberitahuan pengingat dikirim ke AWS akun yang memiliki sumber daya:

- 14 hari kalender sebelum acara pemeliharaan yang direncanakan,
- 7 hari kalender sebelum acara pemeliharaan yang direncanakan, dan
- 1 hari sebelum acara pemeliharaan yang direncanakan.

> **Note**
>
> Hari kalender termasuk hari non-kerja dan hari libur lokal.

Selain itu,

- Terima pemberitahuan di sistem pemantauan atau tiket Anda dengan mengintegrasikan dengan. AWS Health Untuk mengintegrasikan AWS Health, lihat Memantau peristiwa AWS Health dengan Amazon EventBridge di Panduan AWS Health Pengguna.
- Lihat jadwal pemeliharaan yang direncanakan pada Anda AWS Health Dashboard.

Dalam keadaan yang jarang terjadi, acara pemeliharaan yang direncanakan tidak dapat terjadi sesuai jadwal. Jika ini terjadi, kami akan mengirimkan pemberitahuan pembatalan dan akan menjadwal ulang acara di masa mendatang mengikuti proses yang sama seperti di atas.

Perawatan darurat Direct Connect

Peristiwa pemeliharaan darurat dimulai secara kritis untuk mencegah layanan yang berdampak pada peristiwa atau menyelesaikan gangguan yang telah mengakibatkan gangguan pada konektivitas. Dalam kasus seperti itu, mengambil tindakan segera diperlukan untuk mengembalikan titik akhir yang terkena dampak ke keadaan sehat.

Meskipun kami berusaha untuk memberikan pemberitahuan terlebih dahulu bila memungkinkan, beberapa situasi mungkin memerlukan pemeliharaan untuk segera dimulai. Anda akan menerima pemberitahuan ketika pemeliharaan darurat dijadwalkan atau sedang berlangsung, dan sekali lagi ketika selesai.

Peristiwa ini biasanya terjadi selama jendela dua jam di lokasi Direct Connect tempat titik akhir perangkat berada. Kegiatan pemeliharaan biasanya selesai dalam jendela ini. Dalam kasus di mana keadaan yang tidak terduga memerlukan perpanjangan jendela pemeliharaan, seperti penggantian perangkat keras, kami akan mengirimkan pemberitahuan terpisah dengan perkiraan penyelesaian yang direvisi.

Pemeliharaan pihak ketiga

Selain peristiwa pemeliharaan AWS yang dimulai, mitra Pengiriman Direct Connect atau penyedia layanan jaringan Anda yang menyediakan konektivitas jaringan dari lokasi lokal Anda ke lokasi Direct Connect dapat melakukan aktivitas pemeliharaan. Mitra Direct Connect Delivery menerima pemberitahuan acara pemeliharaan AWS sehingga mereka dapat merencanakan jadwal pemeliharaan mereka sendiri untuk menghindari tumpang tindih. AWS tidak memiliki visibilitas ke dalam aktivitas pemeliharaan mitra, jadi Anda harus memeriksa dengan mereka untuk proses penjadwalan, metode pemberitahuan, dan praktik terbaik mereka.

Persiapan acara pemeliharaan

Untuk memastikan beban kerja produksi terus berfungsi selama acara pemeliharaan, Direct Connect merekomendasikan agar Anda menggunakan Direct Connect Resiliency Toolkit untuk mengonfigurasi koneksi jaringan Anda untuk ketahanan maksimum. AWS Untuk contoh model ketahanan maksimum, lihat. Ketahanan maksimum

Menggunakan ketahanan maksimum, koneksi tersebar di setidaknya dua lokasi Direct Connect, dengan penghentian pada dua titik akhir perangkat unik di setiap lokasi Direct Connect. Ini memberikan beberapa lapisan redundansi, yang mengurangi risiko kegagalan titik akhir tunggal dan membantu menjaga konektivitas selama acara pemeliharaan. Direct Connect tidak akan pernah menjadwalkan acara pemeliharaan terencana yang secara bersamaan akan menghapus koneksi berlebihan Anda. Untuk langkah-langkah menggunakan AWS Direct Connect Resiliency Toolkit untuk mengonfigurasi ketahanan maksimum, lihat. Konfigurasikan ketahanan maksimum

Selama acara pemeliharaan yang direncanakan, Direct Connect mengalirkan lalu lintas ke dan dari titik akhir koneksi yang menjalani pemeliharaan dan memaksa lalu lintas untuk menggunakan

koneksi redundan Anda. Hal ini memungkinkan perutean ulang lalu lintas jaringan yang lebih mulus tanpa perlu intervensi manual jika ketahanan maksimum tidak dikonfigurasi. Sebagai alternatif, Anda dapat memilih untuk mengontrol perutean ulang lalu lintas antara koneksi redundan selama jendela pemeliharaan dengan menggunakan komunitas Border Gateway Protocol (BGP) preferensi lokal. Untuk informasi selengkapnya tentang komunitas BGP, lihat. Kebijakan Perutean dan Komunitas BGP

Mengonfigurasi lingkungan Direct Connect Anda dengan model ketahanan maksimum membantu memastikan bisnis Anda tidak terpengaruh selama peristiwa pemeliharaan dan kegagalan infrastruktur. Ketika diterapkan dan diuji dengan benar, Anda biasanya tidak perlu mengambil tindakan apa pun untuk acara pemeliharaan ini.

Validasi ketahanan

Jika Anda telah mengonfigurasi lingkungan Direct Connect agar tangguh, validasi secara teratur bahwa rute lalu lintas Anda melalui koneksi redundan lainnya saat ada koneksi. out-of-service Pengujian proaktif secara teratur dapat membantu mengidentifikasi dan menyelesaikan masalah potensial sebelum berdampak pada beban kerja produksi selama peristiwa pemeliharaan nyata atau skenario kegagalan. Ini akan memastikan kepercayaan yang lebih besar pada keandalan jaringan Anda selama acara pemeliharaan. Gunakan tes Direct Connect Failover untuk memvalidasi ketahanan koneksi redundan Anda. Untuk langkah-langkah menggunakan tes AWS Direct Connect Failover, lihatTes failover Direct Connect.

Anda juga dapat memanfaatkan Amazon CloudWatch Network Monitor untuk menyediakan pemantauan aktif koneksi Direct Connect Anda. Untuk informasi selengkapnya, lihat Memantau konektivitas hybrid dengan Monitor Sintetis CloudWatch Jaringan Amazon.

Permintaan untuk penundaan atau pembatalan acara pemeliharaan

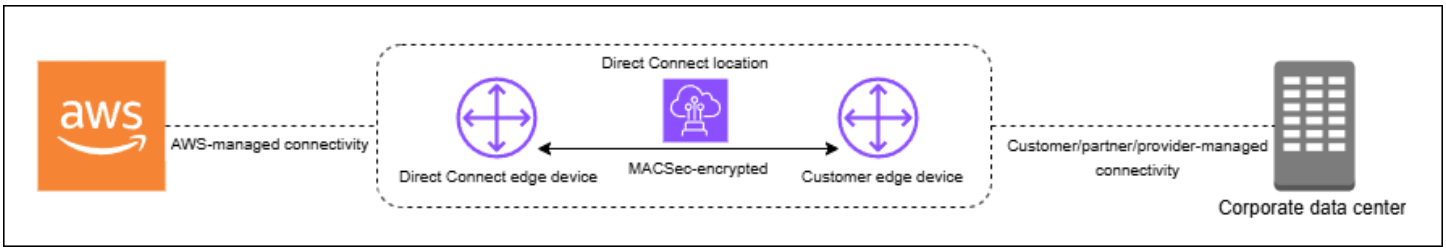
Perangkat Direct Connect dibagikan di beberapa pelanggan. Oleh karena itu, kami tidak mengakomodasi permintaan khusus untuk penjadwalan ulang atau pembatalan pemeliharaan. Permintaan penjadwalan ulang atau pembatalan untuk satu pelanggan dapat berdampak negatif pada pelanggan lain yang menggunakan titik akhir tersebut. Ini juga dapat menimbulkan risiko untuk mengurangi ketersediaan atau masalah keamanan pada waktu yang tepat.

Keamanan MAC di AWS Direct Connect

MAC Security (MACsec) adalah standar IEEE yang menyediakan kerahasiaan data, integritas data, dan keaslian asal data. MACsec menyediakan point-to-point enkripsi Layer 2 melalui cross-connect ke AWS, beroperasi antara dua router Layer 3. Sementara MACsec mengamankan koneksi antara router Anda dan lokasi Direct Connect di Layer 2, AWS memberikan keamanan tambahan dengan mengenkripsi semua data pada lapisan fisik saat mengalir melintasi jaringan antara AWS Direct Connect lokasi dan Wilayah. AWS Ini menciptakan pendekatan keamanan berlapis di mana lalu lintas Anda dilindungi baik selama entri awal ke AWS dan selama transit di seluruh AWS jaringan.

Dalam diagram berikut, AWS Direct Connect sambungan silang harus terhubung ke antarmuka MACsec yang mampu pada perangkat tepi pelanggan. MACsec over Direct Connect menyediakan enkripsi layer 2 untuk point-to-point lalu lintas antara perangkat edge Direct Connect dan perangkat edge pelanggan. Enkripsi ini terjadi setelah kunci keamanan dipertukarkan dan diverifikasi antara antarmuka di kedua ujung sambungan silang.

> **Note**
>
> MACsec memberikan point-to-point keamanan pada tautan Ethernet; oleh karena itu tidak menyediakan end-to-end enkripsi di beberapa Ethernet sekuensial atau segmen jaringan lainnya.



MACsec konsep

Berikut ini adalah konsep kunci untuk MACsec:

- MAC Security (MACsec) — Standar IEEE 802.1 Layer 2 yang menyediakan kerahasiaan data, integritas data, dan keaslian asal data. Untuk informasi selengkapnya tentang protokol, lihat 802.1AE: MAC Security (). MACsec

- Secure Association Key (SAK) — Kunci sesi yang menetapkan MACsec konektivitas antara router lokal pelanggan dan port koneksi di lokasi Direct Connect. SAK tidak dibagikan sebelumnya, melainkan secara otomatis berasal dari CKN/CAK pair through a cryptographic key generation process. This derivation happens at both ends of the connection after you provide and provision the CKN/CAK pasangan. SAK diregenerasi secara berkala untuk tujuan keamanan dan setiap kali MACsec sesi dibuat.
- Connectivity Association Key Name (CKN) dan Connectivity Association Key (CAK) — Nilai dalam pasangan ini digunakan untuk menghasilkan kunci. MACsec Anda menghasilkan nilai pasangan, mengaitkannya dengan AWS Direct Connect koneksi, dan kemudian menyediakannya di perangkat tepi Anda di akhir AWS Direct Connect koneksi Anda. Direct Connect hanya mendukung mode CAK statis tetapi tidak mode CAK dinamis. Karena hanya mode CAK statis yang didukung, Anda disarankan untuk mengikuti kebijakan manajemen kunci Anda sendiri untuk pembuatan kunci, distribusi, dan rotasi.
- Format kunci - Format kunci harus menggunakan karakter heksadesimal, tepatnya 64 karakter panjangnya. Direct Connect hanya mendukung kunci 256-bit Advanced Encryption Standard (AES) untuk koneksi khusus, yang sesuai dengan string heksadesimal 64 karakter.
- Mode enkripsi — Direct Connect mendukung dua mode MACsec enkripsi:
  - must_encrypt — Dalam mode ini, koneksi memerlukan MACsec enkripsi untuk semua lalu lintas. Jika MACsec negosiasi gagal atau enkripsi tidak dapat dibuat, koneksi tidak akan mengirimkan lalu lintas apa pun. Mode ini memberikan jaminan keamanan tertinggi tetapi dapat memengaruhi ketersediaan jika ada masalah MACsec terkait.
  - should_encrypt — Dalam mode ini, koneksi mencoba untuk membuat MACsec enkripsi tetapi akan kembali ke komunikasi yang tidak terenkripsi jika negosiasi gagal. MACsec Mode ini memberikan lebih banyak fleksibilitas dan ketersediaan yang lebih tinggi tetapi memungkinkan lalu lintas yang tidak terenkripsi dalam skenario kegagalan tertentu.

  Mode enkripsi dapat diatur selama konfigurasi koneksi dan dapat dimodifikasi nanti. Secara default, koneksi baru MACsec yang diaktifkan diatur ke mode “should_encrypt” untuk mencegah potensi masalah konektivitas selama penyiapan awal.

MACsec rotasi kunci

- Rotasi CNN/CAK (manual)

  Direct Connect MACsec mendukung MACsec gantungan kunci dengan kapasitas untuk menyimpan hingga tiga CKN/CAK pairs. This allows you to manually rotate these long-term

keys without connection disruption. When you associate a new CKN/CAK pasang menggunakan `associate-mac-sec-key` perintah, Anda harus mengkonfigurasi pasangan yang sama pada perangkat Anda. Perangkat Direct Connect mencoba menggunakan kunci yang paling baru ditambahkan. Jika kunci itu tidak cocok dengan kunci perangkat Anda, kunci tersebut akan kembali ke kunci kerja sebelumnya, memastikan stabilitas koneksi selama rotasi.

Untuk informasi tentang penggunaan`associate-mac-sec-key`, lihat associate-mac-sec-key.

- Rotasi Kunci Asosiasi Aman (SAK) (otomatis)

  SAK, yang berasal dari pasangan CKN/CAK aktif, mengalami rotasi otomatis berdasarkan hal-hal berikut:

  - interval waktu
  - volume lalu lintas terenkripsi
  - MACsec pembentukan sesi

  Rotasi ini ditangani secara otomatis oleh protokol, terjadi secara transparan tanpa mengganggu koneksi, dan tidak memerlukan intervensi manual. SAK tidak pernah disimpan terus-menerus dan diregenerasi melalui proses derivasi kunci aman yang mengikuti standar IEEE 802.1X.

Koneksi yang didukung

MACsec tersedia pada koneksi Direct Connect khusus dan grup agregasi tautan:

MACsec Koneksi yang didukung

- Koneksi khusus
- LAGs

> **Note**
>
> Koneksi yang di-host dan asosiasi Direct Connect Gateway tidak mendukung MACsec enkripsi.

Untuk informasi tentang cara memesan koneksi yang mendukung MACsec, lihat AWS Direct Connect.

Koneksi khusus

Berikut ini membantu Anda menjadi akrab dengan MACsec koneksi AWS Direct Connect khusus. Tidak ada biaya tambahan untuk penggunaan MACsec. Langkah-langkah untuk mengkonfigurasi MACsec pada koneksi khusus dapat ditemukan di MACsec Memulai dengan koneksi khusus.

MACsec prasyarat untuk koneksi khusus

Perhatikan persyaratan berikut untuk MACsec koneksi khusus:

- MACsec didukung pada koneksi Direct Connect khusus 10 Gbps, 100 Gbps, dan 400 Gbps di titik-titik kehadiran tertentu. Untuk koneksi ini, MACsec cipher suite berikut didukung:
  - Untuk koneksi 10Gbps, GCM-AES-256 dan GCM-AES-XPN-256.
  - Untuk koneksi 100 Gbps dan 400 Gbps, GCM-AES-XPN -256.

- Hanya MACsec kunci 256-bit yang didukung.
- Extended Packet Numbering (XPN) diperlukan untuk koneksi 100Gbps dan 400 Gbps. Untuk koneksi 10Gbps Direct Connect mendukung GCM-AES-256 dan -256. GCM-AES-XPN Koneksi berkecepatan tinggi, seperti koneksi khusus 100 Gbps dan 400 Gbps, dapat dengan cepat menghabiskan MACsec ruang penomoran paket 32-bit asli, yang mengharuskan Anda memutar kunci enkripsi Anda setiap beberapa menit untuk membentuk Asosiasi Konektivitas baru. Untuk menghindari situasi ini, amandemen IEEE Std 802.1 AEbw -2013 memperkenalkan penomoran paket diperpanjang, meningkatkan ruang penomoran menjadi 64-bit, mengurangi persyaratan ketepatan waktu untuk rotasi kunci.
- Secure Channel Identifier (SCI) diperlukan dan harus dihidupkan. Pengaturan ini tidak dapat disesuaikan.
- IEEE 802.1Q (dot1q/VLAN) tag q-in-clear offset/dot1 tidak didukung untuk memindahkan tag VLAN di luar muatan terenkripsi.

Selain itu Anda harus menyelesaikan tugas-tugas berikut sebelum Anda mengkonfigurasi MACsec pada koneksi khusus.

- Buat pasangan CKN/CAK untuk kuncinya. MACsec

  Anda dapat membuat pasangan menggunakan alat standar terbuka. Pasangan ini harus memenuhi persyaratan yang ditentukan dalam the section called “Konfigurasikan router lokal Anda”.

- Pastikan Anda memiliki perangkat di ujung koneksi yang mendukungMACsec.
- Secure Channel Identifier (SCI) harus dihidupkan.
- Hanya MACsec kunci 256-bit yang didukung, memberikan perlindungan data canggih terbaru.

LAGs

Persyaratan berikut membantu Anda memahami grup agregasi tautan Direct Connect (LAGs): MACsec

- LAGs harus terdiri dari enkripsi dukungan MACsec koneksi khusus yang MACsec mampu
- Semua koneksi dalam LAG harus memiliki bandwidth dan dukungan yang sama MACsec
- MACsec konfigurasi berlaku secara seragam di semua koneksi di LAG
- Pembuatan dan MACsec pemberdayaan LAG dapat dilakukan secara bersamaan

Peran Tertaut Layanan

AWS Direct Connect menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS Direct Connect Peran terkait layanan telah ditentukan sebelumnya oleh AWS Direct Connect dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda. Peran terkait layanan membuat pengaturan AWS Direct Connect lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS Direct Connect mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS Direct Connect dapat mengambil perannya. Izin yang ditentukan meliputi kebijakan kepercayaan serta kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya. Untuk informasi selengkapnya, lihat the section called “Peran terkait layanan”.

MACsec pertimbangan utama CKN/CAK yang telah dibagikan sebelumnya

AWS Direct Connect menggunakan kunci yang AWS dikelola CMKs untuk kunci yang telah dibagikan sebelumnya yang Anda kaitkan dengan koneksi atau LAGs. Secrets Manager menyimpan pasangan CKN dan CAK yang dibagikan sebelumnya sebagai rahasia yang dienkripsi oleh kunci root Secrets Manager. Untuk informasi selengkapnya, lihat AWS dikelola CMKs di Panduan AWS Key Management Service Pengembang.

Kunci yang disimpan hanya dibaca berdasarkan desain, tetapi Anda dapat menjadwalkan penghapusan tujuh hingga tiga puluh hari menggunakan konsol Secrets AWS Manager atau API. Saat menjadwalkan penghapusan, CKN tidak dapat dibaca, dan ini dapat memengaruhi konektivitas jaringan Anda. Kami menerapkan aturan berikut saat ini terjadi:

- Jika koneksi dalam status tertunda, kami akan memisahkan CKN dari koneksi.
- Jika koneksi dalam status tersedia, kami akan memberi tahu pemilik koneksi melalui email. Jika Anda tidak mengambil tindakan apa pun dalam waktu 30 hari, kami akan memisahkan CKN dari koneksi Anda.

Saat kami memisahkan CKN terakhir dari koneksi Anda dan mode enkripsi koneksi diatur ke “harus mengenkripsi”, kami akan mengatur mode ke “should_encrypt” untuk mencegah hilangnya paket secara tiba-tiba.

Mulai gunakan MACsec pada AWS Direct Connect koneksi khusus

Tugas berikut membuat Anda mulai menyiapkan MACsec untuk digunakan pada koneksi khusus Direct Connect

Langkah 1: Buat koneksi

Untuk mulai menggunakan MACsec, Anda harus mengaktifkan fitur saat Anda membuat koneksi khusus.

(Opsional) Langkah 2: Buat link aggregation group (grup agregasi tautan/ LAG)

Jika Anda menggunakan beberapa koneksi untuk redundansi, Anda dapat membuat LAG yang mendukung. MACsec Untuk informasi selengkapnya, lihat MACsec pertimbangan dan Buat LAG.

Langkah 3: Kaitkan CKN/CAK dengan koneksi atau LAG

Setelah Anda membuat koneksi atau LAG yang mendukung MACsec, Anda perlu mengaitkan CKN/ CAK dengan koneksi. Untuk informasi selengkapnya, lihat hal berikut:

- Kaitkan MACsec CKN/CAK dengan koneksi
- Kaitkan MACsec CKN/CAK dengan LAG

Langkah 4: Konfigurasikan router on-premise

Perbarui router lokal Anda dengan kunci MACsec rahasia. Kunci MACsec rahasia pada router lokal dan di AWS Direct Connect lokasi harus cocok. Untuk informasi selengkapnya, lihat Mengunduh file konfigurasi router.

Langkah 5: (Opsional) Hapus hubungan antara CKN/CAK dan koneksi atau LAG

Anda dapat secara opsional menghapus hubungan antara CKN/CAK dan koneksi atau LAG. jika Anda perlu menghapus asosiasi, lihat salah satu dari berikut ini:

- Hapus hubungan antara kunci MACsec rahasia dan koneksi
- Hapus hubungan antara kunci MACsec rahasia dan LAG

AWS Direct Connect koneksi khusus dan host

AWS Direct Connect memungkinkan Anda untuk membuat koneksi jaringan khusus antara jaringan Anda dan salah satu AWS Direct Connect lokasi.

Ada dua tipe koneksi:

- Koneksi Khusus: Koneksi Ethernet fisik yang terkait dengan satu pelanggan. Pelanggan dapat meminta koneksi khusus melalui AWS Direct Connect konsol, CLI, atau API. Untuk informasi selengkapnya, lihat Koneksi khusus.
- Hosted Connection: Koneksi Ethernet fisik yang AWS Direct Connect disediakan Partner atas nama pelanggan. Pelanggan meminta koneksi yang di-host dengan menghubungi partner di Program Partner AWS Direct Connect , yang menyediakan koneksi tersebut. Untuk informasi selengkapnya, lihat Koneksi yang di-host.

Topik

AWS Direct Connect Koneksi khusus

Untuk membuat koneksi khusus AWS Direct Connect , Anda memerlukan informasi berikut:

AWS Direct Connect lokasi

Bekerja dengan mitra dalam Program AWS Direct Connect Mitra untuk membantu Anda membangun sirkuit jaringan antara AWS Direct Connect lokasi dan pusat data, kantor, atau lingkungan colocation Anda. Mereka juga dapat membantu menyediakan ruang kolokasi dalam fasilitas yang sama dengan lokasi. Untuk informasi selengkapnya, lihat Dukungan Partner APN AWS Direct Connect.

Kecepatan port

Nilai yang mungkin adalah 1 Gbps, 10 Gbps, 100 Gbps, dan 400 Gbps.

Anda tidak dapat mengubah kecepatan port setelah Anda membuat permintaan koneksi. Untuk mengubah kecepatan port, Anda harus membuat dan mengonfigurasi koneksi baru.

Anda dapat membuat koneksi menggunakan wizard Koneksi atau membuat koneksi Klasik. Dengan menggunakan panduan Koneksi, Anda dapat mengatur koneksi menggunakan rekomendasi ketahanan. Wizard disarankan jika Anda menyiapkan koneksi untuk pertama kalinya. Jika mau, Anda dapat menggunakan Classic untuk membuat koneksi one-at-a-time. Klasik direkomendasikan jika Anda sudah memiliki pengaturan yang ada yang ingin Anda tambahkan koneksi. Anda dapat membuat koneksi mandiri, atau Anda dapat membuat koneksi untuk dikaitkan dengan LAG di akun Anda. Jika Anda mengaitkan koneksi dengan LAG, itu dibuat dengan kecepatan port yang sama dan lokasi yang ditentukan dalam LAG.

Setelah Anda meminta koneksi, kami membuat Letter of Authorization and Connecting Facility Assignment (LOA-CFA) tersedia bagi Anda untuk mengunduh atau mengirim email kepada Anda dengan permintaan informasi lebih lanjut. Jika Anda menerima permintaan untuk informasi selengkapnya, Anda harus merespons dalam waktu 7 hari atau koneksi akan dihapus. LOA-CFA adalah otorisasi untuk terhubung AWS, dan diperlukan oleh penyedia jaringan Anda untuk memesan sambungan silang untuk Anda. Jika Anda tidak memiliki peralatan di AWS Direct Connect lokasi, Anda tidak dapat memesan sambungan silang untuk diri sendiri di sana.

Operasi berikut tersedia untuk koneksi khusus:

- Buat koneksi menggunakan wizard Koneksi
- Buat koneksi Klasik
- the section called “Melihat detail koneksi”
- the section called “Perbarui koneksi”
- Kaitkan MACsec CKN/CAK dengan koneksi
- the section called “Hapus hubungan antara kunci MACsec rahasia dan koneksi”
- the section called “Menghapus koneksi”

Anda dapat menambahkan koneksi khusus ke grup agregasi tautan (LAG) yang memungkinkan Anda memperlakukan beberapa koneksi sebagai satu koneksi. Untuk informasi, lihat Mengaitkan koneksi dengan LAG.

Setelah Anda membuat koneksi, buat antarmuka virtual untuk terhubung ke sumber daya AWS publik dan privat. Untuk informasi selengkapnya, lihat Antarmuka virtual dan antarmuka virtual yang dihosting.

Jika Anda tidak memiliki peralatan di suatu AWS Direct Connect lokasi, pertama-tama hubungi AWS Direct Connect Mitra di Program AWS Direct Connect Mitra. Untuk informasi selengkapnya, lihat Dukungan Partner APN AWS Direct Connect.

Jika Anda ingin membuat koneksi yang menggunakan MAC Security (MACsec), tinjau prasyarat sebelum Anda membuat koneksi. Untuk informasi selengkapnya, lihat the section called “MACsec prasyarat untuk koneksi khusus”.

Surat Otorisasi dan Penugasan Fasilitas Penghubung (LOA-CFA)

Setelah kami memproses permintaan koneksi Anda, Anda dapat mengunduh LOA-CFA. Jika tautan tidak diaktifkan, LOA-CFA belum tersedia bagi Anda untuk diunduh. Periksa email Anda untuk permintaan informasi.

LoA yang diunduh ditandatangani secara digital dan diberi tanda air untuk memvalidasi keaslian LoA yang dikeluarkan oleh. AWS Tanda tangan digital dan tanda air di LoA. Dokumen PDF mencegah LoA yang dimodifikasi atau berpotensi curang ditindaklanjuti oleh penyedia fasilitas di situs Direct Connect. Tanda tangan digital dapat diautentikasi dengan membuka PDF dan meninjau panel tanda tangan. Dokumen yang valid akan menunjukkan “Tanda tangan valid” dan “Dokumen belum dimodifikasi sejak tanda tangan diterapkan”. Tanda air mengulangi panel tambalan dan untaian yang ditetapkan di seluruh tubuh LoA sebagai indikator keaslian visual, tetapi tidak aman.

Penagihan secara otomatis dimulai ketika port aktif atau 90 hari setelah LOA dikeluarkan, mana yang lebih dulu. Anda dapat menghindari biaya penagihan dengan menghapus port sebelum aktivasi atau dalam waktu 90 hari sejak LOA dikeluarkan.

Jika koneksi Anda tidak aktif setelah 90 hari, dan LOA-CFA belum dikeluarkan, kami akan mengirimkan email yang memberi tahu Anda bahwa port akan dihapus dalam 10 hari. Jika Anda gagal mengaktifkan port dalam periode 10 hari tambahan, port akan dihapus secara otomatis dan Anda harus memulai ulang proses pembuatan port.

Untuk langkah-langkah mengunduh LoA-CFA, lihat. Unduh LOA-CFA

> **Note**
>
> Untuk informasi lebih lanjut tentang harga, lihat AWS Direct Connect Harga. Jika Anda tidak lagi ingin koneksi setelah LOA-CFA diterbitkan, Anda harus menghapus koneksi sendiri. Untuk informasi selengkapnya, lihat Hapus AWS Direct Connect koneksi.

Topik

Buat koneksi AWS Direct Connect khusus menggunakan wizard Koneksi

Bagian ini menjelaskan pembuatan koneksi menggunakan wizard Koneksi. Jika Anda lebih suka membuat koneksi Klasik, lihat langkah-langkahnya dithe section called “Langkah 2: Minta koneksi AWS Direct Connect khusus”.

Untuk membuat koneksi wizard Koneksi

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Koneksi, lalu pilih Buat koneksi.
3. Pada halaman Buat Koneksi, di bawah Jenis pemesanan koneksi, pilih Wisaya koneksi.
4. Pilih Tingkat Ketahanan untuk koneksi jaringan Anda. Tingkat ketahanan dapat menjadi salah satu dari yang berikut:

   - Ketahanan Maksimum
   - Ketahanan Tinggi
   - Pengembangan dan Pengujian

   Untuk deskripsi dan informasi lebih rinci tentang tingkat ketahanan ini, lihat. AWS Direct Connect Toolkit Ketahanan
5. Pilih Berikutnya.
6. Pada halaman Konfigurasi koneksi, berikan detail berikut.

   a. Dari daftar drop-down Bandwidth, pilih bandwidth yang diperlukan untuk koneksi. Ini bisa di mana saja dari 1Gbps hingga 400 Gbps.

   b. Untuk Lokasi, pilih AWS Direct Connect lokasi yang sesuai, lalu pilih Penyedia layanan lokasi pertama, pilih penyedia layanan yang menyediakan konektivitas untuk koneksi di lokasi ini.

c. Untuk lokasi kedua, pilih yang sesuai AWS Direct Connect di lokasi kedua, lalu pilih penyedia layanan lokasi kedua, pilih penyedia layanan yang menyediakan konektivitas untuk koneksi di lokasi kedua ini.

d. (Opsional) Konfigurasikan keamanan MAC (MACsec) untuk koneksi. Di bawah Pengaturan Tambahan, pilih Minta port yang MACsec mampu.

   MACsec hanya tersedia pada koneksi khusus.

e. (Opsional) Pilih Tambahkan tag untuk menambahkan key/value pasangan untuk membantu mengidentifikasi koneksi ini lebih lanjut.

   - Untuk Kunci, masukkan nama kunci.
   - Untuk Nilai, masukkan nilai kunci.

   Untuk menghapus tag yang ada, pilih tag dan kemudian pilih Hapus tag. Anda tidak dapat memiliki tag kosong.

7. Pilih Berikutnya.
8. Pada halaman Tinjau dan buat, verifikasi koneksi. Halaman ini juga menampilkan perkiraan biaya untuk penggunaan port dan biaya transfer data tambahan.
9. Pilih Buat.
10. Unduh Surat Otorisasi dan Penugasan Fasilitas Penghubung (LOA-CFA) Anda, Untuk informasi lebih lanjut, lihat. the section called “Surat Otorisasi dan Penugasan Fasilitas Penghubung (LOA-CFA)”

Gunakan salah satu perintah berikut ini.

- create-connection (AWS CLI)
- CreateConnection(AWS Direct Connect API)

Buat koneksi AWS Direct Connect Klasik

Untuk koneksi khusus, Anda dapat mengirimkan permintaan koneksi menggunakan AWS Direct Connect konsol. Untuk koneksi yang dihosting, bekerja sama dengan AWS Direct Connect Mitra untuk meminta koneksi yang dihosting. Pastikan bahwa Anda memiliki informasi berikut:

- Kecepatan port yang Anda butuhkan. Untuk koneksi khusus, Anda tidak dapat mengubah kecepatan port setelah membuat permintaan koneksi. Untuk koneksi yang di-host, AWS Direct Connect Mitra Anda dapat mengubah kecepatan.
- AWS Direct Connect Lokasi di mana koneksi akan diakhiri.

> **Note**
>
> Anda tidak dapat menggunakan AWS Direct Connect konsol untuk meminta koneksi yang dihosting. Sebagai gantinya, hubungi AWS Direct Connect Mitra, yang dapat membuat koneksi yang dihosting untuk Anda, yang kemudian Anda terima. Lewati prosedur berikut dan pergi ke Terima koneksi yang di-host.

Untuk membuat AWS Direct Connect koneksi baru

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Pada layar AWS Direct Connect, di bawah Memulai, pilih Buat koneksi.
3. PilihKlasik.
4. Untuk Nama, masukkan nama untuk koneksi.
5. Untuk Lokasi, pilih lokasi AWS Direct Connect yang sesuai.
6. Jika berlaku, untuk Sub-lokasi, pilih lantai yang paling dekat dengan Anda atau penyedia jaringan Anda. Opsi ini hanya tersedia jika lokasi memiliki ruang meet-me (MMRs) di beberapa lantai gedung.
7. Untuk Kecepatan Port, pilih bandwidth koneksi.
8. Untuk On-Premise, pilih Terhubung melalui partner AWS Direct Connect saat Anda menggunakan koneksi ini untuk menghubungkan ke pusat data Anda.
9. Untuk penyedia layanan, pilih AWS Direct Connect Partner. Jika Anda menggunakan partner yang tidak ada dalam daftar, pilih Lainnya.
10. Jika Anda memilih Lainnya untuk Penyedia layanan, untuk Nama penyedia lain, masukkan nama partner yang Anda gunakan.
11. (Opsional) Pilih Tambahkan tag untuk menambahkan key/value pasangan untuk membantu mengidentifikasi koneksi ini lebih lanjut.
    - Untuk Kunci, masukkan nama kunci.
    - Untuk Nilai, masukkan nilai kunci.

Untuk menghapus tag yang ada, pilih tag dan kemudian pilih Hapus tag. Anda tidak dapat memiliki tag kosong.

12. Pilih Buat Koneksi.

Diperlukan waktu hingga 72 jam AWS untuk meninjau permintaan Anda dan menyediakan port untuk koneksi Anda. Selama waktu ini, Anda mungkin menerima email berisi permintaan untuk informasi lebih lanjut tentang kasus penggunaan atau lokasi yang ditentukan. Email dikirim ke alamat email yang Anda gunakan saat mendaftar AWS. Anda harus merespons dalam waktu 7 hari atau koneksi akan dihapus.

Untuk informasi selengkapnya, lihat Koneksi khusus dan host.

Unduh AWS Direct Connect LOA-CFA

Anda dapat mengunduh LOA-CFA menggunakan AWS Direct Connect konsol atau melalui baris perintah. Setelah Anda mengunduh LOA-CFA dan menyediakannya ke jaringan atau penyedia colocation Anda, penyedia tersebut dapat memesan koneksi silang untuk Anda.

Untuk mengunduh LOA-CFA

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Koneksi.
3. Pilih koneksi, kemudian pilih Lihat Detail.
4. Pilih Unduh LOA-CFA.

> **Note**
>
> Jika tautan tidak diaktifkan, LOA-CFA belum tersedia bagi Anda untuk diunduh. Kasus Support akan dibuat meminta informasi tambahan. Setelah Anda menanggapi permintaan, dan permintaan diproses, LOA-CFA akan tersedia untuk diunduh. Jika masih belum tersedia, hubungi AWS Support.

5. Kirim LOA-CFA ke penyedia jaringan atau kolokasi penyedia Anda sehingga mereka dapat memesan koneksi silang untuk Anda. Proses kontak dapat bervariasi untuk setiap penyedia kolokasi. Untuk informasi selengkapnya, lihat Meminta koneksi silang di lokasi AWS Direct Connect.

Untuk mengunduh LOA-CFA menggunakan baris perintah atau API

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct Connect API)

Kaitkan MACsec CKN/CAK dengan koneksi AWS Direct Connect

Setelah Anda membuat koneksi yang mendukung MACsec, Anda dapat mengaitkan CKN/CAK dengan koneksi. Anda dapat membuat asosiasi menggunakan AWS Direct Connect konsol atau melalui baris perintah atau API.

> **Note**
>
> Anda tidak dapat memodifikasi kunci MACsec rahasia setelah Anda mengaitkannya dengan koneksi. Jika Anda perlu mengubah kunci, memisahkan kunci dari koneksi, lalu mengaitkan kunci baru dengan koneksi. Untuk informasi tentang menghapus pengaitan, lihat Hapus hubungan antara kunci MACsec rahasia dan koneksi.

Untuk mengaitkan MACsec kunci dengan koneksi

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel sebelah kiri, pilih Koneksi.
3. Pilih koneksi, kemudian pilih Lihat detail.
4. Pilih Kaitkan kunci.
5. Masukkan MACsec kuncinya.

   [Gunakan CAK/CKN pasangan] Pilih Key Pair, lalu lakukan hal berikut:

   - Untuk Connectivity Association Key (CAK), masukkan CAK.
   - Untuk Connectivity Association Key Name (CKN), masukkan CKN.

   [Gunakan rahasia] Pilih rahasia Manajer Rahasia yang Ada, lalu untuk Rahasia, pilih kunci MACsec rahasia.
6. Pilih Kaitkan kunci.

Untuk mengaitkan MACsec kunci dengan koneksi menggunakan baris perintah atau API

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(AWS Direct Connect API)

Hapus hubungan antara kunci MACsec rahasia dan AWS Direct Connect koneksi

Anda dapat menghapus hubungan antara koneksi dan MACsec kunci menggunakan AWS Direct Connect konsol atau melalui baris perintah atau API.

Untuk menghapus hubungan antara koneksi dan MACsec kunci

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2.
3. Di panel sebelah kiri, pilih Koneksi.
4. Pilih koneksi, kemudian pilih Lihat detail.
5. Pilih MACsec rahasia yang akan dihapus, lalu pilih Disassociate kunci.
6. Di kotak dialog konfirmasi, masukkan pisahkan, lalu pilihPisahkan.

Untuk menghapus asosiasi antara koneksi dan MACsec kunci menggunakan baris perintah atau API

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct Connect API)

AWS Direct Connect Koneksi yang di-host

Untuk membuat koneksi yang AWS Direct Connect di-host, Anda memerlukan informasi berikut:

AWS Direct Connect lokasi

Bekerja dengan AWS Direct Connect Mitra dalam Program AWS Direct Connect Mitra untuk membantu Anda membangun sirkuit jaringan antara AWS Direct Connect lokasi dan pusat data, kantor, atau lingkungan colocation Anda. Mereka juga dapat membantu menyediakan ruang kolokasi dalam fasilitas yang sama dengan lokasi. Untuk informasi selengkapnya, lihat Mitra AWS Direct Connect Pengiriman.

> **Note**
>
> Anda tidak dapat meminta koneksi yang dihosting melalui AWS Direct Connect konsol. Namun, AWS Direct Connect Mitra dapat membuat dan mengonfigurasi koneksi yang dihosting untuk Anda. Setelah dikonfigurasi, koneksi muncul di panel Koneksi di konsol. Anda harus menerima koneksi yang di-host sebelum Anda dapat menggunakannya. Untuk informasi selengkapnya, lihat Terima koneksi yang di-host.

Kecepatan port

Untuk koneksi yang di-host, nilai yang mungkin adalah 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps, dan 25 Gbps. Perhatikan bahwa hanya AWS Direct Connect mitra yang telah memenuhi persyaratan khusus yang dapat membuat koneksi host 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps, atau 25 Gbps. Koneksi 25 Gbps hanya tersedia di lokasi Direct Connect di mana kecepatan port 100 Gbps tersedia.

Perhatikan hal berikut:

- Kecepatan port koneksi hanya dapat diubah oleh AWS Direct Connect Partner Anda. Silakan hubungi AWS Direct Connect Partner Anda untuk melihat apakah mereka mendukung peningkatan atau penurunan versi koneksi yang ada. Jika Mitra mendukung peningkatan/penurunan versi koneksi Anda, Anda tidak lagi diharuskan untuk menghapus dan kemudian membuat ulang koneksi untuk meningkatkan atau menurunkan bandwidth koneksi host yang ada.
- AWS menggunakan kepolisian lalu lintas pada koneksi yang dihosting, yang berarti bahwa ketika tingkat lalu lintas mencapai tingkat maksimum yang dikonfigurasi, kelebihan lalu lintas turun. Hal ini mungkin mengakibatkan lonjakan lalu lintas memiliki throughput yang lebih rendah daripada lalu lintas tanpa lonjakan.
- Frame jumbo dapat diaktifkan pada koneksi hanya jika awalnya diaktifkan pada koneksi induk yang AWS Direct Connect dihosting. Jika bingkai Jumbo tidak diaktifkan pada koneksi induk itu, maka frame Jumbo tidak dapat diaktifkan pada koneksi apa pun.

Operasi konsol berikut tersedia setelah Anda meminta koneksi yang di-host dan menerimanya:

- Menghapus koneksi
- Perbarui koneksi

- Melihat detail koneksi

Setelah Anda menerima koneksi, buat antarmuka virtual untuk terhubung ke sumber daya AWS publik dan privat. Untuk informasi selengkapnya, lihat Antarmuka virtual dan antarmuka virtual yang dihosting.

Terima koneksi yang AWS Direct Connect di-host

Jika Anda tertarik untuk membeli koneksi yang dihosting, Anda harus menghubungi AWS Direct Connect Mitra di Program AWS Direct Connect Mitra. Partner akan menyediakan koneksi untuk Anda. Setelah dikonfigurasi, koneksi tersebut akan muncul di panel Koneksi di konsol AWS Direct Connect .

Sebelum Anda dapat mulai menggunakan koneksi yang di-host, Anda harus menerima koneksi. Anda dapat menerima koneksi yang di-host menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Koneksi.
3. Pilih koneksi yang di-host, dan pilih Lihat detail.
4. Pilih kotak centang konfirmasi dan pilih Terima.

Untuk menerima koneksi host menggunakan baris perintah atau API

- confirm-connection (AWS CLI)
- ConfirmConnection(AWS Direct Connect API)

Hapus AWS Direct Connect koneksi

Anda dapat menghapus koneksi selama tidak ada antarmuka virtual yang terampir. Menghapus koneksi Anda menghentikan semua biaya jam port untuk koneksi ini, tetapi Anda mungkin masih dikenakan biaya sambungan silang atau sirkuit jaringan (lihat di bawah). AWS Direct Connect Biaya transfer data dikaitkan dengan antarmuka virtual. Untuk informasi selengkapnya tentang cara menghapus antarmuka virtual, lihat Hapus antarmuka virtual.

Sebelum menghapus koneksi, unduh LOA untuk koneksi yang berisi informasi lintas akun sehingga Anda memiliki informasi yang relevan tentang sirkuit yang terputus. Untuk langkah-langkah mengunduh koneksi LOA, lihatSurat Otorisasi dan Penugasan Fasilitas Penghubung (LOA-CFA).

Ketika Anda menghapus koneksi, AWS akan menginstruksikan penyedia colocation untuk memutuskan sambungan perangkat jaringan Anda dari router Direct Connect dengan melepas kabel cross-connect serat optik dari panel patch yang berlaku. AWS Namun, penyedia kolokasi atau sirkuit Anda mungkin masih mengisi daya koneksi silang atau muatan sirkuit jaringan karena kabel sambungan silang mungkin masih terhubung ke perangkat jaringan Anda. Biaya untuk sambungan silang ini tidak tergantung pada Direct Connect, dan harus dibatalkan dengan penyedia kolokasi atau sirkuit menggunakan informasi dari LOA.

Jika koneksi adalah bagian dari grup agregasi tautan (LAG), Anda tidak dapat menghapus koneksi jika melakukannya menyebabkan LAG jatuh di bawah pengaturan untuk jumlah minimum koneksi operasional.

Anda dapat menghapus koneksi menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Untuk menghapus koneksi

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Koneksi.
3. Pilih koneksi dan pilih Hapus.
4. Di kotak dialog Hapus konfirmasi, pilih Hapus.

Untuk menghapus koneksi menggunakan baris perintah atau API

- delete-connection (AWS CLI)
- DeleteConnection(AWS Direct Connect API)

Perbarui AWS Direct Connect koneksi

Anda dapat memperbarui atribut koneksi berikut menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

- Nama koneksi.

- Mode MACsec enkripsi koneksi.

> **Note**
>
> MACsec hanya tersedia pada koneksi khusus.

Nilai yang benar adalah:

- `should_encrypt`
- `must_encrypt`

  Saat Anda mengatur mode enkripsi ke nilai ini, koneksi akan mengalami masalah saat enkripsi mengalami masalah.
- `no_encrypt`

Untuk memperbarui koneksi

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Koneksi.
3. Pilih koneksi, kemudian pilih Edit.
4. Modifikasi koneksi:

   [Ubah nama] Untuk Nama, masukkan nama baru.

   [Tambahkan tanda] Pilih Tambahkan tanda dan lakukan hal berikut:

   - Untuk Kunci, masukkan nama kunci.
   - Untuk Nilai, masukkan nilai kunci.

   [Hapus tanda] Di samping tanda, pilih Hapus tanda.
5. Pilih Edit koneksi.

Untuk memperbarui koneksi menggunakan baris perintah atau API

- update-connection (AWS CLI)
- UpdateConnection(AWS Direct Connect API)

Lihat detail AWS Direct Connect koneksi

Anda dapat melihat status koneksi Anda saat ini menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API. Anda juga dapat melihat ID koneksi Anda (misalnya, `dxcon-12nikabc`) dan memverifikasi bahwa ID cocok dengan ID koneksi pada LOA-CFA yang Anda terima atau unduh.

Untuk informasi tentang koneksi pemantauan, lihat Memantau sumber daya Direct Connect.

Untuk melihat detail tentang koneksi

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel sebelah kiri, pilih Koneksi.
3. Pilih koneksi, kemudian pilih Lihat detail.

Untuk mendeskripsikan koneksi menggunakan baris perintah atau API

- describe-connections (AWS CLI)
- DescribeConnections(AWS Direct Connect API)

Meminta koneksi silang di lokasi AWS Direct Connect

Setelah mengunduh Letter of Authorization and Connecting Facility Assignment (LOA-CFA), Anda harus menyelesaikan koneksi lintas jaringan Anda, juga dikenal sebagai koneksi silang. Jika Anda sudah memiliki peralatan yang terletak di suatu AWS Direct Connect lokasi, hubungi penyedia yang sesuai untuk menyelesaikan sambungan silang. Untuk instruksi khusus untuk setiap penyedia, lihat tabel di bawah ini. Mitra dan informasi kontak diatur berdasarkan Wilayah. Untuk harga cross connect tertentu, Anda harus menghubungi Direct Connect Partner secara langsung. Setelah koneksi silang dibuat, Anda dapat membuat antarmuka virtual menggunakan AWS Direct Connect konsol.

Beberapa lokasi ditetapkan sebagai kampus. Untuk informasi selengkapnya, termasuk kecepatan yang tersedia di setiap lokasi, lihat AWS Direct Connect Lokasi.

Jika Anda belum memiliki peralatan yang terletak di suatu AWS Direct Connect lokasi, Anda dapat bekerja dengan salah satu mitra di Jaringan AWS Mitra (APN). Mereka membantu Anda untuk terhubung ke lokasi AWS Direct Connect . Untuk informasi selengkapnya, lihat Partner APN yang mendukung AWS Direct Connect. Anda harus berbagi LOA-CFA dengan penyedia pilihan Anda untuk memfasilitasi permintaan koneksi silang Anda.

AWS Direct Connect Koneksi dapat menyediakan akses ke sumber daya di Wilayah lain. Untuk informasi selengkapnya, lihat Akses ke AWS Direct Connect Daerah Terpencil.

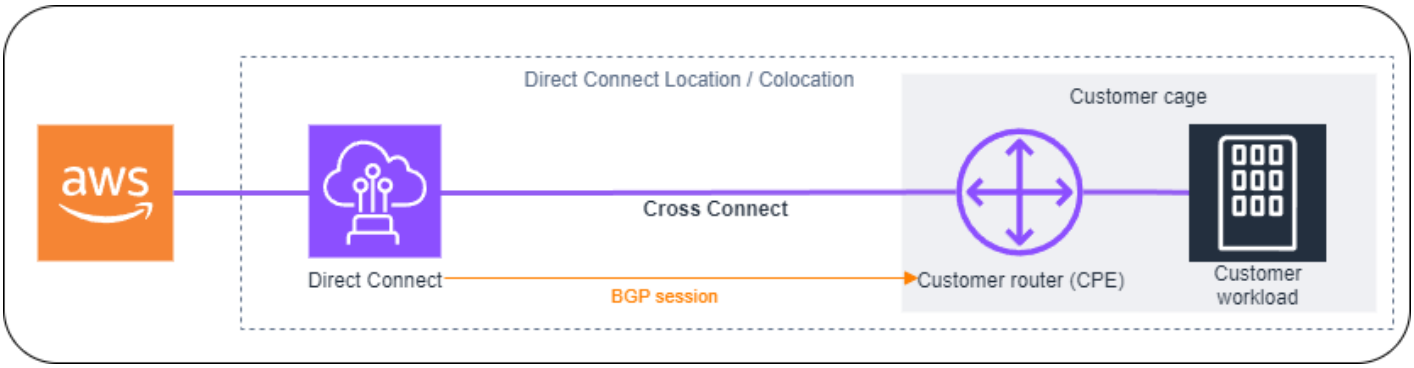
> **Note**
>
> Jika koneksi silang tidak selesai dalam waktu 90 hari, otoritas yang diberikan oleh LOA-CFA akan kedaluwarsa. Untuk memperbarui LOA-CFA yang telah kedaluwarsa, Anda dapat mengunduh lagi dari konsol AWS Direct Connect . Untuk informasi selengkapnya, lihat Surat Otorisasi dan Penugasan Fasilitas Penghubung (LOA-CFA).

Opsi konektivitas

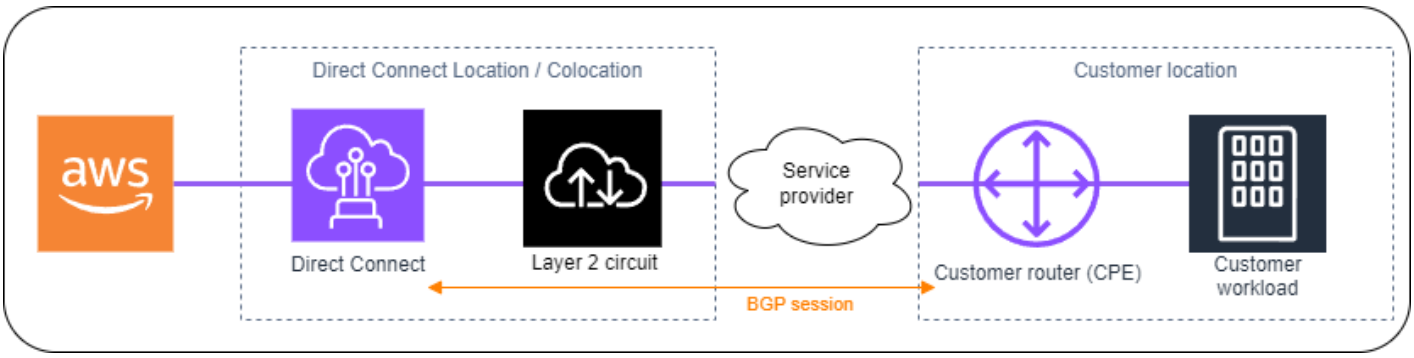
Opsi yang tersedia untuk terhubung ke lokasi Direct Connect mungkin berbeda menurut Mitra dan AWS Wilayah. Anda dapat bekerja dengan salah satu mitra di Jaringan AWS Mitra (APN) yang dapat menyediakan satu atau beberapa opsi konektivitas berikut:

- Jika Anda memiliki sumber daya yang digunakan di center/colocation fasilitas data yang sama dengan lokasi Direct Connect, fasilitas tersebut dapat menyediakan koneksi silang antara AWS

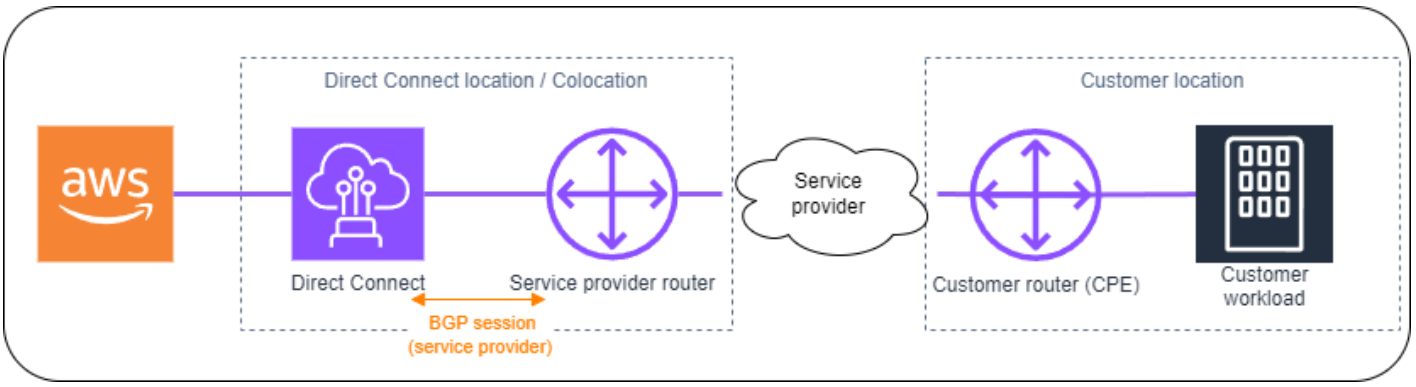
Direct Connect peralatan dan sumber daya Anda. Anda harus terlebih dahulu memberikan LOA-CFA ke fasilitas untuk ini. Untuk informasi selengkapnya, lihat Surat Otorisasi dan Penugasan Fasilitas Penghubung (LOA-CFA). Berikut ini menunjukkan contoh opsi konektivitas Direct Connect ini:



- Perluas koneksi Direct Connect di Layer 2 (layer data link) melalui “sirkuit” dari lokasi Direct Connect ke lokasi pelanggan dengan bekerja sama dengan Direct Connect Partners. Router yang dipasang di lokasi pelanggan akan langsung membentuk sesi BGP dengan peralatan tersebut. AWS Misalnya, teknologi yang dapat digunakan adalah Metro Ethernet, Dark Fibre, atau Wavelength. Berikut ini menunjukkan contoh opsi konektivitas Direct Connect ini.



- Perluas koneksi Direct Connect di Layer 3 (Network layer) dari lokasi Direct Connect ke lokasi Anda dengan bekerja sama dengan Direct Connect Partners. Untuk opsi konektivitas ini, Direct Connect Partner menyediakan router di dalam lokasi Direct Connect yang membentuk sesi Border Gateway Protocol (BGP) dengan peralatan. AWS Mitra Direct Connect kemudian mendirikan BGP lain dengan Anda; misalnya, ini mungkin melalui Multiprotocol Label Switching (MPLS). Berikut ini menunjukkan contoh opsi konektivitas Direct Connect ini.



AS Timur (Ohio)

Lokasi	Cara meminta koneksi
Cologix COL2, Columbus	Hubungi Cologix di sales@cologix.com.
Cologix MIN3, Minneapolis	Hubungi Cologix di sales@cologix.com.
CyrusOne Barat III, Houston	Kirim permintaan menggunakan formulir kontak pelanggan.
Equinix CH2, Chicago	Hubungi Equinix di awsdealreg@equinix.com.
QTS, Chicago	Hubungi QTS di AConnect@qtsdatacenters .com.
Pusat Data Netralitas, 1102 Grand, Kota Kansas	Hubungi Pusat Data Netrality di support@netrality.com.

AS Timur (Virginia Utara)

Lokasi	Cara meminta koneksi
165 Halsey Street, Newark	Hubungi operations@165halsey.com.
CoreSite 32k, New York	Lakukan pemesanan menggunakan Portal CoreSite Pelanggan . Setelah Anda melengkapi formulir, tinjau akurasi pesanan, kemudian setujui pesanan menggunakan situs web.

Lokasi	Cara meminta koneksi
CoreSite VA1-VA2, Reston	Lakukan pemesanan di Portal CoreSite Pelanggan. Setelah Anda melengkapi formulir, tinjau akurasi pesanan, kemudian setujui pesanan menggunakan situs web.
Realty Digital ATL1 &ATL2, Atlanta	Hubungi Digital Realty di amazon.orders@digitalrealty.com.
Realitas Digital IAD38, Ashburn	Hubungi Digital Realty di amazon.orders@digitalrealty.com.
Equinix DC1 - DC6 & DC1 0-D12, Ashburn	Hubungi Equinix di awsdealreg@equinix.com.
Equinix DAA1 - DC3 & DC6, Dallas	Hubungi Equinix di awsdealreg@equinix.com.
Equinix MI1, Miami	Hubungi Equinix di awsdealreg@equinix.com.
Equinix NY5, Seacaucus	Hubungi Equinix di awsdealreg@equinix.com.
Jaringan KIO QRO1, Queretaro, MX	Hubungi Jaringan KIO".
Markley, One Summer Street, Boston	Untuk pelanggan saat ini, buat permintaan menggunakan portal pelanggan. Untuk kueri baru, hubungi sales@markleygroup .com.
Pusat Data Netrality, MMR lantai 2, Philadelphia	Hubungi Pusat Data Netrality di support@netrality.com.
QTS ATL1, Atlanta	Hubungi QTS di AConnect@qtsdatacenters .com.

AS Barat (California Utara)

Lokasi	Cara meminta koneksi
CoreSite, LA1, Los Angeles	Lakukan pemesanan menggunakan Portal CoreSite Pelanggan. Setelah Anda melengkapi formulir, tinjau akurasi pesanan, kemudian setujui pesanan menggunakan situs web.
CoreSite SV2, Milpitas	Lakukan pemesanan menggunakan Portal CoreSite Pelanggan. Setelah Anda melengkapi formulir, tinjau akurasi pesanan, kemudian setujui pesanan menggunakan situs web.
CoreSite SV4Santa Clara	Lakukan pemesanan menggunakan Portal CoreSite Pelanggan. Setelah Anda mengisi formulir, tinjau pesanan untuk akurasi, dan kemudian setujui menggunakan MyCoreSite situs web.
EdgeConneX, Phoenix	Buat pesanan menggunakan Portal Pelanggan EdgeOS. Setelah Anda mengirimkan formulir, EdgeConne X akan memberikan formulir pemesanan layanan untuk persetujuan. Anda dapat mengirim pertanyaan ke cloudaccess@edgeconnex.com.
Equinix, El LA3 Segundo	Hubungi Equinix di awsdealreg@equinix.com.
Equinix SV1 & SV5, San Jose	Hubungi Equinix di awsdealreg@equinix.com.
PhoenixNAP, Phoenix	Hubungi phoenixNAP Provisioning di provisioning@phoenixnap.com.

US West (Oregon)

Lokasi	Cara meminta koneksi
CoreSite DE1, Denver	Lakukan pemesanan menggunakan Portal CoreSite Pelanggan. Setelah Anda melengkapi formulir, tinjau akurasi pesanan, kemudian setujui pesanan menggunakan situs web.

Lokasi	Cara meminta koneksi
Digital Realty SEA1 0, Gedung Westin, Seattle	Hubungi Digital Realty di amazon.orders@digitalrealty.com.
EdgeConneX, Portland	Buat pesanan menggunakan Portal Pelanggan EdgeOS. Setelah Anda mengirimkan formulir, EdgeConne X akan memberikan formulir pemesanan layanan untuk persetujuan. Anda dapat mengirim pertanyaan ke cloudaccess@edgeconnex.com.
Equinix SE2, Seattle	Hubungi Equinix di support@equinix.com.
Pittock Block, Portland	Permintaan dikirimkan melalui email ke crossconnect@pittock.com atau melalui telepon di +1 503 226 6777.
Mando SUPERNAP 8, Las Vegas	Kontak Switch SUPERNAP di orders@supernap.com.
TierPoint Seattle	Hubungi TierPoint di sales@tierpoint.com.

Afrika (Cape Town)

Lokasi	Cara meminta koneksi
Cape Town Internet Exchange/Teraco Data Centres	Hubungi Teraco di support@teraco.co.za untuk pelanggan Teraco yang sudah ada atau connect@teraco.co.za untuk pelanggan baru.
Teraco JB1, Johannesburg, Afrika Selatan	Hubungi Teraco di support@teraco.co.za untuk pelanggan Teraco yang sudah ada atau connect@teraco.co.za untuk pelanggan baru.

Asia Pasifik (Jakarta)

Lokasi	Cara meminta koneksi
DCI JK3, Jakarta	Hubungi DCI Indonesia di awsdx@dci-indonesia.com.
Pusat Data NTT 2, Jakarta	Hubungi NTT di tps.cms.presales@global.ntt.

Asia Pasifik (Mumbai)

Lokasi	Cara meminta koneksi
Equinix, Mumbai	Hubungi Equinix di awsdealreg@equinix.com.
NetMagic DC2, Bangalore	Hubungi NetMagic Sales and Marketing bebas pulsa di 18001033130 atau di marketing@netmagicsolutions.com.
Sify Rabale, Mumbai	Hubungi Sizy di aws.directconnect@sifycorp.com.
STT Delhi, Delhi DC2	Hubungi STT di pertanyaan. AWSDX@sttelemediagdc .in.
STT GDC Pvt. Ltd. VSB, Chennai	Hubungi STT di pertanyaan. AWSDX@sttelemediagdc .in.
STT Haiderabad, Haiderabad DC1	Hubungi STT di pertanyaan. AWSDX@sttelemediagdc .in.

Asia Pasifik (Seoul)

Lokasi	Cara meminta koneksi
Digital Realty ICN1, Seoul	Hubungi Digital Realty di amazon.orders@digitalrealty.com.
KINX Gasan Data Center, Seoul	Hubungi KINX di sales@kinx.net.

Lokasi	Cara meminta koneksi
LG U+ Pyeong-Chon Mega Center, Seoul	Kirim dokumen LOA ke kidcadmin@lguplus.co.kr dan center8@kidc.net.

Asia Pacific (Singapore)

Lokasi	Cara meminta koneksi
Equinix HK1, Tsuen Wan NT, Hong Kong SAR	Hubungi Equinix di awsdealreg@equinix.com.
Equinix SG2, Singapura	Hubungi Equinix di awsdealreg@equinix.com.
Global Switch, Singapore	Hubungi Global Switch di salessingapore@globalswitch.com.
GPX, Mumbai	Hubungi GPX (Equinix) di awsdealreg@equinix.com.
iAdvantandae Mega-i, Hong Kong	Hubungi iAdvantandae di cs@iadvantandae.net atau buat pesanan menggunakan Formulir Elektronik Pesanan Kabel iAdvantandae .
Menara AIMS, Kuala Lumpur	Custom AIMS yang ada dapat meminta pesanan X-Connect menggunakan portal Layanan Pelanggan dengan mengisi Formulir Permintaan Pesanan Kerja Teknik. Menghubungi service.delivery@aims.com.my jika ada masalah dalam mengirimkan permintaan.
Pusat Data TCC, Bangkok	Hubungi TCC Technology Co., Ltd di gateway.ne@tcc-technology.com.

Asia Pasifik (Sydney)

Lokasi	Cara meminta koneksi
CDC Hume 2, Canberra	Masuk ke portal pelanggan di Portal Pelanggan CDC.

Lokasi	Cara meminta koneksi
Datacom, Kota Auckland DH6	Hubungi Datacom di Datacom Orbit —Auckland.
Equinix ME2, Melbourne	Hubungi Equinix di awsdealreg@equinix.com.
Equinix SY3, Sydney	Hubungi Equinix di awsdealreg@equinix.com.
Global Switch, Sydney	Hubungi Global Switch di salessydney@globalswitch.com.
NEXTDC C1, Canberra	Hubungi NEXTDC di nxtops@nextdc.com.
NEXTDC M1, Melbourne	Hubungi NEXTDC di nxtops@nextdc.com.
NEXTDC P1, Perth	Hubungi NEXTDC di nxtops@nextdc.com.
BERIKUTNYADC S2, Sydney	Hubungi NEXTDC di nxtops@nextdc.com.

Asia Pacific (Tokyo)

Lokasi	Cara meminta koneksi
AT Tokyo Chuo Data Center, Tokyo	Hubungi AT TOKYO di at-sales@attokyo.co.jp.
Chief Telecom LY, Taipei	Hubungi Chief Telecom di vicky_chan@chief.com.tw.
Chunghwa Telecom, Taipei	Hubungi CHT Taipei IDC NOC di taipei_idc@cht.com.tw.
Equinix OS1, Osaka	Hubungi Equinix di awsdealreg@equinix.com.
Equinix TY2, Tokyo	Hubungi Equinix di awsdealreg@equinix.com.
NEC Inzai, Inzai	Hubungi NEC Inzai di connection_support@ices.jp.nec.com.

Kanada (Pusat)

Lokasi	Cara meminta koneksi
Telehouse, 250 Depan St W, Toronto	Hubungi product@ca.telehouse.com.
Cologix MTL3, Montreal	Hubungi Cologix di sales@cologix.com.
Cologix VAN2, Vancouver	Hubungi Cologix di sales@cologix.com.
eStruxture, Montreal	Hubungi eStruxture di directconnect@estruxture.com.

China (Beijing)

Lokasi	Cara meminta koneksi
CIDS Jiachuang IDC, Beijing	Hubungi dx-order@sinnet.com.cn.
Sinnet Jiuxianqiao IDC, Beijing	Hubungi dx-order@sinnet.com.cn.
GDS No. 3 Data Center, Shanghai	Hubungi dx@nwcdcloud.cn.
GDS No. 3 Data Center, Shenzhen	Hubungi dx@nwcdcloud.cn.

China (Ningxia)

Lokasi	Cara meminta koneksi
Industrial Park IDC, Ningxia	Hubungi dx@nwcdcloud.cn.
Shapotou IDC, Ningxia	Hubungi dx@nwcdcloud.cn.

Eropa (Frankfurt)

Lokasi	Cara meminta koneksi
CE Colo, Prague, Czech Republic	Hubungi CE Colo di info@cecolo.com.
DigiPlex Ulven, Oslo, Norwegia	Hubungi DigiPlex di helpme@digiplex.com.
Equinix AM3, Amsterdam, Belanda	Hubungi Equinix di awsdealreg@equinix.com.
Equinix FR5, Frankfurt am Main	Hubungi Equinix di awsdealreg@equinix.com.
Equinix HE6, Helsinki	Hubungi Equinix di awsdealreg@equinix.com.
Equinix MU1, München	Hubungi Equinix di awsdealreg@equinix.com.
Equinix WA1, Warsawa	Hubungi Equinix di awsdealreg@equinix.com.
Interxion AMS7, Amsterdam	Hubungi Interxion di customer.services@interxion.com.
Interxion CPH2, Kopenhagen	Hubungi Interxion di customer.services@interxion.com.
Interxion, Frankfurt am Main FRA6	Hubungi Interxion di customer.services@interxion.com.
Interxion MAD2, Madrid	Hubungi Interxion di customer.services@interxion.com.
Interxion VIE2, Wina	Hubungi Interxion di customer.services@interxion.com.
Interxion ZUR1, Zürich	Hubungi Interxion di customer.services@interxion.com.
IPB, Berlin	Hubungi IPB di kontakt@ipb.de.
Equinix ITConic MD2, Madrid	Hubungi Equinix di awsdealreg@equinix.com.

Eropa (Irlandia)

Lokasi	Cara meminta koneksi
Digital Realty (UK), Docklands	Hubungi Digital Realty (UK) di amazon.orders@digitalrealty.com.
Eircom Clonshaugh	Hubungi Eircom di datacentre@eirevo.ie.
Equinix DX1, Dublin	Hubungi Equinix di awsdealreg@equinix.com.
Equinix LD5, London (Slough)	Hubungi Equinix di awsdealreg@equinix.com.
Interxion DUB2, Dublin	Hubungi Interxion di customer.services@interxion.com.
Interksi, Marseille MRS1	Hubungi Interxion di customer.services@interxion.com.

Eropa (Milan)

Lokasi	Cara meminta koneksi
CDLAN srl Via Caldera 21, Milano	Hubungi CDLAN di sales@cdlan.it.
Equinix,, ML2 Milano, Italia	Hubungi Equinix di awsdealreg@equinix.com.

Eropa (London)

Lokasi	Cara meminta koneksi
Digital Realty (UK), Docklands	Hubungi Digital Realty (UK) di amazon.orders@digitalrealty.com.
Equinix LD5, London (Slough)	Hubungi Equinix di awsdealreg@equinix.com.
Equinix MA3, Manchester	Hubungi Equinix di awsdealreg@equinix.com.

Lokasi	Cara meminta koneksi
Telehouse West, London	Hubungi Telehouse UK di sales.support@uk.telehouse.net.

Eropa (Paris)

Lokasi	Cara meminta koneksi
Equinix PA3, Paris	Hubungi Equinix di awsdealreg@equinix.com.
Interksi, Paris PAR7	Hubungi Interxion di customer.services@interxion.com.
Telehouse Voltaire, Paris	Hubungi Telehouse Paris Voltaire menggunakan halaman Hubungi Kami.

Eropa (Stockholm)

Lokasi	Cara meminta koneksi
Interxion STO1, Stockholm	Hubungi Interxion di customer.services@interxion.com.

Eropa (Zürich)

Lokasi	Cara meminta koneksi
Equinix, ZRH51 Oberengstringen, Swiss	Hubungi Equinix di awsdealreg@equinix.com.

Israel (Tel Aviv)

Lokasi	Cara meminta koneksi
MedOne, Haifa	Kontak MedOne di support@Medone.co.il

Lokasi	Cara meminta koneksi
EdgeConnex, Herzliya	Kontak EdgeConnect di info@edgeconnecx.com

Timur Tengah (Bahrain)

Lokasi	Cara meminta koneksi
AWS Bahrain DC53, Manama	Untuk menyelesaikan koneksi, Anda dapat bekerja dengan salah satu partner penyedia jaringan di lokasi untuk membangun konektivitas. Anda kemudian akan memberikan Letter of Authorization (LOA) dari penyedia jaringan ke AWS melalui AWS Support Center. AWS menyelesaikan cross-connect di lokasi ini.
AWS Bahrain DC52, Manama	Untuk menyelesaikan koneksi, Anda dapat bekerja dengan salah satu partner penyedia jaringan di lokasi untuk membangun konektivitas. Anda kemudian akan memberikan Letter of Authorization (LOA) dari penyedia jaringan ke AWS melalui AWS Support Center. AWS menyelesaikan cross-connect di lokasi ini.

Timur Tengah (UEA)

Lokasi	Cara meminta koneksi
Equinix DX1, Dubai, UEA	Hubungi Equinix di awsdealreg@equinix.com.
Pusat SmartHub Data Etisalat, Fujairah, UEA	Hubungi Pusat SmartHub Data Etisalat di IntlSales-C& WS@etisalat.ae.

Amerika Selatan (Sao Paulo)

Lokasi	Cara meminta koneksi
Cirion BNARAGMS, Buenos Aires	Hubungi Cirion di cloud.connect@ciriontechnologies.com.
Equinix RJ2, Rio de Janeiro	Hubungi Equinix di awsdealreg@equinix.com.
Equinix, Sao SP4 Paulo	Hubungi Equinix di awsdealreg@equinix.com.
Tivit	Hubungi Tivit di aws@tivit.com.br.

AWS GovCloud (AS-Timur)

Anda tidak dapat memesan koneksi di Wilayah ini.

AWS GovCloud (AS-Barat)

Lokasi	Cara meminta koneksi
Equinix SV5, San Jose	Hubungi Equinix di awsdealreg@equinix.com.

AWS Direct Connect antarmuka virtual dan antarmuka virtual yang dihosting

Anda harus membuat salah satu antarmuka virtual berikut (VIFs) untuk mulai menggunakan AWS Direct Connect koneksi Anda.

- Antarmuka virtual privat: Antarmuka virtual privat harus digunakan untuk mengakses Amazon VPC menggunakan alamat IP privat.
- Antarmuka virtual publik: Antarmuka virtual publik dapat mengakses semua layanan AWS publik menggunakan alamat IP publik.
- Antarmuka virtual transit: Antarmuka virtual transit harus digunakan untuk mengakses satu atau lebih Amazon VPC Transit Gateway yang terkait dengan gateway Direct Connect. Anda dapat menggunakan antarmuka virtual transit dengan koneksi AWS Direct Connect khusus atau host dengan kecepatan apa pun. Untuk informasi tentang konfigurasi gateway Direct Connect, lihat Gateway Direct Connect.

Untuk terhubung ke AWS layanan lain menggunakan IPv6 alamat, periksa dokumentasi layanan untuk memverifikasi bahwa IPv6 pengalamatan didukung.

Aturan iklan prefiks antarmuka virtual publik

Kami mengiklankan awalan Amazon yang sesuai untuk Anda sehingga Anda dapat mencapai alamat IP publik beban kerja di layanan Anda VPCs dan layanan lainnya. AWS Anda dapat mengakses semua AWS awalan melalui koneksi ini; misalnya, alamat IP publik yang digunakan oleh EC2 instans Amazon, Amazon S3, titik akhir API untuk layanan, dan Amazon.com. AWS Anda tidak memiliki akses ke prefiks non-Amazon. Untuk daftar awalan saat ini yang digunakan oleh AWS, lihat Rentang Alamat AWS IP di Panduan Pengguna Amazon VPC. Di halaman ini Anda dapat mengunduh `.json` file rentang AWS IP yang saat ini diterbitkan. Perhatikan bahwa untuk rentang alamat IP yang dipublikasikan:

- Awalan yang diumumkan melalui BGP melalui antarmuka virtual publik dapat digabungkan atau dideagregasi dibandingkan dengan apa yang tercantum dalam daftar rentang alamat IP. AWS
- Setiap rentang alamat IP yang Anda bawa AWS melalui alamat IP Anda sendiri (BYOIP) tidak termasuk dalam `.json` file, tetapi AWS masih mengiklankan alamat BYOIP ini melalui antarmuka virtual publik.

- AWS tidak mengiklankan ulang awalan pelanggan yang diterima melalui antarmuka virtual publik Direct Connect ke jaringan di luar. AWS Awalan yang diiklankan pada antarmuka virtual publik akan terlihat oleh semua pelanggan. AWS

> **Note**
>
> Kami menyarankan Anda menggunakan filter firewall (berdasarkan source/destination alamat paket) untuk mengontrol lalu lintas ke dan dari beberapa awalan.

Untuk informasi selengkapnya tentang antarmuka virtual publik dan kebijakan perutean, lihat. the section called “Kebijakan perutean antarmuka virtual publik”

SiteLink

Jika Anda membuat antarmuka virtual pribadi atau transit, Anda dapat menggunakannya SiteLink.

SiteLink adalah fitur Direct Connect opsional untuk antarmuka virtual pribadi yang memungkinkan konektivitas antara dua titik kehadiran Direct Connect (PoPs) di AWS partisi yang sama menggunakan jalur terpendek yang tersedia melalui jaringan. AWS Ini memungkinkan Anda untuk menghubungkan jaringan lokal Anda melalui jaringan AWS global tanpa perlu merutekan lalu lintas Anda melalui Wilayah. Untuk informasi selengkapnya, SiteLink lihat Memperkenalkan AWS Direct Connect SiteLink.

> **Note**
>
> - SiteLink tidak tersedia di AWS GovCloud (US) dan Wilayah Tiongkok.
> - SiteLink tidak berfungsi jika router lokal mengiklankan rute yang sama ke beberapa AWS antarmuka virtual.

Ada biaya harga terpisah untuk digunakan SiteLink. Untuk informasi selengkapnya, lihat Harga AWS Direct Connect.

SiteLink tidak mendukung semua jenis antarmuka virtual. Tabel berikut menunjukkan jenis antarmuka dan apakah itu didukung.

Jenis antarmuka virtual	Didukung/Tidak didukung
Antarmuka virtual transit	Didukung
Antarmuka virtual pribadi yang dilampirkan ke gateway Direct Connect dengan gateway virtual	Didukung
Antarmuka virtual pribadi yang dilampirkan ke gateway Direct Connect yang tidak terkait dengan gateway virtual atau gateway transit	Didukung
Antarmuka virtual pribadi yang dilampirkan ke gateway virtual	Tidak didukung
Antarmuka virtual publik	Tidak didukung

Perilaku perutean lalu lintas untuk lalu lintas dari Wilayah AWS (gateway virtual atau transit) ke lokasi lokal melalui antarmuka virtual yang SiteLink diaktifkan sedikit berbeda dari perilaku antarmuka virtual Direct Connect default dengan tambahan jalur. AWS Ketika SiteLink diaktifkan, antarmuka virtual dari Wilayah AWS lebih memilih jalur BGP dengan panjang jalur AS yang lebih rendah dari lokasi Direct Connect, terlepas dari Wilayah terkait. Misalnya, Wilayah terkait diiklankan untuk setiap lokasi Direct Connect. Jika SiteLink dinonaktifkan, lalu lintas default yang berasal dari gateway virtual atau transit lebih memilih lokasi Direct Connect yang terkait dengan itu Wilayah AWS, bahkan jika router dari lokasi Direct Connect yang terkait dengan Wilayah yang berbeda mengiklankan jalur dengan panjang jalur AS yang lebih pendek. Gateway virtual atau transit masih lebih menyukai jalur dari lokasi Direct Connect lokal ke lokasi terkait Wilayah AWS.

SiteLink mendukung ukuran MTU bingkai jumbo maksimum 8500 atau 9001, tergantung pada jenis antarmuka virtual. Untuk informasi selengkapnya, lihat MTUs untuk antarmuka virtual pribadi atau antarmuka virtual transit.

Prasyarat untuk antarmuka virtual

Sebelum Anda membuat antarmuka virtual, lakukan hal berikut:

- Buat koneksi. Untuk informasi selengkapnya, lihat Buat koneksi menggunakan wizard Koneksi.
- Buat grup agregasi tautan (LAG) ketika Anda memiliki beberapa koneksi yang ingin Anda perlakukan sebagai satu koneksi. Untuk informasi, lihat Mengaitkan koneksi dengan LAG.

Untuk membuat antarmuka virtual, Anda memerlukan informasi berikut:

Sumber Daya	Informasi yang diperlukan
Koneksi	Grup agregasi AWS Direct Connect koneksi atau tautan (LAG) tempat Anda membuat antarmuka virtual.
Nama antarmuka virtual	Nama untuk antarmuka virtual.
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID AWS akun dari akun lain.
(Antarmuka virtual privat saja) Koneksi	Untuk menghubungkan ke VPC di AWS Wilayah yang sama, Anda memerlukan gateway pribadi virtual untuk VPC Anda. ASN untuk sisi Amazon sesi BGP diwarisi dari virtual private gateway. Bila Anda membuat virtual private gateway, Anda dapat menentukan ASN privat Anda sendiri. Jika tidak, Amazon menyediakan ASN default. Untuk informasi selengkapnya, lihat Membuat Virtual Private Gateway di Panduan Pengguna Amazon VPC. Untuk terhubung ke VPC melalui gateway Direct Connect, Anda memerlukan gateway Direct Connect. Untuk informasi selengkapnya, lihat Gateway Direct Connect. **Note** • Anda tidak dapat menggunakan ASN yang sama untuk gateway pelanggan dan gateway gateway/Direct Connect virtual di antarmuka virtual.

Sumber Daya	Informasi yang diperlukan
	• Anda dapat menggunakan ASN gateway pelanggan yang sama untuk beberapa antarmuka virtual. • Beberapa antarmuka virtual dapat memiliki gateway virtual gateway/ Direct Connect gateway ASN dan ASN gateway pelanggan yang sama selama mereka adalah bagian dari koneksi Direct Connect yang berbeda. Misalnya: Gateway virtual (ASN 64.496) <--Antarmuka virtual 1 (koneksi Direct Connect 1) ---> Gateway pelanggan (ASN 64.511) Gateway virtual (ASN 64.496) <--Antarmuka virtual 2 (koneksi Direct Connect 2) ---> Gateway pelanggan (ASN 64.511)
VLAN	Tanda virtual local area network (VLAN) unik yang belum digunakan pada koneksi Anda. Nilai harus antara 1 hingga 4094 dan harus sesuai dengan standar Ethernet 802.1Q. Tanda ini diperlukan untuk lalu lintas yang melintasi koneksi AWS Direct Connect . Jika Anda memiliki koneksi yang di-host, AWS Direct Connect Mitra Anda memberikan nilai ini. Anda tidak dapat mengubah nilai setelah Anda membuat antarmuka virtual.

Sumber Daya	Informasi yang diperlukan
Alamat IP rekan	Antarmuka virtual dapat mendukung sesi peering BGP untuk IPv4, IPv6, atau salah satu dari masing-masing (dual-stack). Jangan gunakan Elastic IPs (EIPs) atau Bawa alamat IP Anda sendiri (BYOIP) dari Amazon Pool untuk membuat antarmuka virtual publik. Anda tidak dapat membuat beberapa sesi BGP untuk keluarga pengalamatan IP yang sama pada antarmuka virtual yang sama. Cakupan alamat IP ditetapkan untuk setiap akhir antarmuka virtual untuk sesi peering BGP. • IPv4: • (Hanya antarmuka virtual publik) Anda harus menentukan IPv4 alamat publik unik yang Anda miliki. **Note** • Peering IPs untuk antarmuka virtual pribadi dan transit dapat dari rentang IP yang valid. Ini juga dapat mencakup alamat IP publik milik pelanggan selama ini hanya digunakan untuk membuat sesi peering BGP dan tidak diiklankan melalui antarmuka virtual atau digunakan untuk NAT. • Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk IPv4 alamat publik yang AWS diber ikan. Nilai dapat menjadi salah satu dari yang berikut: • CIDR milik pelanggan IPv4 Ini dapat berupa publik IPs (milik pelanggan atau disediakan oleh AWS), tetapi subnet mask yang sama harus digunakan untuk IP rekan Anda dan IP peer router. AWS Misalnya, jika Anda mengalokasikan `/31` rentang, seperti`203.0.113.0/31` , Anda dapat menggunak

Sumber Daya	Informasi yang diperlukan
	an `203.0.113.0` untuk IP rekan Anda dan `203.0.113.1` untuk IP AWS rekan. Atau, jika Anda mengalokasikan `/24` rentang, seperti`198.51.100.0/24` , Anda dapat menggunakan `198.51.100.10` untuk IP rekan Anda dan `198.51.100.20` untuk IP AWS rekan. • Rentang IP yang dimiliki oleh AWS Direct Connect Mitra atau ISP Anda, bersama dengan otorisasi LOA-CFA. • AWS Disediakan /31 CIDR. Hubungi AWS Support untuk meminta IPv4 CIDR publik (dan memberikan kasus penggunaan dalam permintaan Anda) • (Hanya antarmuka virtual pribadi) Amazon dapat menghasilkan IPv4 alamat pribadi untuk Anda. Jika Anda menentukan sendiri, pastikan bahwa Anda menentukan pribadi CIDRs untuk antarmuka router Anda dan antarmuka AWS Direct Connect saja. Misalnya, jangan tentukan alamat IP lain dari jaringan lokal Anda. Mirip dengan antarmuka virtual publik, subnet mask yang sama harus digunakan untuk IP rekan Anda dan IP peer AWS router. Misalnya, jika Anda mengalokasikan `/30` rentang, seperti`192.168.0.0/30` , Anda dapat menggunakan `192.168.0.1` untuk IP rekan Anda dan `192.168.0.2` untuk IP AWS rekan. • IPv6: Amazon secara otomatis mengalokasikan Anda IPv6 /125 CIDR. Anda tidak dapat menentukan IPv6 alamat rekan Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan berakhir atau. IPv4 IPv6

Sumber Daya	Informasi yang diperlukan
Informasi BGP	• Border Gateway Protocol (BGP) Autonomous System Number (ASN) publik atau privat untuk sisi sesi BGP Anda. Jika Anda menggunakan ASN publik, Anda harus memilikinya. Jika Anda menggunakan ASN pribadi, Anda dapat mengatur nilai ASN kustom. Untuk ASN 16-bit, nilainya harus berada dalam rentang 64512 hingga 65534. Untuk ASN 32-bit, nilainya harus dalam kisaran 1 hingga 2147483647. Penambahan Autonomous System (AS) tidak bekerja jika Anda menggunakan ASN privat untuk antarmuka virtual publik. • AWS memungkinkan secara MD5 default. Anda tidak dapat mengubah opsi ini. • Kunci otentikasi MD5 BGP. Anda dapat memberikan kunci milik Anda sendiri, atau Anda dapat membiarkan Amazon menghasilkannya untuk Anda.

Sumber Daya	Informasi yang diperlukan

(Antarmuka virtual publik saja) Prefiks yang ingin Anda iklankan	IPv4 Rute umum atau IPv6 rute untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: IPv4 CIDR dapat tumpang tindih dengan IPv4 CIDR publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari berikut ini benar:
	  • CIDRs Mereka berasal dari berbagai AWS daerah. Pastikan bahwa Anda menerapkan tanda komunitas BGP pada prefiks publik.
	  • Anda menggunakan AS_PATH ketika Anda memiliki ASN publik dalam konfigurasi. active/passive
	  Untuk informasi selengkapnya, lihat Kebijakan perutean dan komunitas BGP.
	• Melalui antarmuka virtual publik Direct Connect, Anda dapat menentukan panjang awalan dari /1 hingga /32 untuk IPv4 dan dari /1 hingga /64 untuk. IPv6
	• Anda dapat menambahkan awalan tambahan ke VIF publik yang ada dan mengiklankannya dengan menghubungi dukungan.AWS Dalam kasus dukungan Anda, berikan daftar awalan CIDR tambahan yang ingin Anda tambahkan ke VIF publik dan beriklan.

Sumber Daya	Informasi yang diperlukan
(Hanya antarmuka virtual pribadi dan transit) Frame jumbo	Unit transmisi maksimum (MTU) paket over. AWS Direct Connect Default-nya adalah 1500. Mengatur MTU antarmuka virtual ke 8500 (bingkai jumbo) dapat menyebabkan pembaruan untuk koneksi fisik yang mendasari jika itu tidak diperbarui untuk mendukung bingkai jumbo. Memperbarui koneksi mengganggu konektivitas jaringan untuk semua antarmuka virtual yang terkait dengan koneksi hingga 30 detik. Frame jumbo didukung hingga 8500 MTU untuk Direct Connect. Rute statis dan rute propagasi yang dikonfigurasi dalam Tabel Rute Transit Gateway akan mendukung Jumbo Frames, termasuk dari EC2 instance dengan entri tabel rute statis VPC ke Lampiran Transit Gateway. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di AWS Direct Connect konsol dan temukan bingkai Jumbo yang mampu pada antarmuka virtual Halaman konfigurasi umum.

Bila Anda membuat antarmuka virtual, Anda dapat menentukan akun yang memiliki antarmuka virtual. Ketika Anda memilih AWS akun yang bukan akun Anda, aturan berikut berlaku:

- Untuk pribadi VIFs dan transit VIFs, akun berlaku untuk antarmuka virtual dan tujuan gateway gateway/Direct Connect pribadi virtual.
- Untuk publik VIFs, akun digunakan untuk penagihan antarmuka virtual. Penggunaan Data Transfer Out (DTO) diukur ke arah pemilik sumber daya pada kecepatan transfer AWS Direct Connect data.

> **Note**
>
> Awalan 31-Bit didukung pada semua jenis antarmuka virtual Direct Connect. Lihat RFC 3021: Menggunakan Awalan 31-Bit pada Tautan untuk informasi lebih lanjut. IPv4 Point-to-Point

MTUs untuk antarmuka virtual pribadi atau antarmuka virtual transit

AWS Direct Connect mendukung ukuran bingkai Ethernet 1522 atau 9023 byte (14 byte header Ethernet+4 byte tag VLAN+byte untuk datagram IP+4 byte FCS) pada lapisan tautan.

Maximum transmission unit (MTU) dari koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang dapat diizinkan yang dapat dilewatkan melalui koneksi. MTU antarmuka virtual pribadi dapat berupa 1500 atau 9001 (bingkai jumbo). MTU antarmuka virtual transit dapat sebesar 1500 atau 8500 (bingkai jumbo). Anda dapat menentukan MTU saat membuat antarmuka atau memperbaruinya setelah Anda membuatnya. Mengatur MTU antarmuka virtual ke 8500 (bingkai jumbo) atau 9001 (bingkai jumbo) dapat menyebabkan pembaruan untuk koneksi fisik yang mendasari jika itu tidak diperbarui untuk mendukung bingkai jumbo. Memperbarui koneksi mengganggu konektivitas jaringan untuk semua antarmuka virtual yang terkait dengan koneksi hingga 30 detik. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di AWS Direct Connect konsol dan temukan Jumbo Frame Mampu pada tab Ringkasan.

Setelah Anda mengaktifkan bingkai jumbo untuk antarmuka virtual pribadi Anda atau antarmuka virtual transit, Anda hanya dapat mengaitkannya dengan koneksi atau LAG yang mampu bingkai jumbo. Frame jumbo didukung pada antarmuka virtual pribadi yang terpasang pada gateway pribadi virtual atau gateway Direct Connect, atau pada antarmuka virtual transit yang terpasang ke gateway Direct Connect. Jika Anda memiliki dua antarmuka virtual pribadi yang mengiklankan rute yang sama tetapi menggunakan nilai MTU yang berbeda, atau jika Anda memiliki Site-to-Site VPN yang mengiklankan rute yang sama, 1500 MTU digunakan.

Important

Frame jumbo hanya akan berlaku untuk rute yang disebarkan melalui AWS Direct Connect dan rute statis melalui gateway transit. Frame jumbo pada gateway transit hanya mendukung 8500 byte.

Jika sebuah EC2 instance tidak mendukung jumbo frame, itu akan menjatuhkan jumbo frame dari Direct Connect. Semua tipe EC2 instance mendukung frame jumbo kecuali untuk C1,, T1 CC1, dan M1. Untuk informasi selengkapnya, lihat Unit Transmisi Maksimum Jaringan (MTU) untuk EC2 Instans Anda di Panduan EC2 Pengguna Amazon.

Untuk koneksi yang di-host, frame Jumbo hanya dapat diaktifkan jika awalnya diaktifkan pada koneksi induk host Direct Connect. Jika bingkai Jumbo tidak diaktifkan pada koneksi induk itu, maka frame Jumbo tidak dapat diaktifkan pada koneksi apa pun.

MTUs untuk pribadi VIFs adalah standarisasi ke 8500. 9001 akan terus diterima sampai dihapus.

Untuk langkah-langkah untuk mengatur MTU untuk antarmuka virtual pribadi, lihatMengatur MTU dari antarmuka virtual pribadi.

AWS Direct Connect antarmuka virtual

Anda dapat membuat antarmuka virtual transit untuk terhubung ke transit gateway, antarmuka virtual publik untuk terhubung ke sumber daya publik (layanan non-VPC), atau antarmuka virtual privat untuk terhubung ke VPC.

Untuk membuat antarmuka virtual untuk akun di dalam Anda AWS Organizations, atau AWS Organizations yang berbeda dari milik Anda, buat antarmuka virtual yang dihosting.

Lihat berikut ini untuk membuat antarmuka virtual:

- Membuat antarmuka virtual publik
- Membuat antarmuka virtual privat
- Membuat antarmuka virtual transit ke gateway Direct Connect

Prasyarat

Sebelum memulai, pastikan Anda telah membaca informasi di Prasyarat untuk antarmuka virtual.

Prasyarat untuk transit antarmuka virtual ke gateway Direct Connect

Untuk menghubungkan AWS Direct Connect koneksi Anda ke gateway transit, Anda harus membuat antarmuka transit untuk koneksi Anda. Tentukan gateway Direct Connect yang akan dihubungkan.

Maximum transmission unit (MTU) dari koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang dapat diizinkan yang dapat dilewatkan melalui koneksi. MTU antarmuka virtual pribadi dapat berupa 1500 atau 9001 (bingkai jumbo). MTU antarmuka virtual transit dapat sebesar 1500 atau 8500 (bingkai jumbo). Anda dapat menentukan MTU saat membuat antarmuka atau memperbaruinya setelah Anda membuatnya. Mengatur MTU antarmuka virtual ke 8500 (bingkai jumbo) atau 9001 (bingkai jumbo) dapat menyebabkan pembaruan untuk koneksi fisik yang mendasari jika itu tidak diperbarui untuk mendukung bingkai jumbo. Memperbarui koneksi mengganggu konektivitas jaringan untuk semua antarmuka virtual yang terkait dengan koneksi hingga 30 detik. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di konsol AWS Direct Connect dan temukan Kemampuan Bingkai Jumbo di tab Ringkasan.

> **Important**
>
> Jika Anda mengaitkan transit gateway dengan satu atau lebih gateway Direct Connect, Autonomous System Number (ASN) yang digunakan oleh transit gateway dan gateway Direct

Connect harus berbeda. Sebagai contoh, jika Anda menggunakan ASN 64512 default untuk transit gateway dan gateway Direct Connect, permintaan pengaitan akan gagal.

Buat antarmuka virtual AWS Direct Connect publik

Saat Anda membuat antarmuka virtual publik, dibutuhkan waktu hingga 72 jam bagi kami untuk meninjau dan menyetujui permintaan Anda.

Untuk menyediakan antarmuka virtual publik

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Publik.
5. Di bawah Pengaturan antarmuka virtual publik, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.
   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.
   c. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).
   d. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number (ASN) dari router peer lokal Anda untuk antarmuka virtual baru.

      Nilai yang valid adalah 1-2147483647.

      > **Note**
      >
      > Saat membuat sesi peering BGP dengan AWS melalui antarmuka virtual publik, gunakan 7224 sebagai ASN untuk menetapkan sesi BGP di samping. AWS ASN pada router atau perangkat gateway pelanggan Anda harus berbeda dari ASN itu.

6. Di bawah Pengaturan tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

      - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.

- Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

[IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk memberikan kunci BGP Anda sendiri, masukkan kunci MD5 BGP Anda.

Jika Anda tidak memasukkan nilai, kami menghasilkan kunci BGP. Jika Anda memberikan kunci Anda sendiri, atau jika kami membuat kunci untuk Anda, nilai itu ditampilkan di kolom kunci otentikasi BGP pada halaman detail antarmuka virtual antarmuka Virtual.

c. Untuk mengiklankan awalan ke Amazon, untuk Awalan yang ingin Anda iklankan, masukkan alamat tujuan IPv4 CIDR (dipisahkan dengan koma) ke mana lalu lintas harus diarahkan melalui antarmuka virtual.

> **Important**
>
> Anda dapat menambahkan awalan tambahan ke VIF publik yang ada dan mengiklankannya dengan menghubungi dukungan.AWS Dalam kasus dukungan Anda, berikan daftar awalan CIDR tambahan yang ingin Anda tambahkan ke VIF publik dan beriklan.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.
8. Unduh konfigurasi router untuk perangkat anda. Untuk informasi selengkapnya, lihat Mengunduh file konfigurasi router.

Untuk membuat antarmuka virtual publik menggunakan baris perintah atau API

- create-public-virtual-interface (AWS CLI)
- CreatePublicVirtualInterface(AWS Direct Connect API)

Buat antarmuka virtual AWS Direct Connect pribadi

Anda dapat menyediakan antarmuka virtual pribadi ke gateway pribadi virtual di Wilayah yang sama dengan AWS Direct Connect koneksi Anda. Untuk informasi selengkapnya tentang penyediaan antarmuka virtual pribadi ke AWS Direct Connect gateway, lihat. AWS Direct Connect gerbang

Jika Anda menggunakan wizard VPC untuk membuat VPC, propagasi rute secara otomatis diaktifkan untuk Anda. Dengan propagasi rute, rute secara otomatis diisi ke tabel rute di VPC Anda. Jika Anda memilih, Anda dapat menonaktifkan propagasi rute. Untuk informasi selengkapnya, lihat Mengaktifkan Propagasi Rute di Tabel Rute di Panduan Pengguna Amazon VPC.

Maximum transmission unit (MTU) dari koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang dapat diizinkan yang dapat dilewatkan melalui koneksi. MTU antarmuka virtual pribadi dapat berupa 1500 atau 9001 (bingkai jumbo). MTU antarmuka virtual transit dapat sebesar 1500 atau 8500 (bingkai jumbo). Anda dapat menentukan MTU saat membuat antarmuka atau memperbaruinya setelah Anda membuatnya. Mengatur MTU antarmuka virtual ke 8500 (bingkai jumbo) atau 9001 (bingkai jumbo) dapat menyebabkan pembaruan untuk koneksi fisik yang mendasari jika itu tidak diperbarui untuk mendukung bingkai jumbo. Memperbarui koneksi mengganggu konektivitas jaringan untuk semua antarmuka virtual yang terkait dengan koneksi hingga 30 detik. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di konsol AWS Direct Connect dan temukan Kemampuan Bingkai Jumbo di tab Ringkasan.

> **Note**
>
> MTU untuk antarmuka virtual pribadi distandarisasi ke 8500; Namun, 9100 akan terus didukung sampai dihapus.

Untuk menyediakan antarmuka virtual privat bagi VPC

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Tipe antarmuka virtual, pilih Privat.
5. Di bawah Pengaturan antarmuka virtual privat Anda, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.
   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.

c. Untuk pemilik antarmuka Virtual, pilih AWS Akun saya jika antarmuka virtual untuk AWS akun Anda.

d. Untuk Gateway Direct Connect, pilih gateway Direct Connect.

e. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).

f. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

   Nilai yang valid adalah 1 hingga 2147483647.

6. Di bawah Pengaturan Tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

      - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

      > **Important**
      >
      > Saat mengonfigurasi antarmuka virtual AWS Direct Connect, Anda dapat menentukan alamat IP Anda sendiri menggunakan RFC 1918, menggunakan skema pengalamatan lain, atau memilih alamat IPv4 /29 CIDR yang AWS ditetapkan yang dialokasikan dari rentang RFC 3927 169.254.0.0/16 Link-Local untuk konektivitas. IPv4 point-to-point point-to-pointKoneksi ini harus digunakan secara eksklusif untuk mengintip eBGP antara router gateway pelanggan Anda dan titik akhir Direct Connect. Untuk tujuan lalu lintas atau tunneling VPC, seperti AWS Site-to-Site Private IP VPN, atau Transit Gateway Connect, AWS merekomendasikan penggunaan antarmuka loopback atau LAN pada router gateway pelanggan Anda sebagai alamat sumber atau tujuan alih-alih koneksi. point-to-point
      >
      > - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
      > - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat IPv4 Lokal-Tautan.

[IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat rekan secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk mengubah maximum transmission unit (MTU) dari 1500 (default) menjadi 8500 (bingkai jumbo), pilih MTU Jumbo (MTU ukuran 8500).

> **Note**
>
> MTU untuk antarmuka virtual pribadi distandarisasi ke 8500; Namun, 9100 akan terus didukung sampai dihapus.

c. (Opsional) Di bawah Aktifkan SiteLink, pilih Diaktifkan untuk mengaktifkan konektivitas langsung antara titik kehadiran Direct Connect.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.
8. Unduh konfigurasi router untuk perangkat anda. Untuk informasi selengkapnya, lihat Mengunduh file konfigurasi router.

Untuk membuat antarmuka virtual privat menggunakan baris perintah atau API

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface(AWS Direct Connect API)

Buat antarmuka virtual transit ke AWS Direct Connect gateway

Sebelum menghubungkan antarmuka virtual transit ke gateway Direct Connect, biasakan diri Anda dengan teks.

Untuk menyediakan antarmuka virtual transit ke gateway Direct Connect

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Transit.
5. Di bawah Pengaturan antarmuka virtual transit, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.

   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.

   c. Untuk pemilik antarmuka Virtual, pilih AWS Akun saya jika antarmuka virtual untuk AWS akun Anda.

   d. Untuk Gateway Direct Connect, pilih gateway Direct Connect.

   e. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).

   f. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

      Nilai yang valid adalah 1 hingga 2147483647.

6. Di bawah Pengaturan Tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

      - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

      > **Important**
      >
      > Saat mengonfigurasi antarmuka virtual AWS Direct Connect, Anda dapat menentukan alamat IP Anda sendiri menggunakan RFC 1918, menggunakan skema pengalamatan lain, atau memilih alamat IPv4 /29 CIDR yang AWS ditetapkan yang dialokasikan dari rentang RFC 3927 169.254.0.0/16 Link-Local untuk konektivitas. IPv4 point-to-point point-to-pointKoneksi ini harus digunakan secara eksklusif untuk mengintip eBGP antara router gateway pelanggan Anda

dan titik akhir Direct Connect. Untuk tujuan lalu lintas atau tunneling VPC, seperti AWS Site-to-Site Private IP VPN, atau Transit Gateway Connect, AWS merekomendasikan penggunaan antarmuka loopback atau LAN pada router gateway pelanggan Anda sebagai alamat sumber atau tujuan alih-alih koneksi. point-to-point

- Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
- Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat IPv4 Lokal-Tautan.

[IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk mengubah maximum transmission unit (MTU) dari 1500 (default) menjadi 8500 (bingkai jumbo), pilih MTU Jumbo (MTU ukuran 8500).

c. (Opsional) Di bawah Aktifkan SiteLink, pilih Diaktifkan untuk mengaktifkan konektivitas langsung antara titik kehadiran Direct Connect.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.

Setelah Anda membuat antarmuka virtual, Anda dapat mengunduh konfigurasi router untuk perangkat Anda. Untuk informasi selengkapnya, lihat Mengunduh file konfigurasi router.

Untuk membuat antarmuka virtual transit menggunakan baris perintah atau API

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS Direct Connect API)

Untuk melihat antarmuka virtual yang dilampirkan ke gateway Direct Connect menggunakan baris perintah atau API

- describe-direct-connect-gateway-lampiran ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

Unduh file konfigurasi AWS Direct Connect router

Setelah Anda membuat antarmuka virtual dan status antarmuka sudah aktif, Anda dapat mengunduh file konfigurasi router untuk perangkat Anda.

Jika Anda menggunakan salah satu router berikut untuk antarmuka virtual yang telah MACsec dihidupkan, kami secara otomatis membuat file konfigurasi untuk router Anda:

- Cisco Nexus 9K+ Series beralih menjalankan NX-OS 9.3 atau perangkat lunak yang lebih baru
- Router Juniper Networks M/MX Series menjalankan perangkat lunak JunOS 9.5 atau yang lebih baru

Untuk mengunduh file konfigurasi router

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih antarmuka virtual lalu pilih Lihat detail.
4. Pilih Unduh konfigurasi router.
5. Untuk Unduh konfigurasi router, lakukan hal berikut:
   a. Untuk Vendor, pilih produsen router Anda.
   b. Untuk Platform, pilih model router Anda.
   c. Untuk Perangkat Lunak, pilih versi perangkat lunak untuk router Anda.
6. Pilih Unduh, lalu gunakan konfigurasi yang sesuai untuk router Anda guna memastikan bahwa Anda dapat terhubung ke AWS Direct Connect.
7. Jika Anda perlu mengkonfigurasi router Anda secara manual MACsec, gunakan tabel berikut sebagai pedoman.

Parameter	Deskripsi
Panjang CKN	Ini adalah string dengan 64 karakter heksadesimal (0-9, A-E). Gunakan panjang penuh untuk memaksimalkan kompatibilitas lintas platform.
Panjang CAK	Ini adalah string dengan 64 karakter heksadesimal (0-9, A-E). Gunakan panjang penuh untuk memaksimalkan kompatibilitas lintas platform.
Algoritma kriptografi	AES_256_CMAC
Suite Cipher SAK	• Untuk koneksi 100 Gbps: GCM_AES_XPN_256 • Untuk koneksi 10 Gbps: GCM_AES_XPN_256 atau GCM_AES _256
Suite Cipher Kunci	16
Offset Kerahasiaan	0
Indikator ICV	Tidak
Waktu Kunci Ulang SAK	Rollover PN>

Antarmuka AWS Direct Connect virtual yang dihosting

Untuk menggunakan AWS Direct Connect koneksi Anda dengan akun lain, Anda dapat membuat antarmuka virtual yang dihosting untuk akun itu. Pemilik akun lain harus menerima antarmuka virtual yang di-host untuk mulai menggunakannya. Antarmuka virtual yang di-host bekerja sama dengan antarmuka virtual standar dan dapat terhubung ke sumber daya publik atau VPC.

Anda dapat menggunakan antarmuka virtual transit dengan koneksi khusus atau host Direct Connect dengan kecepatan apa pun. Koneksi yang di-host hanya mendukung satu antarmuka virtual.

Untuk membuat antarmuka virtual, Anda memerlukan informasi berikut:

Sumber Daya	Informasi yang diperlukan
Koneksi	Grup agregasi AWS Direct Connect koneksi atau tautan (LAG) tempat Anda membuat antarmuka virtual.
Nama antarmuka virtual	Nama untuk antarmuka virtual.
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID AWS akun dari akun lain.
(Antarmuka virtual privat saja) Koneksi	Untuk menghubungkan ke VPC di AWS Wilayah yang sama, Anda memerlukan gateway pribadi virtual untuk VPC Anda. ASN untuk sisi Amazon sesi BGP diwarisi dari virtual private gateway. Bila Anda membuat virtual private gateway, Anda dapat menentukan ASN privat Anda sendiri. Jika tidak, Amazon menyediakan ASN default. Untuk informasi selengkapnya, lihat Membuat Virtual Private Gateway di Panduan Pengguna Amazon VPC. Untuk terhubung ke VPC melalui gateway Direct Connect, Anda memerlukan gateway Direct Connect. Untuk informasi selengkapnya, lihat Gateway Direct Connect.
VLAN	Tanda virtual local area network (VLAN) unik yang belum digunakan pada koneksi Anda. Nilai harus antara 1 hingga 4094 dan harus sesuai dengan standar Ethernet 802.1Q. Tanda ini diperlukan untuk lalu lintas yang melintasi koneksi AWS Direct Connect . Jika Anda memiliki koneksi yang di-host, AWS Direct Connect Mitra Anda memberikan nilai ini. Anda tidak dapat mengubah nilai setelah Anda membuat antarmuka virtual.
Alamat IP rekan	Antarmuka virtual dapat mendukung sesi peering BGP untuk IPv4, IPv6, atau salah satu dari masing-masing (dual-stack). Jangan gunakan Elastic IPs (EIPs) atau Bawa alamat IP Anda sendiri (BYOIP) dari Amazon Pool untuk membuat antarmuka virtual publik. Anda tidak dapat membuat beberapa sesi BGP untuk keluarga pengalamatan IP yang sama pada antarmuka virtual yang sama. Cakupan alamat IP ditetapkan untuk setiap akhir antarmuka virtual untuk sesi peering BGP.

Sumber Daya	Informasi yang diperlukan
	• IPv4: • (Hanya antarmuka virtual publik) Anda harus menentukan IPv4 alamat publik unik yang Anda miliki. Nilai dapat menjadi salah satu dari yang berikut: • CIDR milik pelanggan IPv4 Ini dapat berupa publik IPs (milik pelanggan atau disediakan oleh AWS), tetapi subnet mask yang sama harus digunakan untuk IP rekan Anda dan IP peer router. AWS Misalnya, jika Anda mengalokasikan `/31` rentang, seperti`203.0.113.0/31` , Anda dapat menggunak an `203.0.113.0` untuk IP rekan Anda dan `203.0.113.1` untuk IP AWS rekan. Atau, jika Anda mengalokasikan `/24` rentang, seperti`198.51.100.0/24` , Anda dapat menggunakan `198.51.10 0.10` untuk IP rekan Anda dan `198.51.100.20` untuk IP AWS rekan. • Rentang IP yang dimiliki oleh AWS Direct Connect Mitra atau ISP Anda, bersama dengan otorisasi LOA-CFA • AWS-Disediakan /31 CIDR. Hubungi AWS Support untuk meminta IPv4 CIDR publik (dan memberikan kasus penggunaan dalam permintaan Anda) **Note** Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk IPv4 alamat publik AWS yang disediakan. • (Hanya antarmuka virtual pribadi) Amazon dapat menghasilkan IPv4 alamat pribadi untuk Anda. Jika Anda menentukan sendiri, pastikan bahwa Anda menentukan pribadi CIDRs untuk antarmuka router Anda dan antarmuka AWS Direct Connect saja. Misalnya, jangan tentukan alamat IP lain dari jaringan lokal Anda. Mirip dengan antarmuka virtual publik, subnet mask yang sama harus digunakan untuk IP peer Anda dan IP peer AWS router. Misalnya, jika Anda mengalokasikan `/30` rentang,

Sumber Daya	Informasi yang diperlukan
	seperti`192.168.0.0/30` , Anda dapat menggunakan `192.168.0.1` untuk IP rekan Anda dan `192.168.0.2` untuk IP AWS rekan. • IPv6: Amazon secara otomatis mengalokasikan Anda IPv6 /125 CIDR. Anda tidak dapat menentukan IPv6 alamat rekan Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan berakhir atau. IPv4 IPv6
Informasi BGP	• Border Gateway Protocol (BGP) Autonomous System Number (ASN) publik atau privat untuk sisi sesi BGP Anda. Jika Anda menggunakan ASN publik, Anda harus memilikinya. Jika Anda menggunakan ASN pribadi, Anda dapat mengatur nilai ASN kustom. Untuk ASN 16-bit, nilainya harus berada dalam rentang 64512 hingga 65534. Untuk ASN 32-bit, nilainya harus dalam kisaran 1 hingga 2147483647. Penambahan Autonomous System (AS) tidak bekerja jika Anda menggunakan ASN privat untuk antarmuka virtual publik. • AWS memungkinkan secara MD5 default. Anda tidak dapat mengubah opsi ini. • Kunci otentikasi MD5 BGP. Anda dapat memberikan kunci milik Anda sendiri, atau Anda dapat membiarkan Amazon menghasilkannya untuk Anda.

Sumber Daya	Informasi yang diperlukan

(Antarmuka virtual publik saja) Prefiks yang ingin Anda iklankan	IPv4 Rute umum atau IPv6 rute untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: IPv4 CIDR dapat tumpang tindih dengan IPv4 CIDR publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari berikut ini benar:
	  • CIDRs Mereka berasal dari berbagai AWS daerah. Pastikan bahwa Anda menerapkan tanda komunitas BGP pada prefiks publik.
	  • Anda menggunakan AS_PATH ketika Anda memiliki ASN publik dalam konfigurasi aktif/pasif.
	  Untuk informasi selengkapnya, lihat Kebijakan perutean dan komunitas BGP.
	• Melalui antarmuka virtual publik Direct Connect, Anda dapat menentukan panjang awalan dari /1 hingga /32 untuk IPv4 dan dari /1 hingga /64 untuk. IPv6
	• Anda dapat menambahkan awalan tambahan ke VIF publik yang ada dan mengiklankannya dengan menghubungi dukungan.AWS Dalam kasus dukungan Anda, berikan daftar awalan CIDR tambahan yang ingin Anda tambahkan ke VIF publik dan beriklan.

(Hanya antarmuka virtual pribadi dan transit) Jumbo frame	Unit transmisi maksimum (MTU) paket over. AWS Direct Connect Default-n ya adalah 1500. Mengatur MTU antarmuka virtual ke 9001 (bingkai jumbo) dapat menyebabkan pembaruan untuk koneksi fisik yang mendasari jika itu tidak diperbarui untuk mendukung bingkai jumbo. Memperbarui koneksi mengganggu konektivitas jaringan untuk semua antarmuka virtual yang terkait dengan koneksi hingga 30 detik. Bingkai jumbo hanya berlaku untuk rute yang disebarkan dari. AWS Direct Connect Jika Anda menambahkan rute statis ke tabel rute yang mengarah ke virtual private gateway, lalu lintas diarahkan melalui rute statis dikirim menggunakan 1500 MTU. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di AWS Direct Connect konsol dan temukan bingkai Jumbo yang mampu pada antarmuka virtual Halaman konfigurasi umum.

Buat antarmuka virtual pribadi yang dihosting di AWS Direct Connect

Sebelum memulai, pastikan Anda telah membaca informasi di Prasyarat untuk antarmuka virtual.

Untuk membuat antarmuka virtual privat yang di-host

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Privat.
5. Di bawah Pengaturan antarmuka virtual privat, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.
   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.
   c. Untuk Pemilik antarmuka virtual, pilih Akun AWS lainnya, lalu untuk Pemilik antarmuka virtual, masukkan ID akun untuk memiliki antarmuka virtual ini.
   d. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).
   e. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

      Nilai yang valid adalah 1-2147483647.
6. Di bawah Pengaturan Tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

      - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

      > **Important**
      >
      > Saat mengonfigurasi antarmuka virtual AWS Direct Connect, Anda dapat menentukan alamat IP Anda sendiri menggunakan RFC 1918, menggunakan skema pengalamatan lain, atau memilih alamat IPv4 /29 CIDR yang AWS ditetapkan yang dialokasikan dari rentang RFC 3927 169.254.0.0/16 Link-Local

untuk konektivitas. IPv4 point-to-point point-to-pointKoneksi ini harus digunakan secara eksklusif untuk mengintip eBGP antara router gateway pelanggan Anda dan titik akhir Direct Connect. Untuk tujuan lalu lintas atau tunneling VPC, seperti AWS Site-to-Site Private IP VPN, atau Transit Gateway Connect, AWS merekomendasikan penggunaan antarmuka loopback atau LAN pada router gateway pelanggan Anda sebagai alamat sumber atau tujuan alih-alih koneksi. point-to-point

- Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
- Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat IPv4 Lokal-Tautan.

[IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk mengubah maximum transmission unit (MTU) dari 1500 (default) menjadi 8500 (bingkai jumbo), pilih MTU Jumbo (MTU ukuran 8500).

> **Note**
>
> MTU untuk antarmuka virtual pribadi distandarisasi ke 8500; Namun, 9100 akan terus didukung sampai dihapus.

c. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Setelah antarmuka virtual yang dihosting diterima oleh pemilik AWS akun lain, Anda dapat mengunduh file konfigurasi. Untuk informasi selengkapnya, lihat Mengunduh file konfigurasi router.

Untuk membuat antarmuka virtual privat yang di-host menggunakan baris perintah atau API

- allocate-private-virtual-interface (AWS CLI)
- AllocatePrivateVirtualInterface(AWS Direct Connect API)

Buat antarmuka virtual publik yang dihosting di AWS Direct Connect

Sebelum memulai, pastikan Anda telah membaca informasi di Prasyarat untuk antarmuka virtual.

Untuk membuat antarmuka virtual publik yang di-host

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Publik.
5. Di bawah Pengaturan Antarmuka Virtual Publik, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.

   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.

   c. Untuk pemilik antarmuka virtual, pilih AWS Akun lain, dan kemudian untuk Pemilik antarmuka virtual, masukkan ID akun untuk memiliki antarmuka virtual ini.

   d. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).

   e. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

      Nilai yang valid adalah 1-2147483647.
6. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

   [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

   - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
   - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

[IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat rekan secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

7. Untuk mengiklankan awalan ke Amazon, untuk Awalan yang ingin Anda iklankan, masukkan alamat tujuan IPv4 CIDR (dipisahkan dengan koma) ke mana lalu lintas harus diarahkan melalui antarmuka virtual.
8. Untuk menyediakan kunci Anda sendiri guna mengautentikasi sesi BGP, di bawah Pengaturan Tambahan, untuk Kunci autentikasi BGP, masukkan kunci.

   Jika Anda tidak memasukkan nilai, kami menghasilkan kunci BGP.
9. (Opsional) Menambahkan atau menghapus tanda.

   [Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

   - Untuk Kunci, masukkan nama kunci.
   - Untuk Nilai, masukkan nilai kunci.

   [Menghapus tanda] Di samping tanda, pilih Hapus tanda.
10. Pilih Buat antarmuka virtual.
11. Setelah antarmuka virtual yang dihosting diterima oleh pemilik AWS akun lain, Anda dapat mengunduh file konfigurasi. Untuk informasi selengkapnya, lihat Mengunduh file konfigurasi router.

Untuk membuat antarmuka virtual publik yang di-host menggunakan baris perintah atau API

- allocate-public-virtual-interface (AWS CLI)
- AllocatePublicVirtualInterface(AWS Direct Connect API)

Buat antarmuka virtual transit yang AWS Direct Connect dihosting

Untuk membuat antarmuka virtual transit yang di-host

> **Important**
>
> Jika Anda mengaitkan transit gateway dengan satu atau lebih gateway Direct Connect, Autonomous System Number (ASN) yang digunakan oleh transit gateway dan gateway Direct

Connect harus berbeda. Sebagai contoh, jika Anda menggunakan ASN 64512 default untuk transit gateway dan gateway Direct Connect, permintaan pengaitan akan gagal.

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Transit.
5. Di bawah Pengaturan antarmuka virtual transit, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.

   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.

   c. Untuk pemilik antarmuka virtual, pilih AWS Akun lain, dan kemudian untuk Pemilik antarmuka virtual, masukkan ID akun untuk memiliki antarmuka virtual ini.

   d. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).

   e. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

      Nilai yang valid adalah 1-2147483647.
6. Di bawah Pengaturan Tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

      - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

      > **Important**
      >
      > Saat mengonfigurasi antarmuka virtual AWS Direct Connect, Anda dapat menentukan alamat IP Anda sendiri menggunakan RFC 1918, menggunakan skema pengalamatan lain, atau memilih alamat IPv4 /29 CIDR yang AWS ditetapkan yang dialokasikan dari rentang RFC 3927 169.254.0.0/16 Link-Local untuk konektivitas. IPv4 point-to-point point-to-pointKoneksi ini harus digunakan

secara eksklusif untuk mengintip eBGP antara router gateway pelanggan Anda dan titik akhir Direct Connect. Untuk tujuan lalu lintas atau tunneling VPC, seperti AWS Site-to-Site Private IP VPN, atau Transit Gateway Connect, AWS merekomendasikan penggunaan antarmuka loopback atau LAN pada router gateway pelanggan Anda sebagai alamat sumber atau tujuan alih-alih koneksi. point-to-point

- Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
- Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat IPv4 Lokal-Tautan.

[IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat rekan secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk mengubah maximum transmission unit (MTU) dari 1500 (default) menjadi 8500 (bingkai jumbo), pilih MTU Jumbo (MTU ukuran 8500).

c. [Opsional] Menambahkan tanda. Lakukan hal berikut:

[Menambahkan tanda] Pilih Tambah tanda dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.
8. Setelah antarmuka virtual yang dihosting diterima oleh pemilik AWS akun lain, Anda dapat mengunduh file konfigurasi router untuk perangkat Anda. Untuk informasi selengkapnya, lihat Mengunduh file konfigurasi router.

Untuk membuat antarmuka virtual transit yang di-host menggunakan baris perintah atau API

- allocate-transit-virtual-interface (AWS CLI)
- AllocateTransitVirtualInterface(AWS Direct Connect API)

Lihat detail antarmuka AWS Direct Connect virtual

Anda dapat melihat status antarmuka virtual Anda saat ini menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API. Rincian meliputi:

- Status koneksi
- Nama
- Lokasi
- VLAN
- Detail BGP
- Alamat IP peer

Untuk melihat detail tentang antarmuka virtual

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel sebelah kiri, pilih Antarmuka Virtual.
3. Pilih antarmuka virtual lalu pilih Lihat detail.

Untuk menggambarkan antarmuka virtual menggunakan baris perintah atau API

- describe-virtual-interfaces (AWS CLI)
- DescribeVirtualInterfaces(AWS Direct Connect API)

Tambahkan rekan BGP ke antarmuka virtual AWS Direct Connect

Tambahkan atau hapus sesi peering IPv4 atau IPv6 BGP ke antarmuka virtual Anda menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Antarmuka virtual dapat mendukung satu sesi peering IPv4 BGP dan satu sesi peering IPv6 BGP. Anda tidak dapat menentukan IPv6 alamat rekan Anda sendiri untuk sesi peering IPv6 BGP. Amazon secara otomatis mengalokasikan Anda IPv6 /125 CIDR.

Multi-protokol BGP tidak didukung. IPv4 dan IPv6 beroperasi dalam mode dual-stack untuk antarmuka virtual.

AWS memungkinkan secara MD5 default. Anda tidak dapat mengubah opsi ini.

Gunakan prosedur berikut untuk menambahkan peer BGP.

Untuk menambahkan peer BGP

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih antarmuka virtual lalu pilih Lihat detail.
4. Pilih Tambahkan peering.
5. (Antarmuka virtual pribadi) Untuk menambahkan rekan IPv4 BGP, lakukan hal berikut:
   - Pilih IPv4.
   - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas. Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS
6. (Antarmuka virtual publik) Untuk menambahkan rekan IPv4 BGP, lakukan hal berikut:
   - Untuk IP rekan router Anda, masukkan alamat tujuan IPv4 CIDR tempat lalu lintas harus dikirim.
   - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

   Important

   Saat mengonfigurasi antarmuka virtual AWS Direct Connect, Anda dapat menentukan alamat IP Anda sendiri menggunakan RFC 1918, menggunakan skema pengalamatan lain, atau memilih alamat IPv4 /29 CIDR yang AWS ditetapkan yang dialokasikan dari rentang RFC 3927 169.254.0.0/16 Link-Local untuk konektivitas. IPv4 point-to-point point-to-pointKoneksi ini harus digunakan secara eksklusif untuk mengintip eBGP antara router gateway pelanggan Anda dan titik akhir Direct Connect. Untuk tujuan lalu lintas atau tunneling VPC, seperti AWS Site-to-Site Private IP VPN, atau Transit Gateway Connect, AWS merekomendasikan penggunaan antarmuka loopback atau LAN pada router gateway pelanggan Anda sebagai alamat sumber atau tujuan alih-alih koneksi. point-to-point

   - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.

- Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat IPv4 Lokal-Tautan.

7. (Antarmuka virtual pribadi atau publik) Untuk menambahkan rekan IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan alamat Amazon; Anda tidak dapat menentukan IPv6 alamat kustom IPv6 .
8. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

   Untuk antarmuka virtual publik, ASN harus privat atau sudah ada pada daftar diizinkan untuk antarmuka virtual.

   Nilai yang valid adalah 1-2147483647.

   Perhatikan bahwa jika Anda tidak memasukkan nilai, kami secara otomatis akan menetapkan nilai.
9. Untuk menyediakan kunci BGP Anda sendiri, untuk Kunci Otentikasi BGP, masukkan kunci BGP Anda. MD5
10. Pilih Tambahkan peering.

Untuk membuat peer BGP menggunakan baris perintah atau API

- create-bgp-peer (AWS CLI)
- Buat BGPPeer (AWS Direct Connect API)

Hapus antarmuka AWS Direct Connect virtual BGP peer

Jika antarmuka virtual Anda memiliki sesi peering IPv4 dan IPv6 BGP, Anda dapat menghapus salah satu sesi peering BGP (tetapi tidak keduanya). Anda dapat menghapus antarmuka virtual BGP peer menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Untuk menghapus peer BGP

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih antarmuka virtual lalu pilih Lihat detail.

4. Di bawah Peering, pilih peering yang ingin Anda hapus, lalu pilih Hapus.
5. Di kotak dialog Hapus peering dari antarmuka virtual, pilih Hapus.

Untuk menghapus peer BGP menggunakan baris perintah atau API

- delete-bgp-peer (AWS CLI)
- Hapus BGPPeer (AWS Direct Connect API)

Mengatur MTU dari antarmuka virtual AWS Direct Connect pribadi

Jika antarmuka virtual Anda memiliki sesi peering IPv4 dan IPv6 BGP, Anda dapat menghapus salah satu sesi peering BGP (tetapi tidak keduanya). Untuk informasi lebih lanjut tentang MTUs dan antarmuka virtual pribadi, lihat MTUs untuk antarmuka virtual pribadi atau antarmuka virtual transit.

Anda dapat mengatur MTU antarmuka virtual pribadi menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Untuk mengatur MTU antarmuka virtual privat

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih antarmuka virtual lalu pilih Edit.
4. Di bawah Jumbo MTU (ukuran MTU 8500), pilih Diaktifkan.
5. Di bawah Pengakuan, pilih Saya memahami koneksi yang dipilih akan tidak aktif dalam jangka waktu singkat. Status antarmuka virtual adalah `pending` hingga pembaruan selesai.

Untuk mengatur MTU antarmuka virtual privat menggunakan baris perintah atau API

- update-virtual-interface-attributes (AWS CLI)
- UpdateVirtualInterfaceAttributes(AWS Direct Connect API)

Menambahkan atau menghapus tag antarmuka AWS Direct Connect virtual

Tanda menyediakan cara untuk mengidentifikasi antarmuka virtual. Anda dapat menambahkan atau menghapus tag menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API jika Anda adalah pemilik akun untuk antarmuka virtual.

Untuk menambah atau menghapus tanda antarmuka virtual

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih antarmuka virtual lalu pilih Edit.
4. Menambah atau menghapus tanda.

   [Menambahkan tanda] Pilih Tambah tanda dan lakukan hal berikut:

   - Untuk Kunci, masukkan nama kunci.
   - Untuk Nilai, masukkan nilai kunci.

   [Menghapus tanda] Di samping tanda, pilih Hapus tanda.
5. Pilih Edit antarmuka virtual.

Untuk menambah tanda atau menghapus tanda menggunakan baris perintah

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Hapus antarmuka AWS Direct Connect virtual

Menghapus satu atau lebih antarmuka virtual. Sebelum dapat menghapus koneksi, Anda harus menghapus antarmuka virtualnya. Menghapus antarmuka virtual menghentikan biaya transfer AWS Direct Connect data yang terkait dengan antarmuka virtual.

Anda dapat menghapus antarmuka virtual menggunakan AWS Direct Connect konsol atau baris perintah atau API.

Untuk menghapus antarmuka virtual

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel sebelah kiri, pilih Antarmuka Virtual.
3. Pilih antarmuka virtual lalu pilih Hapus.
4. Di kotak dialog konfirmasi Hapus, pilih Hapus.

Untuk menghapus antarmuka virtual menggunakan baris perintah atau API

- delete-virtual-interface (AWS CLI)
- DeleteVirtualInterface(AWS Direct Connect API)

Terima antarmuka AWS Direct Connect virtual yang dihosting

Sebelum dapat mulai menggunakan antarmuka virtual yang di-host, Anda harus menerima antarmuka virtual. Untuk antarmuka virtual privat, Anda juga harus memiliki virtual private gateway yang ada atau gateway Direct Connect. Untuk antarmuka virtual transit, Anda harus memiliki transit gateway yang ada atau gateway Direct Connect.

Anda dapat menerima antarmuka virtual yang dihosting menggunakan AWS Direct Connect konsol atau baris perintah atau API.

Untuk menerima antarmuka virtual yang di-host

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih antarmuka virtual lalu pilih Lihat detail.
4. Pilih Terima.
5. Ini berlaku untuk antarmuka virtual privat dan antarmuka virtual transit.

   (Antarmuka virtual transit) Pada kotak dialog Terima antarmuka virtual, pilih gateway Direct Connect, lalu pilih Terima antarmuka virtual.

   (Antarmuka virtual privat) Pada kotak dialog Terima antarmuka virtual, pilih virtual private gateway atau gateway Direct Connect, lalu pilih Terima antarmuka virtual.

6. Setelah Anda menerima antarmuka virtual yang di-host, pemilik koneksi AWS Direct Connect dapat mengunduh file konfigurasi router. Opsi Unduh konfigurasi router tidak tersedia untuk akun yang menerima antarmuka virtual yang di-host.

Untuk menerima antarmuka virtual privat yang di-host menggunakan baris perintah atau API

- confirm-private-virtual-interface (AWS CLI)
- ConfirmPrivateVirtualInterface(AWS Direct Connect API)

Untuk menerima antarmuka virtual publik yang di-host menggunakan baris perintah atau API

- confirm-public-virtual-interface (AWS CLI)
- ConfirmPublicVirtualInterface(AWS Direct Connect API)

Untuk menerima antarmuka virtual transit yang di-host menggunakan baris perintah atau API

- confirm-transit-virtual-interface (AWS CLI)
- ConfirmTransitVirtualInterface(AWS Direct Connect API)

Migrasi antarmuka AWS Direct Connect virtual

Gunakan prosedur ini ketika Anda ingin melakukan salah satu operasi migrasi antarmuka virtual berikut:

- Memigrasi antarmuka virtual yang ada dan terkait dengan koneksi ke LAG lain.
- Memigrasi antarmuka virtual yang ada dan terkait dengan LAG yang ada ke LAG yang baru.
- Memigrasi antarmuka virtual yang ada dan terkait dengan koneksi ke koneksi lain.

> **Note**
>
> - Anda dapat memigrasikan antarmuka virtual ke koneksi baru dalam Wilayah yang sama, tetapi Anda tidak dapat memigrasikannya dari satu Wilayah ke Wilayah lainnya. Saat Anda memigrasikan atau mengaitkan antarmuka virtual yang ada ke koneksi baru, parameter konfigurasi yang terkait dengan antarmuka virtual tersebut sama. Untuk mengatasinya,

Anda dapat melakukan pra-tahap konfigurasi pada koneksi, dan kemudian memperbarui konfigurasi BGP.

- Anda tidak dapat memigrasikan VIF dari satu koneksi yang dihosting ke koneksi host lainnya. VLAN IDs unik; oleh karena itu, memigrasikan VIF dengan cara ini berarti VLANs tidak cocok. Anda juga perlu menghapus koneksi atau VIF, dan kemudian membuatnya menggunakan VLAN yang sama untuk koneksi dan VIF.

Important

Antarmuka virtual akan turun untuk waktu yang singkat. Kami sarankan Anda melakukan prosedur ini selama jendela pemeliharaan.

Untuk memigrasikan antarmuka virtual

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih antarmuka virtual, lalu pilih Edit.
4. Untuk Koneksi, pilih LAG atau koneksi.
5. Pilih Edit antarmuka virtual.

Untuk memigrasi antarmuka virtual menggunakan baris perintah atau API

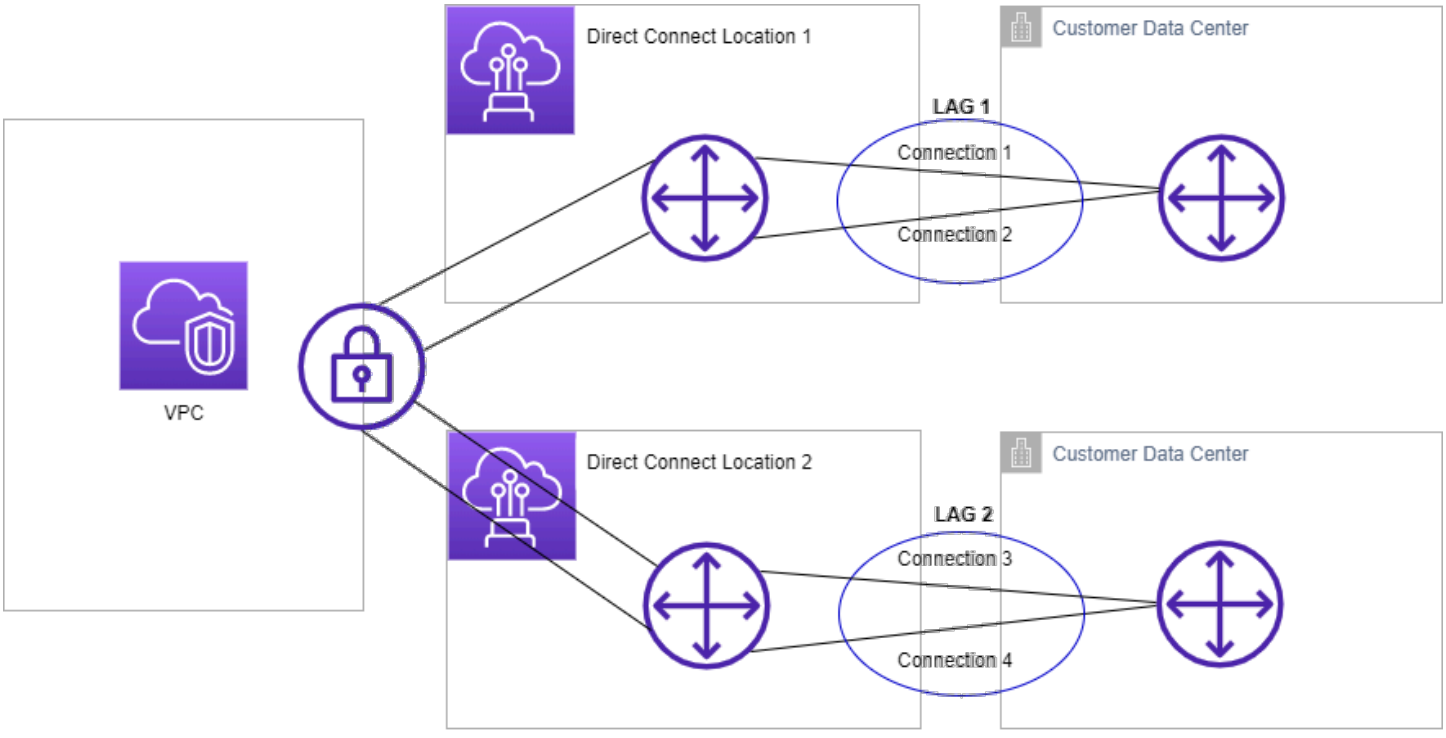
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface(AWS Direct Connect API)

AWS Direct Connect grup agregasi tautan () LAGs

Anda dapat menggunakan beberapa koneksi untuk meningkatkan bandwidth yang tersedia. Grup agregasi tautan (LAG) adalah antarmuka logis yang menggunakan Link Aggregation Control Protocol (LACP) untuk menggabungkan beberapa koneksi pada satu AWS Direct Connect titik akhir, memungkinkan Anda memperlakukannya sebagai koneksi tunggal yang dikelola. LAGs merampingkan konfigurasi karena konfigurasi LAG berlaku untuk semua koneksi dalam grup.

> **Note**
>
> Multi-chassis LAG (MLAG) tidak didukung oleh. AWS

Dalam diagram berikut, Anda memiliki empat koneksi, dengan dua koneksi ke setiap lokasi. Anda dapat membuat LAG untuk koneksi yang berakhir pada AWS perangkat yang sama dan di lokasi yang sama, dan kemudian menggunakan keduanya LAGs alih-alih empat koneksi untuk konfigurasi dan manajemen.



Anda dapat membuat LAG dari koneksi yang ada, atau Anda dapat menyediakan koneksi baru. Setelah membuat LAG, Anda dapat mengaitkan koneksi yang ada (baik mandiri atau bagian dari LAG lain) dengan LAG.

Aturan-aturan berikut berlaku:

- Semua koneksi harus koneksi khusus dan memiliki kecepatan port 1 Gbps, 10 Gbps, 100 Gbps, atau 400 Gbps.
- Semua koneksi di LAG harus menggunakan bandwidth yang sama.
- Anda dapat memiliki maksimum dua koneksi 100 Gbps atau 400 Gbps, atau empat koneksi dengan kecepatan port kurang dari 100 Gbps dalam LAG. Setiap koneksi di LAG dihitung terhadap batas koneksi Anda secara keseluruhan untuk Wilayah.
- Semua koneksi di LAG harus berakhir pada titik AWS Direct Connect akhir yang sama.
- LAGs didukung untuk semua jenis antarmuka virtual—publik, pribadi, dan transit.

Saat Anda membuat LAG, Anda dapat mengunduh Letter of Authorization and Connecting Facility Assignment (LOA-CFA) untuk koneksi fisik baru satu per satu dari konsol. AWS Direct Connect Untuk informasi selengkapnya, lihat Surat Otorisasi dan Penugasan Fasilitas Penghubung (LOA-CFA).

Semua LAGs memiliki atribut yang menentukan jumlah minimum koneksi di LAG yang harus operasional agar LAG itu sendiri dapat beroperasi. Secara default, baru LAGs memiliki atribut ini disetel ke 0. Anda dapat memperbarui LAG untuk menentukan nilai yang berbeda—melakukannya berarti seluruh LAG Anda menjadi nonoperasional jika jumlah koneksi operasional berada di bawah ambang batas ini. Atribut ini dapat digunakan untuk mencegah pemanfaatan berlebih dari koneksi yang tersisa.

Semua koneksi dalam LAG beroperasi dalam mode Aktif/Aktif.

> **Note**
>
> Saat Anda membuat LAG atau mengaitkan lebih banyak koneksi dengan LAG, kami mungkin tidak dapat menjamin cukup port yang tersedia pada AWS Direct Connect titik akhir tertentu.

Topik

- MACsec pertimbangan untuk AWS Direct Connect
- Buat LAG di titik AWS Direct Connect akhir
- Lihat detail LAG di titik AWS Direct Connect akhir
- Memperbarui LAG di titik AWS Direct Connect akhir
- Kaitkan koneksi dengan LAG di titik AWS Direct Connect akhir

- Putuskan koneksi dari LAG pada titik akhir AWS Direct Connect
- Kaitkan MACsec CKN/CAK dengan LAG titik akhir AWS Direct Connect
- Hapus hubungan antara kunci MACsec rahasia dan AWS Direct Connect titik akhir LAG
- Hapus AWS Direct Connect LAG titik akhir

MACsec pertimbangan untuk AWS Direct Connect

Pertimbangkan hal berikut saat Anda ingin mengonfigurasi MACsec LAGs:

- Saat Anda membuat LAG dari koneksi yang ada, kami memisahkan semua MACsec kunci dari koneksi. Kemudian kami menambahkan koneksi ke LAG, dan mengaitkan MACsec kunci LAG dengan koneksi.
- Saat Anda mengaitkan koneksi yang ada ke LAG, MACsec kunci yang saat ini terkait dengan LAG dikaitkan dengan koneksi. Oleh karena itu, kami melepaskan MACsec kunci dari koneksi, menambahkan koneksi ke LAG, dan kemudian mengaitkan MACsec kunci LAG dengan koneksi.

Buat LAG di titik AWS Direct Connect akhir

Anda dapat membuat LAG dengan menyediakan koneksi baru, atau mengagregat koneksi yang ada.

Anda tidak dapat membuat LAG dengan koneksi baru jika ini mengakibatkan Anda melebihi batas koneksi keseluruhan untuk Wilayah.

Untuk membuat LAG dari koneksi yang ada, koneksi harus berada di AWS perangkat yang sama (berakhir pada AWS Direct Connect titik akhir yang sama). LAG juga harus menggunakan bandwidth yang sama. Anda tidak dapat memigrasi koneksi dari LAG yang ada jika menghapus koneksi menyebabkan LAG asli berada di bawah pengaturan jumlah minimum koneksi operasional.

> **Important**
>
> Untuk koneksi yang ada, konektivitas ke AWS terganggu selama pembuatan LAG.

Untuk membuat LAG dengan koneksi baru

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.

2. Di panel navigasi, pilih LAGs.
3. Pilih Buat LAG.
4. Di bawah Jenis pembuatan lag, pilih Minta koneksi baru, dan berikan informasi berikut:
   - Nama LAG: Nama untuk LAG.
   - Lokasi: Lokasi untuk LAG.
   - Kecepatan port: Kecepatan port untuk koneksi.
   - Jumlah koneksi baru: Jumlah koneksi baru untuk membuat LAG. Anda dapat memiliki maksimum empat koneksi ketika kecepatan port 1G atau 10G, atau dua ketika kecepatan port 100 Gbps atau 400 Gbps.
   - (Opsional) Konfigurasikan keamanan MAC (MACsec) untuk koneksi. Di bawah Pengaturan Tambahan, pilih Minta port yang MACsec mampu.

     MACsec hanya tersedia pada koneksi khusus.
   - (Opsional) Tambahkan atau hapus tag.

     [Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:
     - Untuk Kunci, masukkan nama kunci.
     - Untuk Nilai, masukkan nilai kunci.

     [Menghapus tanda] Di samping tanda, pilih Hapus tanda.
5. Pilih Buat LAG.

Untuk membuat LAG dari koneksi yang ada

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAGs.
3. Pilih Buat LAG.
4. Di bawah Jenis pembuatan lag, pilihGunakan koneksi yang ada, dan berikan informasi berikut:
   - Nama LAG: Nama untuk LAG.
   - Koneksi yang ada: Koneksi Direct Connect yang akan digunakan untuk LAG.
   - (Opsional) Jumlah koneksi baru: Jumlah koneksi baru yang akan dibuat. Anda dapat memiliki maksimum empat koneksi ketika kecepatan port 1G atau 10G, atau dua ketika kecepatan port 100 Gbps atau 400 Gbps.

- Tautan minimum: Jumlah minimum koneksi yang harus operasional agar LAG itu sendiri dapat menjadi operasional. Jika Anda tidak menentukan nilai, kami menetapkan nilai default yaitu 0.

5. (Opsional) Menambahkan atau menghapus tanda.

   [Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

   - Untuk Kunci, masukkan nama kunci.
   - Untuk Nilai, masukkan nilai kunci.

   [Menghapus tanda] Di samping tanda, pilih Hapus tanda.

6. Pilih Buat LAG.

Untuk membuat LAG menggunakan baris perintah atau API

- create-lag (AWS CLI)
- CreateLag(AWS Direct Connect API)

Untuk mendeskripsikan Anda LAGs menggunakan baris perintah atau API

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct Connect API)

Untuk mengunduh LOA-CFA menggunakan baris perintah atau API

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct Connect API)

Setelah membuat LAG, Anda dapat mengaitkan atau memisahkan koneksi dari LAG. Untuk informasi selengkapnya, lihat Mengaitkan koneksi dengan LAG dan Memutuskan koneksi dari LAG.

Lihat detail LAG di titik AWS Direct Connect akhir

Setelah membuat LAG, Anda dapat melihat detailnya menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Untuk melihat informasi tentang LAG Anda

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAGs.
3. Pilih LAG dan pilih Lihat detail.
4. Anda dapat melihat informasi tentang LAG, termasuk ID-nya, dan AWS Direct Connect titik akhir di mana koneksi berakhir.

Untuk melihat informasi tentang LAG menggunakan baris perintah atau API

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct Connect API)

Memperbarui LAG di titik AWS Direct Connect akhir

Anda dapat memperbarui atribut grup agregasi tautan (LAG) berikut menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API:

- Nama LAG.
- Nilai minimum dari jumlah koneksi yang harus operasional agar LAG itu sendiri dapat menjadi operasional.
- Mode MACsec enkripsi LAG.

  MACsec hanya tersedia pada koneksi khusus.

  AWS memberikan nilai ini ke setiap koneksi yang merupakan bagian dari LAG.

  Nilai yang valid adalah:

  - `should_encrypt`
  - `must_encrypt`

    Saat Anda mengatur mode enkripsi ke nilai ini, koneksi turun saat enkripsi turun.
  - `no_encrypt`
- Tanda.

> **Note**
>
> Jika Anda menyesuaikan nilai ambang batas untuk jumlah minimum dari koneksi operasional, pastikan bahwa nilai baru tidak menyebabkan LAG berada di bawah ambang batas dan menjadi nonoperasional.

Untuk memperbarui LAG

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAGs.
3. Pilih LAG, lalu pilih Edit.
4. Mengubah LAG

   [Mengganti nama] untuk Nama LAG, masukkan nama LAG baru.

   [Menyesuaikan jumlah minimum koneksi] Untuk Tautan Minimum, masukkan jumlah minimum koneksi operasional.

   [Menambahkan tanda] Pilih Tambah tanda dan lakukan hal berikut:

   - Untuk Kunci, masukkan nama kunci.
   - Untuk Nilai, masukkan nilai kunci.

   [Menghapus tanda] Di samping tanda, pilih Hapus tanda.
5. Pilih Edit LAG.

Untuk memperbarui LAG menggunakan baris perintah atau API

- update-lag (AWS CLI)
- UpdateLag(AWS Direct Connect API)

Kaitkan koneksi dengan LAG di titik AWS Direct Connect akhir

Anda dapat mengaitkan koneksi yang ada dengan LAG menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API. Koneksi dapat bersifat mandiri, atau dapat berupa bagian dari LAG lain. Koneksi harus pada AWS perangkat yang sama dan harus menggunakan

bandwidth yang sama dengan LAG. Jika koneksi sudah terkait dengan LAG lain, Anda tidak dapat mengaitkannya kembali jika menghapus koneksi menyebabkan LAG asli berada di bawah ambang batas untuk jumlah minimum koneksi operasional.

Mengaitkan koneksi ke LAG membuat antarmuka virtual ke LAG dikaitkan kembali secara otomatis.

> **Important**
>
> Konektivitas ke AWS melalui koneksi terputus selama asosiasi.

Untuk mengaitkan koneksi dengan LAG

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAGs.
3. Pilih LAG, lalu pilih Lihat detail.
4. Di bawah Koneksi, pilih Kaitkan koneksi.
5. Untuk Koneksi, pilih koneksi Direct Connect untuk digunakan LAG.
6. Pilih Kaitkan Koneksi.

Untuk mengaitkan koneksi menggunakan baris perintah atau API

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag(AWS Direct Connect API)

Putuskan koneksi dari LAG pada titik akhir AWS Direct Connect

Konversikan koneksi menjadi mandiri dengan memutuskannya dari LAG menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API. Anda tidak dapat memisahkan koneksi jika hal itu menyebabkan LAG berada di bawah ambang batas untuk jumlah minimum koneksi operasional.

Memisah koneksi dari LAG tidak memisahkan antarmuka virtual secara otomatis.

> **Important**
>
> Koneksi Anda AWS terputus selama disasosiasi.

Untuk memisahkan koneksi dari LAG

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel kiri, pilih LAGs.
3. Pilih LAG, lalu pilih Lihat detail.
4. Di bawah Koneksi, pilih koneksi dari daftar koneksi yang tersedia dan pilih Pisahkan.
5. Di kotak dialog konfirmasi, pilih Pisahkan.

Untuk memutuskan koneksi menggunakan baris perintah atau API

- disassociate-connection-from-lag (AWS CLI)
- DisassociateConnectionFromLag(AWS Direct Connect API)

Kaitkan MACsec CKN/CAK dengan LAG titik akhir AWS Direct Connect

Setelah Anda membuat LAG yang mendukung MACsec, Anda dapat mengaitkan CKN/CAK dengan koneksi menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

> **Note**
>
> Anda tidak dapat memodifikasi kunci MACsec rahasia setelah Anda mengaitkannya dengan LAG. Jika Anda perlu mengubah kunci, memisahkan kunci dari koneksi, lalu mengaitkan kunci baru dengan koneksi. Untuk informasi tentang menghapus pengaitan, lihat the section called “Hapus hubungan antara kunci MACsec rahasia dan LAG”.

Untuk mengaitkan MACsec kunci dengan LAG

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAGs.
3. Pilih LAG dan pilih Lihat detail.
4. Pilih Kaitkan kunci.
5. Masukkan MACsec kuncinya.

[Menggunakan pasangan CAK/CKN] Pilih Pasangan Kunci, lalu lakukan hal berikut:

- Untuk Connectivity Association Key (CAK), masukkan CAK.
- Untuk Connectivity Association Key Name (CKN), masukkan CKN.

[Gunakan rahasia] Pilih rahasia Manajer Rahasia yang Ada, lalu untuk Rahasia, pilih kunci MACsec rahasia.

6. Pilih Kaitkan kunci.

Untuk mengaitkan MACsec kunci dengan LAG menggunakan baris perintah atau API

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(AWS Direct Connect API)

Hapus hubungan antara kunci MACsec rahasia dan AWS Direct Connect titik akhir LAG

Anda dapat menghapus hubungan antara LAG dan MACsec kunci menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Untuk menghapus asosiasi antara LAG dan MACsec kunci

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAGs.
3. Pilih LAG dan pilih Lihat detail.
4. Pilih MACsec rahasia yang akan dihapus, lalu pilih Disassociate kunci.
5. Di kotak dialog konfirmasi, masukkan pisahkan, lalu pilihPisahkan.

Untuk menghapus asosiasi antara LAG dan MACsec kunci menggunakan baris perintah atau API

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct Connect API)

Hapus AWS Direct Connect LAG titik akhir

Jika Anda tidak perlu lagi LAGs, Anda dapat menghapusnya. Anda tidak dapat menghapus LAG jika memiliki antarmuka virtual yang dikaitkan dengan LAG. Anda harus terlebih dahulu menghapus antarmuka virtual, atau mengaitkannya dengan LAG atau koneksi yang berbeda. Menghapus LAG tidak menghapus koneksi di LAG; Anda harus menghapus koneksi sendiri. Untuk informasi selengkapnya, lihat Menghapus koneksi.

Anda dapat menghapus LAG menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Untuk menghapus LAG

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAGs.
3. Pilih LAGs, dan kemudian pilih Hapus.
4. Di kotak dialog konfirmasi, pilih Hapus.

Untuk menghapus LAG menggunakan baris perintah atau API

- delete-lag (AWS CLI)
- DeleteLag(AWS Direct Connect API)

AWS Direct Connect gerbang

Anda dapat bekerja dengan AWS Direct Connect gateway menggunakan konsol VPC Amazon atau. AWS CLI

- Gateway Direct Connect

  Menggunakan gateway Direct Connect, Anda dapat mengaitkan gateway Direct Connect dengan gateway transit dengan beberapa VPCs, gateway pribadi virtual, atau jika Anda menggunakan AWS Cloud WAN, ke jaringan inti Cloud WAN.

- Keterkaitan virtual private gateway

  Menggunakan gateway pribadi virtual, Anda dapat mengaitkan gateway Direct Connect melalui antarmuka virtual pribadi ke satu atau lebih VPCs di akun mana pun yang terletak di Wilayah yang sama atau berbeda.

- Keterkaitan transit gateway

  Gunakan gateway Direct Connect untuk menghubungkan koneksi Direct Connect Anda melalui antarmuka virtual transit ke VPCs atau VPNs yang dilampirkan ke gateway transit Anda.

- Asosiasi jaringan inti WAN awan

  Gunakan gateway Direct Connect untuk mengaitkan gateway Direct Connect dengan jaringan AWS Network Manager inti.

- Interaksi prefiks yang diizinkan

  Gunakan awalan yang diizinkan untuk berinteraksi dengan gateway transit dan gateway pribadi virtual.

Topik

AWS Direct Connect gerbang

Gunakan AWS Direct Connect gateway untuk menghubungkan Anda VPCs. Anda mengaitkan AWS Direct Connect gateway dengan salah satu dari berikut ini:

- Gateway transit ketika Anda memiliki beberapa VPCs di Wilayah yang sama
- Virtual private gateway
- Jaringan inti AWS Cloud WAN

Anda juga dapat menggunakan virtual private gateway untuk memperluas Local Zone Anda. Konfigurasi ini memungkinkan VPC yang terkait dengan Local Zone untuk terhubung ke gateway Direct Connect. Gateway Direct Connect terhubung ke lokasi Direct Connect di suatu Wilayah. Pusat data lokal memiliki sambungan Direct Connect ke lokasi Direct Connect. Untuk informasi selengkapnya, lihat Mengakses Local Zones menggunakan gateway Direct Connect di Panduan Pengguna Amazon VPC.

Gateway Direct Connect adalah sumber daya yang tersedia secara global. Anda dapat terhubung ke Wilayah mana pun secara global menggunakan gateway Direct Connect. Ini termasuk AWS GovCloud (US), tetapi tidak termasuk Wilayah AWS Tiongkok. Gateway Direct Connect adalah komponen virtual Direct Connect yang dirancang untuk bertindak sebagai seperangkat reflektor rute BGP terdistribusi. Karena beroperasi di luar jalur lalu lintas data, ia menghindari menciptakan satu titik kegagalan atau memperkenalkan dependensi pada spesifik. Wilayah AWS Ketersediaan tinggi secara inheren dibangun ke dalam desainnya, menghilangkan kebutuhan akan beberapa gateway Direct Connect.

Pelanggan yang menggunakan Direct Connect dengan VPCs yang saat ini melewati Availability Zone induk tidak akan dapat memigrasikan koneksi Direct Connect atau antarmuka virtual mereka.

Berikut ini menjelaskan skenario di mana Anda dapat menggunakan gateway Direct Connect.

Gateway Direct Connect tidak mengizinkan keterkaitan gateway yang berada di gateway Direct Connect yang sama untuk mengirim lalu lintas ke satu sama lain (misalnya, virtual private gateway ke virtual private gateway lain). Pengecualian untuk aturan ini, diterapkan pada November 2021, adalah ketika supernet diiklankan di dua atau lebih VPCs, yang memiliki gateway pribadi virtual terlampir (VGWs) yang terkait dengan gateway Direct Connect yang sama dan pada antarmuka virtual yang sama. Dalam hal ini, VPCs dapat berkomunikasi satu sama lain melalui titik akhir Direct Connect. Misalnya, jika Anda mengiklankan supernet (misalnya, 10.0.0.0/8 atau 0.0.0.0/0) yang tumpang tindih

dengan gateway Direct Connect yang terpasang VPCs (misalnya, 10.0.0.0/24 dan 10.0.1.0/24), dan pada antarmuka virtual yang sama, kemudian dari jaringan lokal Anda, dapat berkomunikasi satu sama lain. VPCs

Jika Anda ingin memblokir VPC-to-VPC komunikasi dalam gateway Direct Connect, lakukan hal berikut:

1. Siapkan grup keamanan pada instance dan sumber daya lain di VPC untuk memblokir lalu lintas di VPCs antaranya, juga menggunakan ini sebagai bagian dari grup keamanan default di VPC.
2. Hindari mengiklankan supernet dari jaringan lokal Anda yang tumpang tindih dengan Anda. VPCs Sebagai gantinya, Anda dapat mengiklankan rute yang lebih spesifik dari jaringan lokal yang tidak tumpang tindih dengan Anda. VPCs
3. Menyediakan satu Direct Connect Gateway untuk setiap VPC yang ingin Anda sambungkan ke jaringan lokal, bukan menggunakan Direct Connect Gateway yang sama untuk beberapa. VPCs Misalnya, alih-alih menggunakan satu Direct Connect Gateway untuk pengembangan dan produksi Anda VPCs, gunakan Direct Connect Gateways terpisah untuk masing-masing gerbang tersebut. VPCs

Gateway Direct Connect tidak mencegah lalu lintas dikirim dari satu keterkaitan gateway kembali ke keterkaitan gateway itu sendiri (misalnya saat Anda memiliki rute supernet on-premise yang berisi prefiks dari keterkaitan gateway). Jika Anda memiliki konfigurasi dengan beberapa gateway transit yang VPCs terhubung ke gateway Direct Connect yang sama, gateway tersebut VPCs dapat berkomunikasi. Untuk VPCs mencegah komunikasi, kaitkan tabel rute dengan lampiran VPC yang memiliki opsi lubang hitam yang disetel.

Topik

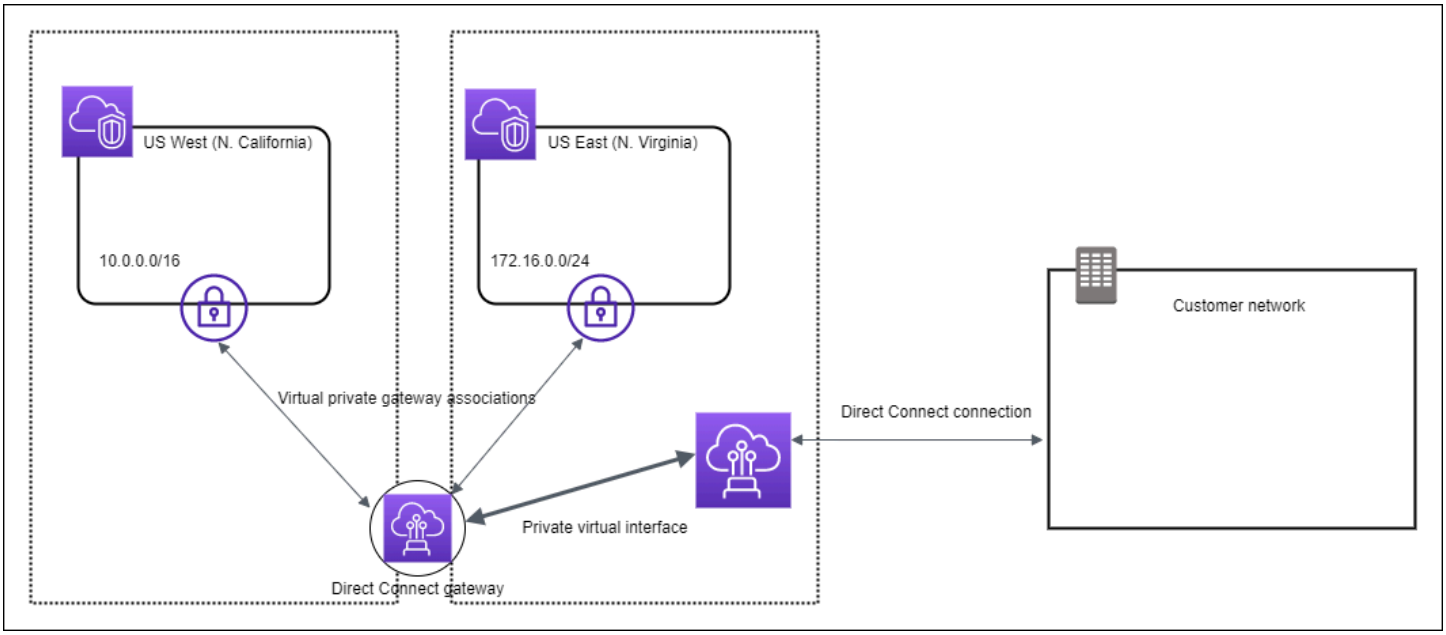
Skenario

Berikut ini menjelaskan hanya beberapa skenario untuk menggunakan gateway Direct Connect.

Skenario: Asosiasi gateway pribadi virtual

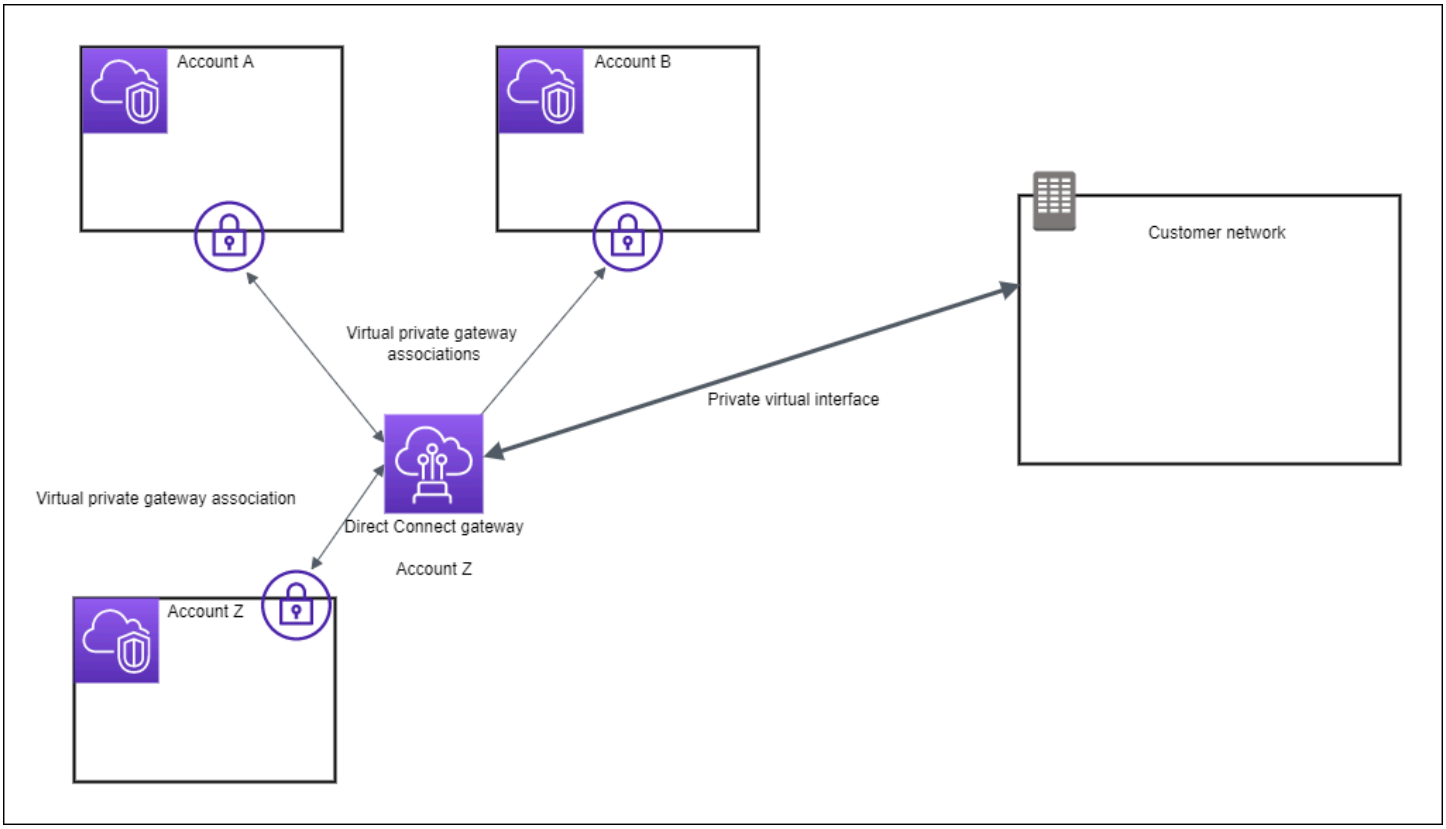
Dalam diagram berikut, gateway Direct Connect memungkinkan Anda untuk menggunakan AWS Direct Connect koneksi Anda di Wilayah AS Timur (Virginia N.) untuk mengakses akun Anda VPCs di Wilayah AS Timur (Virginia N.) dan AS Barat (California N.).

Setiap VPC memiliki virtual private gateway yang terhubung ke gateway Direct Connect menggunakan keterkaitan virtual private gateway. Gateway Direct Connect menggunakan antarmuka virtual pribadi untuk koneksi ke AWS Direct Connect lokasi. Ada koneksi AWS Direct Connect dari lokasi ke pusat data pelanggan.



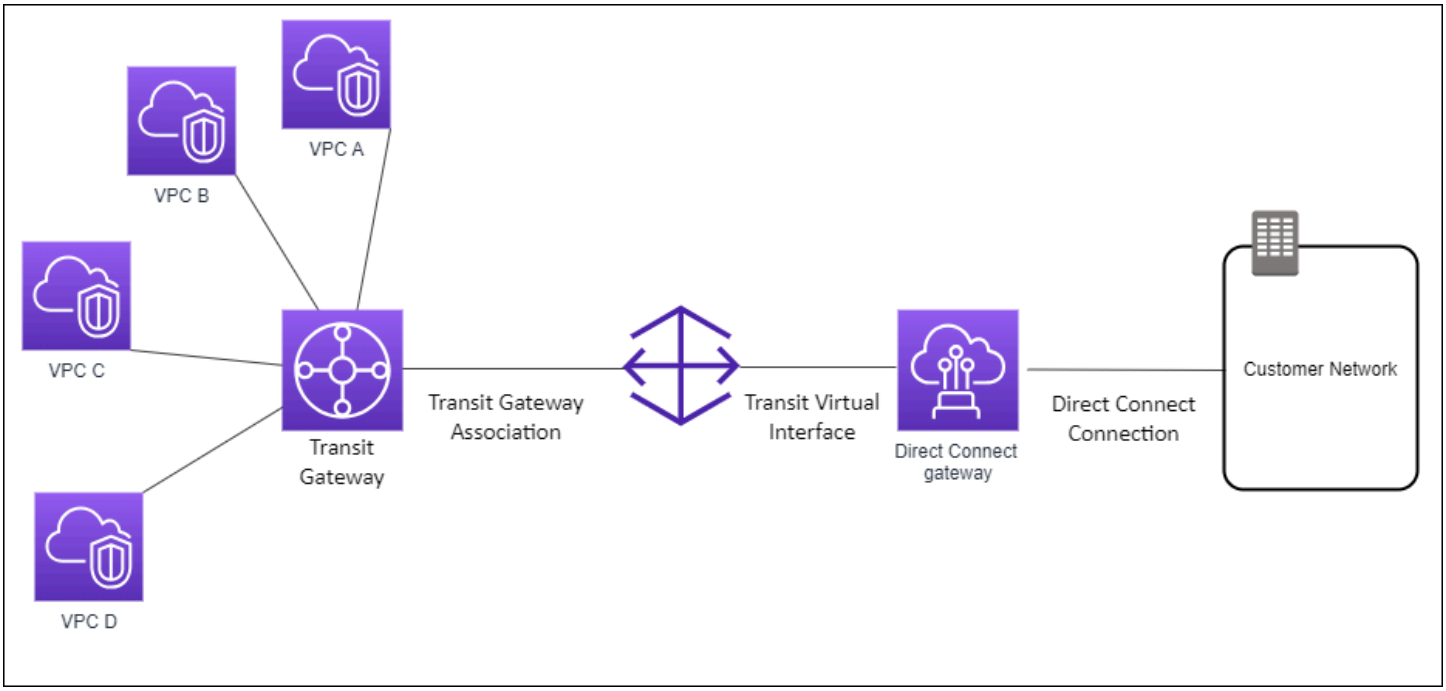
Skenario: Asosiasi gateway pribadi virtual di seluruh akun

Pertimbangkan skenario pemilik gateway Direct Connect (Akun Z) yang memiliki gateway Direct Connect ini. Akun A dan Akun B ingin menggunakan gateway Direct Connect. Akun A dan Akun B masing-masing mengirim proposal keterkaitan ke Akun Z. Akun Z menerima proposal keterkaitan dan secara opsional dapat memperbarui prefiks yang diizinkan dari virtual private gateway Akun A atau virtual private gateway Akun B. Setelah Akun Z menerima proposal, Akun A dan Akun B dapat merutekan lalu lintas dari virtual private gateway mereka ke gateway Direct Connect. Akun Z juga memiliki perutean ke pelanggan karena Akun Z memiliki gateway.



Skenario: Asosiasi gateway transit

Diagram berikut mengilustrasikan bagaimana gateway Direct Connect memungkinkan Anda membuat satu koneksi ke koneksi Direct Connect yang VPCs dapat Anda gunakan.



Solusinya melibatkan komponen berikut:

- Transit gateway yang memiliki lampiran VPC.
- Sebuah gateway Direct Connect.
- Keterkaitan antara gateway Direct Connect dan transit gateway.
- Antarmuka virtual transit yang terlampir ke gateway Direct Connect.

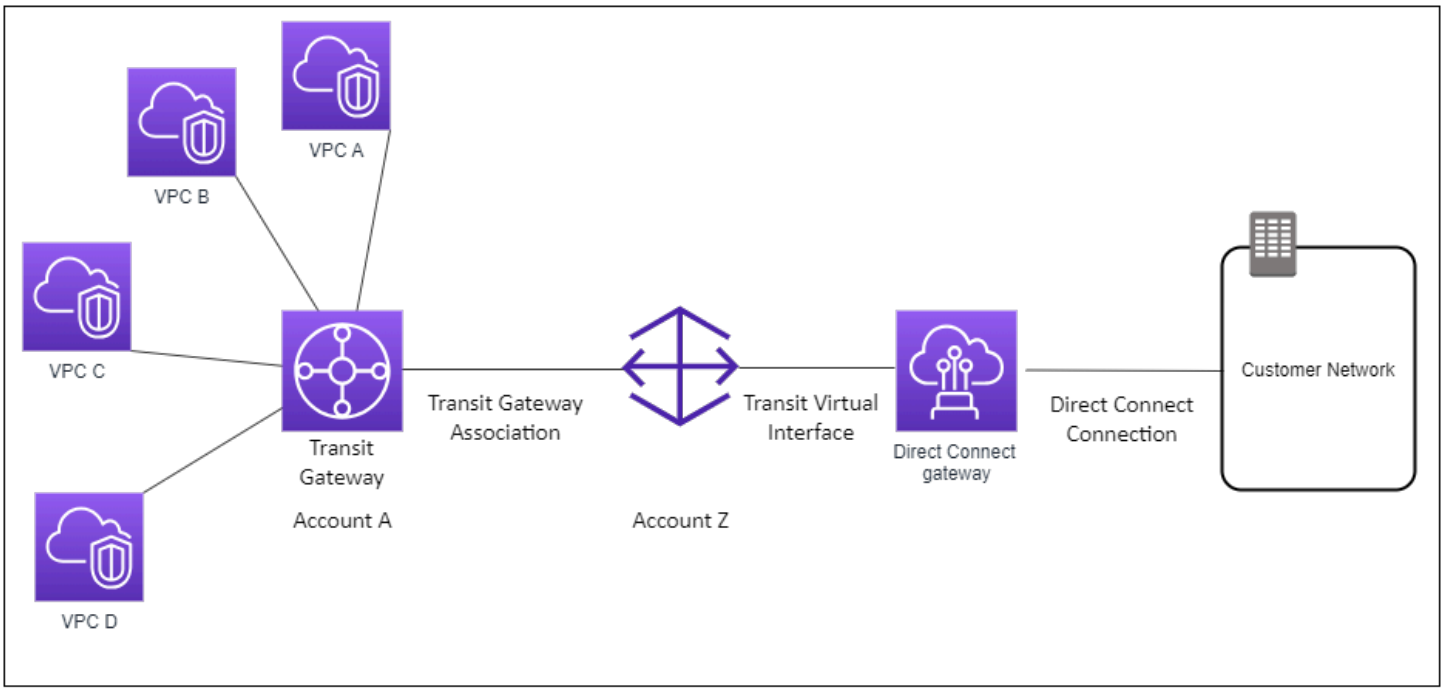
Konfigurasi ini menawarkan manfaat sebagai berikut. Anda dapat:

- Kelola satu koneksi untuk beberapa VPCs atau VPNs yang berada di Wilayah yang sama.
- Iklankan awalan dari lokal ke AWS dan dari ke lokal. AWS

Untuk informasi tentang mengonfigurasi transit gateway, lihat Bekerja dengan Transit Gateway di Panduan Transit Amazon VPC.

Skenario: Asosiasi gateway transit lintas akun

Pertimbangkan skenario pemilik gateway Direct Connect (Akun Z) yang memiliki gateway Direct Connect ini. Akun A memiliki transit gateway dan ingin menggunakan gateway Direct Connect. Akun Z menerima proposal keterkaitan dan secara opsional dapat memperbarui prefiks yang diizinkan dari transit gateway Akun A. Setelah Akun Z menerima proposal, yang VPCs dilampirkan ke gateway transit dapat merutekan lalu lintas dari gateway transit ke gateway Direct Connect. Akun Z juga memiliki perutean ke pelanggan karena Akun Z memiliki gateway.



Buat AWS Direct Connect gateway

Anda dapat membuat gateway Direct Connect di Wilayah mana pun yang didukung menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Untuk membuat gateway Direct Connect

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Gateway Direct Connect.
3. Pilih Buat Gateway Direct Connect.
4. Tentukan informasi berikut, dan pilih Buat Gateway Direct Connect.
   - Nama: Masukkan nama untuk membantu Anda mengidentifikasi gateway Direct Connect.
   - ASN sisi Amazon: Tentukan ASN untuk sisi Amazon sesi BGP. ASN harus berada dalam rentang 64.512 hingga 65.534 atau 4.200.000.000 hingga 4.294.967,294.

> **Note**
>
> Jika Anda ingin membuat gateway Direct Connect untuk digunakan dengan jaringan inti AWS Cloud WAN. ASN tidak boleh berada dalam kisaran yang sama dengan ASN jaringan inti.

Untuk membuat gateway Direct Connect menggunakan baris perintah atau API

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway(AWS Direct Connect API)

Bermigrasi dari gateway pribadi virtual ke gateway AWS Direct Connect

Anda dapat memigrasikan gateway pribadi virtual yang dilampirkan ke antarmuka virtual ke gateway Direct Connect.

Jika Anda menggunakan Direct Connect dengan VPCs yang saat ini melewati Availability Zone induk, Anda tidak akan dapat memigrasikan koneksi Direct Connect atau antarmuka virtual.

Langkah-langkah berikut menjelaskan langkah-langkah yang perlu Anda ambil untuk memigrasikan gateway pribadi virtual ke gateway Direct Connect.

Untuk bermigrasi ke gateway Direct Connect

1. Buat gateway Direct Connect.

   Jika gateway Direct Connect belum ada, Anda harus membuatnya. Untuk langkah-langkah membuat gateway Direct Connect, lihatBuat gateway Direct Connect.
2. Buat antarmuka virtual untuk gateway Direct Connect.

   Antarmuka virtual diperlukan untuk migrasi. Jika antarmuka tidak ada, Anda harus membuatnya. Untuk langkah-langkah membuat antarmuka virtual, lihatAntarmuka virtual.
3. Kaitkan virtual private gateway dengan gateway Direct Connect.

   Baik gateway Direct Connect dan gateway pribadi virtual perlu dikaitkan. Untuk langkah-langkah untuk membuat asosiasi, lihatKaitkan atau lepaskan gateway pribadi virtual.
4. Hapus antarmuka virtual yang dikaitkan dengan virtual private gateway. Untuk informasi selengkapnya, lihat Hapus antarmuka virtual.

Hapus AWS Direct Connect gateway

Jika Anda tidak lagi memerlukan gateway Direct Connect, Anda dapat menghapusnya. Anda harus terlebih dulu memisahkan semua virtual private gateway terkait dan menghapus antarmuka virtual privat terlampir. Setelah Anda melepaskan gateway pribadi virtual terkait dan menghapus antarmuka

virtual pribadi terlampir, Anda dapat menghapus gateway Direct Connect menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

- Untuk langkah-langkah untuk memisahkan gateway pribadi virutal, lihat. Kaitkan atau lepaskan gateway pribadi virtual
- Untuk langkah-langkah menghapus antarmuka virtual, lihatHapus antarmuka virtual.

Menghapus gateway Direct Connect

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilihGateway Direct Connect.
3. Pilih gateway dan pilih Hapus.

Untuk menghapus gateway Direct Connect menggunakan baris perintah atau API

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway(AWS Direct Connect API)

AWS Direct Connect asosiasi gateway pribadi virtual

Anda dapat menggunakan AWS Direct Connect gateway untuk menghubungkan AWS Direct Connect koneksi Anda melalui antarmuka virtual pribadi ke satu atau lebih VPCs di akun mana pun yang berada di Wilayah yang sama atau berbeda. Anda mengaitkan gateway Direct Connect dengan virtual private gateway untuk VPC. Kemudian, Anda membuat antarmuka virtual pribadi untuk AWS Direct Connect koneksi Anda ke gateway Direct Connect. Anda dapat melampirkan beberapa antarmuka virtual privat ke gateway Direct Connect Anda.

Aturan berikut berlaku untuk keterkaitan virtual private gateway:

- Jangan aktifkan propagasi rute sampai setelah Anda mengaitkan gateway virtual dengan gateway Direct Connect. Jika Anda mengaktifkan propagasi rute sebelum mengaitkan gateway, rute mungkin disebarkan secara tidak benar.
- Ada batasan untuk membuat dan menggunakan gateway Direct Connect. Untuk informasi selengkapnya, lihat Kuota Direct Connect.
- Anda tidak dapat melampirkan gateway Direct Connect ke gateway pribadi virtual ketika gateway Direct Connect sudah dikaitkan dengan gateway transit.

- Yang VPCs Anda sambungkan melalui gateway Direct Connect tidak dapat memiliki blok CIDR yang tumpang tindih. Jika Anda menambahkan blok IPv4 CIDR ke VPC yang terkait dengan gateway Direct Connect, pastikan bahwa blok CIDR tidak tumpang tindih dengan blok CIDR yang ada untuk VPC terkait lainnya. Untuk informasi selengkapnya, lihat Menambahkan Blok IPv4 CIDR ke VPC di Panduan Pengguna Amazon VPC.
- Anda tidak dapat membuat antarmuka virtual publik ke gatewat Direct Connect.
- Gateway Direct Connect mendukung komunikasi antara antarmuka virtual pribadi terlampir dan gateway pribadi virtual terkait saja, dan dapat mengaktifkan gateway pribadi virtual ke gateway pribadi lainnya. Arus lalu lintas berikut tidak didukung:
  - Komunikasi langsung antara VPCs yang terkait dengan gateway Direct Connect tunggal. Ini termasuk lalu lintas dari satu VPC ke yang lain dengan menggunakan hairpin melalui jaringan on-premise melalui gateway Direct Connect tunggal.
  - Komunikasi langsung antara antarmuka virtual yang dilampirkan ke gateway Direct Connect tunggal.
  - Komunikasi langsung antara antarmuka virtual yang dilampirkan ke gateway Direct Connect tunggal dan koneksi VPN di virtual private gateway yang terkait dengan gateway Direct Connect yang sama.
- Anda tidak dapat mengaitkan virtual private gateway dengan lebih dari satu langsung Connect gateway dan Anda tidak dapat melampirkan antarmuka virtual privat untuk lebih dari satu gateway Direct Connect.
- Virtual private gateway yang Anda kaitkan dengan gateway Direct Connect harus dilampirkan ke VPC.
- Proposal keterkaitan virtual private gateway kedaluwarsa 7 hari setelah dibuat.
- Proposal virtual private gateway yang diterima, atau proposal virtual private gateway yang dihapus tetap terlihat selama 3 hari.
- Sebuah virtual private gateway dapat dikaitkan dengan gateway Direct Connect dan juga dilampirkan pada antarmuka virtual.
- Melepaskan gateway pribadi virtual dari VPC juga memisahkan gateway pribadi virtual dari gateway Direct Connect.
- Jika Anda berencana menggunakan virtual private gateway untuk gateway Direct Connect dan koneksi VPN dinamis, atur ASN pada virtual private gateway ke nilai yang Anda perlukan untuk koneksi VPN. Jika tidak, ASN pada virtual private gateway dapat diatur ke nilai yang diizinkan. Gateway Direct Connect mengiklankan semua yang terhubung VPCs melalui ASN yang ditetapkan padanya.

Untuk menghubungkan AWS Direct Connect koneksi Anda ke VPC di Wilayah yang sama saja, Anda dapat membuat gateway Direct Connect. Atau, Anda dapat membuat antarmuka virtual privat dan melampirkannya ke virtual private gateway untuk VPC. Untuk informasi selengkapnya, lihat Membuat antarmuka virtual privat dan VPN CloudHub.

Untuk menggunakan AWS Direct Connect koneksi Anda dengan VPC di akun lain, Anda dapat membuat antarmuka virtual pribadi yang dihosting untuk akun tersebut. Saat pemilik akun lain menerima antarmuka virtual yang di-host, mereka dapat memilih untuk melampirkannya baik ke virtual private gateway atau ke gateway Direct Connect di akun mereka. Untuk informasi selengkapnya, lihat Antarmuka virtual dan antarmuka virtual yang dihosting.

Topik

Buat gateway pribadi AWS Direct Connect virtual

Virtual private gateway harus dilampirkan ke VPC yang ingin Anda hubungkan. Anda dapat membuat gateway pribadi virtual dan melampirkannya ke VPC menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

> **Note**
>
> Jika Anda berencana menggunakan virtual private gateway untuk gateway Direct Connect dan koneksi VPN dinamis, atur ASN pada virtual private gateway ke nilai yang Anda perlukan untuk koneksi VPN. Jika tidak, ASN pada virtual private gateway dapat diatur ke nilai yang diizinkan. Gateway Direct Connect mengiklankan semua yang terhubung VPCs melalui ASN yang ditetapkan padanya.

Setelah Anda membuat gateway privat virtual, Anda harus melampirkannya ke VPC Anda.

Untuk membuat gateway privat virtual dan melampirkannya ke VPC Anda

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.

2. Di panel navigasi, pilih Virtual Private Gateways, lalu pilih Create Virtual Private Gateway.
3. (Opsional) Masukkan nama untuk gateway privat virtual Anda. Dengan melakukan hal tersebut akan menciptakan tanda dengan kunci `Name` dan nilai yang Anda tentukan.
4. Untuk ASN, tinggalkan pilihan default agar dapat menggunakan Amazon ASN default. Jika tidak, mohon untuk memilih ASN kustom dan silahkan memasukkan sebuah nilai. Untuk ASN 16-bit, nilainya harus berada dalam rentang 64512 hingga 65534. Untuk ASN 32-bit, nilainya harus berada dalam rentang 4200000000 hingga 4294967294.
5. Pilih Buat Gateway Privat Virtual.
6. Pilih gateway privat virtual yang telah Anda buat, dan kemudian pilih Tindakan, Lampirkan ke VPC.
7. Pilih VPC Anda dari daftar dan pilih Ya, lampirkan.

Untuk membuat gateway privat virtual menggunakan baris perintah atau API

- CreateVpnGateway(API EC2 Kueri Amazon)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

Untuk melampirkan gateway privat virtual ke VPC menggunakan baris perintah atau API

- AttachVpnGateway(API EC2 Kueri Amazon)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Kaitkan atau lepaskan gateway pribadi AWS Direct Connect virtual

Anda dapat mengaitkan atau memisahkan gateway pribadi virtual dan gateway Direct Connect menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API. Pemilik akun virtual private gateway melakukan operasi ini.

Untuk mengaitkan virtual private gateway

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih gateway Direct Connect dan kemudian pilih gateway Direct Connect.

3. Pilih Lihat detail.
4. Pilih asosiasi Gateway, lalu pilih Gateway asosiasi.
5. Untuk Gateway, pilih virtual private gateway untuk dikaitkan, kemudian pilih Keterkaitan gateway.

Anda dapat melihat semua virtual private gateway yang terkait dengan gateway Direct Connect dengan memilih Keterkaitan gateway.

Untuk memisahkan virtual private gateway

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Gateway Direct Connect, lalu pilih gateway Direct Connect.
3. Pilih Lihat detail.
4. Pilih Keterkaitan gateway, kemudian pilih virtual private gateway.
5. Pilih Pisahkan.

Untuk menghubungkan virtual private gateway menggunakan baris perintah atau API

- create-direct-connect-gateway-asosiasi ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

Untuk melihat virtual private gateway yang terkait dengan gateway Direct Connect menggunakan baris perintah atau API

- describe-direct-connect-gateway-asosiasi ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

Untuk memisahkan virtual private gateway menggunakan baris perintah atau API

- delete-direct-connect-gateway-asosiasi ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

Buat antarmuka virtual pribadi ke AWS Direct Connect gateway

Untuk menghubungkan AWS Direct Connect koneksi Anda ke VPC jarak jauh, Anda harus membuat antarmuka virtual pribadi untuk koneksi Anda. Tentukan gateway Direct Connect yang akan

dihubungkan. Anda dapat membuat antarmuka virtual pribadi menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

> **Note**
>
> Jika Anda menerima antarmuka virtual privat yang di-host, Anda dapat mengaitkannya dengan gateway Direct Connect di akun Anda. Untuk informasi selengkapnya, lihat Menerima antarmuka virtual yang di-host.

Untuk menyediakan antarmuka virtual privat ke gateway Direct Connect

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.
4. Di bawah Tipe antarmuka virtual, pilih Privat.
5. Di bawah Pengaturan antarmuka virtual privat Anda, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.

   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.

   c. Untuk pemilik antarmuka Virtual, pilih AWS Akun saya jika antarmuka virtual untuk AWS akun Anda.

   d. Untuk Gateway Direct Connect, pilih gateway Direct Connect.

   e. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).

   f. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

      Nilai yang valid adalah 1 hingga 2147483647.
6. Di bawah Pengaturan Tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

      - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.

- Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

> **Important**
>
> Saat mengonfigurasi antarmuka virtual AWS Direct Connect, Anda dapat menentukan alamat IP Anda sendiri menggunakan RFC 1918, menggunakan skema pengalamatan lain, atau memilih alamat IPv4 /29 CIDR yang AWS ditetapkan yang dialokasikan dari rentang RFC 3927 169.254.0.0/16 Link-Local untuk konektivitas. IPv4 point-to-point point-to-pointKoneksi ini harus digunakan secara eksklusif untuk mengintip eBGP antara router gateway pelanggan Anda dan titik akhir Direct Connect. Untuk tujuan lalu lintas atau tunneling VPC, seperti AWS Site-to-Site Private IP VPN, atau Transit Gateway Connect, AWS merekomendasikan penggunaan antarmuka loopback atau LAN pada router gateway pelanggan Anda sebagai alamat sumber atau tujuan alih-alih koneksi. point-to-point
>
> - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
> - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat IPv4 Lokal-Tautan.

[IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk mengubah maximum transmission unit (MTU) dari 1500 (default) menjadi 9001 (bingkai jumbo), pilih MTU Jumbo (MTU ukuran 9001).

c. (Opsional) Di bawah Aktifkan SiteLink, pilih Diaktifkan untuk mengaktifkan konektivitas langsung antara titik kehadiran Direct Connect.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.

Setelah membuat antarmuka virtual, Anda dapat mengunduh konfigurasi router untuk perangkat Anda. Untuk informasi selengkapnya, lihat Mengunduh file konfigurasi router.

Untuk membuat antarmuka virtual privat menggunakan baris perintah atau API

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface(AWS Direct Connect API)

Untuk melihat antarmuka virtual yang dilampirkan ke gateway Direct Connect menggunakan baris perintah atau API

- describe-direct-connect-gateway-lampiran ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

Kaitkan gateway pribadi AWS Direct Connect virtual di seluruh akun

Anda dapat mengaitkan gateway Direct Connect dengan gateway pribadi virtual yang dimiliki oleh AWS akun apa pun. Gateway Direct Connect dapat berupa gateway yang ada, atau Anda dapat membuat gateway baru. Pemilik virtual private gateway akan membuat proposal keterkaitan dan pemilik gateway Direct Connect harus menerima proposal keterkaitan.

Proposal keterkaitan dapat berisi prefiks yang akan diizinkan dari virtual private gateway. Pemilik gateway Direct Connect opsional dapat mengganti prefiks yang diminta dalam proposal keterkaitan.

Prefiks yang diizinkan

Saat Anda mengaitkan virtual private gateway dengan gateway Direct Connect, Anda menentukan daftar prefiks Amazon VPC untuk diiklankan ke gateway Direct Connect. Daftar awalan bertindak sebagai filter yang memungkinkan hal yang sama CIDRs, atau lebih kecil CIDRs untuk diiklankan ke gateway Direct Connect. Anda harus mengatur Prefiks yang diizinkan ke rentang yang sama atau lebih lebar dari VPC CIDR karena kami menyediakan seluruh VPC CIDR pada virtual private gateway.

Pertimbangkan kasus dengan VPC CIDR adalah 10.0.0.0/16. Anda dapat mengatur Prefiks yang diizinkan ke 10.0.0.0/16 (nilai VPC CIDR), atau 10.0.0.0/15 (nilai yang lebih lebar dari VPC CIDR).

Setiap antarmuka virtual di dalam awalan jaringan yang diiklankan melalui Direct Connect hanya disebarkan ke gateway transit di seluruh Wilayah, bukan dalam Wilayah yang sama. Untuk informasi elengkapnya tentang bagaimana prefiks yang diizinkan berinteraksi dengan virtual private gateway dan transit gateway, lihat Interaksi prefiks yang diizinkan.

AWS Direct Connect gateway dan asosiasi gateway transit

Anda dapat menggunakan AWS Direct Connect gateway untuk menghubungkan koneksi Direct Connect melalui antarmuka virtual transit ke VPCs atau VPNs yang dilampirkan ke gateway transit Anda. Anda mengaitkan gateway Direct Connect dengan transit gateway. Kemudian, buat antarmuka virtual transit untuk AWS Direct Connect koneksi Anda ke gateway Direct Connect.

Aturan berikut berlaku untuk keterkaitan transit gateway:

- Anda tidak dapat melampirkan gateway Direct Connect ke transit gateway saat gateway Direct Connect sudah terkait dengan virtual private gateway atau terlampir ke antarmuka virtual privat.
- Ada batasan untuk membuat dan menggunakan gateway Direct Connect. Untuk informasi selengkapnya, lihat Kuota Direct Connect.
- Gateway Direct Connect mendukung komunikasi antara antarmuka virtual transit terlampir dan gateway transit terkait.
- Jika Anda terhubung ke beberapa gateway transit yang berada di Wilayah berbeda, gunakan unik ASNs untuk setiap gateway transit.
- Alamat point-to-point konektivitas apa pun yang menggunakan `/30` rentang `192.168.0.0/30` — misalnya, — tidak menyebar ke gateway transit.

Mengaitkan transit gateway di seluruh akun

Anda dapat mengaitkan gateway Direct Connect yang sudah ada atau gateway Direct Connect baru dengan gateway transit yang dimiliki oleh AWS akun apa pun. Pemilik transit gateway akan membuat proposal keterkaitan dan pemilik gateway Direct Connect harus menerima proposal keterkaitan.

Sebuah proposal keterkaitan dapat berisi prefiks yang akan diizinkan dari transit gateway. Pemilik gateway Direct Connect opsional dapat mengganti prefiks yang diminta dalam proposal keterkaitan.

Prefiks yang diizinkan

Untuk keterkaitan transit gateway, Anda menyediakan daftar prefiks yang diizinkan di gateway Direct Connect. Daftar ini digunakan untuk merutekan lalu lintas dari lokal AWS ke gateway transit

meskipun yang VPCs dilampirkan ke gateway transit tidak ditetapkan CIDRs. Prefiks dalam daftar prefiks Direct Connect yang diizinkan berasal dari gateway Direct Connect dan diiklankan ke jaringan on-premise. Untuk informasi selengkapnya tentang cara awalan yang diizinkan berinteraksi dengan gateway transit dan gateway pribadi virtual, lihat. Interaksi prefiks yang diizinkan

Topik

- Mengasosiasikan atau memisahkan AWS Direct Connect diri dengan gateway transit
- Buat antarmuka virtual transit ke AWS Direct Connect gateway
- Buat gateway transit dan proposal AWS Direct Connect asosiasi
- Menerima atau menolak gateway transit dan proposal AWS Direct Connect asosiasi
- Perbarui awalan yang diizinkan untuk gateway dan asosiasi transit AWS Direct Connect
- Hapus gateway transit dan proposal AWS Direct Connect asosiasi

Mengasosiasikan atau memisahkan AWS Direct Connect diri dengan gateway transit

Kaitkan atau pisahkan gateway transit menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Untuk mengaitkan transit gateway

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Gateway Direct Connect, lalu pilih gateway Direct Connect.
3. Pilih Lihat detail.
4. Pilih Keterkaitan gateway, lalu pilihKaitkan gateway.
5. Untuk Gateway, pilih transit gateway untuk dikaitkan.
6. Di Prefiks yang diizinkan, masukkan prefiks (dipisahkan dengan koma, atau pada baris baru) yang diiklankan gateway Direct Connect ke pusat data on-premise. Untuk informasi selengkapnya tentang awalan yang diizinkan, lihat. Interaksi prefiks yang diizinkan
7. Pilih Kaitkan gateway

Anda dapat melihat semua gateway yang terkait dengan gateway Direct Connect dengan memilih Keterkaitan gateway.

Untuk memisahkan transit gateway

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Gateway Direct Connect lalu pilih gateway Direct Connect.
3. Pilih Lihat detail.
4. Pilih Keterkaitan gateway lalu pilih transit gateway.
5. Pilih Pisahkan.

Untuk memperbarui awalan yang diizinkan untuk gateway transit

Anda dapat menambah atau menghapus awalan yang diizinkan ke gateway transit.

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih gateway Direct Connect dan kemudian pilih gateway Direct Connect yang ingin Anda tambahkan atau hapus awalan yang diizinkan.
3. Pilih tab Asosiasi Gateway.
4. Pilih gateway yang ingin Anda ubah awalan yang diizinkan, lalu pilih Edit.
5. Dalam awalan Diizinkan, masukkan awalan yang diiklankan oleh gateway Direct Connect ke pusat data lokal. Untuk beberapa awalan, pisahkan setiap awalan dengan koma atau letakkan setiap awalan pada baris baru. Awalan yang Anda tambahkan harus cocok dengan VPC Amazon CIDRs untuk semua gateway pribadi virtual. Untuk informasi selengkapnya tentang awalan yang diizinkan, lihat. Interaksi prefiks yang diizinkan
6. Pilih Edit asosiasi.

   Di bagian asosiasi Gateway, Negara menampilkan pemutakhiran. Ketika selesai, Negara berubah menjadi terkait. Ini mungkin memakan waktu beberapa menit atau lebih lama untuk menyelesaikannya.

Untuk mengaitkan transit gateway menggunakan baris perintah atau API

- create-direct-connect-gateway-asosiasi ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

Untuk melihat transit gateway yang terkait dengan gateway Direct Connect menggunakan baris perintah atau API

- describe-direct-connect-gateway-asosiasi ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

Untuk memisahkan transit gateway menggunakan baris perintah atau API

- delete-direct-connect-gateway-asosiasi ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

Untuk memperbarui awalan yang diizinkan untuk gateway transit menggunakan baris perintah atau API

- update-direct-connect-gateway-asosiasi ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Buat antarmuka virtual transit ke AWS Direct Connect gateway

Untuk menghubungkan AWS Direct Connect koneksi Anda ke gateway transit, Anda harus membuat antarmuka transit untuk koneksi Anda. Tentukan gateway Direct Connect yang akan dihubungkan. Anda dapat menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

> **Important**
>
> Jika Anda mengaitkan transit gateway dengan satu atau lebih gateway Direct Connect, Autonomous System Number (ASN) yang digunakan oleh transit gateway dan gateway Direct Connect harus berbeda. Sebagai contoh, jika Anda menggunakan ASN 64512 default untuk transit gateway dan gateway Direct Connect, permintaan pengaitan akan gagal.

Untuk menyediakan antarmuka virtual transit ke gateway Direct Connect

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Antarmuka Virtual.
3. Pilih Buat antarmuka virtual.

4. Di bawah Jenis antarmuka virtual, untuk Jenis, pilih Transit.
5. Di bawah Pengaturan antarmuka virtual transit, lakukan hal berikut:

   a. Untuk Nama antarmuka virtual, masukkan nama untuk antarmuka virtual.

   b. Untuk Koneksi, pilih koneksi Direct Connect yang ingin Anda gunakan untuk antarmuka ini.

   c. Untuk pemilik antarmuka Virtual, pilih AWS Akun saya jika antarmuka virtual untuk AWS akun Anda.

   d. Untuk Gateway Direct Connect, pilih gateway Direct Connect.

   e. Untuk VLAN, masukkan nomor ID untuk virtual local area network (VLAN).

   f. Untuk BGP ASN, masukkan Border Gateway Protocol Autonomous System Number dari router peer on-premise Anda untuk antarmuka virtual baru.

      Nilai yang valid adalah 1 hingga 2147483647.

6. Di bawah Pengaturan Tambahan, lakukan hal berikut:

   a. Untuk mengkonfigurasi IPv4 BGP atau IPv6 rekan, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer IPv4 BGP, pilih IPv4dan lakukan salah satu hal berikut:

      - Untuk menentukan alamat IP ini sendiri, untuk IP rekan router Anda, masukkan alamat IPv4 CIDR tujuan tempat Amazon harus mengirim lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat IPv4 CIDR yang akan digunakan untuk mengirim lalu lintas ke. AWS

      > **Important**
      >
      > Saat mengonfigurasi antarmuka virtual AWS Direct Connect, Anda dapat menentukan alamat IP Anda sendiri menggunakan RFC 1918, menggunakan skema pengalamatan lain, atau memilih alamat IPv4 /29 CIDR yang AWS ditetapkan yang dialokasikan dari rentang RFC 3927 169.254.0.0/16 Link-Local untuk konektivitas. IPv4 point-to-point point-to-pointKoneksi ini harus digunakan secara eksklusif untuk mengintip eBGP antara router gateway pelanggan Anda dan titik akhir Direct Connect. Untuk tujuan lalu lintas atau tunneling VPC, seperti AWS Site-to-Site Private IP VPN, atau Transit Gateway Connect, AWS merekomendasikan penggunaan antarmuka loopback atau LAN pada router gateway pelanggan Anda sebagai alamat sumber atau tujuan alih-alih koneksi. point-to-point

- Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
- Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat IPv4 Lokal-Tautan.

[IPv6] Untuk mengonfigurasi peer IPv6 BGP, pilih. IPv6 IPv6 Alamat peer secara otomatis ditetapkan dari kumpulan IPv6 alamat Amazon. Anda tidak dapat menentukan IPv6 alamat kustom.

b. Untuk mengubah maximum transmission unit (MTU) dari 1500 (default) menjadi 8500 (bingkai jumbo), pilih MTU Jumbo (MTU ukuran 8500).

c. (Opsional) Di bawah Aktifkan SiteLink, pilih Diaktifkan untuk mengaktifkan konektivitas langsung antara titik kehadiran Direct Connect.

d. (Opsional) Tambahkan atau hapus tag.

[Tambahkan tag] Pilih Tambah tag dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Menghapus tanda] Di samping tanda, pilih Hapus tanda.

7. Pilih Buat antarmuka virtual.

Setelah membuat antarmuka virtual, Anda dapat mengunduh konfigurasi router untuk perangkat Anda. Untuk informasi selengkapnya, lihat Mengunduh file konfigurasi router.

Untuk membuat antarmuka virtual transit menggunakan baris perintah atau API

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS Direct Connect API)

Untuk melihat antarmuka virtual yang dilampirkan ke gateway Direct Connect menggunakan baris perintah atau API

- describe-direct-connect-gateway-lampiran ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

Buat gateway transit dan proposal AWS Direct Connect asosiasi

Jika Anda memiliki transit gateway, Anda harus membuat proposal keterkaitan. Gateway transit harus dilampirkan ke VPC atau VPN di akun Anda AWS . Pemilik gateway Direct Connect harus berbagi ID gateway Direct Connect dan ID akun AWS -nya. Setelah membuat proposal, pemilik gateway Direct Connect harus menerimanya agar Anda dapat memperoleh akses ke jaringan on-premise melalui AWS Direct Connect. Anda dapat membuat proposal asosiasi menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Untuk membuat proposal keterkaitan

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Transit gateway lalu pilih transit gateway.
3. Pilih Lihat detail.
4. Pilih Keterkaitan gateway Direct Connect, kemudian pilih Kaitkan gateway Direct Connect.
5. Di bawah Tipe akun keterkaitan, untuk Pemilik akun, pilih Akun lain.
6. Untuk Pemilik gateway Direct Connect, masukkan ID akun yang memiliki gateway Direct Connect.
7. Di bawah Pengaturan keterkaitan Anda, lakukan hal berikut:
   a. Untuk ID gateway Direct Connect, masukkan ID gateway Direct Connect.
   b. Untuk Pemilik antarmuka virtual, masukkan ID akun yang memiliki antarmuka virtual untuk keterkaitan.
   c. (Opsional) Untuk menentukan daftar prefiks yang diizinkan dari transit gateway, tambahkan prefiks ke Prefiks yang diizinkan, memisahkannya menggunakan koma, atau memasukkannya ke baris terpisah.
8. Pilih Kaitkan gateway Gateway Direct Connect.

Untuk membuat proposal keterkaitan menggunakan baris perintah atau API

- create-direct-connect-gateway-asosiasi-proposal ()AWS CLI
- CreateDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Menerima atau menolak gateway transit dan proposal AWS Direct Connect asosiasi

Jika Anda memiliki gateway Direct Connect, Anda harus menerima proposal keterkaitan untuk membuat keterkaitan. Anda juga memiliki opsi untuk menolak proposal keterkaitan. Anda dapat menerima atau menolak proposal asosiasi menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Untuk menerima proposal keterkaitan

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Gateway Direct Connect.
3. Pilih gateway Direct Connect dengan proposal yang tertunda, lalu pilih Lihat detail.
4. Pada tab Proposal tertunda, pilih proposal, kemudian pilih Terima proposal.
5. ((Opsional) Untuk menentukan daftar prefiks yang diizinkan dari transit gateway, tambahkan prefiks ke Prefiks yang diizinkan, memisahkannya menggunakan koma, atau memasukkannya ke baris terpisah.
6. Pilih Terima proposal.

Untuk menolak proposal keterkaitan

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Gateway Direct Connect.
3. Pilih gateway Direct Connect dengan proposal yang tertunda, lalu pilih Lihat detail.
4. Pada tab Proposal tertunda, pilih transit gateway, kemudian pilih Tolak proposal.
5. Di kotak dialog Tolak proposal, masukkan Hapus, kemudian pilih Tolak proposal.

Untuk melihat proposal keterkaitan menggunakan baris perintah atau API

- describe-direct-connect-gateway-asosiasi-proposal ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals(AWS Direct Connect API)

Untuk menerima proposal keterkaitan menggunakan baris perintah atau API

- accept-direct-connect-gateway-asosiasi-proposal ()AWS CLI

- AcceptDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Untuk menolak proposal keterkaitan menggunakan baris perintah atau API

- delete-direct-connect-gateway-asosiasi-proposal ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Perbarui awalan yang diizinkan untuk gateway dan asosiasi transit AWS Direct Connect

Anda dapat memperbarui awalan yang diizinkan dari gateway transit melalui gateway Direct Connect menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API. Untuk memperbarui awalan yang diizinkan untuk gateway transit dan asosiasi Direct Connect menggunakan konsol, AWS Direct Connect

- Jika Anda pemilik gateway transit. Anda harus membuat proposal asosiasi baru untuk gateway Direct Connect tersebut, dengan menentukan awalan yang akan diizinkan. Untuk langkah-langkah membuat proposal asosiasi baru, lihatBuat proposal asosiasi gateway transit.
- Jika Anda pemilik gateway Direct Connect, Anda dapat memperbarui awalan yang diizinkan saat menerima proposal asosiasi, atau jika Anda memperbarui awalan yang diizinkan untuk asosiasi yang ada. Untuk langkah-langkah memperbarui awalan yang diizinkan saat Anda menerima asosiasi, lihat. Menerima atau menolak proposal asosiasi gateway transit

Untuk memperbarui prefiks yang diizinkan untuk keterkaitan yang ada menggunakan baris perintah atau API

- update-direct-connect-gateway-asosiasi ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Hapus gateway transit dan proposal AWS Direct Connect asosiasi

Pemilik transit gateway dapat menghapus proposal keterkaitan gateway Direct Connect jika masih menunggu penerimaan. Setelah proposal keterkaitan diterima, Anda tidak dapat menghapusnya, tetapi Anda dapat memisahkan transit gateway dari gateway Direct Connect. Untuk informasi selengkapnya, lihat Buat proposal asosiasi gateway transit.

Anda dapat menghapus gateway transit dan proposal asosiasi Direct Connect menggunakan AWS Direct Connect konsol atau menggunakan baris perintah atau API.

Untuk menghapus proposal keterkaitan

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Transit gateway lalu pilih transit gateway.
3. Pilih Lihat detail.
4. Pilih Keterkaitan gateway tertunda, pilih keterkaitan, kemudian pilih Hapus keterkaitan.
5. Di kotak dialog Hapus proposal keterkaitan, masukkan Hapus, kemudian pilih Hapus.

Untuk menghapus proposal keterkaitan tertunda menggunakan baris perintah atau API

- delete-direct-connect-gateway-asosiasi-proposal ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

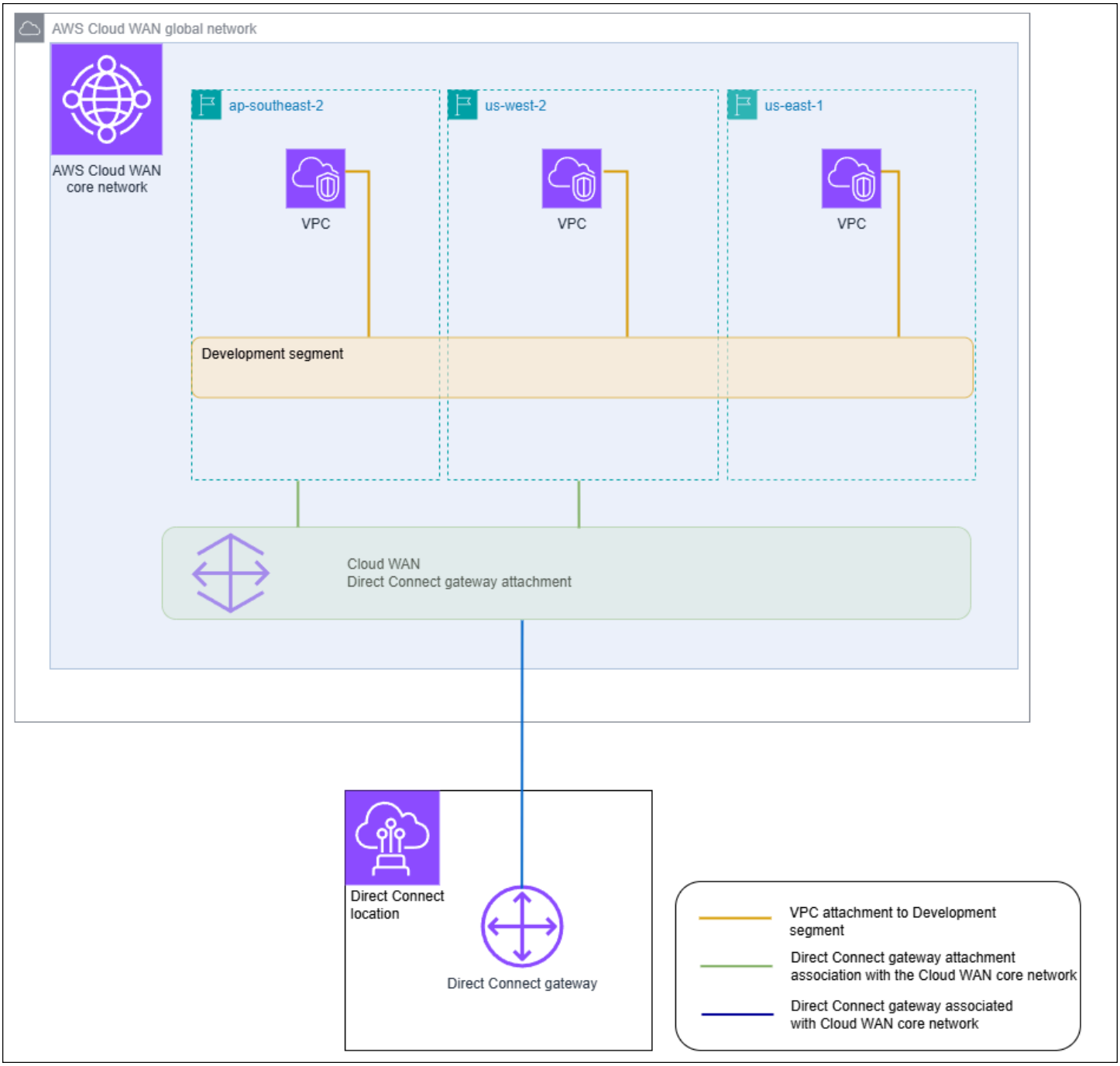
AWS Direct Connect gateway dan asosiasi jaringan inti AWS Cloud WAN

Kaitkan AWS Direct Connect gateway ke jaringan inti AWS Cloud WAN menggunakan jenis lampiran Direct Connect di Cloud WAN. Asosiasi langsung ini merutekan lalu lintas antara lokasi tepi yang dipilih jaringan inti Anda dan koneksi Direct Connect Anda menggunakan jalur terpendek yang tersedia

Jenis lampiran gateway Direct Connect mendukung BGP (protokol Border Gateway) untuk propagasi otomatis informasi perutean antara jaringan inti Anda dan lokasi lokal. Lampiran Direct Connect juga mendukung fitur Cloud WAN standar seperti manajemen berbasis kebijakan pusat, otomatisasi lampiran berbasis tag, dan segmentasi untuk konfigurasi keamanan tingkat lanjut.

> **Note**
>
> Hubungan antara jaringan inti dan gateway Direct Connect dibuat, dihapus, dan dikelola dari Cloud WAN Console di Network Manager. Saat menggunakan gateway Direct Connect dengan Cloud WAN, Konsol Direct Connect dan APIs dan CLI akan mencerminkan asosiasi, tetapi tidak dapat digunakan untuk memodifikasinya. Namun, Anda dapat menggunakan Direct Connect API atau baris perintah untuk memverifikasi apakah asosiasi telah dibuat.

Contoh berikut menunjukkan jaringan global Cloud WAN dengan tiga Wilayah dalam jaringan inti Cloud WAN. Setiap Wilayah memiliki VPC sendiri yang terhubung ke segmen Pengembangan jaringan inti yang dibagi di ketiga Wilayah tersebut. Menggunakan Cloud WAN, lampiran gateway Direct Connect dibuat dalam Cloud WAN menggunakan gateway Direct Connect, yang dibuat menggunakan Direct Connect. Lampiran dikaitkan dengan dua dari tiga Wilayah, ap-southeast-2 dan us-west-2 dan diizinkan akses ke segmen Pembangunan. Meskipun us-east-1 berbagi segmen Pengembangan yang sama, lampiran gateway Direct Connect tidak dibagikan dengan Wilayah tersebut dan oleh karena itu tidak tersedia.



Topik

- Prasyarat
- Pertimbangan
- Asosiasi gateway Direct Connect ke jaringan inti Cloud WAN
- Verifikasi asosiasi AWS Direct Connect gateway ke jaringan inti AWS Cloud WAN

Prasyarat

Sebuah asosiasi gateway Direct Connect dengan jaringan inti Cloud WAN memerlukan hal-hal berikut:

- Gateway Direct Connect yang ada. Untuk langkah-langkah membuat gateway Direct Connect, lihatBuat gateway Direct Connect.
- Jaringan inti AWS Cloud WAN. Untuk informasi tentang Cloud WAN, lihat Panduan Pengguna AWS Cloud WAN.

Pertimbangan

Batasan berikut berlaku untuk asosiasi gateway Direct Connect dengan jaringan inti Cloud WAN:

- Gateway Direct Connect dapat dikaitkan dengan jaringan inti Cloud WAN tunggal dan ke satu segmen jaringan inti tersebut. Setelah asosiasi dibuat, gateway tersebut tidak dapat dikaitkan dengan sumber daya lain di AWS wilayah. Jika Anda memisahkan gateway dari jaringan inti, Anda kemudian dapat menggunakan gateway itu untuk jenis asosiasi lainnya.
- Lampiran gateway Cloud WAN Direct Connect menggunakan jenis antarmuka virtual transit untuk konektivitas.
- Lampiran Cloud WAN tidak mendukung daftar awalan yang diizinkan. Semua awalan dalam segmen jaringan inti akan diiklankan ke gateway Direct Connect yang terkait dengan segmen tersebut.
- Kuota untuk awalan maksimum yang dapat diiklankan dari lokal ke AWS melalui antarmuka virtual transit berbeda dari kuota untuk awalan yang diiklankan dari jaringan inti WAN Cloud ke lokal. Kuota untuk sumber daya Direct Connect lainnya yang digunakan dengan asosiasi Cloud WAN juga berlaku. Lihat Kuota Direct Connect.
- Atribut AS-PATH BGP akan dipertahankan di seluruh jaringan inti, gateway Direct Connect, dan antarmuka virtual.
- ASN gateway Direct Connect harus berada di luar rentang ASN yang dikonfigurasi untuk jaringan inti Cloud WAN. Misalnya, jika Anda memiliki rentang ASN 64512 - 65534 untuk jaringan inti, ASN gateway Direct Connect harus menggunakan ASN di luar rentang itu.
- Cloud WAN mungkin tidak mendukung jenis lampiran tertentu menggunakan jenis lampiran Direct Connect untuk transportasi. Untuk informasi selengkapnya tentang lampiran gateway Direct Connect ke jaringan inti Cloud WAN, lihat lampiran gateway Direct Connect di AWS Cloud WAN di Panduan Pengguna AWS Cloud WAN.

- CloudWatch Network Monitor mendukung metrik latensi dan kehilangan paket saat digunakan dengan tipe lampiran gateway Cloud WAN Direct Connect. Fitur Indikator Kesehatan Jaringan tidak didukung. Untuk informasi selengkapnya, lihat Menggunakan Monitor Amazon CloudWatch Jaringan di Panduan Amazon CloudWatch Pengguna.

Asosiasi gateway Direct Connect ke jaringan inti Cloud WAN

Mengaitkan gateway Direct Connect ke jaringan inti AWS Cloud WAN dilakukan menggunakan konsol AWS Cloud WAN atau Cloud WAN APIs atau baris perintah.

Untuk mengaitkan gateway Direct connect yang ada ke jaringan inti Cloud WAN, buat lampiran Direct Connect baru di Cloud WAN Console. Setelah lampiran Direct Connect dibuat, asosiasi dibuat. Secara default, saat membuat asosiasi Anda dapat memilih default untuk menyertakan semua lokasi tepi jaringan inti di segmen jaringan inti yang dipilih. Atau, Anda dapat menentukan lokasi tepi individu.

Untuk informasi selengkapnya tentang lampiran gateway Direct Connect ke jaringan inti Cloud WAN, lihat lampiran gateway Direct Connect di AWS Cloud WAN di Panduan Pengguna AWS Cloud WAN.

Verifikasi asosiasi AWS Direct Connect gateway ke jaringan inti AWS Cloud WAN

Anda dapat memverifikasi asosiasi gateway Direct Connect ke jaringan inti Cloud WAN menggunakan konsol Direct Connect atau Direct Connect API atau baris perintah.

Untuk memverifikasi asosiasi gateway Direct Connect ke jaringan inti Cloud WAN menggunakan konsol

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Pilih gateway Direct Connect di panel navigasi.
3. Pilih lampiran gateway Direct Connect yang ingin Anda lihat asosiasi.
4. Pilih tab Asosiasi Gateway.
    - Kolom ID menampilkan ID jaringan inti yang terkait dengan gateway Direct Connect.
    - Kolom State menampilkan terkait.
    - Kolom tipe Asosiasi menampilkan Cloud WAN Core Network.

Untuk memverifikasi asosiasi gateway Direct Connect ke jaringan inti Cloud WAN menggunakan baris perintah atau API

- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)
- describe-direct-connect-gateway-asosiasi ()AWS CLI

Interaksi awalan yang diizinkan untuk gateway AWS Direct Connect

Pelajari bagaimana prefiks yang diizinkan berinteraksi dengan transit gateway dan virtual private gateway. Untuk informasi selengkapnya, lihat Kebijakan Perutean dan Komunitas BGP.

Keterkaitan virtual private gateway

Daftar awalan (IPv4 dan IPv6) bertindak sebagai filter yang memungkinkan hal yang sama CIDRs, atau rentang yang lebih kecil CIDRs untuk diiklankan ke gateway Direct Connect. Anda harus menetapkan prefiks untuk rentang yang sama atau lebih lebar dari blok CIDR VPC.

> **Note**
>
> Daftar yang diizinkan hanya berfungsi sebagai filter, dan hanya CIDR VPC terkait yang akan diiklankan ke gateway pelanggan.

Pertimbangkan skenario saat Anda memiliki VPC dengan CIDR 10.0.0.0/16 terlampir ke virtual private gateway.

- Saat daftar prefiks yang diizinkan diatur ke 22.0.0.0/24, Anda tidak menerima rute apa pun karena 22.0.0.0/24 tidak sama dengan, atau lebih lebar dari 10.0.0.0/16.
- Saat daftar prefiks yang diizinkan diatur ke 10.0.0.0/24, Anda tidak menerima rute apa pun karena 10.0.0.0/24 tidak sama dengan 10.0.0.0/16.
- Saat daftar prefiks yang diizinkan diatur ke 10.0.0.0/15, Anda menerima 10.0.0.0/16, karena alamat IP lebih lebar dari 10.0.0.0/16.

Saat Anda menghapus atau menambahkan awalan yang diizinkan, lalu lintas yang tidak menggunakan awalan itu tidak terpengaruh. Selama pembaruan status berubah dari `associated` keu`pdating`. Memodifikasi awalan yang ada dapat menunda atau menjatuhkan hanya lalu lintas yang menggunakan awalan itu.

Keterkaitan transit gateway

Untuk keterkaitan transit gateway, Anda menyediakan daftar prefiks yang diizinkan di gateway Direct Connect. Daftar ini merutekan lalu lintas lokal ke atau dari gateway Direct Connect ke gateway transit, bahkan saat yang VPCs dilampirkan ke gateway transit belum ditetapkan CIDRs. Awalan yang diizinkan bekerja secara berbeda, tergantung pada jenis gateway:

- Untuk asosiasi gateway transit, hanya awalan yang diizinkan yang dimasukkan yang akan diiklankan ke lokal. Ini akan ditampilkan sebagai berasal dari gateway Direct Connect ASN.
- Untuk gateway pribadi virtual, awalan yang diizinkan dimasukkan bertindak sebagai filter untuk memungkinkan yang sama atau lebih kecil. CIDRs

Pertimbangkan skenario saat Anda memiliki VPC dengan CIDR 10.0.0.0/16 yang terlampir pada transit gateway.

- Saat daftar prefiks yang diizinkan diatur ke 22.0.0.0/24, Anda menerima 22.0.0.0/24 melalui BGP pada antarmuka virtual transit Anda. Anda tidak menerima 10.0.0.0/16 karena kami secara langsung menyediakan prefiks yang ada di daftar prefiks yang diiziinkan.
- Jika daftar prefiks yang diizinkan diatur ke 10.0.0.0/24, Anda menerima 10.0.0.0/24 melalui BGP antarmuka virtual transit Anda. Anda tidak menerima 10.0.0.0/16 karena kami secara langsung menyediakan prefiks yang ada di daftar prefiks yang diizinkan.
- Saat daftar prefiks yang diizinkan diatur ke 10.0.0.0/8, Anda menerima 10.0.0.0/8 melalui BGP pada antarmuka virtual transit Anda.

Tumpang tindih awalan yang diizinkan tidak diperbolehkan ketika beberapa gateway transit dikaitkan dengan gateway Direct Connect. Misalnya, jika Anda memiliki gateway transit dengan daftar awalan yang diizinkan yang mencakup 10.1.0.0/16, dan gateway transit kedua dengan daftar awalan yang diizinkan yang mencakup 10.2.0.0/16 dan 0.0.0.0/0, Anda tidak dapat mengatur asosiasi dari gateway transit kedua ke 0.0.0.0/0. Karena 0.0.0.0/0 menyertakan semua IPv4 jaringan, Anda tidak dapat mengonfigurasi 0.0.0.0/0 jika beberapa gateway transit dikaitkan dengan gateway Direct Connect. Kesalahan ditampilkan yang menunjukkan bahwa rute yang diizinkan tumpang tindih dengan satu atau beberapa rute yang diizinkan yang ada di gateway Direct Connect.

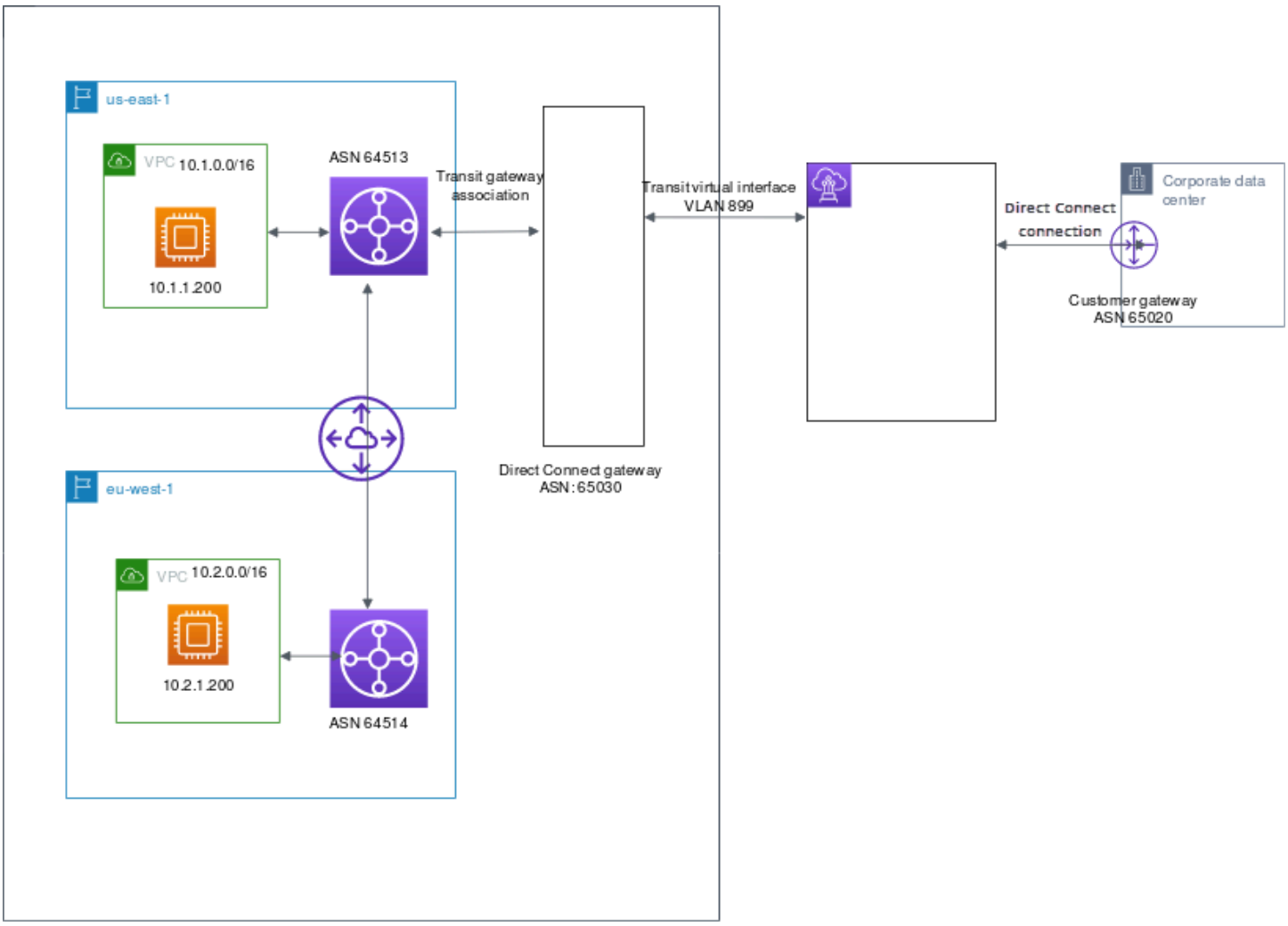
Saat Anda menghapus atau menambahkan awalan yang diizinkan, lalu lintas yang tidak menggunakan awalan itu tidak terpengaruh. Selama pembaruan status berubah dari `associated`

keupdating. Memodifikasi awalan yang ada dapat menunda atau menjatuhkan hanya lalu lintas yang menggunakan awalan itu.

Contoh: Diizinkan untuk prefiks dalam konfigurasi transit gateway

Pertimbangkan konfigurasi di mana Anda memiliki instance di dua AWS Wilayah berbeda yang perlu mengakses pusat data perusahaan. Anda dapat menggunakan sumber daya berikut untuk konfigurasi ini:

- Transit gateway di setiap Wilayah.
- Sebuah koneksi peering transit gateway.
- Sebuah gateway Direct Connect.
- Sebuah keterkaitan transit gateway antara salah satu transit gateway (yang ada di us-east-1) ke gateway Direct Connect.
- Antarmuka virtual transit dari lokasi on-premise dan lokasi AWS Direct Connect .



Konfigurasikan opsi berikut untuk sumber daya.

- Gateway Direct Connect: Atur ASN ke 65030. Untuk informasi selengkapnya, lihat Buat gateway Direct Connect.
- Transit antarmuka virtual: Atur VLAN ke 899, dan ASN ke 65020. Untuk informasi selengkapnya, lihat Membuat antarmuka virtual transit ke gateway Direct Connect.
- Keterkaitan gateway Direct Connect dengan transit gateway: Atur prefiks yang diizinkan ke 10.0.0.0/8.

  Blok CIDR ini mencakup kedua blok CIDR VPC. Untuk informasi selengkapnya, lihat Kaitkan atau pisahkan gateway transit dengan Direct Connect..
- Rute VPC: Untuk merutekan lalu lintas dari 10.2.0.0 VPC, buat rute dalam tabel rute VPC yang memiliki Tujuan 0.0.0.0/0 dan ID transit gateway sebagai Target. Untuk informasi selengkapnya

tentang perutean ke transit gateway, lihat Perutean untuk transit gateway di Panduan Pengguna Amazon VPC.

AWS Direct Connect Sumber daya tag

Tag adalah label yang diberikan pemilik sumber daya ke sumber AWS Direct Connect daya mereka. Setiap tag terdiri dari kunci dan nilai opsional, yang keduanya Anda tentukan. Tag memungkinkan pemilik sumber daya untuk mengkategorikan AWS Direct Connect sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, atau lingkungan. Hal ini berguna ketika Anda memiliki banyak sumber daya dengan jenis yang sama—Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tanda yang telah Anda tetapkan.

Misalnya, Anda memiliki dua AWS Direct Connect koneksi di Wilayah, masing-masing di lokasi yang berbeda. Koneksi `dxcon-11aa22bb` adalah koneksi melayani lalu lintas produksi, dan berhubungan dengan antarmuka virtual `dxvif-33cc44dd`. Koneksi `dxcon-abcabcab` adalah koneksi berlebihan (cadangan), dan berhubungan dengan antarmuka virtual `dxvif-12312312`. Anda dapat memilih untuk menandai koneksi dan antarmuka virtual sebagai berikut, untuk membantu membedakannya:

ID Sumber Daya	Kunci tanda	Nilai tanda
`dxcon-11aa22bb`	Tujuan umum	Produksi
	Lokasi	Amsterdam
`dxvif-33cc44dd`	Tujuan umum	Produksi
`dxcon-abcabcab`	Tujuan umum	Cadangan
	Lokasi	Frankfurt
`dxvif-12312312`	Tujuan umum	Cadangan

Kami menyarankan agar Anda merancang serangkaian kunci tanda yang memenuhi kebutuhan Anda untuk setiap jenis sumber daya. Penggunaan set kunci tag yang konsisten akan memudahkan manajemen sumber daya Anda. Tag tidak memiliki arti semantik AWS Direct Connect dan ditafsirkan secara ketat sebagai serangkaian karakter. Selain itu, tag tidak secara otomatis ditetapkan ke sumber daya Anda. Anda dapat mengedit kunci dan nilai tanda, dan dapat menghapus tanda dari sumber daya kapan saja. Anda dapat mengatur nilai tanda ke string kosong, tetapi tidak dapat mengatur nilai tanda ke null. Jika Anda menambahkan tanda yang memiliki kunci yang sama dengan tanda yang

telah ada pada sumber daya tersebut, nilai yang baru akan menimpa nilai yang lama. Jika sumber daya dihapus, semua tanda untuk sumber daya tersebut juga akan dihapus.

Anda dapat menandai AWS Direct Connect sumber daya berikut menggunakan AWS Direct Connect konsol, AWS Direct Connect API AWS CLI, AWS Tools for Windows PowerShell, atau AWS SDK. Ketika Anda menggunakan alat ini untuk mengelola tanda, Anda harus menentukan Amazon Resource Name (ARN) untuk sumber daya. Untuk informasi selengkapnya ARNs, lihat Amazon Resource Names (ARNs) di Referensi Umum Amazon Web.

Sumber daya	Dukungan tanda	Dukungan tanda saat penciptaan	Mendukung tanda yang mengendalikan akses dan alokasi sumber daya	Mendukung alokasi biaya
Koneksi	Ya	Ya	Ya	Ya
Antarmuka virtual	Ya	Ya	Ya	Tidak
Kelompok agregasi tautan (LAG)	Ya	Ya	Ya	Ya
Antarkoneksi	Ya	Ya	Ya	Ya
Gateway Direct Connect	Ya	Ya	Ya	Tidak

Batasan tanda

Batasan dan aturan berikut berlaku untuk tanda:

- Jumlah maksimum tanda per sumber daya: 50
- Panjang kunci maksimum: 128 karakter Unicode
- Panjang nilai maksimum: 256 karakter Unicode

- Kunci dan nilai tag peka huruf besar dan kecil.
- `aws:`Awalan dicadangkan untuk AWS digunakan. Anda tidak dapat mengedit atau menghapus kunci atau nilai tanda jika tanda memiliki kunci tanda dengan `aws:` prefiks. Tanda dengan kunci tanda dengan prefiks `aws:` tidak dihitung terhadap tanda Anda per batas sumber daya.
- Karakter yang diperbolehkan adalah: huruf, spasi, dan angka yang dapat mewakili dalam UTF-8, serta karakter berikut: + - = . _ : / @
- Hanya pemilik sumber daya yang dapat menambahkan atau menghapus tanda. Misalnya, jika ada koneksi yang di-host, partner tidak akan dapat menambahkan, menghapus, atau melihat tanda.
- Tag alokasi biaya hanya didukung untuk koneksi, interkoneksi, dan. LAGs Untuk informasi tentang cara menggunakan tag dengan manajemen biaya, lihat Menggunakan Tag Alokasi Biaya di Panduan AWS Manajemen Penagihan dan Biaya Pengguna.

Bekerja dengan tanda menggunakan CLI atau API

Gunakan yang berikut ini untuk menambahkan, memperbarui, membuat daftar, dan menghapus tanda untuk sumber daya Anda.

Tugas	API	CLI
Tambahkan atau timpa satu atau beberapa tanda.	TagResource	tag-sumber daya
Hapus satu atau beberapa tanda.	UntagResource	untag-sumber daya
Penjelasan satu tanda atau lebih	DescribeTags	describe-tags

Contoh

Menggunakan perintah tag-resource untuk menandai `dxcon-11aa22bb` Koneksi.

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

Menggunakan perintah describe-tags untuk menjelaskan tanda `dxcon-11aa22bb` Koneksi.

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb
```

Gunakan perintah untag-resource untuk menghapus tanda dari Koneksi `dxcon-11aa22bb`.

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

Keamanan di AWS Direct Connect

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

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku AWS Direct Connect, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

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

Topik

Perlindungan data di AWS Direct Connect

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Direct Connect. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS Direct Connect atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log

penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Untuk informasi selengkapnya tentang perlindungan data, lihat postingan blog AWS postingan blog Model Tanggung Jawab Bersama dan Peraturan Perlindungan Data Umum (GDPR) di AWS Blog Keamanan.

Topik

- Privasi lalu lintas inter-jaringan di AWS Direct Connect
- Enkripsi dalam AWS Direct Connect

Privasi lalu lintas inter-jaringan di AWS Direct Connect

Lalu lintas antara layanan dan aplikasi serta klien on-premise

Anda memiliki dua opsi konektivitas antara jaringan pribadi Anda dan AWS:

- Keterkaitan ke AWS Site-to-Site VPN. Untuk informasi selengkapnya, lihat Keamanan infrastruktur.
- Sebuah asosiasi untuk VPCs. Untuk informasi selengkapnya, silakan lihat Keterkaitan virtual private gateway dan Keterkaitan transit gateway.

Lalu lintas antar AWS sumber daya di Wilayah yang sama

Anda memiliki dua opsi konektivitas:

- Keterkaitan ke AWS Site-to-Site VPN. Untuk informasi selengkapnya, lihat Keamanan infrastruktur.
- Sebuah asosiasi untuk VPCs. Untuk informasi selengkapnya, silakan lihat Keterkaitan virtual private gateway dan Keterkaitan transit gateway.

Enkripsi dalam AWS Direct Connect

AWS Direct Connect tidak mengenkripsi lalu lintas Anda yang sedang transit secara default. Untuk mengenkripsi data dalam perjalanan yang melintasi AWS Direct Connect, Anda harus menggunakan opsi enkripsi transit untuk layanan tersebut. Untuk mempelajari enkripsi lalu lintas EC2 instance, lihat Enkripsi dalam Transit di Panduan EC2 Pengguna Amazon.

Dengan AWS Direct Connect dan AWS Site-to-Site VPN, Anda dapat menggabungkan satu atau lebih koneksi jaringan AWS Direct Connect khusus dengan Amazon VPC VPN. Kombinasi ini menyediakan koneksi pribadi IPsec terenkripsi yang juga mengurangi biaya jaringan, meningkatkan throughput bandwidth, dan memberikan pengalaman jaringan yang lebih konsisten daripada koneksi VPN berbasis internet. Untuk informasi selengkapnya, lihat Opsi Konektivitas Amazon VPC-to-Amazon VPC.

MAC Security (MACsec) adalah standar IEEE yang menyediakan kerahasiaan data, integritas data, dan keaslian asal data. Anda dapat menggunakan AWS Direct Connect koneksi yang mendukung MACsec untuk mengenkripsi data Anda dari pusat data perusahaan Anda ke AWS Direct Connect lokasi. Untuk informasi selengkapnya, lihat Keamanan MAC (MACsec).

Identity and Access Management untuk Direct Connect

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

Topik

Audiens

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

Pengguna layanan – Jika Anda menggunakan layanan Direct Connect untuk melakukan tugas, administrator Anda akan memberikan kredensial dan izin yang dibutuhkan. Saat Anda menggunakan

lebih banyak fitur Direct Connect untuk melakukan pekerjaan, Anda mungkin memerlukan izin tambahan. Memahami bagaimana cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Direct Connect, lihat Pemecahan masalah akses dan identitas Direct Connect.

Administrator layanan – Jika Anda bertanggung jawab atas sumber daya Direct Connect di perusahaan, Anda mungkin memiliki akses penuh ke Direct Connect. Tugas Anda adalah menentukan fitur dan sumber daya Direct Connect mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari selengkapnya tentang cara perusahaan Anda dapat menggunakan IAM dengan Direct Connect, lihat Cara Direct Connect berfungsi dengan IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih terperinci tentang cara Anda dapat menulis kebijakan untuk mengelola akses ke Direct Connect. Untuk melihat contoh kebijakan berbasis identitas Direct Connect yang dapat Anda gunakan di IAM, lihat Contoh kebijakan berbasis identitas untuk Direct Connect.

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 pengguna IAM, atau dengan mengasumsikan peran IAM.

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

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

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang

penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

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

Akun AWS pengguna root

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

Identitas gabungan

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

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan 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 Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

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

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

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

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

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Buat peran untuk penyedia identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas

tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .

- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM dalam 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 pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI

atau AWS permintaan API. 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 peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. 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 di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

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

Kebijakan berbasis identitas

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

lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

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

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip 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 selengkapnya ACLs, lihat Ringkasan 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.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda

dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCPs) — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi 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 dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, 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 eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

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

Cara Direct Connect berfungsi dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Direct Connect, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Direct Connect.

Fitur IAM yang dapat Anda gunakan dengan Direct Connect

Fitur IAM	Dukungan Direct Connect
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Ya
Peran terkait layanan	Tidak

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

Kebijakan berbasis identitas untuk Direct Connect

Mendukung kebijakan berbasis identitas: Ya

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

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

Contoh kebijakan berbasis identitas untuk Direct Connect

Untuk melihat contoh kebijakan berbasis identitas Direct Connect, lihat Contoh kebijakan berbasis identitas untuk Direct Connect.

Kebijakan berbasis sumber daya dalam Direct Connect

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun

yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk Direct Connect

Mendukung tindakan kebijakan: Ya

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

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

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

Untuk melihat daftar tindakan Direct Connect, lihat Tindakan yang Ditentukan oleh Direct Connect di Referensi Otorisasi Layanan.

Tindakan kebijakan di Direct Connect menggunakan awalan berikut sebelum tindakan:

```
Direct Connect
```

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

```
"Action": [
      "directconnect:action1",
      "directconnectaction2"
         ]
```

Sumber daya kebijakan untuk Direct Connect

Mendukung sumber daya kebijakan: Ya

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

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis sumber daya Direct Connect dan jenis resource ARNs, lihat Resources Defined by Direct Connect di Referensi AWS Direct Connect API. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh Direct Connect.

Untuk melihat contoh kebijakan berbasis identitas Direct Connect, lihat Contoh kebijakan berbasis identitas untuk Direct Connect.

Untuk melihat contoh kebijakan berbasis sumber daya Direct Connect, lihat Contoh kebijakan berbasis identitas Direct Connect menggunakan kondisi berbasis tag.

Kunci kondisi kebijakan untuk Direct Connect

Mendukung kunci kondisi kebijakan khusus layanan: Yes

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

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

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

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

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

Untuk melihat daftar kunci kondisi Direct Connect, lihat Condition Keys for Direct Connect di Referensi AWS Direct Connect API. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk Direct Connect di Referensi Otorisasi Layanan.

Untuk melihat contoh kebijakan berbasis identitas Direct Connect, lihat Contoh kebijakan berbasis identitas untuk Direct Connect.

ACLs di Direct Connect

Mendukung ACLs: Tidak

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

ABAC dengan Direct Connect

Mendukung ABAC (tag dalam kebijakan): Sebagian

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

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

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

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

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensial sementara dengan Direct Connect

Mendukung kredensial sementara: Ya

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

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

Anda dapat membuat kredenal sementara secara manual menggunakan API AWS CLI atau AWS . 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 Kredensial keamanan sementara di IAM.

Izin utama lintas layanan untuk Direct Connect

Mendukung sesi akses maju (FAS): Ya

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

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

Peran layanan untuk Direct Connect

Mendukung peran layanan: Ya

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

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

Peran terkait layanan untuk Direct Connect

Mendukung peran terkait layanan: Tidak

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

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Direct Connect

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

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

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Direct Connect, termasuk format ARNs untuk setiap jenis sumber daya, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk Direct Connect di Referensi Otorisasi Layanan.

Topik

Praktik terbaik kebijakan

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

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

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

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

Tindakan, sumber daya, dan kondisi Direct Connect

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Direct Connect mendukung tindakan, sumber daya, dan kunci ketentuan tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi Elemen Kebijakan IAM JSON dalam Panduan Pengguna IAM.

Tindakan

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

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

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

Tindakan kebijakan di Direct Connect menggunakan prefiks berikut sebelum tindakan: `directconnect:`. Misalnya, untuk memberikan izin kepada seseorang untuk menjalankan EC2 instance Amazon dengan operasi Amazon EC2 `DescribeVpnGateways` API, Anda menyertakan `ec2:DescribeVpnGateways` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Direct Connect menentukan serangkaian tindakannya sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

Contoh kebijakan berikut memberikan akses baca ke AWS Direct Connect.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh kebijakan berikut memberikan akses penuh ke AWS Direct Connect.

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

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

Untuk melihat daftar tindakan Direct Connect, lihat Tindakan yang Ditentukan oleh Direct Connect di Panduan Pengguna IAM.

Sumber daya

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

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Direct Connect menggunakan yang berikut ini ARNs:

Sumber daya koneksi langsung ARNs

Jenis Sumber Daya	ARN
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`

Jenis Sumber Daya	ARN
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`

Untuk informasi selengkapnya tentang format ARNs, lihat Amazon Resource Names (ARNs) dan Ruang Nama AWS Layanan.

Misalnya, untuk menentukan antarmuka `dxcon-11aa22bb` dalam pernyataan Anda, gunakan ARN berikut:

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

Untuk menentukan semua antarmuka virtual milik akun tertentu, gunakan wildcard (*):

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

Beberapa tindakan Direct Connect, seperti yang digunakan untuk membuat sumber daya, tidak dapat dilakukan pada sumber daya tertentu. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

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

Untuk melihat daftar jenis sumber daya Direct Connect dan jenisnya ARNs, lihat Jenis Sumber Daya yang Ditentukan oleh AWS Direct Connect dalam Panduan Pengguna IAM. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh Direct Connect.

Jika ARN sumber daya atau pola ARN sumber daya selain * ditentukan di `Resource` bidang pernyataan kebijakan IAM untuk DescribeConnections,,,, atau DescribeVirtualInterfaces DescribeDirectConnectGateways DescribeInterconnects DescribeLags, maka yang ditentukan tidak `Effect` akan terjadi kecuali ID sumber daya yang cocok juga diteruskan dalam panggilan API. Namun, jika Anda memberikan * sebagai sumber daya alih-alih ID sumber daya tertentu dalam pernyataan kebijakan IAM, yang ditentukan `Effect` akan berfungsi.

Dalam contoh berikut, tidak ada yang ditentukan `Effect` akan berhasil jika `DescribeConnections` tindakan dipanggil tanpa `connectionId` diteruskan dalam permintaan.

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/*"
        ]
    },
{
        "Effect": "Deny",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/example1"
        ]
    }
]
```

Namun, dalam contoh berikut, `"Effect": "Allow"` akan berhasil untuk `DescribeConnections` tindakan `*` karena disediakan untuk `Resource` bidang pernyataan kebijakan IAM, terlepas dari `connectionId` apakah ditentukan dalam permintaan.

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

Kunci syarat

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

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

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

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

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

Direct Connect menentukan set kunci ketentuannya sendiri dan juga mendukung penggunaan beberapa kunci ketentuan global. Untuk melihat semua kunci kondisi AWS global, lihat Kunci Konteks Kondisi AWS Global di Panduan Pengguna IAM.

Anda dapat menggunakan kunci ketentuan dengan sumber daya tanda. Untuk informasi selengkapnya, lihat Contoh: Membatasi Akses ke Wilayah Tertentu.

Untuk melihat daftar tombol kondisi Direct Connect, lihat Condition Keys untuk Direct Connect di Panduan Pengguna IAM. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang Ditentukan oleh Direct Connect.

Menggunakan konsol Direct Connect

Untuk mengakses konsol Direct Connect, Anda harus memiliki rangkaian izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Direct Connect di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin

minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana dimaksud untuk entitas (s atau peran) dengan kebijakan tersebut.

Untuk memastikan bahwa entitas tersebut masih dapat menggunakan konsol Direct Connect, lampirkan juga kebijakan AWS terkelola berikut ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke Pengguna dalam Panduan Pengguna IAM:

```
directconnect
```

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai alternatif, hanya izinkan akses ke tindakan yang cocok dengan operasi API yang sedang Anda coba lakukan.

Izinkan para pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
```

```
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Akses hanya-baca ke AWS Direct Connect

Contoh kebijakan berikut memberikan akses baca ke AWS Direct Connect.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Akses penuh ke AWS Direct Connect

Contoh kebijakan berikut memberikan akses penuh ke AWS Direct Connect.

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

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

Contoh kebijakan berbasis identitas Direct Connect menggunakan kondisi berbasis tag

Anda dapat mengontrol akses ke sumber daya dan permintaan menggunakan ketentuan kunci tanda. Anda juga dapat menggunakan ketentuan dalam kebijakan IAM Anda untuk mengontrol apakah kunci tanda tertentu dapat digunakan pada sumber daya atau dalam permintaan.

Untuk informasi tentang cara menggunakan tag dengan kebijakan IAM, lihat Mengontrol Akses Menggunakan Tag di Panduan Pengguna IAM.

Mengaitkan antarmuka virtual Direct Connect berdasarkan tanda

Contoh berikut menunjukkan cara membuat kebijakan yang membantu menghubungkan antarmuka virtual saja jika tanda berisi kunci lingkungan dan nilai praproduksi atau produksi.

```
 {
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "directconnect:AssociateVirtualInterface"
    ],
    "Resource": "arn:aws:directconnect:*:*:dxvif/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/environment": [
          "preprod",
          "production"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "directconnect:DescribeVirtualInterfaces",
    "Resource": "*"
  }
```

```
    ]
}
```

Mengontrol akses ke permintaan berdasarkan tanda

Anda dapat menggunakan kondisi dalam kebijakan IAM untuk mengontrol pasangan nilai kunci tag mana yang dapat diteruskan dalam permintaan yang menandai sumber daya. AWS Contoh berikut menunjukkan cara membuat kebijakan yang memungkinkan penggunaan AWS Direct Connect TagResource tindakan untuk melampirkan tag ke antarmuka virtual hanya jika tag berisi kunci lingkungan dan nilai preprod atau produksi. Sebagai praktik terbaik, gunakan pengubah `ForAllValues` dengan kunci ketentuan `aws:TagKeys` untuk menunjukkan bahwa hanya lingkungan kunci yang diperbolehkan dalam permintaan.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "directconnect:TagResource",
        "Resource": "arn:aws:directconnect:*:*:dxvif/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/environment": [
                    "preprod",
                    "production"
                ]
            },
            "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
        }
    }
}
```

Mengontrol kunci tanda

Anda dapat menggunakan ketentuan dalam kebijakan IAM Anda untuk mengontrol apakah kunci tanda tertentu dapat digunakan pada sumber daya atau dalam permintaan.

Contoh berikut menunjukkan cara membuat kebijakan yang memungkinkan Anda menandai sumber daya, namun hanya dengan lingkungan kunci tanda

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

```
    "Statement": {
      "Effect": "Allow",
      "Action": "directconnect:TagResource",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "environment"
          ]
        }
      }
    }
}
```

Peran terkait layanan untuk AWS Direct Connect

AWS Direct Connect menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS Direct Connect Peran terkait layanan telah ditentukan sebelumnya oleh AWS Direct Connect dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AWS Direct Connect lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS Direct Connect mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS Direct Connect dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi AWS Direct Connect sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk AWS Direct Connect

AWS Direct Connect menggunakan peran terkait layanan bernama. `AWSServiceRoleForDirectConnect` Ini memungkinkan AWS Direct Connect untuk mengambil MACSec rahasia yang disimpan atas nama Anda. AWS Secrets Manager

`AWSServiceRoleForDirectConnect` peran terkait layanan memercayakan layanan berikut untuk menjalankan peran tersebut:

- `directconnect.amazonaws.com`

`AWSServiceRoleForDirectConnect`Peran terkait layanan menggunakan kebijakan terkelola. `AWSDirectConnectServiceRolePolicy`

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Agar peran `AWSServiceRoleForDirectConnect` terkait layanan berhasil dibuat, identitas IAM yang Anda gunakan harus memiliki AWS Direct Connect izin yang diperlukan. Untuk memberikan izin yang diperlukan, lampirkan kebijakan berikut untuk identitas IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "directconnect.amazonaws.com"
                }
            },
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:GetRole",
            "Effect": "Allow",
            "Resource": "*"
       }
    ]
}
```

Untuk informasi lebih lanjut, lihat Izin Peran Terkait Layanan dalam Panduan Pengguna IAM.

Membuat peran terkait layanan untuk AWS Direct Connect

Anda tidak perlu membuat peran terkait layanan secara manual. AWS Direct Connect menciptakan peran terkait layanan untuk Anda. Saat Anda menjalankan `associate-mac-sec-key` perintah,

AWS buat peran terkait layanan yang memungkinkan AWS Direct Connect untuk mengambil MACsec rahasia yang disimpan atas nama Anda AWS Secrets Manager di, API AWS Management Console AWS CLI, atau API. AWS

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Untuk mempelajari lebih lanjut, lihat Peran Baru yang Muncul di Akun IAM Saya.

Jika Anda menghapus peran terkait layanan ini, dan kemudian perlu membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran di akun Anda. AWS Direct Connect menciptakan peran terkait layanan untuk Anda lagi.

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaan Direct AWS Connect. Di AWS CLI atau AWS API, buat peran terkait layanan dengan nama `directconnect.amazonaws.com` layanan. Untuk informasi selengkapnya, lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit peran terkait layanan untuk AWS Direct Connect

AWS Direct Connect tidak memungkinkan Anda untuk mengedit peran `AWSServiceRoleForDirectConnect` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran tertaut layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk AWS Direct Connect

Anda tidak perlu menghapus peran `AWSServiceRoleForDirectConnect` secara manual. Saat menghapus peran terkait layanan, Anda harus menghapus semua sumber daya terkait yang disimpan dalam layanan AWS Secrets Manager web. The AWS Management Console, the AWS CLI, atau AWS API, AWS Direct Connect membersihkan sumber daya dan menghapus peran terkait layanan untuk Anda.

Anda juga dapat menggunakan konsol IAM untuk menghapus peran terkait layanan. Untuk melakukan ini, Anda harus terlebih dahulu membersihkan sumber daya secara manual untuk peran terkait layanan Anda dan kemudian Anda dapat menghapusnya.

> **Note**
>
> Jika AWS Direct Connect layanan menggunakan peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika ini terjadi, tunggu beberapa menit, lalu coba operasi lagi.

Untuk menghapus AWS Direct Connect sumber daya yang digunakan oleh **`AWSServiceRoleForDirectConnect`**

1. Hapus hubungan antara semua MACsec kunci dan koneksi. Untuk informasi selengkapnya, silakan lihat the section called “Hapus hubungan antara kunci MACsec rahasia dan koneksi”
2. Hapus hubungan antara semua MACsec kunci dan LAGs. Untuk informasi selengkapnya, silakan lihat the section called “Hapus hubungan antara kunci MACsec rahasia dan LAG”

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

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

Wilayah yang didukung untuk AWS Direct Connect peran terkait layanan

AWS Direct Connect mendukung penggunaan peran terkait layanan di semua Wilayah AWS tempat fitur Keamanan MAC tersedia. Untuk informasi selengkapnya, lihat AWS Direct Connect Lokasi.

AWS kebijakan terkelola untuk AWS Direct Connect

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 operasi API baru tersedia untuk layanan yang ada.

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

AWS kebijakan terkelola: AWSDirect ConnectFullAccess

Anda dapat melampirkan kebijakan `AWSDirectConnectFullAccess` ke identitas IAM Anda. Kebijakan ini memberikan izin yang memungkinkan akses penuh ke. AWS Direct Connect

Untuk menampilkan izin untuk kebijakan ini, lihat AWSDirectConnectFullAccess di AWS Management Console.

AWS kebijakan terkelola: AWSDirect ConnectReadOnlyAccess

Anda dapat melampirkan kebijakan `AWSDirectConnectReadOnlyAccess` ke identitas IAM Anda. Kebijakan ini memberikan izin yang memungkinkan akses hanya-baca. AWS Direct Connect

Untuk menampilkan izin untuk kebijakan ini, lihat AWSDirectConnectReadOnlyAccess di AWS Management Console.

AWS kebijakan terkelola: AWSDirect ConnectServiceRolePolicy

Kebijakan ini dilampirkan ke peran terkait layanan yang diberi nama AWSServiceRoleForDirectConnect AWS Direct Connect untuk memungkinkan mengambil rahasia Keamanan MAC atas nama Anda. Untuk informasi selengkapnya, lihat the section called “Peran terkait layanan”.

Untuk menampilkan izin untuk kebijakan ini, lihat AWSDirectConnectServiceRolePolicy di AWS Management Console.

AWS Direct Connect pembaruan kebijakan AWS terkelola

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

Perubahan	Deskripsi	Tanggal
AWSDirectConnectServiceRolePolicy- Kebijakan baru	Untuk mendukung Keamanan MAC, peran AWSServiceRoleForDirectConnectterkait layanan ditambahkan.	31 Maret 2021
AWS Direct Connect mulai melacak perubahan	AWS Direct Connect mulai melacak perubahan pada kebijakan AWS terkelolanya.	31 Maret 2021

Pemecahan masalah akses dan identitas Direct Connect

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temukan saat bekerja dengan Direct Connect dan IAM.

Topik

- Saya tidak diotorisasi untuk melakukan tindakan di Direct Connect
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS mengakses sumber daya Direct Connect saya

Saya tidak diotorisasi untuk melakukan tindakan di Direct Connect

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `directconnect:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 directconnect:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `directconnect:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Direct Connect.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi saat pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Direct Connect. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS mengakses sumber daya Direct Connect saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Direct Connect mendukung fitur berikut, lihat Cara Direct Connect berfungsi dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Penebangan dan pemantauan di AWS Direct Connect

Anda dapat menggunakan alat pemantauan otomatis berikut untuk melihat AWS Direct Connect dan melaporkan saat terjadi kesalahan:

- CloudWatch Alarm Amazon - Tonton satu metrik selama periode waktu yang Anda tentukan. Lakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas selama periode waktu tertentu. Tindakannya adalah pemberitahuan yang dikirim ke topik Amazon SNS. CloudWatch alarm tidak memanggil tindakan hanya karena mereka berada dalam keadaan tertentu; negara harus telah berubah dan dipertahankan untuk sejumlah periode tertentu. Untuk informasi selengkapnya, lihat Monitor dengan Amazon CloudWatch.
- AWS CloudTrail Pemantauan Log - Bagikan file log antar akun dan pantau file CloudTrail log secara real time dengan mengirimkannya ke CloudWatch Log. Anda juga dapat menulis aplikasi pemrosesan log di Java dan memvalidasi bahwa file log Anda tidak berubah setelah pengiriman oleh CloudTrail. Untuk informasi selengkapnya, lihat Log panggilan AWS Direct Connect API menggunakan AWS CloudTrail dan Bekerja dengan File CloudTrail Log di Panduan AWS CloudTrail Pengguna.

Untuk informasi selengkapnya, lihat Memantau sumber daya Direct Connect.

Validasi kepatuhan untuk AWS Direct Connect

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

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

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

- Kepatuhan dan Tata Kelola Keamanan – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- Referensi Layanan yang Memenuhi Syarat HIPAA — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan,

seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.

- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS Direct Connect

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

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

Selain infrastruktur AWS global, AWS Direct Connect menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Untuk informasi tentang cara menggunakan VPN AWS Direct Connect, lihat AWS Direct Connect Plus VPN.

Failover

AWS Direct Connect Resiliency Toolkit menyediakan wizard koneksi dengan beberapa model ketahanan yang membantu Anda memesan koneksi khusus untuk mencapai tujuan SLA Anda. Anda memilih model ketahanan, dan kemudian AWS Direct Connect Resiliency Toolkit memandu Anda melalui proses pemesanan koneksi khusus. Model ketahanan didesain untuk memastikan Anda memiliki jumlah koneksi khusus yang sesuai di beberapa lokasi.

- Ketahanan Maksimum: Anda dapat mencapai ketahanan maksimum untuk beban kerja kritis dengan menggunakan koneksi terpisah yang berakhir pada perangkat terpisah di lebih dari satu lokasi. Model ini memberikan ketahanan terhadap perangkat, konektivitas, dan kegagalan lokasi lengkap.

- Ketahanan Tinggi: Anda dapat mencapai ketahanan tinggi untuk beban kerja kritis dengan menggunakan dua koneksi tunggal ke beberapa lokasi. Model ini memberikan ketahanan terhadap kegagalan konektivitas yang disebabkan oleh pemotongan serat atau kegagalan perangkat. Ini juga membantu mencegah kegagalan lokasi lengkap.
- Pengembangan dan Pengujian: Anda bisa mendapatkan pengembangan dan uji ketahanan untuk beban kerja non-kritis dengan menggunakan koneksi terpisah yang berakhir pada perangkat terpisah di satu lokasi. Model ini memberikan ketahanan terhadap kegagalan perangkat, tetapi tidak memberikan ketahanan terhadap kegagalan lokasi.

Untuk informasi selengkapnya, lihat AWS Direct Connect Toolkit Ketahanan.

Keamanan infrastruktur di AWS Direct Connect

Sebagai layanan terkelola, AWS Direct Connect dilindungi oleh prosedur keamanan jaringan AWS global. Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS Direct Connect melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.2 atau versi yang lebih baru. Kami merekomendasikan TLS 1.3. Klien juga harus mendukung cipher suite dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

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

Anda dapat memanggil operasi API ini dari lokasi jaringan mana pun, tetapi AWS Direct Connect mendukung kebijakan akses berbasis sumber daya, yang dapat mencakup pembatasan berdasarkan alamat IP sumber. Anda juga dapat menggunakan AWS Direct Connect kebijakan untuk mengontrol akses dari titik akhir Amazon Virtual Private Cloud (Amazon VPC) tertentu atau spesifik. VPCs Secara efektif, ini mengisolasi akses jaringan ke AWS Direct Connect sumber daya tertentu hanya dari VPC tertentu dalam AWS jaringan. Sebagai contoh, lihat the section called “Contoh kebijakan berbasis identitas untuk Direct Connect”.

Keamanan Border Gateway Protocol (BGP)

Internet sebagian besar bergantung pada BGP untuk merutekan informasi antara sistem jaringan. Perutean BGP terkadang rentan terhadap serangan berbahaya, atau pembajakan BGP. Untuk

memahami cara AWS kerja untuk melindungi jaringan Anda dari pembajakan BGP dengan lebih aman, lihat Cara AWS membantu mengamankan perutean internet.

Gunakan AWS Direct Connect CLI

Anda dapat menggunakan AWS CLI untuk membuat dan bekerja dengan AWS Direct Connect sumber daya.

Contoh berikut menggunakan AWS CLI perintah untuk membuat AWS Direct Connect koneksi. Anda juga dapat mengunduh Letter of Authorization and Connecting Facility Assignment (LOA-CFA) atau menyediakan antarmuka virtual privat atau publik.

Sebelum memulai, pastikan Anda telah menginstal dan mengonfigurasi AWS CLI. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Command Line Interface.

Daftar Isi

Langkah 1: Buat koneksi

Langkah pertama adalah mengirimkan permintaan koneksi. Pastikan Anda mengetahui kecepatan port yang Anda butuhkan dan AWS Direct Connect lokasi. Untuk informasi selengkapnya, lihat Koneksi khusus dan host.

Untuk membuat permintaan koneksi

1. Jelaskan AWS Direct Connect lokasi untuk Wilayah Anda saat ini. Dalam output yang dihasilkan, perhatikan kode lokasi untuk lokasi di mana Anda ingin membuat koneksi.

```
aws directconnect describe-locations
```

```
{
    "locations": [
        {
            "locationName": "City 1, United States",
            "locationCode": "Example Location 1"
        },
        {
            "locationName": "City 2, United States",
```

```
            "locationCode": "Example location"
        }
    ]
}
```

2. Buat koneksi dan tentukan nama, kecepatan port, dan kode lokasi. Dalam output yang dihasilkan, perhatikan ID koneksi. Anda perlu ID untuk mendapatkan LOA-CFA di langkah berikutnya.

```
aws directconnect create-connection --location Example location --bandwidth 1Gbps
 --connection-name "Connection to AWS"
```

```
{
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-EXAMPLE",
    "connectionState": "requested",
    "bandwidth": "1Gbps",
    "location": "Example location",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

Langkah 2: Unduh LOA-CFA

Setelah meminta koneksi, Anda bisa mendapatkan LOA-CFA menggunakan perintah `describe-loa`. Output-nya dikodekan base64. Anda harus mengekstraksi konten LOA yang relevan, memecahkan kode, dan membuat file PDF.

Untuk mendapatkan LOA-CFA menggunakan Linux atau macOS

Dalam contoh ini, bagian terakhir dari perintah mendekode konten menggunakan utilitas base64, dan mengirimkan output ke file PDF.

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

Untuk mendapatkan LOA-CFA menggunakan Windows

Dalam contoh ini, output diekstraksi ke file bernama myLoaCfa .base64. Perintah kedua menggunakan utilitas `certutil` untuk memecahkan kode file dan mengirim output ke file PDF.

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

Setelah Anda mengunduh LOA-CFA, kirimkan ke penyedia jaringan atau penyedia kolokasi Anda.

Langkah 3: Buat antarmuka virtual dan dapatkan konfigurasi router

Setelah Anda memesan AWS Direct Connect koneksi, Anda harus membuat antarmuka virtual untuk mulai menggunakannya. Anda dapat membuat antarmuka virtual privat untuk terhubung ke VPC Anda. Atau, Anda dapat membuat antarmuka virtual publik untuk terhubung ke AWS layanan yang tidak ada dalam VPC. Anda dapat membuat antarmuka virtual yang mendukung IPv4 atau IPv6 lalu lintas.

Sebelum memulai, pastikan Anda telah membaca prasyarat di the section called “Prasyarat untuk antarmuka virtual”.

Saat Anda membuat antarmuka virtual menggunakan AWS CLI, output mencakup informasi konfigurasi router generik. Untuk membuat konfigurasi router yang khusus untuk perangkat Anda, gunakan AWS Direct Connect konsol. Untuk informasi selengkapnya, lihat Mengunduh file konfigurasi router.

Untuk membuat antarmuka virtual privat

1. Dapatkan ID virtual private gateway (vgw-xxxxxxxx) yang terpasang pada VPC Anda. Anda memerlukan ID untuk membuat antarmuka virtual pada langkah berikutnya.

   ```
   aws ec2 describe-vpn-gateways
   ```

   ```
   {
       "VpnGateways": [
           {
               "State": "available",
               "Tags": [
                   {
                       "Value": "DX_VGW",
                       "Key": "Name"
                   }
   ```

```
            ],
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-ebaa27db",
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-24f33d4d"
                }
            ]
        }
    ]
}
```

2. Buat antarmuka virtual privat. Anda harus menentukan nama, VLAN ID, dan BGP Autonomous System Number (ASN).

   Untuk IPv4 lalu lintas, Anda memerlukan IPv4 alamat pribadi untuk setiap akhir sesi peering BGP. Anda dapat menentukan IPv4 alamat Anda sendiri, atau Anda dapat membiarkan Amazon menghasilkan alamat untuk Anda. Dalam contoh berikut, IPv4 alamat dibuat untuk Anda.

```
aws directconnect create-private-virtual-interface --
connection-id dxcon-fg31dyv6 --new-private-virtual-interface
 virtualInterfaceName=PrivateVirtualInterface,vlan=101,asn=65000,virtualGatewayId=vgw-
ebaa27db,addressFamily=ipv4
```

```
{
    "virtualInterfaceState": "pending",
    "asn": 65000,
    "vlan": 101,
    "customerAddress": "192.168.1.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "vgw-ebaa27db",
    "virtualInterfaceId": "dxvif-ffhhk74f",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "192.168.1.2/30",
```

```
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "pending",
            "amazonAddress": "192.168.1.1/30",
            "asn": 65000
        }
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-ffhhk74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>private</connection_type>\n</
logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "PrivateVirtualInterface"
}
```

Untuk membuat antarmuka virtual pribadi yang mendukung IPv6 lalu lintas, gunakan perintah yang sama seperti di atas dan tentukan `ipv6` `addressFamily` parameternya. Anda tidak dapat menentukan IPv6 alamat Anda sendiri untuk sesi peering BGP; Amazon mengalokasikan alamat Anda. IPv6

3. Untuk melihat informasi konfigurasi router dalam format XML, uraikan antarmuka virtual yang Anda buat. Menggunakan parameter `--query` untuk mengekstraksi informasi `customerRouterConfig`, dan parameter `--output` untuk mengatur teks menjadi garis berbatas tab.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-ffhhk74f
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhhk74f">
  <vlan>101</vlan>
  <customer_address>192.168.1.2/30</customer_address>
  <amazon_address>192.168.1.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>private</connection_type>
</logical_connection>
```

Untuk membuat antarmuka virtual publik

1. Untuk membuat antarmuka virtual publik, Anda harus menentukan nama, VLAN ID, dan Autonomous System Number (ASN) BGP.

   Untuk IPv4 lalu lintas, Anda juga harus menentukan IPv4 alamat publik untuk setiap akhir sesi peering BGP, dan IPv4 rute publik yang akan Anda iklankan melalui BGP. Contoh berikut menciptakan antarmuka virtual publik untuk IPv4 lalu lintas.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/
{cidr=203.0.113.4/30}]
```

```
{
    "virtualInterfaceState": "verifying",
    "asn": 65000,
    "vlan": 2000,
    "customerAddress": "203.0.113.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "",
    "virtualInterfaceId": "dxvif-fgh0hcrk",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [
        {
            "cidr": "203.0.113.0/30"
        },
        {
            "cidr": "203.0.113.4/30"
        }
    ],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "203.0.113.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "verifying",
            "amazonAddress": "203.0.113.1/30",
```

```
            "asn": 65000
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>public</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

Untuk membuat antarmuka virtual publik yang mendukung IPv6 lalu lintas, Anda dapat menentukan IPv6 rute yang akan Anda iklankan melalui BGP. Anda tidak dapat menentukan IPv6 alamat untuk sesi peering; Amazon mengalokasikan IPv6 alamat untuk Anda. Contoh berikut menciptakan antarmuka virtual publik untuk IPv6 lalu lintas.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,addressFamily=ipv6,routeFi
{cidr=2001:db8:64ce:ba01::/64}]
```

2. Untuk melihat informasi konfigurasi router dalam format XML, uraikan antarmuka virtual yang Anda buat. Menggunakan parameter `--query` untuk mengekstraksi informasi `customerRouterConfig`, dan parameter `--output` untuk mengatur teks menjadi garis berbatas tab.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-fgh0hcrk
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-fgh0hcrk">
  <vlan>2000</vlan>
  <customer_address>203.0.113.2/30</customer_address>
  <amazon_address>203.0.113.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
```

```
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>public</connection_type>
</logical_connection>
```

Log panggilan AWS Direct Connect API menggunakan AWS CloudTrail

AWS Direct Connect terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di AWS Direct Connect. CloudTrail menangkap semua panggilan API untuk AWS Direct Connect sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari AWS Direct Connect konsol dan panggilan kode ke operasi AWS Direct Connect API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk. AWS Direct Connect Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AWS Direct Connect, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

AWS Direct Connect informasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di AWS Direct Connect, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS . Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk AWS Direct Connect, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua AWS Wilayah. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran Umum untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengkonfigurasi Notifikasi Amazon SNS untuk CloudTrail

- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

Semua AWS Direct Connect tindakan dicatat oleh CloudTrail dan didokumentasikan dalam Referensi AWS Direct Connect API. Misalnya, panggilan ke `CreateConnection` dan `CreatePrivateVirtualInterface` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan dibuat dengan kredenal root atau AWS Identity and Access Management (pengguna IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat CloudTrail `userIdentity` Elemen.

Memahami entri file AWS Direct Connect log

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

Berikut ini adalah contoh catatan CloudTrail log untuk AWS Direct Connect.

Example Contoh: CreateConnection

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
```

```
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:28:16Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "location": "EqSE2",
            "connectionName": "MyExampleConnection",
            "bandwidth": "1Gbps"
        },
        "responseElements": {
            "location": "EqSE2",
            "region": "us-west-2",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-fhajolyy",
            "connectionName": "MyExampleConnection"
        }
    },
    ...
  ]
}
```

Example Contoh: CreatePrivateVirtualInterface

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
```

```
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
                "customerAddress": "[PROTECTED]",
                "authKey": "[PROTECTED]",
                "asn": -1,
                "virtualGatewayId": "vgw-bb09d4a5",
                "amazonAddress": "[PROTECTED]",
                "vlan": 123
            }
        },
        "responseElements": {
            "virtualInterfaceId": "dxvif-fgq61m6w",
            "authKey": "[PROTECTED]",
            "virtualGatewayId": "vgw-bb09d4a5",
            "customerRouterConfig": "[PROTECTED]",
            "virtualInterfaceType": "private",
            "asn": -1,
            "routeFilterPrefixes": [],
            "virtualInterfaceName": "MyVirtualInterface",
            "virtualInterfaceState": "pending",
            "customerAddress": "[PROTECTED]",
            "vlan": 123,
            "ownerAccount": "123456789012",
```

```
            "amazonAddress": "[PROTECTED]",
            "connectionId": "dxcon-fhajolyy",
            "location": "EqSE2"
        }
    },
    ...
  ]
}
```

Example Contoh: DescribeConnections

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:27:28Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeConnections",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": null,
        "responseElements": null
    },
    ...
  ]
}
```

Example Contoh: DescribeVirtualInterfaces


```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:37:53Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeVirtualInterfaces",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy"
        },
        "responseElements": null
    },
    ...
  ]
}
```

Pantau AWS Direct Connect sumber daya

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja sumber daya Direct Connect Anda. Anda harus mengumpulkan data pemantauan dari semua bagian AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi. Sebelum Anda mulai memantau Direct Connect; namun, Anda harus membuat rencana pemantauan yang mencakup jawaban atas pertanyaan-pertanyaan berikut:

- Apa tujuan pemantauan Anda?
- Apa saja sumber daya yang harus dipantau?
- Seberapa sering Anda harus memantau sumber daya ini?
- Apa alat pemantauan yang akan Anda gunakan?
- Siapa yang melakukan tugas pemantauan?
- Siapa yang harus diberi tahu saat terjadi kesalahan?

Langkah selanjutnya adalah menetapkan dasar untuk kinerja Direct Connect normal di lingkungan Anda, dengan mengukur kinerja pada berbagai waktu dan dalam kondisi beban yang berbeda. Saat Anda memantau Direct Connect, simpan data pemantauan historis. Dengan cara ini, Anda dapat membandingkannya dengan data performa saat ini, mengidentifikasi pola performa normal dan anomali performa, serta merancang metode untuk mengatasi masalah.

Untuk menetapkan baseline, Anda harus memantau penggunaan, status, dan kesehatan koneksi Direct Connect fisik Anda.

Daftar Isi

Alat pemantauan

AWS menyediakan berbagai alat yang dapat Anda gunakan untuk memantau AWS Direct Connect koneksi. Anda dapat mengonfigurasi beberapa alat ini untuk melakukan pemantauan untuk Anda, sementara beberapa alat memerlukan intervensi manual. Kami menyarankan agar Anda mengautomasi tugas pemantauan sebanyak mungkin.

Alat pemantauan otomatis

Anda dapat menggunakan alat pemantauan otomatis berikut untuk menonton Direct Connect dan melaporkan ketika ada sesuatu yang salah:

- CloudWatch Alarm Amazon - Tonton satu metrik selama periode waktu yang Anda tentukan. Lakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas selama periode waktu tertentu. Tindakannya adalah pemberitahuan yang dikirim ke topik Amazon SNS. CloudWatch alarm tidak memanggil tindakan hanya karena mereka berada dalam keadaan tertentu; negara harus telah berubah dan dipertahankan untuk sejumlah periode tertentu. Untuk informasi tentang metrik dan dimensi yang tersedia, lihat Monitor dengan Amazon CloudWatch.
- AWS CloudTrail Pemantauan Log - Bagikan file log antar akun dan pantau file CloudTrail log secara real time dengan mengirimkannya ke CloudWatch Log. Anda juga dapat menulis aplikasi pemrosesan log di Java dan memvalidasi bahwa file log Anda tidak berubah setelah pengiriman oleh CloudTrail. Untuk informasi selengkapnya, lihat Log panggilan API dan Bekerja dengan File CloudTrail Log di Panduan AWS CloudTrail Pengguna.

Alat pemantauan manual

Bagian penting lainnya dari pemantauan AWS Direct Connect koneksi melibatkan pemantauan secara manual item-item yang tidak tercakup oleh CloudWatch alarm. Dasbor Direct Connect dan CloudWatch konsol memberikan at-a-glance tampilan keadaan AWS lingkungan Anda.

- AWS Direct Connect Konsol menunjukkan:
  - Status koneksi (lihat kolom Status)
  - Status antarmuka virtual (lihat kolom Status)
- CloudWatch Halaman beranda menunjukkan:
  - Alarm dan status saat ini
  - Grafik alarm dan sumber daya
  - Status kesehatan layanan

  Selain itu, Anda dapat menggunakan CloudWatch untuk melakukan hal berikut:
  - Buat dasbor yang disesuaikan untuk memantau layanan yang Anda pedulikan.
  - Data metrik grafik untuk memecahkan masalah dan menemukan tren.
  - Cari dan telusuri semua metrik AWS sumber daya Anda.

- Buat dan sunting alarm untuk menerima pemberitahuan tentang masalah.

Monitor dengan Amazon CloudWatch

Anda dapat memantau AWS Direct Connect koneksi fisik, dan antarmuka virtual, menggunakan CloudWatch. CloudWatch mengumpulkan data mentah dari Direct Connect, dan memprosesnya menjadi metrik yang dapat dibaca. Secara default, CloudWatch menyediakan data metrik Direct Connect dalam interval 5 menit. Data metrik dalam setiap interval adalah agregasi dari setidaknya dua sampel yang dikumpulkan selama interval tersebut.

Untuk informasi selengkapnya CloudWatch, lihat Panduan CloudWatch Pengguna Amazon. Anda juga dapat memantau layanan Anda CloudWatch untuk melihat apa yang menggunakan sumber daya. Untuk informasi selengkapnya, lihat AWS layanan yang mempublikasikan CloudWatch metrik.

Daftar Isi

AWS Direct Connect metrik dan dimensi

Metrik tersedia untuk koneksi AWS Direct Connect fisik, dan antarmuka virtual.

AWS Direct Connect Metrik koneksi

Metrik berikut tersedia dari koneksi khusus Direct Connect.

Metrik	Deskripsi
`ConnectionState`	Status connection.1 mengindikasikan naik dan 0 mengindikasikan turun. Metrik ini tersedia untuk koneksi khusus dan yang di-host.

Metrik	Deskripsi
	Note Metrik ini juga tersedia di akun pemilik antarmuka virtual yang dihosting selain akun pemilik koneksi. Unit: Tidak ada unit yang dikembalikan untuk metrik ini.
`ConnectionBpsEgress`	Bitrate untuk data keluar dari AWS sisi koneksi. Jumlah yang dilaporkan adalah agregat (rata-rata) selama periode waktu yang ditentukan (5 menit secara default, 1 menit minimum). Anda dapat mengubah agregat default. Metrik ini mungkin tidak tersedia untuk koneksi baru, atau saat perangkat di-boot ulang. Metrik dimulai saat koneksi digunakan untuk mengirim atau menerima lalu lintas. Unit: Bit per detik
`ConnectionBpsIngress`	Bitrate untuk data masuk ke AWS sisi koneksi. Metrik ini mungkin tidak tersedia untuk koneksi baru, atau saat perangkat di-boot ulang. Metrik dimulai saat koneksi digunakan untuk mengirim atau menerima lalu lintas. Unit: Bit per detik

Metrik	Deskripsi
`ConnectionPpsEgress`	` Tingkat paket untuk data keluar dari AWS sisi koneksi. Jumlah yang dilaporkan adalah agregat (rata-rata) selama periode waktu yang ditentukan (5 menit secara default, 1 menit minimum). Anda dapat mengubah agregat default. Metrik ini mungkin tidak tersedia untuk koneksi baru, atau saat perangkat di-boot ulang. Metrik dimulai saat koneksi digunakan untuk mengirim atau menerima lalu lintas. Unit: Paket per detik
`ConnectionPpsIngress`	Tingkat paket untuk data masuk ke AWS sisi koneksi. Jumlah yang dilaporkan adalah agregat (rata-rata) selama periode waktu yang ditentukan (5 menit secara default, 1 menit minimum). Anda dapat mengubah agregat default. Metrik ini mungkin tidak tersedia untuk koneksi baru, atau saat perangkat di-boot ulang. Metrik dimulai saat koneksi digunakan untuk mengirim atau menerima lalu lintas. Unit: Paket per detik
`ConnectionCRCErrorCount`	Penghitungan ini tidak lagi digunakan. Sebagai gantinya, gunakan `ConnectionErrorCount` .

Metrik	Deskripsi
`ConnectionErrorCount`	Jumlah kesalahan total untuk semua jenis kesalahan tingkat MAC pada perangkat AWS . Total ini termasuk kesalahan pemeriksaan redundansi siklik (CRC). Metrik ini adalah jumlah kesalahan yang terjadi sejak titik data terakhir dilaporkan. Bila ada kesalahan pada antarmuka, metrik melaporkan nilai bukan nol. Untuk mendapatkan jumlah total semua kesalahan untuk interval yang dipilih CloudWatch, misalnya, 5 menit, terapkan statistik “jumlah”. Nilai metrik diatur ke 0 ketika kesalahan pada antarmuka berhenti. **Note** Metrik ini menggantikan `ConnectionCRCErrorCount` , yang tidak lagi digunakan. Unit: Jumlah
`ConnectionLightLevelTx`	Menunjukkan kesehatan koneksi serat untuk lalu lintas keluar (jalan keluar) dari AWS sisi koneksi. Ada dua dimensi untuk metrik ini. Untuk informasi selengkapnya, lihat Dimensi yang tersedia Direct Connect. Unit: dBm

Metrik	Deskripsi
`ConnectionLightLevelRx`	Menunjukkan kesehatan koneksi serat untuk lalu lintas masuk (masuknya) ke AWS sisi koneksi. Ada dua dimensi untuk metrik ini. Untuk informasi selengkapnya, lihat Dimensi yang tersedia Direct Connect. Unit: dBm
`ConnectionEncryptionState`	Menunjukkan status enkripsi koneksi. 1 menunjukkan enkripsi koneksi adalah up, dan 0 menunjukkan enkripsi koneksi adalah down. Ketika metrik ini diterapkan ke LAG, 1 menunjukkan bahwa semua koneksi di LAG memiliki enkripsiup. 0 menunjukkan setidaknya satu enkripsi koneksi LAGdown.

AWS Direct Connect metrik antarmuka virtual

Metrik berikut tersedia dari antarmuka AWS Direct Connect virtual.

Metrik	Deskripsi
`VirtualInterfaceBpsEgress`	Bitrate untuk data keluar dari AWS sisi antarmuka virtual. Jumlah yang dilaporkan adalah agregat (rata-rata) selama periode waktu yang ditentukan (5 menit secara default). Unit: Bit per detik
`VirtualInterfaceBpsIngress`	Bitrate untuk data masuk ke AWS sisi antarmuka virtual.

Metrik	Deskripsi
	Jumlah yang dilaporkan adalah agregat (rata-rata) selama periode waktu yang ditentukan (5 menit secara default). Unit: Bit per detik
`VirtualInterfacePpsEgress`	Tingkat paket untuk data keluar dari AWS sisi antarmuka virtual. Jumlah yang dilaporkan adalah agregat (rata-rata) selama periode waktu yang ditentukan (5 menit secara default). Unit: Paket per detik
`VirtualInterfacePpsIngress`	Tingkat paket untuk data masuk ke AWS sisi antarmuka virtual. Jumlah yang dilaporkan adalah agregat (rata-rata) selama periode waktu yang ditentukan (5 menit secara default). Unit: Paket per detik

AWS Direct Connect dimensi yang tersedia

Anda dapat memfilter AWS Direct Connect data menggunakan dimensi berikut.

Dimensi	Deskripsi
`ConnectionId`	Dimensi ini tersedia pada metrik untuk koneksi Direct Connect, dan antarmuka virtual. Dimensi ini memfilter data menurut koneksi.
`OpticalLaneNumber`	Dimensi ini menyaring `ConnectionLightLevelTx` data dan `ConnectionLightLevelRx` data, dan memfilter data dengan nomor jalur optik koneksi Direct Connect.

Dimensi	Deskripsi
`VirtualInterfaceId`	Dimensi ini tersedia pada metrik untuk antarmuka virtual Direct Connect, dan memfilter data dengan antarmuka virtual.

Topik

- Lihat AWS Direct Connect CloudWatch metrik
- Buat CloudWatch alarm Amazon untuk memantau koneksi AWS Direct Connect

Lihat AWS Direct Connect CloudWatch metrik

AWS Direct Connect mengirimkan metrik berikut tentang koneksi Direct Connect Anda. Amazon CloudWatch kemudian menggabungkan titik-titik data ini ke interval 1 menit atau 5 menit. Secara default, data metrik Direct Connect ditulis CloudWatch pada interval 5 menit.

> **Note**
>
> Saat memantau Direct Connect CloudWatch, Anda dapat meminta metrik dengan interval 1 menit. Namun, frekuensi pembaruan aktual dikendalikan oleh CloudWatch. Karena CloudWatch mengontrol interval, Direct Connect tidak selalu dapat menjamin interval yang lebih pendek dari lima menit.

Anda dapat menggunakan prosedur berikut untuk melihat metrik koneksi Direct Connect.

Untuk melihat metrik menggunakan konsol CloudWatch

Metrik dikelompokkan terlebih dahulu berdasarkan namespace layanan, lalu berdasarkan berbagai kombinasi dimensi dalam setiap namespace. Untuk informasi selengkapnya tentang penggunaan Amazon CloudWatch untuk melihat metrik Direct Connect, termasuk menambahkan fungsi matematika atau kueri bawaan, lihat Menggunakan Amazon CloudWatch metrik di Panduan Pengguna Amazon. CloudWatch

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Metrik, dan kemudian pilih Semua metrik.
3. Di bagian Metrik, pilih DX.

4. Pilih nama ConnectionIdatau Metrik, lalu pilih salah satu dari berikut ini untuk menentukan metrik lebih lanjut:

   - Tambahkan ke pencarian — Menambahkan metrik ini ke hasil pencarian Anda.
   - Cari ini saja — Pencarian hanya untuk metrik ini.
   - Hapus dari grafik - Menghapus metrik ini dari grafik.
   - Grafik metrik ini saja — Grafik hanya metrik ini.
   - Grafik semua hasil pencarian — Grafik semua metrik.
   - Grafik dengan kueri SQL - Membuka Metric Insights -query builder, memungkinkan Anda memilih apa yang ingin Anda grafik dengan membuat kueri SQL. Untuk informasi selengkapnya tentang penggunaan Wawasan Metrik, lihat Kueri metrik Anda dengan Wawasan CloudWatch Metrik di Panduan Pengguna Amazon. CloudWatch

Untuk melihat metrik menggunakan konsol AWS Direct Connect

1. Buka AWS Direct Connectkonsol di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Koneksi.
3. Pilih koneksi Anda.
4. Pilih tab Monitoring untuk menampilkan metrik koneksi Anda.

Untuk melihat metrik menggunakan AWS CLI

Pada prompt perintah, gunakan perintah berikut.

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```

Buat CloudWatch alarm Amazon untuk memantau koneksi AWS Direct Connect

Anda dapat membuat CloudWatch alarm yang mengirimkan pesan Amazon SNS saat alarm berubah status. Alarm mengawasi satu metrik selama suatu periode waktu yang Anda tentukan. Alarm mengirimkan pemberitahuan ke topik Amazon SNS berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu.

Misalnya, Anda dapat membuat alarm yang memantau status koneksi AWS Direct Connect . Alarm akan mengirimkan pemberitahuan ketika status koneksi turun selama lima periode 1 menit berturut-

turut. Untuk detail tentang hal yang perlu diketahui untuk membuat alarm dan untuk informasi selengkapnya tentang membuat alarm, lihat Menggunakan CloudWatch Alarm Amazon di Panduan CloudWatch Pengguna Amazon.

Untuk membuat CloudWatch alarm.

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Alarm, dan kemudian pilih Semua alarm.
3. Pilih Buat Alarm.
4. Pilih Pilih metrik, lalu pilih DX.
5. Pilih metrik Connection Metrics.
6. Pilih AWS Direct Connect koneksi, lalu pilih metrik Select metrik.
7. Pada halaman Tentukan metrik dan kondisi, konfigurasikan parameter untuk alarm. Untuk menentukan metrik dan ketentuan lainnya, lihat Menggunakan CloudWatchAlarm Amazon di Panduan Pengguna Amazon CloudWatch .
8. Pilih Berikutnya.
9. Konfigurasikan tindakan alarm pada halaman Konfigurasi tindakan. Untuk informasi selengkapnya tentang mengonfigurasi tindakan alarm, lihat Tindakan alarm di Panduan CloudWatch Pengguna Amazon.
10. Pilih Berikutnya.
11. Pada halaman Tambahkan nama dan deskripsi, masukkan Nama dan deskripsi Alarm opsional untuk mendeskripsikan alarm ini, lalu pilih Berikutnya.
12. Verifikasi alarm yang diusulkan pada halaman Pratinjau dan buat.
13. Jika diperlukan pilih Edit untuk mengubah informasi apa pun, lalu pilih Buat alarm.

    Halaman Alarm menampilkan baris baru dengan informasi tentang alarm baru. Status Tindakan menampilkan Tindakan diaktifkan, yang menunjukkan bahwa alarm aktif.

AWS Direct Connect kuota

Tabel berikut mencantumkan kuota yang terkait AWS Direct Connect dengan.

Komponen	Kuota	Komentar
Antarmuka virtual pribadi atau publik per koneksi AWS Direct Connect khusus	50	Batas ini tidak dapat dinaikkan.
Transit antarmuka virtual per koneksi AWS Direct Connect khusus. Antarmuka virtual transit dapat digunakan untuk terhubung ke Transit Gateway atau jaringan inti AWS Cloud WAN. Untuk informasi selengkapnya, lihat Gerbang.	4	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Antarmuka virtual pribadi atau publik per koneksi AWS Direct Connect khusus dan antarmuka virtual transit per AWS Direct Connect koneksi khusus	51	Ketika AWS Direct Connect dukungan untuk Amazon VPC Transit Gateways diluncurkan, kuota satu (1) antarmuka virtual transit ditambahkan ke kuota 50 antarmuka virtual pribadi atau publik per koneksi khusus. Jumlah antarmuka virtual transit yang diizinkan sekarang empat (4) dan dihitung terhadap maksimum 51 antarmuka virtual per koneksi khusus. Batas ini tidak dapat dinaikkan.
Antarmuka virtual pribadi, publik, atau transit per koneksi yang AWS Direct Connect dihosting	1	Batas ini tidak dapat dinaikkan.
AWS Direct Connect Koneksi aktif per lokasi Direct Connect per Wilayah per akun	10	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Jumlah antarmuka virtual per Grup Agregasi Tautan (LAG)	54	Ketika AWS Direct Connect dukungan untuk Amazon VPC Transit Gateways

Komponen	Kuota	Komentar
		diluncurkan, kuota satu (1) antarmuka virtual transit ditambahkan ke kuota 50 antarmuka virtual pribadi atau publik per LAG. Jumlah antarmuka virtual transit yang diizinkan sekarang empat (4) dan dihitung terhadap maksimum 51 antarmuka virtual per LAG. Batas ini tidak dapat dinaikkan.
Rute per sesi Border Gateway Protocol (BGP) pada antarmuka virtual pribadi atau antarmuka virtual transit dari lokal ke lokasi. AWS Jika Anda mengiklankan lebih dari 100 rute masing-masing untuk IPv4 dan IPv6 selama sesi BGP, sesi BGP akan masuk ke keadaan idle dengan sesi BGP DOWN.	100 masing-masing untuk IPv4 dan IPv6	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Rute per sesi Border Gateway Protocol (BGP) pada antarmuka virtual publik	1.000	Batas ini tidak dapat ditingkatkan.
Koneksi khusus per grup agregasi tautan (LAG)	4 saat kecepatan port kurang dari 100G 2 saat kecepatan port 100G	

Komponen	Kuota	Komentar
Tautkan grup agregasi (LAGs) per Wilayah	10	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
AWS Direct Connect gateway per akun	200	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Gateway pribadi virtual per gateway AWS Direct Connect	20	Batas ini tidak dapat dinaikkan.
Gerbang transit per gerbang AWS Direct Connect	6	Batas ini tidak dapat dinaikkan.
Jumlah maksimum awalan rute yang diiklankan dari lampiran gateway Direct Connect jaringan inti AWS Cloud WAN ke lokal. **Note** Semua antarmuka virtual transit yang dilampirkan ke gateway Direct Connect akan menerima semua awalan rute yang diiklankan oleh jaringan inti.	5.000	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Antarmuka virtual (pribadi atau transit) per gateway AWS Direct Connect	30	Batas ini tidak dapat dinaikkan.

Komponen	Kuota	Komentar
Jumlah awalan per AWS Transit Gateway dari AWS ke on-premise pada antarmuka virtual transit	200 total gabungan untuk IPv4 dan IPv6	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Jumlah antarmuka per virtual private gateway	Tidak ada batasnya.	
Jumlah gateway Direct Connect yang terkait dengan gateway transit	20	Batas ini tidak dapat dinaikkan.
SiteLink batas awalan	100	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.

AWS Direct Connect mendukung kecepatan port ini melalui serat mode tunggal: 1 Gbps: 1000BASE-LX (1310 nm), 10 Gbps: 10GBASE-LR (1310 nm), 100Gbps: 100GBASE-, dan 400 Gbps: 400GBASE-. LR4 LR4

Kuota BGP

Berikut adalah kuota BGP. Pengatur waktu BGP bernegosiasi ke nilai terendah antara router. Interval BFD ditentukan oleh perangkat paling lambat.

- Pengatur waktu hold default: 90 detik
- Pengatur waktu hold minimum: 3 detik

  Nilai hold 0 tidak didukung.
- Pengatur waktu keepalive default: 30 detik
- Pengatur waktu keepalive minimum: 1 detik
- Pengatur waktu mulai ulang graceful: 120 detik

Kami menyarankan agar Anda tidak mengonfigurasi mulai ulang graceful dan BFD pada saat yang sama.

- Interval minimum deteksi liveness BFD: 300 milidetik
- Pengganda minimum BFD: 3

Pertimbangan keseimbangan beban

Jika Anda ingin menggunakan load balancing dengan beberapa publik VIFs, semua VIFs harus berada di Wilayah yang sama.

Pemecahan masalah AWS Direct Connect

Informasi pemecahan masalah berikut dapat membantu Anda mendiagnosis dan memperbaiki masalah dengan koneksi AWS Direct Connect Anda.

Daftar Isi

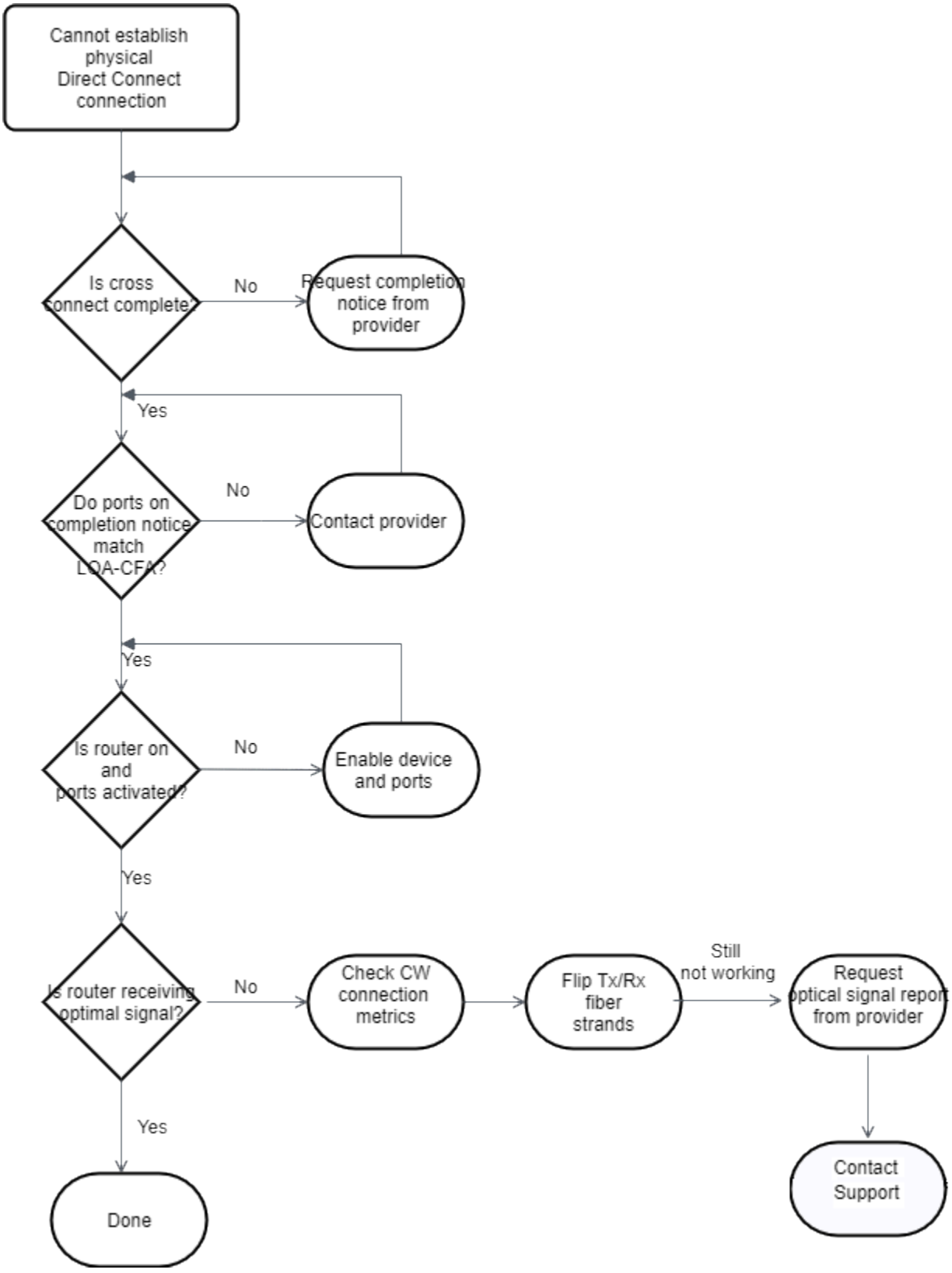
Pemecahan masalah lapisan 1 (fisik)

Jika Anda atau penyedia jaringan mengalami kesulitan dalam membangun konektivitas fisik ke AWS Direct Connect perangkat, gunakan langkah-langkah berikut untuk memecahkan masalah tersebut.

1. Verifikasi dengan penyedia kolokasi bahwa koneksi silang selesai. Minta mereka atau penyedia jaringan Anda untuk memberi Anda pemberitahuan penyelesaian koneksi silang dan bandingkan port dengan yang terdaftar di LOA-CFA Anda.
2. Verifikasi bahwa router atau router penyedia Anda diaktifkan dan bahwa port diaktifkan.
3. Pastikan router menggunakan transceiver optik yang benar. Negosiasi otomatis untuk port harus dinonaktifkan jika Anda memiliki koneksi dengan kecepatan port lebih dari 1 Gbps. Namun, tergantung pada titik akhir AWS Direct Connect yang melayani koneksi Anda, negosiasi otomatis mungkin perlu diaktifkan atau dinonaktifkan untuk koneksi 1 Gbps. Jika negosiasi otomatis perlu dinonaktifkan untuk koneksi Anda, kecepatan port dan mode dupleks penuh harus dikonfigurasi secara manual. Jika antarmuka virtual Anda tetap down, lihatPemecahan masalah lapisan 2 (tautan data). Bergantung pada titik akhir Direct Connect yang melayani koneksi Anda berakhir, negosiasi otomatis mungkin perlu diaktifkan atau dinonaktifkan.
4. Verifikasi bahwa router menerima sinyal optik yang dapat diterima melalui koneksi silang.
5. Cobalah membalik (juga dikenal sebagai menggulung) untaian serat Tx/Rx.
6. Periksa CloudWatch metrik Amazon untuk AWS Direct Connect. Anda dapat memverifikasi pembacaan optik Tx/Rx AWS Direct Connect perangkat (baik 1 Gbps dan 10 Gbps), jumlah kesalahan fisik, dan status operasional. Untuk informasi selengkapnya, lihat Memantau dengan Amazon CloudWatch.

7. Hubungi penyedia kolokasi dan minta laporan tertulis untuk sinyal optik Tx/Rx melintasi sambungan silang.
8. Jika langkah-langkah di atas tidak menyelesaikan masalah konektivitas fisik, hubungi AWS Dukungan dan berikan pemberitahuan penyelesaian koneksi silang dan laporan sinyal optik dari penyedia kolokasi.

Bagan alir berikut berisi langkah-langkah untuk mendiagnosis masalah dengan koneksi fisik.

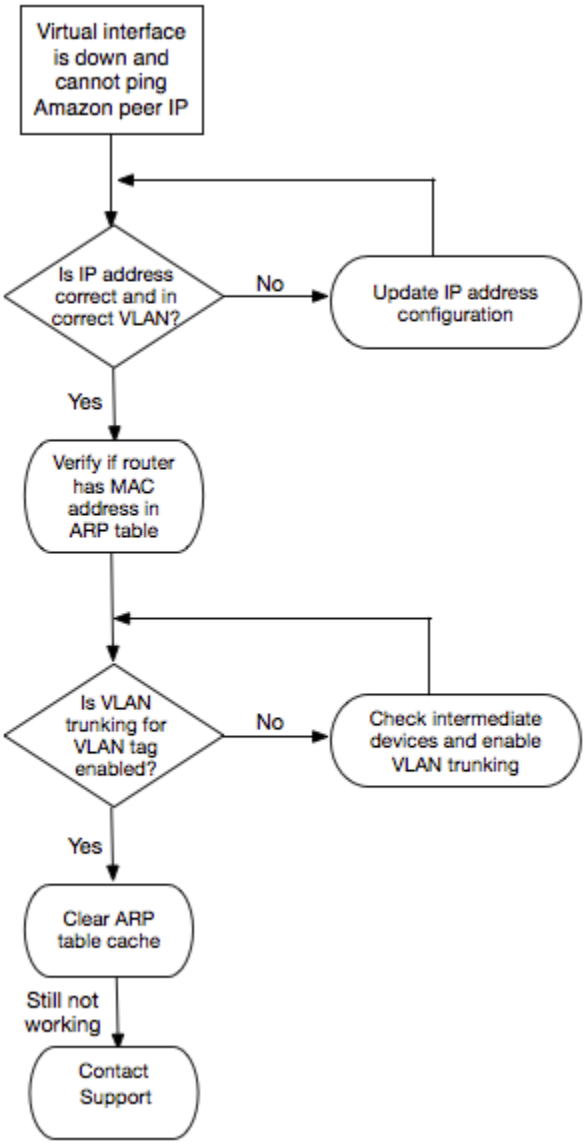

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

Pemecahan masalah lapisan 2 (tautan data)

Jika koneksi AWS Direct Connect fisik Anda naik tetapi antarmuka virtual Anda sedang down, gunakan langkah-langkah berikut untuk memecahkan masalah.

1. Jika Anda tidak dapat melakukan ping ke alamat IP peer Amazon, pastikan alamat IP peer Anda dikonfigurasi dengan benar dan dalam VLAN yang benar. Pastikan alamat IP dikonfigurasi dalam subinterface VLAN dan bukan antarmuka fisik (misalnya, GigabitEthernet 0/0.123 bukan 0/0). GigabitEthernet
2. Verifikasi apakah router memiliki entri alamat MAC dari AWS titik akhir dalam tabel protokol resolusi alamat (ARP) Anda.
3. Pastikan bahwa setiap perangkat perantara antara titik akhir memiliki trunking VLAN yang diaktifkan untuk tanda VLAN 802.1Q Anda. ARP tidak dapat dibuat di AWS samping sampai AWS menerima lalu lintas yang ditandai.
4. Hapus cache tabel ARP atau penyedia Anda.
5. Jika langkah-langkah di atas tidak membuat ARP atau Anda masih tidak dapat melakukan ping ke IP peer Amazon, hubungi Support AWS.

Bagan alir berikut berisi langkah-langkah untuk mendiagnosis masalah dengan tautan data.



Jika sesi BGP masih belum ditetapkan setelah memverifikasi langkah-langkah ini, lihat Pemecahan masalah lapisan 3/4 (Jaringan/Transportasi). Jika sesi BGP didirikan tetapi Anda mengalami masalah perutean, lihat Masalah perutean pemecahan masalah.

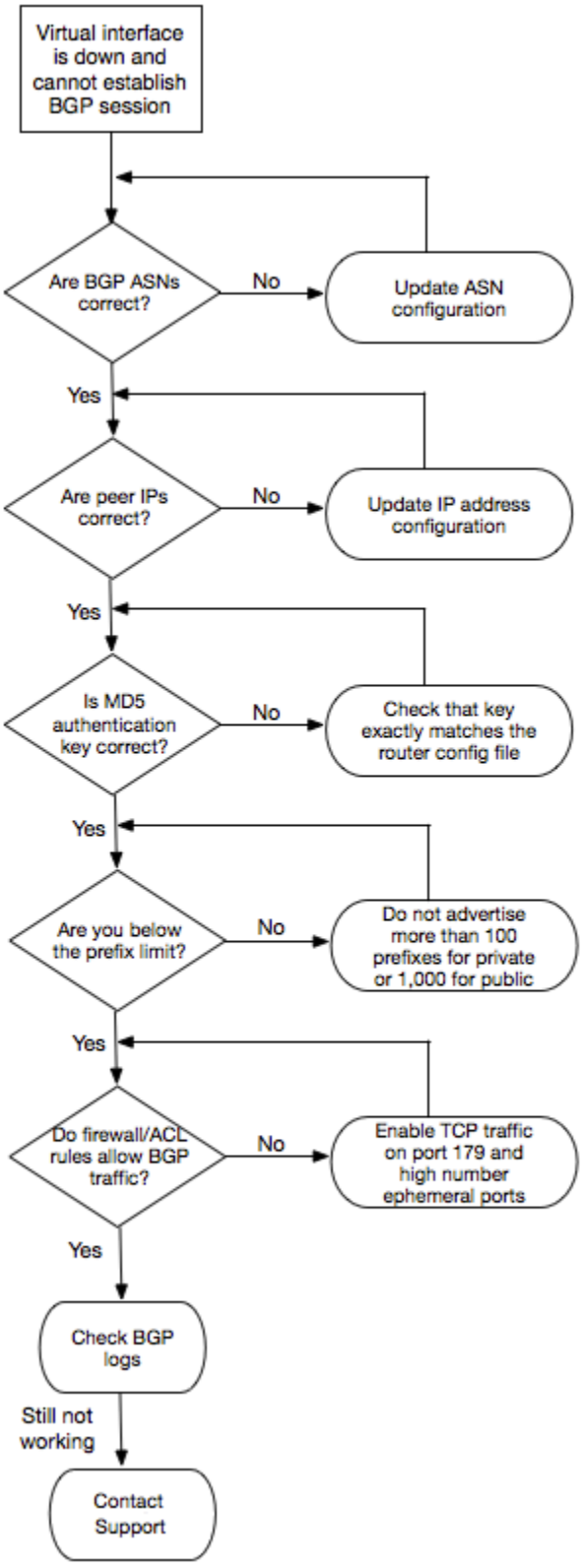
Pemecahan masalah lapisan 3/4 (Jaringan/Transportasi)

Pertimbangkan situasi di mana koneksi AWS Direct Connect fisik Anda aktif dan Anda dapat melakukan ping ke alamat IP peer Amazon. Jika antarmuka virtual Anda aktif dan sesi peering BGP tidak dapat dibuat, gunakan langkah-langkah berikut untuk memecahkan masalah:

1. Pastikan Autonomous System Number (ASN) lokal BGP Anda dan ASN Amazon dikonfigurasi dengan benar.

2. Pastikan bahwa peer IPs untuk kedua sisi sesi peering BGP dikonfigurasi dengan benar.
3. Pastikan kunci MD5 otentikasi Anda dikonfigurasi dan sama persis dengan kunci dalam file konfigurasi router yang diunduh. Pastikan tidak ada spasi atau karakter tambahan.
4. Pastikan Anda atau penyedia Anda tidak mengiklankan lebih dari 100 prefiks untuk antarmuka virtual privat atau 1.000 prefiks untuk antarmuka virtual publik. Ini adalah batasan yang sulit dan tidak dapat dilampaui.
5. Pastikan tidak ada aturan firewall atau ACL yang memblokir port TCP 179 atau port TCP ephemeral bernomor tinggi. Port ini diperlukan untuk BGP untuk membuat koneksi TCP antara rekan-rekan.
6. Periksa log BGP Anda untuk kesalahan atau pesan peringatan.
7. Jika langkah-langkah di atas tidak menetapkan sesi peering BGP, hubungi Support. AWS

Bagan alir berikut berisi langkah-langkah untuk mendiagnosis masalah dengan sesi peering BGP.



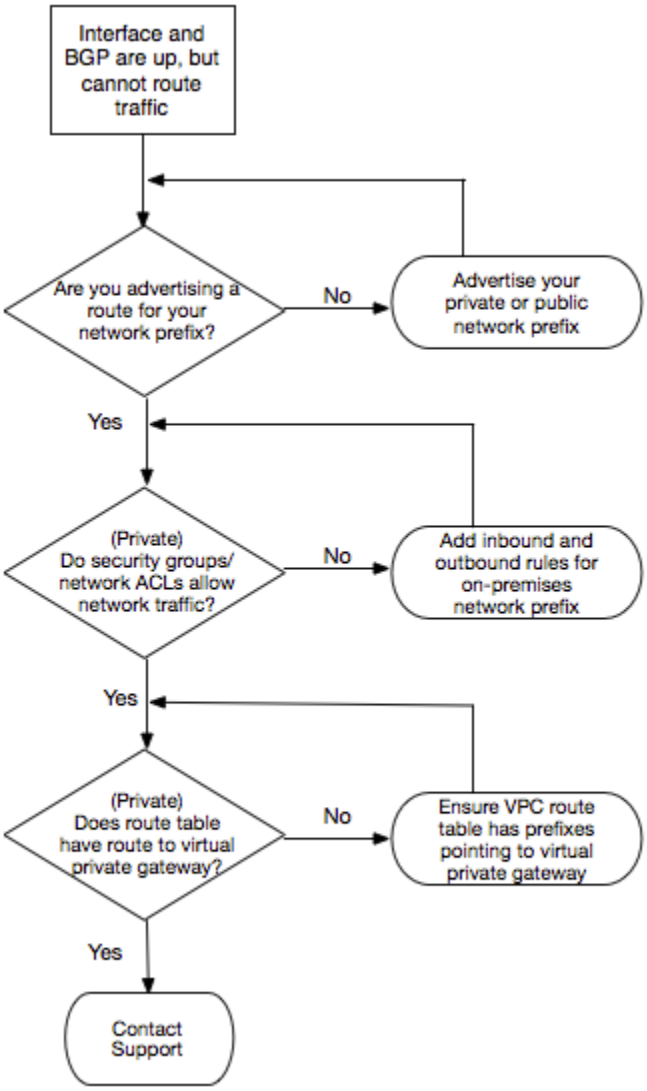
Jika sesi peering BGP dibuat tetapi Anda mengalami masalah perutean, lihat Masalah perutean pemecahan masalah.

Masalah perutean pemecahan masalah

Pertimbangkan situasi di mana antarmuka virtual Anda aktif dan Anda telah membuat sesi peering BGP. Jika Anda tidak dapat mengarahkan lalu lintas melalui antarmuka virtual, gunakan langkah-langkah berikut untuk memecahkan masalah:

1. Pastikan Anda mengiklankan rute untuk prefiks jaringan lokal Anda selama sesi BGP. Untuk antarmuka virtual privat, ini bisa menjadi prefiks jaringan privat atau publik. Untuk antarmuka virtual publik, ini harus menjadi prefiks jaringan Anda yang dapat dirutekan secara publik.
2. Untuk antarmuka virtual pribadi, pastikan grup dan jaringan keamanan VPC Anda ACLs mengizinkan lalu lintas masuk dan keluar untuk awalan jaringan lokal Anda. Untuk informasi selengkapnya, lihat Grup Keamanan dan Jaringan ACLs di Panduan Pengguna Amazon VPC.
3. Untuk antarmuka virtual privat, pastikan bahwa tabel rute VPC Anda memiliki prefiks yang mengarah ke virtual private gateway yang terhubung dengan antarmuka virtual privat Anda. Misalnya, jika Anda lebih suka agar semua lalu lintas dirutekan ke jaringan lokal secara default, Anda dapat menambahkan rute default (0.0.0.0/0 atau ::/0) dengan virtual private gateway sebagai target di VPC Anda tabel rute.
   - Atau, aktifkan propagasi rute untuk memperbarui rute secara otomatis di tabel rute Anda berdasarkan iklan rute BGP dinamis Anda. Anda dapat memiliki hingga 100 rute yang disebarkan per tabel rute. Batas ini tidak dapat ditingkatkan. Untuk informasi lebih lanjut, lihat Mengaktifkan dan Menonaktifkan Propagasi Rute di Panduan Pengguna Amazon VPC.
4. Jika langkah-langkah di atas tidak menyelesaikan masalah perutean Anda, hubungi AWS Support.

Bagan alir berikut berisi langkah-langkah untuk mendiagnosis masalah perutean.


Interface and BGP are up, but cannot route traffic
Are you advertising a route for your network prefix?
No
Advertise your private or public network prefix
Yes
(Private) Do security groups/ network ACLs allow network traffic?
No
Add inbound and outbound rules for on-premises network prefix
Yes
(Private) Does route table have route to virtual private gateway?
No
Ensure VPC route table has prefixes pointing to virtual private gateway
Yes
Contact Support

Riwayat dokumen

Tabel berikut menjelaskan rilis untuk AWS Direct Connect. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Buat hubungan antara gateway Direct Connect dan jaringan AWS Network Manager inti	Anda sekarang dapat membuat asosiasi gateway Direct Connect secara langsung antara Direct Connect dan jaringan inti AWS Cloud WAN.	November 25, 2024
Support untuk 400G	Topik yang diperbarui untuk menyertakan dukungan untuk koneksi 400G.	Juli 18, 2024
Menambahkan SiteLink batas awalan	Batas awalan untuk SiteLink ditambahkan ke topik kuota dan batas.	15 Juni 2023
Support untuk SiteLink	Anda dapat membuat antarmuka virtual pribadi yang memungkinkan konektivitas antara dua titik Direct Connect dari presence (PoPs) di AWS Region yang sama.	1 Desember 2021
Support MAC Security	Anda dapat menggunakan AWS Direct Connect koneksi yang mendukung MACsec untuk mengenkripsi data Anda dari pusat data perusahaan Anda ke AWS Direct Connect lokasi.	31 Maret 2021

Support untuk 100G	Topik yang diperbarui untuk menyertakan dukungan untuk koneksi khusus 100G.	12 Februari 2021
Lokasi baru di Italia	Topik yang diperbarui untuk memasukkan penambahan lokasi baru di Italia.	22 Januari 2021
Lokasi baru di Israel	Topik diperbarui untuk memasukkan penambahan lokasi baru di Israel.	7 Juli 2020
Dukungan Pengujian Failover Toolkit Ketahanan	Gunakan fitur Resiliency Toolkit Failover Testing untuk menguji ketahanan koneksi Anda.	3 Juni 2020
CloudWatch Dukungan metrik VIF	Anda dapat memantau AWS Direct Connect koneksi fisik, dan antarmuka virtual, menggunakan CloudWatch.	11 Mei 2020
AWS Direct Connect Toolkit Ketahanan	AWS Direct Connect Resiliency Toolkit menyediakan wizard koneksi dengan beberapa model ketahanan yang membantu Anda memesan koneksi khusus untuk mencapai tujuan SLA Anda.	7 Oktober 2019
Dukungan Wilayah tambahan untuk Support untuk AWS Transit Gateway seluruh akun	Dukungan Wilayah tambahan untuk AWS Transit Gateway seluruh akun.	30 September 2019

AWS Direct Connect dukungan untuk AWS Transit Gateway	Anda dapat menggunakan AWS Direct Connect gateway untuk menghubungkan AWS Direct Connect koneksi Anda melalui antarmuka virtual transit ke VPCs atau VPNs terhubung ke gateway transit Anda. Anda mengaitkan gateway Direct Connect dengan transit gateway. Kemudian, buat antarmuka virtual transit untuk AWS Direct Connect koneksi Anda ke gateway Direct Connect.	27 Maret 2019
Dukungan bingkai jumbo	Anda dapat mengirim bingkai jumbo (9001 MTU). AWS Direct Connect	11 Oktober 2018
Komunitas BGP preferensi lokal	Anda dapat menggunak an tanda komunitas BGP preferensi lokal untuk mendapatkan penyeimba ngan beban dan preferensi rute untuk lalu lintas masuk ke jaringan Anda.	6 Februari 2018
AWS Direct Connect pintu gerbang	Anda dapat menggunakan gateway Direct Connect untuk menghubungkan AWS Direct Connect koneksi Anda ke VPCs Wilayah terpencil.	1 November 2017
CloudWatch Metrik Amazon	Anda dapat melihat CloudWatch metrik untuk AWS Direct Connect koneksi Anda.	29 Juni 2017

Tautkan grup agregasi	Anda dapat membuat grup agregasi tautan (LAG) untuk menggabungkan beberapa AWS Direct Connect koneksi.	13 Februari 2017
IPv6 dukungan	Antarmuka virtual Anda sekarang dapat mendukung sesi IPv6 peering BGP.	1 Desember 2016
Dukungan penandaan	Anda sekarang dapat menandai AWS Direct Connect sumber daya Anda.	4 November 2016
Layanan mandiri LOA-CFA	Anda sekarang dapat mengunduh Letter of Authorization and Connecting Facility Assignment (LOA-CFA) menggunakan konsol atau API. AWS Direct Connect	22 Juni 2016
Lokasi baru di Silicon Valley	Topik yang diperbarui untuk menyertakan penambahan lokasi Silicon Valley baru di Wilayah US West (N. California).	Juni 3, 2016
Lokasi baru di Amsterdam	Topik yang diperbarui untuk menyertakan penambahan lokasi Amsterdam baru di Wilayah Eropa (Frankfurt).	Mei 19, 2016
Lokasi baru di Portland, Oregon, dan Singapura	Topik yang diperbarui untuk menyertakan penambahan lokasi Portland, Oregon, dan Singapura baru di US West (Oregon) dan Asia Pacific (Singapore).	27 April 2016

Lokasi baru di Sao Paulo, Brasil	Topik yang diperbarui untuk untuk menyertakan penambahan lokasi Sao Paulo baru di Wilayah South America (São Paulo).	9 Desember 2015
Lokasi baru di Dallas, London, Silicon Valley, dan Mumbai	Topik yang diperbarui untuk memasukkan penambahan lokasi baru di Dallas (Wilayah AS Timur (Virginia N.)), Wilayah London (Eropa (Irlandia)), Lembah Silikon (Wilayah AWS GovCloud (AS-Barat)), dan Wilayah Mumbai (Asia Pasifik (Singapura)).	27 November 2015
Lokasi baru di Wilayah Tiongkok (Beijing)	Topik terbaru untuk menyertakan penambahan lokasi Beijing baru di Wilayah China (Beijing) .	April 14, 2015
Lokasi Las Vegas baru di Wilayah Barat AS (Oregon)	Topik yang diperbarui untuk memasukkan penambahan lokasi AWS Direct Connect Las Vegas baru di Wilayah Barat AS (Oregon).	10 November 2014
Wilayah Uni Eropa Baru (Frankfurt)	Topik yang diperbarui untuk memasukkan penambahan AWS Direct Connect lokasi baru yang melayani Wilayah UE (Frankfurt).	23 Oktober 2014

Lokasi baru di Wilayah Asia Pasifik (Sydney)	Topik yang diperbarui untuk memasukkan penambahan AWS Direct Connect lokasi baru yang melayani Wilayah Asia Pasifik (Sydney).	Juli 14, 2014
Support untuk AWS CloudTrail	Menambahkan topik baru untuk menjelaskan bagaimana Anda dapat menggunakan CloudTrail untuk login aktivitas AWS Direct Connect.	April 4, 2014
Support untuk mengakses Wilayah terpencil AWS	Penambahan topik baru untuk menjelaskan bagaimana Anda dapat mengakses sumber daya publik di Wilayah jarak jauh.	19 Desember 2013
Support untuk koneksi yang di-host	Topik yang diperbarui untuk menyertakan dukungan untuk koneksi yang di-host.	Oktober 22, 2013
Lokasi baru di Wilayah UE (Irlandia)	Topik yang diperbarui untuk memasukkan penambahan AWS Direct Connect lokasi baru yang melayani Wilayah UE (Irlandia).	24 Juni 2013
Lokasi Seattle baru di Wilayah Barat AS (Oregon)	Topik yang diperbarui untuk memasukkan penambahan AWS Direct Connect lokasi baru di Seattle yang melayani Wilayah Barat AS (Oregon).	8 Mei 2013
Support untuk menggunakan IAM dengan AWS Direct Connect	Menambahkan topik tentang menggunakan AWS Identity and Access Management dengan AWS Direct Connect.	21 Desember 2012

Wilayah Asia Pasifik Baru (Sydney)	Topik yang diperbarui untuk memasukkan penambahan AWS Direct Connect lokasi baru yang melayani Wilayah Asia Pasifik (Sydney).	14 Desember 2012
AWS Direct Connect Konsol baru, dan Wilayah AS Timur (Virginia N.) dan Amerika Selatan (Sao Paulo)	Mengganti Panduan AWS Direct Connect Memulai dengan Panduan AWS Direct Connect Pengguna. Menambahkan topik baru untuk membahas AWS Direct Connect konsol baru, menambahkan topik penagihan, menambahkan informasi konfigurasi router, dan topik yang diperbarui untuk menyertakan penambahan dua AWS Direct Connect lokasi baru yang melayani Wilayah AS Timur (Virginia N.) dan Amerika Selatan (Sao Paulo).	Agustus 13, 2012
Dukungan untuk Wilayah UE (Irlandia), Asia Pasifik (Singapura), dan Asia Pasifik (Tokyo)	Menambahkan bagian pemecahan masalah baru dan topik yang diperbarui untuk memasukkan penambahan empat AWS Direct Connect lokasi baru yang melayani Wilayah AS Barat (California Utara), UE (Irlandia), Asia Pasifik (Singapura), dan Asia Pasifik (Tokyo).	Januari 10, 2012

Support untuk Wilayah AS Barat (California Utara)	Topik terbaru untuk menyertakan penambahan Wilayah US West (Northern California).	September 8, 2011
Rilis publik	Rilis pertama AWS Direct Connect.	3 Agustus 2011

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