Panduan Pengguna

AWS Direct Connect

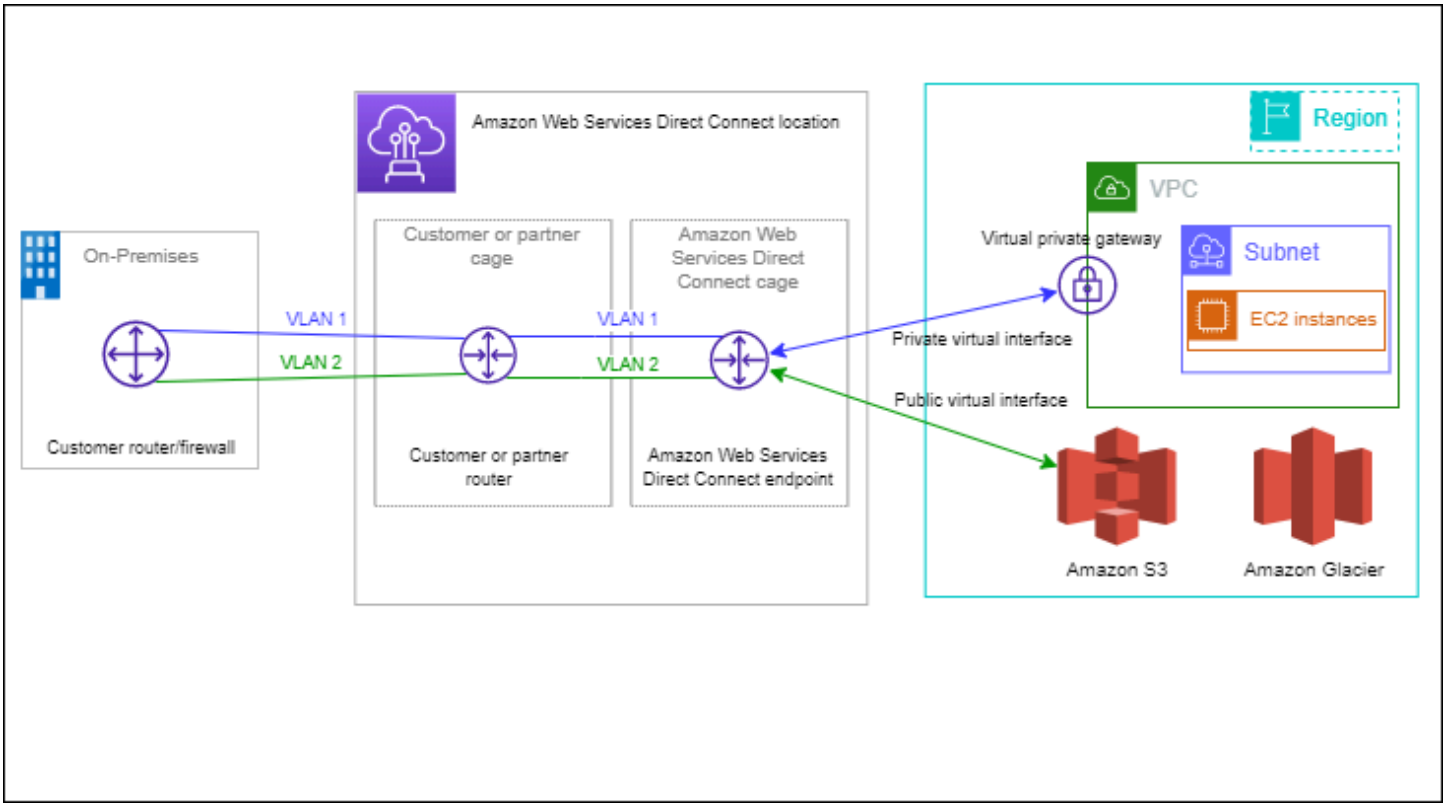
AWS Direct Connect: Panduan Pengguna

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.

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



Daftar Isi

- Perawatan Direct Connect
- Mengakses Wilayah AWS jarak jauh
- Kebijakan perutean dan komunitas BGP

AWS Direct Connect komponen

Berikut ini adalah komponen kunci yang Anda gunakan untuk AWS 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.

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. Untuk informasi selengkapnya, lihat Antarmuka virtual AWS Direct Connect dan Prasyarat untuk antarmuka virtual.

Persyaratan jaringan

Untuk digunakan AWS Direct Connect di suatu AWS Direct Connect lokasi, jaringan Anda harus memenuhi salah satu dari 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 Ethernet 1 gigabit, transceiver 10GBASE-LR (1310 nm) untuk 10 gigabit, atau 100GBASE-LR4 untuk Ethernet 100 gigabit.

- Negosiasi otomatis untuk port harus dinonaktifkan untuk 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 antarmuka virtual Anda tetap down, lihatPemecahan masalah lapisan 2 (tautan data).
- Enkapsulasi VLAN 802.1Q harus didukung di seluruh koneksi, termasuk perangkat perantara.
- Perangkat Anda harus mendukung autentikasi Border Gateway Protocol (BGP) dan BGP MD5.
- (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 komunikasi IPv4 dan IPv6. Alamat IPv6 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 Mengatur MTU jaringan untuk antarmuka virtual privat atau antarmuka virtual transit.

Harga untuk AWS 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, instans EC2 Klasik, atau lalu lintas EC2 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.

AWS Direct Connect pemeliharaan

AWS Direct Connect adalah layanan yang dikelola sepenuhnya di mana secara berkala, Direct Connect melakukan aktivitas pemeliharaan pada armada perangkat keras yang mendukung layanan tersebut. Koneksi Direct Connect disediakan pada perangkat keras mandiri yang memungkinkan Anda membuat koneksi jaringan yang sangat tangguh antara Amazon Virtual Private Cloud dan infrastruktur lokal Anda. Kemampuan ini memungkinkan Anda untuk mengakses AWS sumber daya Anda dengan cara yang andal, terukur, dan hemat biaya. Untuk informasi lebih lanjut, lihat Rekomendasi AWS Direct Connect Ketahanan.

Ada dua jenis perawatan Direct Connect: pemeliharaan terencana dan darurat:

- Pemeliharaan yang direncanakan. Pemeliharaan yang direncanakan dijadwalkan sebelumnya untuk meningkatkan ketersediaan dan menghadirkan fitur baru. Jenis pemeliharaan ini dijadwalkan selama jendela pemeliharaan di mana kami menyediakan tiga pemberitahuan: 14 hari kalender, 7 hari kalender, dan 1 hari kalender.

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

- Perawatan darurat. Pemeliharaan darurat dimulai secara kritis karena layanan yang berdampak pada kegagalan yang memerlukan tindakan segera AWS untuk memulihkan layanan. Jenis perawatan ini tidak direncanakan sebelumnya. Pelanggan yang terkena dampak diberitahu tentang perawatan darurat hingga 60 menit sebelum pemeliharaan.

Kami menyarankan Anda mengikuti Rekomendasi AWS Direct Connect Ketahanan sehingga Anda dapat dengan anggun dan proaktif mengalihkan lalu lintas ke koneksi koneksi Langsung yang berlebihan selama pemeliharaan. Kami juga menyarankan agar Anda secara proaktif menguji ketahanan koneksi redundan Anda secara teratur untuk memvalidasi bahwa failover berfungsi sebagaimana dimaksud. Dengan menggunakan the section called “Pengujian Failover AWS Direct Connect” fungsionalitas, Anda dapat memverifikasi bahwa rute lalu lintas Anda melalui salah satu antarmuka virtual Anda yang berlebihan.

Untuk panduan seputar kriteria kelayakan untuk memulai permintaan pembatalan pemeliharaan yang direncanakan, lihat Bagaimana cara membatalkan acara pemeliharaan Direct Connect? .

> **Note**
>
> Permintaan pemeliharaan darurat tidak dapat dibatalkan karena AWS harus segera bertindak untuk memulihkan layanan.

Untuk informasi selengkapnya tentang peristiwa pemeliharaan, lihat Acara pemeliharaan di AWS Direct Connect FAQ.

Perawatan Direct Connect

AWS Direct Connect adalah layanan yang dikelola sepenuhnya di mana secara berkala, Direct Connect melakukan aktivitas pemeliharaan pada armada perangkat keras yang mendukung layanan tersebut. Koneksi Direct Connect disediakan pada perangkat keras mandiri yang memungkinkan Anda membuat koneksi jaringan yang sangat tangguh antara Amazon Virtual Private Cloud dan infrastruktur lokal Anda. Kemampuan ini memungkinkan Anda untuk mengakses AWS sumber daya Anda dengan cara yang andal, terukur, dan hemat biaya. Untuk informasi lebih lanjut, lihat Rekomendasi AWS Direct Connect Ketahanan.

Ada dua jenis perawatan Direct Connect: pemeliharaan terencana dan darurat:

- Pemeliharaan yang direncanakan. Pemeliharaan yang direncanakan dijadwalkan sebelumnya untuk meningkatkan ketersediaan dan menghadirkan fitur baru. Jenis pemeliharaan ini dijadwalkan selama jendela pemeliharaan di mana kami menyediakan tiga pemberitahuan: 10 hari kalender, hari 5 kalender, dan 1 hari kalender.

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

- Perawatan darurat. Pemeliharaan darurat dimulai secara kritis karena layanan yang berdampak pada kegagalan yang memerlukan tindakan segera AWS untuk memulihkan layanan. Jenis perawatan ini tidak direncanakan sebelumnya. Pelanggan yang terkena dampak diberitahu tentang perawatan darurat hingga 60 menit sebelum pemeliharaan.

Selama acara pemeliharaan, AWS berhenti beriklan atau menerima rute. Sesi BGP biasanya tetap aktif selama acara (kecuali perangkat perlu di-restart), jadi sebaiknya Anda mengandalkan BGP untuk failover daripada menggunakan rute statis dengan pelacakan status tautan.

Kami menyarankan Anda mengikuti Rekomendasi AWS Direct Connect Ketahanan sehingga lalu lintas dapat dengan anggun dan proaktif ke koneksi koneksi Langsung Anda yang berlebihan selama pemeliharaan. Kami juga menyarankan agar Anda secara proaktif menguji ketahanan koneksi redundan Anda secara teratur untuk memvalidasi bahwa failover berfungsi sebagaimana dimaksud. Dengan menggunakan the section called “Pengujian Failover AWS Direct Connect” fungsionalitas, Anda dapat memverifikasi bahwa rute lalu lintas Anda melalui salah satu antarmuka virtual Anda yang berlebihan.

Untuk panduan seputar kriteria kelayakan untuk memulai permintaan pembatalan pemeliharaan yang direncanakan, lihat Bagaimana cara membatalkan acara pemeliharaan Direct Connect? .

> **Note**
>
> Permintaan pemeliharaan darurat tidak dapat dibatalkan karena AWS harus segera bertindak untuk memulihkan layanan.

Untuk informasi selengkapnya tentang peristiwa pemeliharaan, lihat Acara pemeliharaan di AWS Direct Connect FAQ.

Mengakses Wilayah AWS jarak jauh

Lokasi AWS Direct Connect di Wilayah publik atau AWS GovCloud (US) dapat mengakses layanan publik di Wilayah publik lainnya (tidak termasuk China (Beijing dan Ningxia)). Selain itu, koneksi AWS Direct Connect di Wilayah publik atau AWS GovCloud (US) dapat dikonfigurasi untuk mengakses VPC di akun Anda di Wilayah publik lainnya (tidak termasuk China (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 global AWS, terlepas dari apakah Anda mengakses layanan AWS 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.

Mengakses layanan publik di Wilayah jarak jauh

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 AWS Direct Connect.

Setelah membuat antarmuka virtual publik dan membuat sesi BGP, router Anda mempelajari rute Wilayah AWS publik lainnya. Untuk informasi selengkapnya tentang prefiks yang saat ini diiklankan olehAWS, lihat AWSCamera Alamat IP dalam prefiks Referensi Umum Amazon Web Services.

Mengakses VPC di Wilayah jarak jauh

Anda dapat membuat gateway Direct Connect di Wilayah publik mana saja. Gunakan untuk menghubungkan koneksi AWS Direct Connect melalui antarmuka virtual privat bagi VPC di akun Anda yang berlokasi di Wilayah yang berbeda atau ke transit gateway. Untuk informasi selengkapnya, lihat Bekerja dengan gateway Direct Connect.

Selain itu, Anda dapat membuat antarmuka virtual publik untuk koneksi AWS Direct Connect lalu membuat koneksi VPN ke VPC Anda di Wilayah jarak jauh. Untuk informasi selengkapnya tentang mengonfigurasi konektivitas VPN ke VPC, lihat Skenario untuk Menggunakan Amazon Virtual Private Cloud dalam Panduan Pengguna Amazon VPC.

Opsi Konektivitas Jaringan ke Amazon VPC

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

- Konektivitas Amazon Virtual Private Cloud

Kebijakan perutean 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 IPv4 publik atau awalan IPv6 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 China hanya diiklankan di Wilayah AWS China. 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 sejawat dengan Jaringan AWS Global
  - Penyedia transit Amazon

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 awalan IPv4 atau IPv6 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 akan memuat berbagi di beberapa transit atau antarmuka virtual pribadi ketika awalan memiliki panjang dan atribut BGP yang sama.

Antarmuka virtual privat dan transit komunitas BGP antarmuka virtual

Saat Wilayah AWS merutekan lalu lintas ke lokasi lokal melalui antarmuka virtual private atau transit Direct Connect, lokasi Direct Connect Wilayah AWS yang terkait memengaruhi kemampuan untuk menggunakan perutean multi-jalur (ECMP) dengan biaya sama. 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.

Ketika tidak ada tag komunitas preferensi lokal yang diterapkan, Direct Connect mendukung ECMP melalui antarmuka virtual pribadi atau transit untuk awalan dengan panjang yang sama, panjang AS_PATH, dan nilai MED 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 atau Active/Passive Direct Connect dari AWS 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.

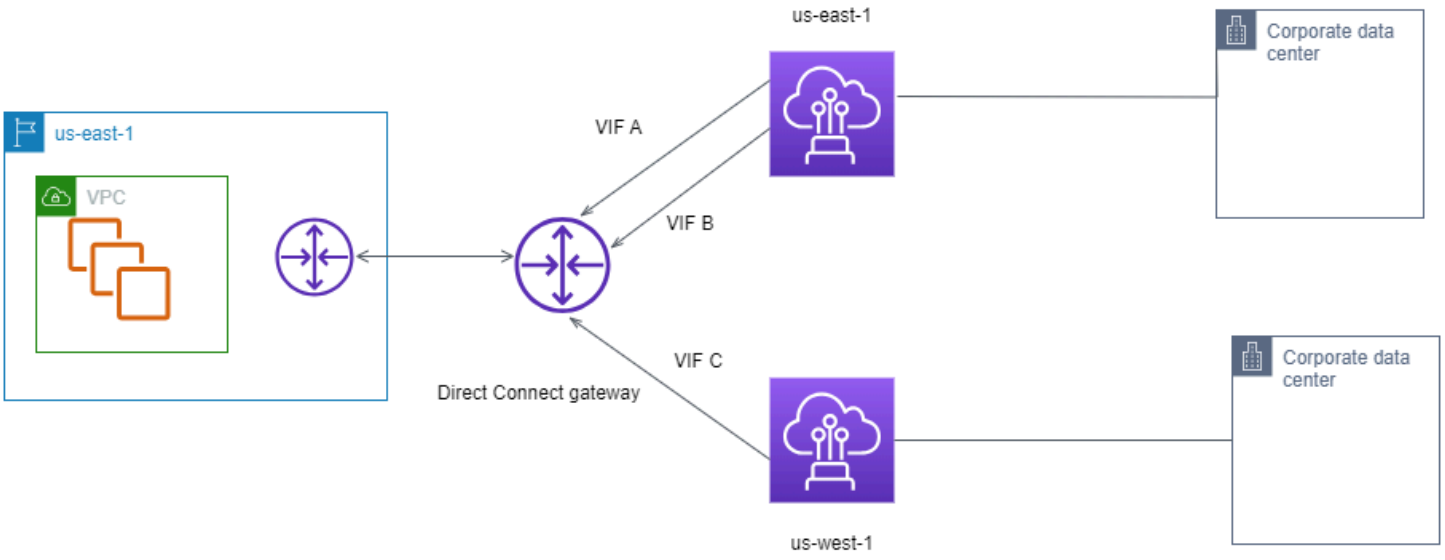
Preferensi lokal tanda komunitas BGP dievaluasi sebelum atribut AS_PATH, dan dievaluasi dalam urutan dari terendah ke preferensi tertinggi (di mana preferensi tertinggi lebih disukai).

Contoh perutean antarmuka virtual privat

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 VIF pribadi (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.

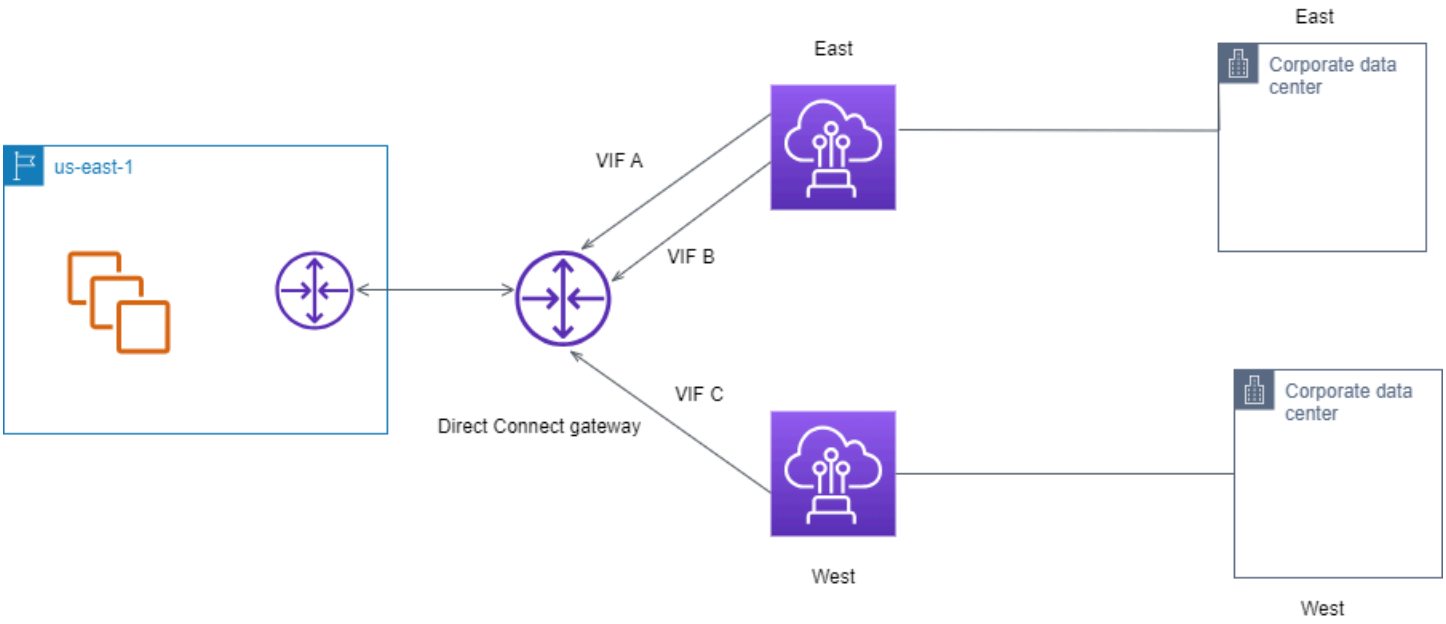
VIF memiliki konfigurasi berikut:

- 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



Menggunakan Kit Alat Ketahanan AWS Direct Connect untuk memulai

AWS menawarkan pelanggan kemampuan untuk mencapai koneksi jaringan yang sangat tangguh antara Amazon Virtual Private Cloud (Amazon VPC) dan infrastruktur on-premise mereka. Kit Alat Ketahanan AWS Direct Connect 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, lalu Kit Alat Ketahanan AWS Direct Connect memandu Anda melalui proses pemesanan koneksi khusus. Model ketahanan dirancang untuk memastikan bahwa Anda memiliki jumlah koneksi khusus yang sesuai di beberapa lokasi.

Kit Alat Ketahanan AWS Direct Connect memiliki manfaat 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.
- Menyetujui koneksi khusus secara otomatis ketika Anda memiliki akun AWS dan memilih Partner AWS Direct Connect yang diketahui. Letter of Authority (LOA) tersedia untuk pengunduhan segera.
- Membuat tiket dukungan secara otomatis untuk persetujuan koneksi khusus ketika Anda adalah pelanggan baru AWS, atau Anda memilih partner yang tidak diketahui (Lainnya).
- 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 (LAG), dan menambahkan jumlah koneksi khusus yang sesuai ke LAG saat Anda memilih kecepatan selain 1 Gbps, 10 Gbps, atau 100 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 “Pengujian Failover AWS Direct Connect”.

- Menyediakan CloudWatch metrik Amazon untuk koneksi dan antarmuka virtual. Untuk informasi selengkapnya, lihat Pemantauan.

Model ketahanan berikut tersedia di Kit Alat Ketahanan 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 Kit Alat Ketahanan AWS Direct Connect untuk memesan koneksi khusus guna mencapai tujuan SLA.

Setelah Anda memilih model ketahanan, Kit Alat Ketahanan AWS Direct Connect 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 single-mode: transceiver 1000BASE-LX (1310 nm) untuk Ethernet 1 gigabit, transceiver 10GBASE-LR (1310 nm) untuk 10 gigabit, atau 100GBASE-LR4 untuk Ethernet 100 gigabit.

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

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

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

- Jaringan Anda harus menggunakan serat single-mode dengan transceiver 1000BASE-LX (1310 nm) untuk Ethernet 1 gigabit, transceiver 10GBASE-LR (1310 nm) untuk 10 gigabit, atau 100GBASE-LR4 untuk Ethernet 100 gigabit.
- Negosiasi otomatis untuk port harus dinonaktifkan untuk 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 antarmuka virtual Anda tetap down, lihatPemecahan masalah lapisan 2 (tautan data).
- Enkapsulasi VLAN 802.1Q harus didukung di seluruh koneksi, termasuk perangkat perantara.
- Perangkat Anda harus mendukung autentikasi Border Gateway Protocol (BGP) dan BGP MD5.
- (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.

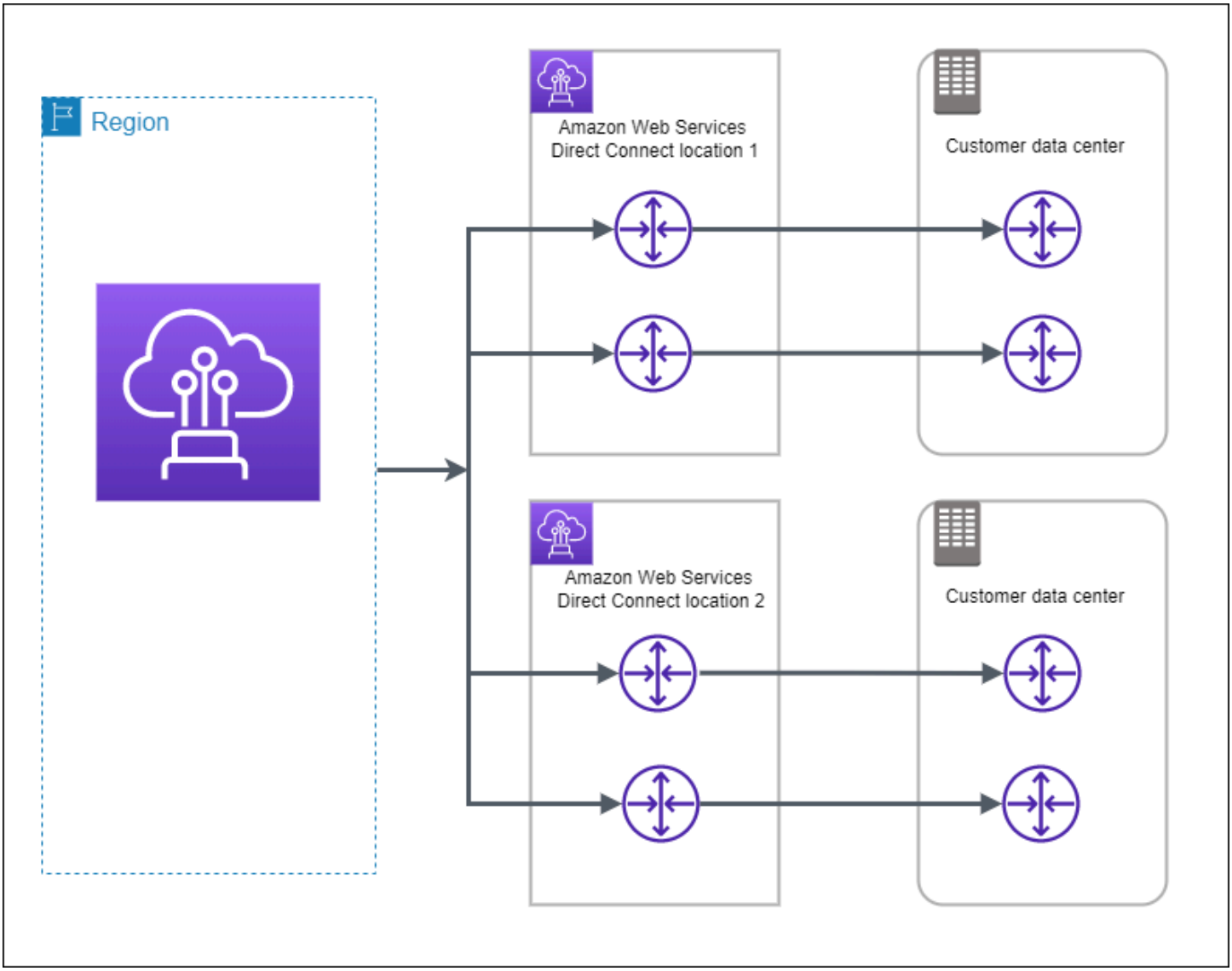
Pastikan Anda memiliki informasi berikut sebelum memulai konfigurasi:

- 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 yang mengarah ke lokasi AWS Direct Connect yang sama. Secara opsionla, Anda dapat membuat setiap koneksi dari pusat data pelanggan mengarah ke lokasi yang berbeda.



Prosedur berikut menunjukkan cara menggunakan Kit Alat Ketahanan AWS Direct Connect untuk mengonfigurasi model ketahanan maksimum.

Topik

- Langkah 1: Mendaftar di 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 di AWS

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

Mendaftar Akun AWS

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

Untuk mendaftar Akun AWS

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

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

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

AWS akan mengirimkan email konfirmasi kepada Anda setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun saat ini dan mengelola akun dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Membuat pengguna administratif

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

Mengamankan Pengguna root akun AWS Anda

1. Masuk ke AWS Management Console sebagai pemilik akun dengan memilih Pengguna root dan memasukkan alamat email Akun AWS Anda. Di halaman berikutnya, masukkan kata sandi Anda.

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

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

Membuat pengguna 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 sebuah pengguna administratif.

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

Masuk sebagai pengguna administratif

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

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

Langkah 2: Mengonfigurasi model ketahanan

Untuk mengonfigurasi model ketahanan maksimum

1. Buka konsol AWS Direct Connect 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 location service pertama, pilih lokasi AWS Direct Connect 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 (MMR) 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 location service kedua, pilih lokasi AWS Direct Connect 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 (MMR) 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.

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

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

   Jika LOA sudah siap, Anda dapat memilih Unduh LOA, lalu klik Lanjutkan.

   AWS memerlukan waktu hingga 72 jam 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 di 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 layanan AWS publik yang tidak ada di 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 privat untuk terhubung ke tiga VPC.

Sebelum memulai, pastikan Anda memiliki informasi berikut:

Sumber Daya	Informasi yang diperlukan
Koneksi	Koneksi AWS Direct Connect atau grup agregasi tautan (LAG) yang Anda buat antarmuka virtualnya.
Nama antarmuka virtual	Nama untuk antarmuka virtual.
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID akun AWS dari akun lainnya.
(Antarmuka virtual privat saja) Koneksi	Untuk terhubung ke VPC di Wilayah AWS yang sama, Anda memerluka n virtual private gateway 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, Partner AWS Direct Connect 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 satunya (dual-stack). Jangan gunakan IP Elastis (EIP) atau Bawa alamat IP Anda sendiri (BYOIP) dari Amazon Pool untuk membuat antarmuka

Sumber Daya	Informasi yang diperlukan
	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: • (Antarmuka virtual publik saja) Anda harus menentukan alamat IPv4 publik yang unik yang Anda miliki. Nilai dapat menjadi salah satu dari yang berikut: • IPv4 CIDR milik pelanggan Ini bisa berupa IP publik (milik pelanggan atau disediakan olehAWS), 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 AWSSupport untuk meminta IPv4 CIDR publik (dan berikan kasus penggunaan dalam permintaan Anda) **Note** Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk alamat AWS IPv4 publik yang disediakan. • (Antarmuka virtual privat saja) Amazon dapat menghasilkan alamat IPv4 privat untuk Anda. Jika Anda menentukan sendiri, pastikan Anda menentukan CIDR pribadi untuk antarmuka router Anda dan antarmuka Direct AWS Connect saja. Misalnya, jangan tentukan alamat IP lain dari

Sumber Daya	Informasi yang diperlukan
	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 CIDR IPv6 /125. Anda tidak dapat menentukan alamat IPv6 peer Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan melalui IPv4 atau 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 mengaktifkan MD5 secara default. Anda tidak dapat mengubah opsi ini. • Kunci autentikasi 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	Rute IPv4 atau rute IPv6 publik untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: CIDR IPv4 dapat tumpang tindih dengan CIDR IPv4 publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari hal berikut ini benar:
	  • CIDR berasal dari Wilayah AWS yang berbeda. 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.
	• IPv6: Tentukan panjang prefiks /64 atau lebih pendek.
	• 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.
	• Anda dapat menentukan panjang awalan apa pun melalui antarmuka virtual publik Direct Connect. IPv4 harus mendukung apa pun dari /1 - /32, dan IPv6 harus mendukung apa pun dari /1 - /64.

Sumber Daya	Informasi yang diperlukan
(Antarmuka virtual privat saja) Bingkai Jumbo	Maximum transmission unit (MTU) paket melewati AWS Direct Connect. Default-nya 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 menambahk an 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 konsol AWS Direct Connect dan temukan Kemampuan bingkai jumbo di halaman Konfigurasi umum antarmuka virtual.
(Antarmuka virtual transit saja) Bingkai jumbo	Maximum transmission unit (MTU) paket melewati 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 instans EC2 dengan entri tabel rute statis VPC ke Lampiran Transit Gateway. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di konsol AWS Direct Connect dan temukan Kemampuan bingkai jumbo di halaman Konfigurasi umum antarmuka virtual.

Jika prefiks publik atau ASN merupakan milik ISP atau operator jaringan, kami meminta informasi tambahan dari Anda. Ini bisa berupa dokumen yang menggunakan kop surat perusahaan resmi, atau email dari nama domain perusahaan yang memverifikasi bahwa prefiks jaringan/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 konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.
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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer BGP IPv4, pilih IPv4 dan lakukan salah satu hal berikut:
      - Untuk menentukan alamat IP ini sendiri, untuk IP peer router, masukkan alamat CIDR IPv4 tujuan tempat Amazon harus mengirimkan lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat CIDR IPv4 yang akan digunakan untuk mengirim lalu lintas ke AWS.

      [IPv6] Untuk mengonfigurasi peer BGP IPv6, pilih IPv6. Alamat IPv6 peer secara otomatis ditetapkan dari kolam alamat IPv6 Amazon. Anda tidak dapat menentukan alamat IPv6 kustom.
   b. Untuk menyediakan kunci BGP Anda sendiri, masukkan kunci BGP MD5 Anda.

      Jika Anda tidak memasukkan nilai, kami menghasilkan kunci BGP.
   c. Untuk mengiklankan prefiks ke Amazon, untuk Prefiks yang ingin Anda iklankan, masukkan alamat tujuan CIDR IPv4 (dipisahkan dengan koma) tempat lalu lintas harus diarahkan melalui antarmuka virtual.
   d. (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.

7. Pilih Buat antarmuka virtual.

Untuk menyediakan antarmuka virtual privat bagi VPC

1. Buka konsol AWS Direct Connect 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 Akun AWS lainnya, lalu masukkan akun AWS.
   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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

> **Important**
>
> Jika Anda membiarkan AWS auto-menetapkan alamat IPv4, /29 CIDR akan dialokasikan dari 169.254.0.0/16 IPv4 Link-Local menurut RFC 3927 untuk konektivitas. point-to-point AWStidak merekomendasikan opsi ini jika Anda bermaksud menggunakan alamat IP rekan router pelanggan sebagai sumber dan/atau tujuan untuk lalu lintas VPC. Sebagai gantinya, Anda harus menggunakan RFC 1918 atau pengalamatan lainnya, dan tentukan sendiri alamatnya.
>
> - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
> - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat Lokal-Tautan IPv4.

[IPv6] Untuk mengonfigurasi peer BGP IPv6, pilih IPv6. Alamat IPv6 peer secara otomatis ditetapkan dari kolam alamat IPv6 Amazon. Anda tidak dapat menentukan alamat IPv6 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 telah menetapkan antarmuka virtual ke AWS Cloud atau Amazon VPC, lakukan pengujian failover antarmuka virtual untuk memverifikasi bahwa konfigurasi Anda memenuhi

persyaratan ketahanan. Untuk informasi selengkapnya, lihat the section called “Pengujian Failover AWS Direct Connect”.

Langkah 5: Memverifikasi konektivitas antarmuka virtual

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

Untuk memverifikasi koneksi antarmuka virtual Anda ke Cloud AWS

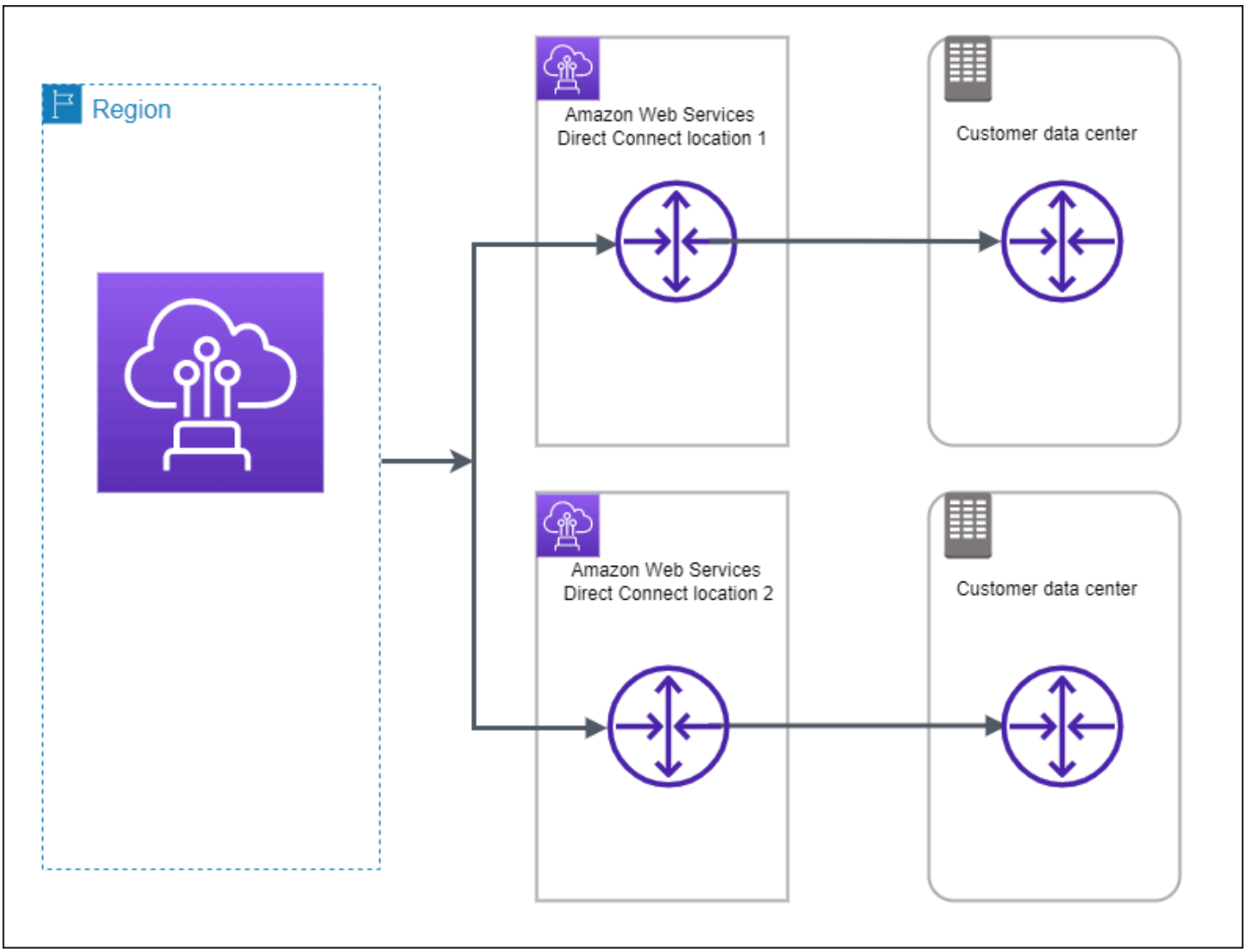
- Jalankan `traceroute` dan verifikasi bahwa pengidentifikasi AWS Direct Connect berada di jejak jaringan.

Untuk memverifikasi koneksi antarmuka virtual Anda ke Amazon VPC

1. Menggunakan AMI yang dapat di-ping, seperti Amazon Linux AMI, luncurkan instans EC2 ke VPC yang terlampir ke virtual private gateway Anda. AMI Amazon Linux tersedia di tab Quick Start saat Anda menggunakan wizard launch wizard instans di konsol Amazon EC2. Untuk informasi selengkapnya, lihat Luncurkan Instans di Panduan Pengguna Amazon EC2 untuk Instans Linux. Pastikan bahwa grup keamanan yang terkait dengan instans mencakup aturan yang mengizinkan lalu lintas ICMP masuk (untuk permintaan ping).
2. Setelah instans berjalan, dapatkan alamat IPv4 privatnya (misalnya, 10.0.0.4). Konsol Amazon EC2 akan menampilkan alamat sebagai bagian dari detail instans.
3. Ping alamat IPv4 privat dan dapatkan respons.

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.



Prosedur berikut menunjukkan cara menggunakan Kit Alat Ketahanan AWS Direct Connect untuk mengonfigurasi model ketahanan tinggi.

Topik

- Langkah 1: Mendaftar di 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 di AWS

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

Mendaftar Akun AWS

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

Untuk mendaftar Akun AWS

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

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

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

AWS akan mengirimkan email konfirmasi kepada Anda setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun saat ini dan mengelola akun dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Membuat pengguna administratif

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

Mengamankan Pengguna root akun AWS Anda

1. Masuk ke AWS Management Console sebagai pemilik akun dengan memilih Pengguna root dan memasukkan alamat email Akun AWS Anda. Di halaman berikutnya, masukkan kata sandi Anda.

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

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

Membuat pengguna 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 sebuah pengguna administratif.

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

Masuk sebagai pengguna administratif

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

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

Langkah 2: Mengonfigurasi model ketahanan

Untuk mengonfigurasi model ketahanan tinggi

1. Buka konsol AWS Direct Connect 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 location service pertama, pilih lokasi AWS Direct Connect 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 (MMR) 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 location service kedua, pilih lokasi AWS Direct Connect 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 (MMR) 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.

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

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

   Jika LOA sudah siap, Anda dapat memilih Unduh LOA, lalu klik Lanjutkan.

   AWS memerlukan waktu hingga 72 jam 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 di 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 layanan AWS publik yang tidak ada di 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 privat untuk terhubung ke tiga VPC.

Sebelum memulai, pastikan Anda memiliki informasi berikut:

Sumber Daya	Informasi yang diperlukan
Koneksi	Koneksi AWS Direct Connect atau grup agregasi tautan (LAG) yang Anda buat antarmuka virtualnya.
Nama antarmuka virtual	Nama untuk antarmuka virtual.
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID akun AWS dari akun lainnya.
(Antarmuka virtual privat saja) Koneksi	Untuk terhubung ke VPC di Wilayah AWS yang sama, Anda memerluka n virtual private gateway 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, Partner AWS Direct Connect 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 satunya (dual-stack). Jangan gunakan IP Elastis (EIP) atau Bawa alamat IP Anda sendiri (BYOIP) dari Amazon Pool untuk membuat antarmuka virtual publik. Anda tidak dapat membuat beberapa sesi BGP untuk keluarga

Sumber Daya	Informasi yang diperlukan

	pengalamatan IP yang sama pada antarmuka virtual yang sama. Cakupan alamat IP ditetapkan untuk setiap akhir antarmuka virtual untuk sesi peering BGP.
	
	• IPv4:
	  • (Antarmuka virtual publik saja) Anda harus menentukan alamat IPv4 publik yang unik yang Anda miliki. Nilai dapat menjadi salah satu dari yang berikut:
	  • IPv4 CIDR milik pelanggan
	
	  Ini bisa berupa IP publik (milik pelanggan atau disediakan olehAWS), 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 AWSSupport untuk meminta IPv4 CIDR publik (dan berikan kasus penggunaan dalam permintaan Anda)
	
	  Note
	  Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk alamat AWS IPv4 publik yang disediakan.
	  • (Antarmuka virtual privat saja) Amazon dapat menghasilkan alamat IPv4 privat untuk Anda. Jika Anda menentukan sendiri, pastikan Anda menentukan CIDR pribadi untuk antarmuka router Anda dan antarmuka Direct AWS Connect saja. Misalnya, jangan tentukan alamat IP lain dari jaringan lokal Anda. Mirip dengan antarmuka virtual publik, subnet mask

Sumber Daya	Informasi yang diperlukan
	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 CIDR IPv6 /125. Anda tidak dapat menentukan alamat IPv6 peer Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan melalui IPv4 atau 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 mengaktifkan MD5 secara default. Anda tidak dapat mengubah opsi ini. • Kunci autentikasi 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	Rute IPv4 atau rute IPv6 publik untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: CIDR IPv4 dapat tumpang tindih dengan CIDR IPv4 publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari hal berikut ini benar:
	  • CIDR berasal dari Wilayah AWS yang berbeda. 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.
	• IPv6: Tentukan panjang prefiks /64 atau lebih pendek.
	• 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.
	• Anda dapat menentukan panjang awalan apa pun melalui antarmuka virtual publik Direct Connect. IPv4 harus mendukung apa pun dari /1 - /32, dan IPv6 harus mendukung apa pun dari /1 - /64.

Sumber Daya	Informasi yang diperlukan
(Antarmuka virtual privat saja) Bingkai Jumbo	Maximum transmission unit (MTU) paket melewati AWS Direct Connect. Default-nya 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 menambahk an 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 konsol AWS Direct Connect dan temukan Kemampuan bingkai jumbo di halaman Konfigurasi umum antarmuka virtual.
(Antarmuka virtual transit saja) Bingkai jumbo	Maximum transmission unit (MTU) paket melewati 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 instans EC2 dengan entri tabel rute statis VPC ke Lampiran Transit Gateway. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di konsol AWS Direct Connect dan temukan Kemampuan bingkai jumbo di halaman Konfigurasi umum antarmuka virtual.

Jika prefiks publik atau ASN merupakan milik ISP atau operator jaringan, AWS meminta informasi tambahan dari Anda. Ini bisa berupa dokumen yang menggunakan kop surat perusahaan resmi, atau email dari nama domain perusahaan yang memverifikasi bahwa prefiks jaringan/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 konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.
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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer BGP IPv4, pilih IPv4 dan lakukan salah satu hal berikut:
      - Untuk menentukan alamat IP ini sendiri, untuk IP peer router, masukkan alamat CIDR IPv4 tujuan tempat Amazon harus mengirimkan lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat CIDR IPv4 yang akan digunakan untuk mengirim lalu lintas ke AWS.

      [IPv6] Untuk mengonfigurasi peer BGP IPv6, pilih IPv6. Alamat IPv6 peer secara otomatis ditetapkan dari kolam alamat IPv6 Amazon. Anda tidak dapat menentukan alamat IPv6 kustom.
   b. Untuk menyediakan kunci BGP Anda sendiri, masukkan kunci BGP MD5 Anda.

      Jika Anda tidak memasukkan nilai, kami menghasilkan kunci BGP.
   c. Untuk mengiklankan prefiks ke Amazon, untuk Prefiks yang ingin Anda iklankan, masukkan alamat tujuan CIDR IPv4 (dipisahkan dengan koma) tempat lalu lintas harus diarahkan melalui antarmuka virtual.
   d. (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.

7. Pilih Buat antarmuka virtual.

Untuk menyediakan antarmuka virtual privat bagi VPC

1. Buka konsol AWS Direct Connect 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 Akun AWS lainnya, lalu masukkan akun AWS.
   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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

> **Important**
>
> Jika Anda membiarkan AWS auto-menetapkan alamat IPv4, /29 CIDR akan dialokasikan dari 169.254.0.0/16 IPv4 Link-Local menurut RFC 3927 untuk konektivitas. point-to-point AWStidak merekomendasikan opsi ini jika Anda bermaksud menggunakan alamat IP rekan router pelanggan sebagai sumber dan/atau tujuan untuk lalu lintas VPC. Sebagai gantinya, Anda harus menggunakan RFC 1918 atau pengalamatan lainnya, dan tentukan sendiri alamatnya.
>
> - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
> - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat Lokal-Tautan IPv4.

[IPv6] Untuk mengonfigurasi peer BGP IPv6, pilih IPv6. Alamat IPv6 peer secara otomatis ditetapkan dari kolam alamat IPv6 Amazon. Anda tidak dapat menentukan alamat IPv6 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 telah menetapkan antarmuka virtual ke AWS Cloud atau Amazon VPC, lakukan pengujian failover antarmuka virtual untuk memverifikasi bahwa konfigurasi Anda memenuhi

persyaratan ketahanan. Untuk informasi selengkapnya, lihat the section called “Pengujian Failover AWS Direct Connect”.

Langkah 5: Memverifikasi konektivitas antarmuka virtual

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

Untuk memverifikasi koneksi antarmuka virtual Anda ke Cloud AWS

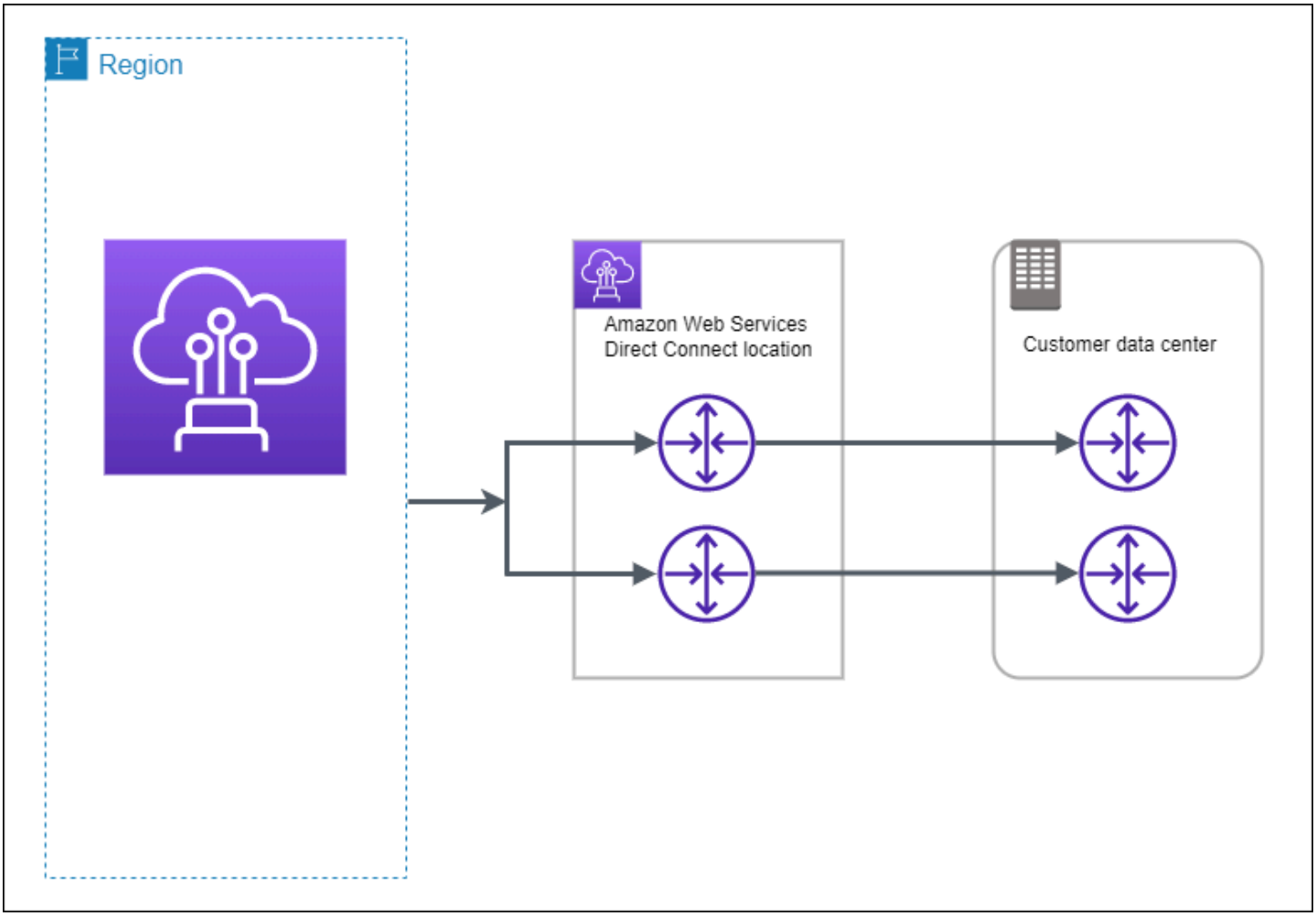
- Jalankan `traceroute` dan verifikasi bahwa pengidentifikasi AWS Direct Connect berada di jejak jaringan.

Untuk memverifikasi koneksi antarmuka virtual Anda ke Amazon VPC

1. Menggunakan AMI yang dapat di-ping, seperti Amazon Linux AMI, luncurkan instans EC2 ke VPC yang terlampir ke virtual private gateway Anda. AMI Amazon Linux tersedia di tab Quick Start saat Anda menggunakan wizard launch wizard instans di konsol Amazon EC2. Untuk informasi selengkapnya, lihat Luncurkan Instans di Panduan Pengguna Amazon EC2 untuk Instans Linux. Pastikan bahwa grup keamanan yang terkait dengan instans mencakup aturan yang mengizinkan lalu lintas ICMP masuk (untuk permintaan ping).
2. Setelah instans berjalan, dapatkan alamat IPv4 privatnya (misalnya, 10.0.0.4). Konsol Amazon EC2 akan menampilkan alamat sebagai bagian dari detail instans.
3. Ping alamat IPv4 privat dan dapatkan respons.

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.



Prosedur berikut menunjukkan cara menggunakan Kit Alat Ketahanan AWS Direct Connect untuk mengonfigurasi model ketahanan pengembangan dan pengujian.

Topik

- Langkah 1: Mendaftar di 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 di AWS

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

Mendaftar Akun AWS

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

Untuk mendaftar Akun AWS

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

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

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

AWS akan mengirimkan email konfirmasi kepada Anda setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun saat ini dan mengelola akun dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Membuat pengguna administratif

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

Mengamankan Pengguna root akun AWS Anda

1. Masuk ke AWS Management Console sebagai pemilik akun dengan memilih Pengguna root dan memasukkan alamat email Akun AWS Anda. Di halaman berikutnya, masukkan kata sandi Anda.

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

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

Membuat pengguna 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 sebuah pengguna administratif.

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

Masuk sebagai pengguna administratif

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

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

Langkah 2: Mengonfigurasi model ketahanan

Untuk mengonfigurasi model ketahanan

1. Buka konsol AWS Direct Connect 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 location service pertama, pilih lokasi AWS Direct Connect 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 (MMR) 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.

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

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

Jika LOA sudah siap, Anda dapat memilih Unduh LOA, lalu klik Lanjutkan.

AWS memerlukan waktu hingga 72 jam 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 di AWS. Anda harus merespons dalam waktu 7 hari atau koneksi dihapus.

Langkah 3: Membuat antarmuka virtual

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

Sebelum memulai, pastikan Anda memiliki informasi berikut:

Sumber Daya	Informasi yang diperlukan
Koneksi	Koneksi AWS Direct Connect atau grup agregasi tautan (LAG) yang Anda buat antarmuka virtualnya.

Sumber Daya	Informasi yang diperlukan
Nama antarmuka virtual	Nama untuk antarmuka virtual.
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID akun AWS dari akun lainnya.
(Antarmuka virtual privat saja) Koneksi	Untuk terhubung ke VPC di Wilayah AWS yang sama, Anda memerluka n virtual private gateway 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, Partner AWS Direct Connect 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 satunya (dual-stack). Jangan gunakan IP Elastis (EIP) 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:
	  • (Antarmuka virtual publik saja) Anda harus menentukan alamat IPv4 publik yang unik yang Anda miliki. Nilai dapat menjadi salah satu dari yang berikut:
	  • IPv4 CIDR milik pelanggan
	
	Ini bisa berupa IP publik (milik pelanggan atau disediakan olehAWS), 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 AWSSupport untuk meminta IPv4 CIDR publik (dan berikan kasus penggunaan dalam permintaan Anda)
	
	Note
	Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk alamat AWS IPv4 publik yang disediakan.

Sumber Daya	Informasi yang diperlukan
	• (Antarmuka virtual privat saja) Amazon dapat menghasilkan alamat IPv4 privat untuk Anda. Jika Anda menentukan sendiri, pastikan Anda menentukan CIDR pribadi untuk antarmuka router Anda dan antarmuka Direct AWS 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 CIDR IPv6 /125. Anda tidak dapat menentukan alamat IPv6 peer Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan melalui IPv4 atau 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 mengaktifkan MD5 secara default. Anda tidak dapat mengubah opsi ini. • Kunci autentikasi 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	Rute IPv4 atau rute IPv6 publik untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: CIDR IPv4 dapat tumpang tindih dengan CIDR IPv4 publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari hal berikut ini benar:
	  • CIDR berasal dari Wilayah AWS yang berbeda. 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.
	• IPv6: Tentukan panjang prefiks /64 atau lebih pendek.
	• 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.
	• Anda dapat menentukan panjang awalan apa pun melalui antarmuka virtual publik Direct Connect. IPv4 harus mendukung apa pun dari /1 - /32, dan IPv6 harus mendukung apa pun dari /1 - /64.

Sumber Daya	Informasi yang diperlukan
(Antarmuka virtual privat saja) Bingkai Jumbo	Maximum transmission unit (MTU) paket melewati AWS Direct Connect. Default-nya 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 menambahk an 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 konsol AWS Direct Connect dan temukan Kemampuan bingkai jumbo di halaman Konfigurasi umum antarmuka virtual.
(Antarmuka virtual transit saja) Bingkai jumbo	Maximum transmission unit (MTU) paket melewati 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 instans EC2 dengan entri tabel rute statis VPC ke Lampiran Transit Gateway. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di konsol AWS Direct Connect dan temukan Kemampuan bingkai jumbo di halaman Konfigurasi umum antarmuka virtual.

Jika prefiks publik atau ASN merupakan milik ISP atau operator jaringan, kami meminta informasi tambahan dari Anda. Ini bisa berupa dokumen yang menggunakan kop surat perusahaan resmi, atau email dari nama domain perusahaan yang memverifikasi bahwa prefiks jaringan/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 konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.
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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

      [IPv4] Untuk mengonfigurasi peer BGP IPv4, pilih IPv4 dan lakukan salah satu hal berikut:
      - Untuk menentukan alamat IP ini sendiri, untuk IP peer router, masukkan alamat CIDR IPv4 tujuan tempat Amazon harus mengirimkan lalu lintas.
      - Untuk IP peer router Amazon, masukkan alamat CIDR IPv4 yang akan digunakan untuk mengirim lalu lintas ke AWS.

      [IPv6] Untuk mengonfigurasi peer BGP IPv6, pilih IPv6. Alamat IPv6 peer secara otomatis ditetapkan dari kolam alamat IPv6 Amazon. Anda tidak dapat menentukan alamat IPv6 kustom.
   b. Untuk menyediakan kunci BGP Anda sendiri, masukkan kunci BGP MD5 Anda.

      Jika Anda tidak memasukkan nilai, kami menghasilkan kunci BGP.
   c. Untuk mengiklankan prefiks ke Amazon, untuk Prefiks yang ingin Anda iklankan, masukkan alamat tujuan CIDR IPv4 (dipisahkan dengan koma) tempat lalu lintas harus diarahkan melalui antarmuka virtual.
   d. (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.

7. Pilih Buat antarmuka virtual.

Untuk menyediakan antarmuka virtual privat bagi VPC

1. Buka konsol AWS Direct Connect 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 Akun AWS lainnya, lalu masukkan akun AWS.
   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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

> **Important**
>
> Jika Anda membiarkan AWS auto-menetapkan alamat IPv4, /29 CIDR akan dialokasikan dari 169.254.0.0/16 IPv4 Link-Local menurut RFC 3927 untuk konektivitas. point-to-point AWStidak merekomendasikan opsi ini jika Anda bermaksud menggunakan alamat IP rekan router pelanggan sebagai sumber dan/atau tujuan untuk lalu lintas VPC. Sebagai gantinya, Anda harus menggunakan RFC 1918 atau pengalamatan lainnya, dan tentukan sendiri alamatnya.
>
> - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
> - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat Lokal-Tautan IPv4.

[IPv6] Untuk mengonfigurasi peer BGP IPv6, pilih IPv6. Alamat IPv6 peer secara otomatis ditetapkan dari kolam alamat IPv6 Amazon. Anda tidak dapat menentukan alamat IPv6 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 telah menetapkan antarmuka virtual ke AWS Cloud atau Amazon VPC, lakukan pengujian failover antarmuka virtual untuk memverifikasi bahwa konfigurasi Anda memenuhi

persyaratan ketahanan. Untuk informasi selengkapnya, lihat the section called “Pengujian Failover AWS Direct Connect”.

Langkah 5: Memverifikasi antarmuka virtual

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

Untuk memverifikasi koneksi antarmuka virtual Anda ke Cloud AWS

- Jalankan `traceroute` dan verifikasi bahwa pengidentifikasi AWS Direct Connect berada di jejak jaringan.

Untuk memverifikasi koneksi antarmuka virtual Anda ke Amazon VPC

1. Menggunakan AMI yang dapat di-ping, seperti Amazon Linux AMI, luncurkan instans EC2 ke VPC yang terlampir ke virtual private gateway Anda. AMI Amazon Linux tersedia di tab Quick Start saat Anda menggunakan wizard launch wizard instans di konsol Amazon EC2. Untuk informasi selengkapnya, lihat Luncurkan Instans di Panduan Pengguna Amazon EC2 untuk Instans Linux. Pastikan bahwa grup keamanan yang terkait dengan instans mencakup aturan yang mengizinkan lalu lintas ICMP masuk (untuk permintaan ping).
2. Setelah instans berjalan, dapatkan alamat IPv4 privatnya (misalnya, 10.0.0.4). Konsol Amazon EC2 akan menampilkan alamat sebagai bagian dari detail instans.
3. Ping alamat IPv4 privat dan dapatkan respons.

Klasik

Pilih Klasik jika Anda memiliki koneksi yang ada.

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

Daftar Isi

- Langkah 4: Buat antarmuka virtual
- Langkah 5: Unduh konfigurasi router
- Langkah 6: Verifikasi antarmuka virtual
- (Direkomendasikan) Langkah 7: Konfigurasikan koneksi redundan

Prasyarat

Untuk koneksi ke AWS Direct Connectdengan 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, atau 100GBASE-LR4 untuk 100 gigabit Ethernet.
- Negosiasi otomatis untuk port harus dinonaktifkan untuk 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 antarmuka virtual Anda tetap down, lihatPemecahan masalah lapisan 2 (tautan data).
- Enkapsulasi VLAN 802.1Q harus didukung di seluruh koneksi, termasuk perangkat perantara.
- Perangkat Anda harus mendukung autentikasi Border Gateway Protocol (BGP) dan BGP MD5.
- (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.

Langkah 1: Mendaftar di AWS

Untuk menggunakan AWS Direct Connect, Anda memerlukan akun jika belum memiliki akun.

Mendaftar Akun AWS

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

Untuk mendaftar Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.

2. Ikuti petunjuk secara online.

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

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

AWS akan mengirimkan email konfirmasi kepada Anda setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun saat ini dan mengelola akun dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Membuat pengguna administratif

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

Mengamankan Pengguna root akun AWS Anda

1. Masuk ke AWS Management Console sebagai pemilik akun dengan memilih Pengguna root dan memasukkan alamat email Akun AWS Anda. Di halaman berikutnya, masukkan kata sandi Anda.

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

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

Membuat pengguna 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 sebuah pengguna administratif.

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

Masuk sebagai pengguna administratif

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

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

Langkah 2: Minta koneksi AWS Direct Connect khusus

Untuk koneksi khusus, Anda dapat mengirimkan permintaan koneksi menggunakan konsol AWS Direct Connect. Untuk koneksi yang di-host, bekerja dengan Partner AWS Direct Connect untuk meminta koneksi yang di-host. Pastikan bahwa Anda memiliki informasi berikut:

- Kecepatan port yang Anda butuhkan. Anda tidak dapat mengubah kecepatan port setelah Anda membuat permintaan koneksi.
- Lokasi AWS Direct Connect tempat koneksi harus dihentikan.

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

Untuk membuat koneksi AWS Direct Connect baru

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.
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 pertemuan (MMR) di beberapa lantai gedung.

d. Untuk Kecepatan Port, pilih bandwidth koneksi.

e. Untuk On-premise, pilih Hubungkan melalui partner AWS Direct Connect saat Anda menggunakan koneksi ini untuk menhubungkan ke pusat data Anda.

f. Untuk Penyedia layanan, pilih Partner AWS Direct Connect. 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.

Ini dapat memakan 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 di AWS. Anda harus merespons dalam waktu 7 hari atau koneksi akan dihapus.

Untuk informasi selengkapnya, lihat AWS Direct Connect koneksi.

Terima koneksi yang di-host

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

Untuk menerima antarmuka virtual yang di-host

1. Buka konsol AWS Direct Connect 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 ke AWS, dan diperlukan oleh penyedia kolokasi atau penyedia jaringan Anda untuk membuat koneksi lintas jaringan (koneksi silang).

Untuk mengunduh LOA-CFA

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.
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 AWSSupport.

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

   - Jika Anda bekerja dengan Partner AWS Direct Connect atau penyedia jaringan, kirimi mereka LOA-CFA 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 lokasi AWS Direct Connect, hubungi penyedia kolokasi untuk meminta koneksi lintas jaringan. Anda harus menjadi pelanggan penyedia kolokasi. Anda juga harus menunjukkan LOA-CFA kepada mereka yang memberikan otorisasi untuk koneksi ke router AWS, dan informasi yang diperlukan untuk terhubung ke jaringan Anda.

Lokasi AWS Direct Connect yang tercantum sebagai beberapa lokasi (misalnya, Equinix DC1-DC6 & DC10-DC11) disiapkan 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**
>
> Sebuah kampus diperlakukan sebagai satu lokasi AWS Direct Connect. 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 koneksi AWS Direct Connect, Anda harus membuat antarmuka virtual. Anda dapat membuat antarmuka virtual privat untuk terhubung ke VPC. Atau, Anda dapat membuat antarmuka virtual publik untuk terhubung ke layanan AWS publik yang tidak ada dalam 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 privat untuk terhubung ke tiga VPC.

Sebelum memulai, pastikan Anda memiliki informasi berikut:

Sumber Daya	Informasi yang diperlukan
Koneksi	Koneksi AWS Direct Connect atau grup agregasi tautan (LAG) yang Anda buat antarmuka virtualnya.
Nama antarmuka virtual	Nama untuk antarmuka virtual.

Sumber Daya	Informasi yang diperlukan
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID akun AWS dari akun lainnya.
(Antarmuka virtual privat saja) Koneksi	Untuk terhubung ke VPC di Wilayah AWS yang sama, Anda memerlukan virtual private gateway 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, Partner AWS Direct Connect 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 satunya (dual-stack). Jangan gunakan IP Elastis (EIP) 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:
	  • (Antarmuka virtual publik saja) Anda harus menentukan alamat IPv4 publik yang unik yang Anda miliki. Nilai dapat menjadi salah satu dari yang berikut:
	  • IPv4 CIDR milik pelanggan
	
	Ini bisa berupa IP publik (milik pelanggan atau disediakan olehAWS), 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 AWSSupport untuk meminta IPv4 CIDR publik (dan berikan kasus penggunaan dalam permintaan Anda)
	
	Note
	Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk alamat AWS IPv4 publik yang disediakan.

Sumber Daya	Informasi yang diperlukan
	• (Antarmuka virtual privat saja) Amazon dapat menghasilkan alamat IPv4 privat untuk Anda. Jika Anda menentukan sendiri, pastikan Anda menentukan CIDR pribadi untuk antarmuka router Anda dan antarmuka Direct AWS 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 CIDR IPv6 /125. Anda tidak dapat menentukan alamat IPv6 peer Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan melalui IPv4 atau 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 mengaktifkan MD5 secara default. Anda tidak dapat mengubah opsi ini. • Kunci autentikasi 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	Rute IPv4 atau rute IPv6 publik untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: CIDR IPv4 dapat tumpang tindih dengan CIDR IPv4 publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari hal berikut ini benar:
	  • CIDR berasal dari Wilayah AWS yang berbeda. 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.
	• IPv6: Tentukan panjang prefiks /64 atau lebih pendek.
	• 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.
	• Anda dapat menentukan panjang awalan apa pun melalui antarmuka virtual publik Direct Connect. IPv4 harus mendukung apa pun dari /1 - /32, dan IPv6 harus mendukung apa pun dari /1 - /64.

Sumber Daya	Informasi yang diperlukan
(Antarmuka virtual privat saja) Bingkai Jumbo	Maximum transmission unit (MTU) paket melewati AWS Direct Connect. Default-nya 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 menambahk an 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 konsol AWS Direct Connect dan temukan Kemampuan bingkai jumbo di halaman Konfigurasi umum antarmuka virtual.
(Antarmuka virtual transit saja) Bingkai jumbo	Maximum transmission unit (MTU) paket melewati 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 instans EC2 dengan entri tabel rute statis VPC ke Lampiran Transit Gateway. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di konsol AWS Direct Connect dan temukan Bingkai jumbo yang berkemampuan di halaman Konfigurasi umum antarmuka virtual.

Kami meminta informasi tambahan dari Anda jika prefiks publik atau ASN milik ISP atau operator jaringan. Ini bisa berupa dokumen yang menggunakan kop surat perusahaan resmi atau email dari nama domain perusahaan yang memverifikasi bahwa prefiks jaringan/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 privat virtual 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 Berkemampuan Bingkai Jumbo di tab Ringkasan.

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 konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.
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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

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

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

   Jika Anda tidak memasukkan nilai, kami menghasilkan kunci BGP.

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

d. (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.

7. Pilih Buat antarmuka virtual.

Untuk menyediakan antarmuka virtual privat bagi VPC

1. Buka konsol AWS Direct Connect 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 Akun AWS lainnya, lalu masukkan akun AWS.

   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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

      > **Important**
      >
      > Jika Anda membiarkan AWS auto-menetapkan alamat IPv4, /29 CIDR akan dialokasikan dari 169.254.0.0/16 IPv4 Link-Local menurut RFC 3927 untuk konektivitas. point-to-point AWStidak merekomendasikan opsi ini jika Anda bermaksud menggunakan alamat IP rekan router pelanggan sebagai sumber dan/atau tujuan untuk lalu lintas VPC. Sebagai gantinya, Anda harus menggunakan RFC 1918 atau pengalamatan lainnya, dan tentukan sendiri alamatnya.
      >
      > - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
      > - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat Lokal-Tautan IPv4.

      [IPv6] Untuk mengonfigurasi peer BGP IPv6, pilih IPv6. Alamat IPv6 peer secara otomatis ditetapkan dari kolam alamat IPv6 Amazon. Anda tidak dapat menentukan alamat IPv6 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 koneksi AWS Direct Connect, 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 konsol AWS Direct Connect 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, kemudian gunakan konfigurasi yang sesuai untuk router Anda untuk memastikan bahwa Anda dapat terhubung ke AWS Direct Connect.

Untuk contoh file konfigurasi, lihat Contoh File Konfigurasi Router.

Setelah Anda mengonfigurasi router, status antarmuka virtual akan berubah menjadi UP. Jika antarmuka virtual tetap bermasalah dan Anda tidak dapat menge-ping alamat IP peer perangkat AWS Direct Connect, lihat Pemecahan 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 menetapkan antarmuka virtual ke Cloud AWS atau Amazon VPC, Anda dapat memverifikasi koneksi AWS Direct Connect menggunakan prosedur berikut.

Untuk memverifikasi koneksi antarmuka virtual Anda ke Cloud AWS

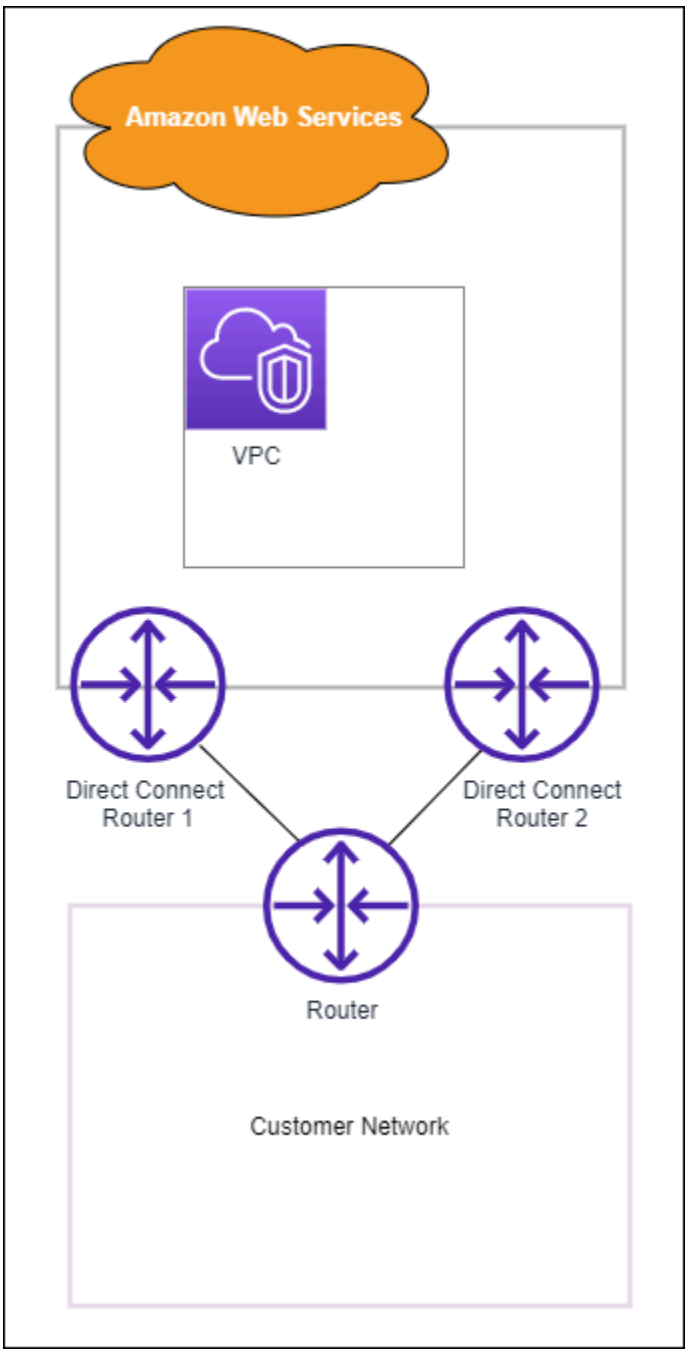
- Jalankan `traceroute` dan verifikasi bahwa pengidentifikasi AWS Direct Connect berada di jejak jaringan.

Untuk memverifikasi koneksi antarmuka virtual Anda ke Amazon VPC

1. Menggunakan AMI yang dapat di-ping, seperti Amazon Linux AMI, luncurkan instans EC2 ke VPC yang terlampir ke virtual private gateway Anda. AMI Amazon Linux tersedia di tab Quick Start saat Anda menggunakan wizard launch wizard instans di konsol Amazon EC2. Untuk informasi selengkapnya, lihat Luncurkan Instans di Panduan Pengguna Amazon EC2 untuk Instans Linux. Pastikan bahwa grup keamanan yang terkait dengan instans mencakup aturan yang mengizinkan lalu lintas ICMP masuk (untuk permintaan ping).
2. Setelah instans berjalan, dapatkan alamat IPv4 privatnya (misalnya, 10.0.0.4). Konsol Amazon EC2 akan menampilkan alamat sebagai bagian dari detail instans.
3. Ping alamat IPv4 privat dan dapatkan respons.

(Direkomendasikan) Langkah 7: Konfigurasikan koneksi redundan

Untuk menyediakan failover, kami merekomendasikan agar Anda meminta dan mengonfigurasikan dua koneksi khusus untuk AWS, seperti yang ditunjukkan dalam 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, dengan kedua koneksi aktif. AWS Direct Connect mendukung pembuatan multijalur ke beberapa antarmuka virtual dalam lokasi yang sama, dan beban untuk lalu lintas dibagi di antara antarmuka berdasarkan alur. 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 merekomendasikan agar Anda mengonfigurasi koneksi ke berbagai lokasi AWS Direct Connect.

Untuk informasi selengkapnya tentang ketahanan AWS Direct Connect, lihat AWS Direct ConnectRekomendasi Ketahanan.

Pengujian Failover AWS Direct Connect

Model ketahanan Kit Alat Ketahanan AWS Direct Connect dirancang untuk memastikan bahwa Anda memiliki jumlah koneksi antarmuka virtual yang sesuai di beberapa lokasi. Setelah Anda menyelesaikan wizard, gunakan pengujian failover Kit Alat Ketahanan AWS Direct Connect untuk menurunkan sesi peering BGP guna memverifikasi lalu lintas tersebut dirutekan ke salah satu antarmuka virtual redundan, dan memenuhi persyaratan ketahanan.

Gunakan pengujian untuk memastikan bahwa lalu lintas dirutekan melalui antarmuka virtual redundan ketika antarmuka virtual tidak berjalan. Anda memulai pengujian dengan memilih antarmuka virtual, sesi peering BGP, dan durasi untuk menjalankan pengujian. AWS menempatkan sesi peering BGP antarmuka virtual yang dipilih dalam status 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. Saat pengujian selesai, atau Anda menghentikan pengujian secara manual, AWS memulihkan sesi BGP. Setelah

pengujian selesai, Anda dapat menggunakan Kit Alat Ketahanan AWS Direct Connect untuk menyesuaikan konfigurasi.

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

Riwayat Pengujian

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 AWS CloudTrail bahwa pengujian berjalan pada antarmuka virtual.

Memulai pengujian failover antarmuka virtual

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

Untuk memulai pengujian failover antarmuka virtual dari konsol AWS Direct Connect

1. Buka konsol AWS Direct Connect 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. Untuk Peering untuk diturunkan ke pengujian, pilih sesi peering 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 pengujian failover antarmuka virtual menggunakan AWS CLI

Gunakan StartBgpFailoverTest.

Melihat riwayat pengujian failover antarmuka virtual

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

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

1. Buka konsol AWS Direct Connect 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.

Menghentikan pengujian failover antarmuka virtual

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

Untuk menghentikan pengujian failover antarmuka virtual dari konsol AWS Direct Connect

1. Buka konsol AWS Direct Connect 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 memulihkan sesi peering BGP. Riwayat pengujian menampilkan "dibatalkan" untuk pengujian.

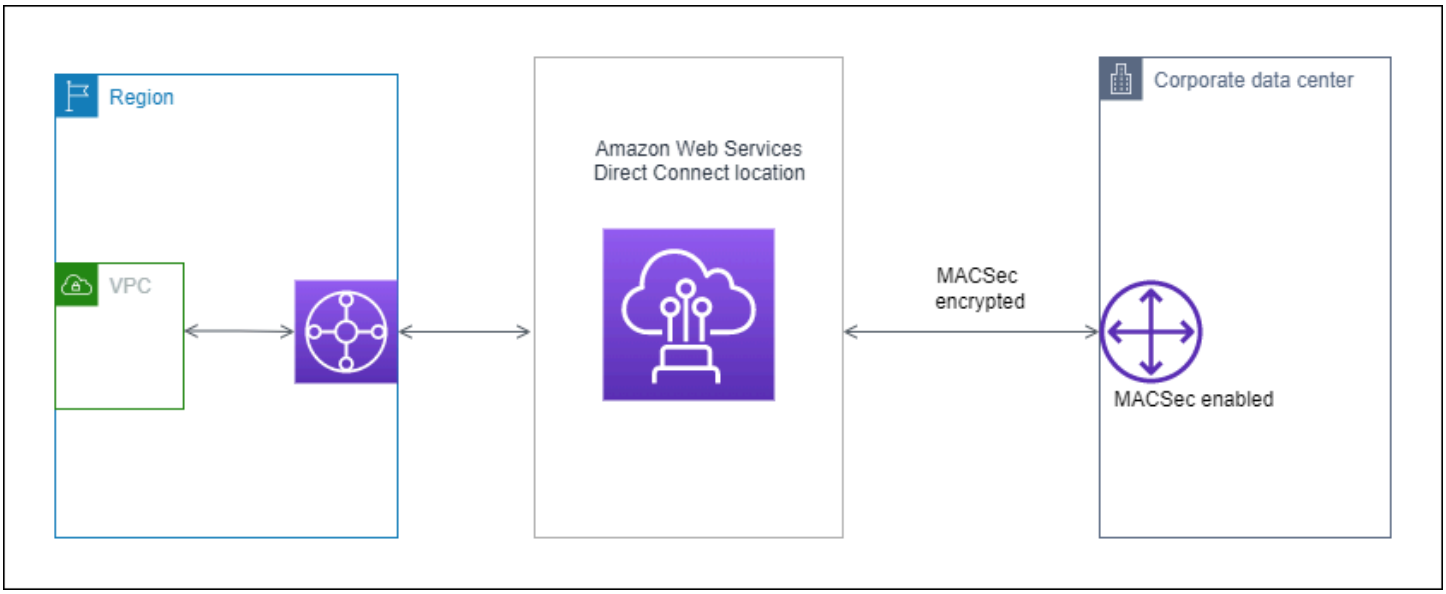
Untuk menghentikan pengujian failover antarmuka virtual menggunakan AWS CLI

Gunakan StopBgpFailoverTest.

Keamanan MAC

MAC Security (MACsec) adalah standar IEEE yang menyediakan kerahasiaan data, integritas data, dan autentisitas asal data. Anda dapat menggunakan AWS Direct Connect yang mendukung MacSec untuk mengenkripsi data Anda dari pusat data perusahaan Anda ke lokasi AWS Direct Connect. Semua data yang mengalir di jaringanAWS global yang terhubung dengan pusat data dan Wilayah secara otomatis dienkripsi pada lapisan fisik sebelum meninggalkan pusat data.

Dalam diagram berikut, baik koneksi khusus dan sumber daya on-premise Anda harus mendukung MacSec. Lalu lintas lapisan 2 yang bergerak melalui koneksi khusus ke atau dari pusat data dienkripsi.



Konsep MacSec

Berikut ini adalah konsep utama untuk MacSec:

- Keamanan MAC (MacSec)— Standar IEEE 802.1 Lapisan 2 yang menyediakan kerahasiaan data, integritas data, dan keaslian asal data. Untuk informasi selengkapnya tentang protokol, lihat 802.1AE: Keamanan MAC (MacSec).
- Kunci rahasia MACsec— Kunci yang dibagikan sebelumnya yang menetapkan konektivitas MACsec antara router lokal pelanggan dan port koneksi di lokasi AWS Direct Connect. Kunci dihasilkan oleh perangkat di ujung koneksi menggunakan pasangan CKN/CAK yang Anda berikan untuk AWS dan juga telah disediakan di perangkat Anda.

- Nama Kunci Koneksi (CKN) dan Kunci Asosiasi Konektivitas (CAK)— Nilai-nilai dalam pasangan ini digunakan untuk menghasilkan kunci rahasia MacSec. Anda menghasilkan nilai pasangan, mengasosiasikan mereka dengan koneksi AWS Direct Connect, dan menyediakannya di perangkat edge Anda di akhir koneksi AWS Direct Connect.

Koneksi yang didukung

MacSec tersedia pada koneksi khusus. Untuk informasi tentang cara memesan koneksi yang mendukung MacSec, lihat AWS Direct Connect.

Memulai dengan MACsec pada koneksi khusus

Tugas-tugas berikut membantu Anda menjadi akrab dengan MacSec pada koneksi AWS Direct Connect khusus. Tidak ada biaya tambahan untuk menggunakan MacSec.

Sebelum mengonfigurasi MacSec pada koneksi khusus, perhatikan hal berikut:

- MacSec didukung pada koneksi Direct Connect khusus 10 Gbps dan 100 Gbps di titik-titik kehadiran tertentu. Untuk koneksi ini, suite cipher MacSec berikut didukung:
  - Untuk koneksi 10Gbps, GCM-AES-256 dan GCM-AES-XPN-256.
  - Untuk koneksi 100 Gbps, GCM-AES-XPN-256.
- Hanya kunci MacSec 256-bit yang didukung.
- Extended Packet Numbering (XPN) diperlukan untuk koneksi 100Gbps. Untuk koneksi 10Gbps Direct Connect mendukung GCM-AES-256 dan GCM-AES-XPN-256. Koneksi berkecepatan tinggi, seperti koneksi khusus 100 Gbps, dapat dengan cepat menghabiskan ruang penomoran paket 32-bit asli MacSec, yang mengharuskan Anda memutar kunci enkripsi Anda setiap beberapa menit untuk membentuk Asosiasi Konektivitas baru. Untuk menghindari situasi ini, amandemen IEEE Std 802.1AEBW-2013 memperkenalkan penomoran paket yang diperluas, 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.

Untuk informasi tambahan tentang Direct Connect dan MacSec, lihat bagian MacSec di AWS Direct Connect FAQ.

Topik

Prasyarat MACsec

Selesaikan tugas-tugas berikut sebelum Anda mengonfigurasi MACsec pada koneksi khusus.

- Buat pasangan CKN/CAK untuk kunci rahasia MACsec.

  Anda dapat membuat pasangan menggunakan alat standar terbuka. Pasangan ini harus memenuhi persyaratan yang ditentukan dalam the section called “Langkah 4: Konfigurasikan router on-premise”.
- Pastikan Anda memiliki perangkat di sisi koneksi yang mendukung MACsec.
- Secure Channel Identifier (SCI) harus dihidupkan.
- Hanya kunci MacSec 256-bit yang didukung, memberikan perlindungan data canggih terbaru.

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 tertaut layanan”.

Pertimbangan kunci CKN/CAK yang dibagikan sebelumnya MACsec

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

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.

Langkah 1: Buat koneksi

Untuk mulai menggunakan MACsec, Anda harus mengaktifkan fitur saat membuat koneksi khusus. Untuk informasi selengkapnya, lihat the section called “Buat koneksi menggunakan wizard Koneksi”.

(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 the section called “Pertimbangan MACsec” dan the section called “Membuat 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:

- the section called “Kaitkan MACsec CKN/CAK dengan koneksi”
- the section called “Mengaitkan CKN/CAK MACsec dengan LAG”

Langkah 4: Konfigurasikan router on-premise

Perbarui router on-premise dengan kunci rahasia MACsec. Kunci rahasia MacSec pada router lokal dan di AWS Direct Connect lokasi harus cocok. Untuk informasi selengkapnya, lihat the section called “Mengunduh file konfigurasi router”.

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

Jika Anda perlu menghapus hubungan antara kunci MACsec dan koneksi atau LAG, lihat salah satu hal berikut:

- the section called “Hapus keterkaitan antara kunci rahasia MACsec dan koneksi”
- the section called “Menghapus pengaitan antara semua kunci rahasia MACsec dan LAG.”

AWS Direct Connect koneksi

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: Sebuah 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 the section called “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 the section called “Koneksi yang di-host”.

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, dan 100 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 diunduh, atau mengirimi Anda email dengan permintaan untuk informasi selengkapnya. 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:

- the section called “Buat koneksi menggunakan wizard Koneksi”
- the section called “Buat koneksi Klasik”
- the section called “Lihat detail koneksi Anda”
- the section called “Perbarui koneksi”
- the section called “Kaitkan MACsec CKN/CAK dengan koneksi”
- the section called “Hapus keterkaitan antara kunci rahasia MACsec dan koneksi”
- the section called “Hapus 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 AWS Direct Connect.

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 “Prasyarat MACsec ”.

Buat koneksi 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 konsol AWS Direct Connect 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. Menggunakan Kit Alat Ketahanan AWS Direct Connect untuk memulai
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 100Gbps.
   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) Mengonfigurasi MAC Security (MACsec) untuk koneksi. Di bawah Pengaturan Tambahan, pilih Minta port berkemampuan MACsec.

      MACsec hanya tersedia pada koneksi khusus.
   e. (Opsional) Pilih Tambahkan tag untuk menambahkan pasangan kunci/nilai 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 “Unduh LOA-CFA”

Gunakan salah satu perintah berikut ini.

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

Buat koneksi 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 dihentikan.

> **Note**
>
> Anda tidak dapat menggunakan AWS Direct Connect konsol untuk meminta koneksi yang dihosting. Sebaliknya, hubungi AWS Direct Connect Mitra, yang dapat membuat koneksi host 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 konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.
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 pertemuan (MMR) 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 pasangan kunci/nilai 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 AWS Direct Connect koneksi.

Unduh 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.

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.

> **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 koneksi.

Console

Untuk mengunduh LOA-CFA

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.
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.

Command line

Untuk mengunduh LOA-CFA menggunakan baris perintah atau API

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

Perbarui koneksi

Anda dapat memperbarui atribut koneksi berikut:

- Nama koneksi.
- Mode enkripsi MACsec 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`

Console

Untuk memperbarui koneksi

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.

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.

Command line

Untuk menambahkan tanda atau menghapus tanda menggunakan baris perintah

- tag-resource (AWS CLI)
- untanda-resource (AWS CLI)

Untuk memperbarui koneksi menggunakan baris perintah atau API

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

Kaitkan MACsec CKN/CAK dengan koneksi

Setelah Anda membuat koneksi yang mendukung MACsec, Anda dapat mengaitkan CKN/CAK dengan koneksi.

> **Note**
>
> Anda tidak dapat mengubah kunci rahasia MACsec setelah Anda mengaitkannya dengan koneksi. Jika Anda perlu memodifikasi kunci, pisahkan kunci dari koneksi, kemudian kaitkan kunci baru dengan koneksi. Untuk informasi tentang menghapus keterkaitan, lihat the section called “Hapus keterkaitan antara kunci rahasia MACsec dan koneksi”.

Console

Untuk mengaitkan kunci MACsec dengan koneksi

1. Buka konsol AWS Direct Connect 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 kunci MACsec.

   [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.

   [Menggunakan rahasia] Pilih Rahasia Secret Manager yang ada, lalu untuk Rahasia, pilih kunci rahasia MACsec.
6. Pilih Kaitkan kunci.

Command line

Untuk mengaitkan kunci MACsec dengan koneksi

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

Hapus keterkaitan antara kunci rahasia MACsec dan koneksi

Anda dapat menghapus hubungan antara koneksi dan kunci MACsec.

Console

Untuk menghapus keterkaitan antara koneksi dan kunci MACsec

1. Buka konsol AWS Direct Connect 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 rahasia MACsec untuk dihapus, kemudian pilih Pisahkan kunci.
6. Di kotak dialog konfirmasi, masukkan pisahkan, lalu pilihPisahkan.

Command line

Untuk menghapus terkaitan antara koneksi dan kunci MACsec

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

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 the section called “Terima koneksi yang di-host”.

Kecepatan port

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

Perhatikan hal berikut:

- Kecepatan port koneksi hanya dapat diubah oleh AWS Direct Connect Mitra Anda. Untuk mengubah kecepatan port Anda, hubungi AWS Direct Connect Partner yang mengelola koneksi host Anda.
- 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:

- the section called “Lihat detail koneksi Anda”
- the section called “Perbarui koneksi”
- the section called “Hapus koneksi”

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

Terima koneksi yang 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.

Console

1. Buka konsol AWS Direct Connect 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.

Command line

Untuk menerima koneksi host menggunakan baris perintah atau API

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

Lihat detail koneksi Anda

Anda dapat melihat status koneksi Anda saat ini. 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 Pemantauan.

Console

Untuk melihat detail tentang koneksi

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.
2. Di panel sebelah kiri, pilih Koneksi.
3. Pilih koneksi, kemudian pilih Lihat detail.

Command line

Untuk mendeskripsikan koneksi menggunakan baris perintah atau API

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

Hapus 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 Menghapus 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, lihatthe section called “Unduh 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.

Console

Untuk menghapus koneksi

1. Buka konsol AWS Direct Connect 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.

Command line

Untuk menghapus koneksi menggunakan baris perintah atau API

- delete-connection (AWS CLI)
- DeleteConnection(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 petunjuk khusus untuk setiap penyedia, lihat tabel di bawah ini. Hubungi penyedia Anda untuk harga koneksi silang. Setelah koneksi silang dibuat, Anda dapat membuat antarmuka virtual menggunakan konsol AWS Direct Connect .

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 Mengakses Wilayah AWS jarak jauh.

> **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 Unduh LOA-CFA.

Kolokasi

- AS Timur (Ohio)
- AS Timur (Virginia Utara)
- AS Barat (California Utara)
- US West (Oregon)
- Afrika (Cape Town)
- Asia Pasifik (Jakarta)

- Asia Pasifik (Mumbai)
- Asia Pasifik (Seoul)
- Asia Pacific (Singapore)
- Asia Pasifik (Sydney)
- Asia Pacific (Tokyo)
- Kanada (Pusat)
- China (Beijing)
- China (Ningxia)
- Eropa (Frankfurt)
- Eropa (Irlandia)
- Eropa (Milan)
- Eropa (London)
- Eropa (Paris)
- Eropa (Stockholm)
- Eropa (Zurich)
- Israel (Tel Aviv)
- Timur Tengah (Bahrain)
- Timur Tengah (UEA)
- Amerika Selatan (Sao Paulo)
- AWS GovCloud (AS-Timur)
- AWS GovCloud (AS-Barat)

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 portal pelanggan.

Lokasi	Cara meminta koneksi
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.
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.
Realty Digital IAD38, Ashburn	Hubungi Digital Realty di amazon.orders@digitalrealty.com.
Equinix DC1-DC6 & DC10-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.

Lokasi	Cara meminta koneksi
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 SV4, Santa 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 LA3, El Segundo	Hubungi Equinix di awsdealreg@equinix.com.

Lokasi	Cara meminta koneksi
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.
Digital Realty SEA10, 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, South Africa	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 jessie.w@dci-indonesia.com.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 DC2, Delhi	Hubungi STT di pertanyaan. AWSDX@sttelemediagdc .in.
STT GDC Pvt. Ltd. VSB, Chennai	Hubungi STT di pertanyaan. AWSDX@sttelemediagdc .in.

Lokasi	Cara meminta koneksi
STT Hyderabad DC1, Hyderabad	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.
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, Singapore	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. Menghubun

Lokasi	Cara meminta koneksi
	gi 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.
Datacom DH6, Kota Auckland	Hubungi Datacom di Datacom Orbit —Auckland.
Equinix ME2, Melbourne	Hubungi Equinix di awsdealreg@equinix.com.
Equinix SY3, Jakarta	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.

Lokasi	Cara meminta koneksi
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
Allied 250 Front St W, Toronto	Hubungi driches@alliedreit.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, Netherlands	Hubungi Equinix di awsdealreg@equinix.com.
Equinix FR5, Frankfurt	Hubungi Equinix di awsdealreg@equinix.com.
Equinix HE6, Helsinki	Hubungi Equinix di awsdealreg@equinix.com.
Equinix MU1, Munich	Hubungi Equinix di awsdealreg@equinix.com.
Equinix WA1, Warsaw	Hubungi Equinix di awsdealreg@equinix.com.
Interxion AMS7, Amsterdam	Hubungi Interxion di customer.services@interxion.com.
Interxion CPH2, Copenhagen	Hubungi Interxion di customer.services@interxion.com.
Interxion FRA6, Frankfurt	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.

Lokasi	Cara meminta koneksi
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 awsorders@eircom.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.
Interxion MRS1, Marseille	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, Italy	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.
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.
Interxion PAR7, Paris	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 (Zurich)

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
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
Equinix RJ2, Rio de Janeiro	Hubungi Equinix di awsdealreg@equinix.com.
Equinix SP4, São 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.

Antarmuka virtual AWS Direct Connect

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

- 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 publik AWS 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 the section called “Gateway Direct Connect”.

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

Aturan iklan prefiks antarmuka virtual publik

Kami mengiklankan prefiks Amazon yang sesuai untuk Anda sehingga Anda dapat mencapai VPC atau layanan AWS lainnya. Anda dapat mengakses semua prefiks AWS melalui koneksi ini; misalnya, Amazon EC2, Amazon S3, dan Amazon.com. Anda tidak memiliki akses ke prefiks non-Amazon. Untuk daftar awalan saat ini yang diiklankan olehAWS, lihat Rentang Alamat AWS IP di. Referensi Umum Amazon Web Services AWStidak mengiklankan ulang prefiks pelanggan yang diterima melalui antarmuka virtual publik Direct AWS Connect ke pelanggan lain. Untuk informasi selengkapnya tentang antarmuka virtual publik dan kebijakan perutean, lihat. the section called “Kebijakan perutean antarmuka virtual publik”

> **Note**
>
> Kami sarankan Anda menggunakan filter firewall (berdasarkan alamat sumber/tujuan paket) untuk mengontrol lalu lintas ke dan dari beberapa prefiks. Jika Anda menggunakan filter prefiks (peta rute), pastikan prefiks dengan pencocokan tepat atau lebih lama diterima.

Prefiks yang diiklankan dari AWS Direct Connect dapat digabungkan dan mungkin berbeda dari prefiks yang didefinisikan dalam filter prefiks Anda.

Antarmuka virtual yang di-host

Untuk menggunakan koneksi AWS Direct Connect dengan akun lain, Anda dapat membuat antarmuka virtual yang di-host untuk akun tersebut. 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	Koneksi AWS Direct Connect atau grup agregasi tautan (LAG) yang Anda buat antarmuka virtualnya.
Nama antarmuka virtual	Nama untuk antarmuka virtual.
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID akun AWS dari akun lainnya.
(Antarmuka virtual privat saja) Koneksi	Untuk terhubung ke VPC di Wilayah AWS yang sama, Anda memerluka n virtual private gateway 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

Sumber Daya	Informasi yang diperlukan
	standar Ethernet 802.1Q. Tanda ini diperlukan untuk lalu lintas yang melintasi koneksi AWS Direct Connect. Jika Anda memiliki koneksi yang di-host, Partner AWS Direct Connect 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 satunya (dual-stack). Jangan gunakan IP Elastis (EIP) 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:
	  • (Antarmuka virtual publik saja) Anda harus menentukan alamat IPv4 publik yang unik yang Anda miliki. Nilai dapat menjadi salah satu dari yang berikut:
	  • IPv4 CIDR milik pelanggan
	
	Ini bisa berupa IP publik (milik pelanggan atau disediakan olehAWS), 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 AWSSupport untuk meminta IPv4 CIDR publik (dan berikan kasus penggunaan dalam permintaan Anda)
	
	Note
	Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk alamat AWS IPv4 publik yang disediakan.

Sumber Daya	Informasi yang diperlukan
	• (Antarmuka virtual privat saja) Amazon dapat menghasilkan alamat IPv4 privat untuk Anda. Jika Anda menentukan sendiri, pastikan Anda menentukan CIDR pribadi untuk antarmuka router Anda dan antarmuka Direct AWS 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 CIDR IPv6 /125. Anda tidak dapat menentukan alamat IPv6 peer Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan melalui IPv4 atau 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 mengaktifkan MD5 secara default. Anda tidak dapat mengubah opsi ini. • Kunci autentikasi 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	Rute IPv4 atau rute IPv6 publik untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: CIDR IPv4 dapat tumpang tindih dengan CIDR IPv4 publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari hal berikut ini benar:
	  • CIDR berasal dari Wilayah AWS yang berbeda. 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.
	• IPv6: Tentukan panjang prefiks /64 atau lebih pendek.
	• 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.
	• Anda dapat menentukan panjang awalan apa pun melalui antarmuka virtual publik Direct Connect. IPv4 harus mendukung apa pun dari /1 - /32, dan IPv6 harus mendukung apa pun dari /1 - /64.

Sumber Daya	Informasi yang diperlukan
(Antarmuka virtual privat saja) Bingkai Jumbo	Maximum transmission unit (MTU) paket melewati AWS Direct Connect. Default-nya 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 menambahk an 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 konsol AWS Direct Connect dan temukan Kemampuan bingkai jumbo di halaman Konfigurasi umum antarmuka virtual.
(Antarmuka virtual transit saja) Bingkai jumbo	Maximum transmission unit (MTU) paket melewati 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 instans EC2 dengan entri tabel rute statis VPC ke Lampiran Transit Gateway. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di konsol AWS Direct Connect dan temukan Kemampuan bingkai jumbo di halaman Konfigurasi umum antarmuka virtual.

SiteLink

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

SiteLink adalah fitur Direct Connect opsional untuk antarmuka pribadi virtual 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 China.

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 ituWilayah 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 memilih jalur dari lokasi Direct Connect lokal ke lokasi terkaitWilayah AWS.

SiteLink mendukung ukuran MTU bingkai jumbo maksimum 8500 atau 9001, tergantung pada jenis antarmuka virtual. Untuk informasi selengkapnya, lihat the section called “Mengatur MTU jaringan untuk antarmuka virtual privat atau antarmuka virtual transit”.

Prasyarat untuk antarmuka virtual

Sebelum Anda membuat antarmuka virtual, lakukan hal berikut:

- Buat koneksi. Untuk informasi selengkapnya, lihat the section called “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	Koneksi AWS Direct Connect atau grup agregasi tautan (LAG) yang Anda buat antarmuka virtualnya.
Nama antarmuka virtual	Nama untuk antarmuka virtual.
Pemilik antarmuka virtual	Jika Anda membuat antarmuka virtual untuk akun lain, Anda memerlukan ID akun AWS dari akun lainnya.
(Antarmuka virtual privat saja) Koneksi	Untuk terhubung ke VPC di Wilayah AWS yang sama, Anda memerluka n virtual private gateway 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,

Sumber Daya	Informasi yang diperlukan
	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, Partner AWS Direct Connect 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 satunya (dual-stack). Jangan gunakan IP Elastis (EIP) 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:
	  • (Antarmuka virtual publik saja) Anda harus menentukan alamat IPv4 publik yang unik yang Anda miliki. Nilai dapat menjadi salah satu dari yang berikut:
	  • IPv4 CIDR milik pelanggan
	
	Ini bisa berupa IP publik (milik pelanggan atau disediakan olehAWS), 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 AWSSupport untuk meminta IPv4 CIDR publik (dan berikan kasus penggunaan dalam permintaan Anda)
	
	Note
	Kami tidak dapat menjamin bahwa kami akan dapat memenuhi semua permintaan untuk alamat AWS IPv4 publik yang disediakan.

Sumber Daya	Informasi yang diperlukan
	• (Antarmuka virtual privat saja) Amazon dapat menghasilkan alamat IPv4 privat untuk Anda. Jika Anda menentukan sendiri, pastikan Anda menentukan CIDR pribadi untuk antarmuka router Anda dan antarmuka Direct AWS 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 CIDR IPv6 /125. Anda tidak dapat menentukan alamat IPv6 peer Anda sendiri.
Alamat keluarga	Apakah sesi peering BGP akan melalui IPv4 atau 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 mengaktifkan MD5 secara default. Anda tidak dapat mengubah opsi ini. • Kunci autentikasi 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	Rute IPv4 atau rute IPv6 publik untuk beriklan melalui BGP. Anda harus mengiklankan setidaknya satu prefiks menggunakan BGP, maksimum hingga 1.000 prefiks.
	• IPv4: CIDR IPv4 dapat tumpang tindih dengan CIDR IPv4 publik lain yang diumumkan menggunakan AWS Direct Connect ketika salah satu dari hal berikut ini benar:
	  • CIDR berasal dari Wilayah AWS yang berbeda. 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.
	• IPv6: Tentukan panjang prefiks /64 atau lebih pendek.
	• 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.
	• Anda dapat menentukan panjang awalan apa pun melalui antarmuka virtual publik Direct Connect. IPv4 harus mendukung apa pun dari /1 - /32, dan IPv6 harus mendukung apa pun dari /1 - /64.

Sumber Daya	Informasi yang diperlukan
(Antarmuka virtual privat saja) Bingkai Jumbo	Maximum transmission unit (MTU) paket melewati AWS Direct Connect. Default-nya 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 menambahk an 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 konsol AWS Direct Connect dan temukan Kemampuan bingkai jumbo di halaman Konfigurasi umum antarmuka virtual.
(Antarmuka virtual transit saja) Bingkai jumbo	Maximum transmission unit (MTU) paket melewati 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 instans EC2 dengan entri tabel rute statis VPC ke Lampiran Transit Gateway. Untuk memeriksa apakah koneksi atau antarmuka virtual mendukung bingkai jumbo, pilih di konsol AWS Direct Connect dan temukan Kemampuan bingkai jumbo di halaman Konfigurasi umum antarmuka virtual.

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

- Untuk VIF privat dan VIF transit, akun ini berlaku untuk antarmuka virtual dan virtual private gateway/Direct Connect gateway tujuan.

- Untuk VIF publik, akun ini digunakan untuk penagihan antarmuka virtual. Penggunaan Data Transfer Out (DTO) diukur terhadap pemilik sumber daya pada laju transfer data AWS Direct Connect.

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

Membuat 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 bagi akun dalam AWS Organizations, atau AWS Organizations yang berbeda dari milik Anda, buat antarmuka virtual yang di-host. Untuk informasi selengkapnya, lihat the section called “Membuat antarmuka virtual yang di-host”.

Prasyarat

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

Membuat antarmuka virtual 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 konsol AWS Direct Connect 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 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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

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

   b. Untuk menyediakan kunci BGP Anda sendiri, masukkan kunci BGP MD5 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 prefiks ke Amazon, untuk Prefiks yang ingin Anda iklankan, masukkan alamat tujuan CIDR IPv4 (dipisahkan dengan koma) tempat 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 ConnectAPI)

Membuat antarmuka virtual privat

Anda dapat menyediakan antarmuka virtual privat ke virtual private gateway di Wilayah yang sama dengan koneksi AWS Direct Connect. Untuk informasi lebih lanjut tentang penyediaan antarmuka virtual privat ke gateway AWS Direct Connect, lihat Bekerja dengan gateway Direct Connect.

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 privat virtual dapat sebesar 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.

Untuk menyediakan antarmuka virtual privat bagi VPC

1. Buka konsol AWS Direct Connect 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 Akun AWS saya jika antarmuka virtual adalah untuk akun AWS 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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

      > **Important**
      >
      > Jika Anda membiarkan AWS auto-menetapkan alamat IPv4, /29 CIDR akan dialokasikan dari 169.254.0.0/16 IPv4 Link-Local menurut RFC 3927 untuk konektivitas. point-to-point AWStidak merekomendasikan opsi ini jika Anda bermaksud menggunakan alamat IP rekan router pelanggan sebagai sumber dan/atau tujuan untuk lalu lintas VPC. Sebaliknya Anda harus menggunakan RFC 1918 atau pengalamatan lain (non-RFC 1918), dan tentukan sendiri alamatnya.

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

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

Membuat antarmuka virtual transit ke gateway Direct Connect

Untuk menghubungkan koneksi AWS Direct Connect transit gateway, 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 privat

virtual dapat sebesar 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.

Untuk menyediakan antarmuka virtual transit ke gateway Direct Connect

1. Buka konsol AWS Direct Connect 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 Akun AWS saya jika antarmuka virtual adalah untuk akun AWS 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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

> **Important**
>
> Jika Anda membiarkan AWS auto-menetapkan alamat IPv4, /29 CIDR akan dialokasikan dari 169.254.0.0/16 IPv4 Link-Local menurut RFC 3927 untuk konektivitas. point-to-point AWStidak merekomendasikan opsi ini jika Anda bermaksud menggunakan alamat IP rekan router pelanggan sebagai sumber dan/atau tujuan untuk lalu lintas VPC. Sebaliknya Anda harus menggunakan RFC 1918 atau pengalamatan lain (non-RFC 1918), dan tentukan sendiri alamatnya.
>
> - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
> - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat Lokal-Tautan IPv4.

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

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 ConnectAPI)

Mengunduh file konfigurasi 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 dengan MACsec diaktifkan, 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

1. Buka konsol AWS Direct Connect 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.

Pertimbangan MACsec

Jika Anda perlu mengonfigurasi router secara manual untuk 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>

Lihat detail antarmuka virtual

Anda dapat melihat status antarmuka virtual saat ini. Rincian meliputi:

- Status koneksi
- Nama
- Lokasi
- VLAN
- Detail BGP
- Alamat IP peer

Untuk melihat detail tentang antarmuka virtual

1. Buka konsol AWS Direct Connect 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 ConnectAPI)

Menambahkan atau menghapus peer BGP

Menambahkan atau menghapus sesi peering BGP IPv4 atau IPv6 ke antarmuka virtual Anda.

Antarmuka virtual dapat mendukung sesi peering BGP IPv4 tunggal dan sesi peering BGP IPv6 tunggal.

Anda tidak dapat menentukan alamat IPv6 peer Anda sendiri untuk sesi peering BGP IPv6. Amazon secara otomatis mengalokasikan Anda CIDR IPv6 /125.

BGP multiprotokol tidak didukung. IPv4 dan IPv6 beroperasi dalam mode dual-stack untuk antarmuka virtual.

AWS mengaktifkan MD5 secara default. Anda tidak dapat mengubah opsi ini.

Menambahkan peer BGP

Gunakan prosedur berikut untuk menambahkan peer BGP.

Untuk menambahkan peer BGP

1. Buka konsol AWS Direct Connect 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 privat) Untuk menambahkan peer BGP IPv4, lakukan hal berikut:
   - Pilih IPv4.
   - Untuk menentukan alamat IP ini sendiri, untuk IP peer router, masukkan alamat CIDR IPv4 tujuan tempat Amazon harus mengirimkan lalu lintas. Untuk IP peer router Amazon, masukkan alamat CIDR IPv4 yang akan digunakan untuk mengirim lalu lintas ke AWS.
6. (Antarmuka virtual publik) Untuk menambahkan peer BGP IPv4, lakukan hal berikut:
   - Untuk IP peer router Anda, masukkan alamat tujuan CIDR IPv4 tempat lalu lintas harus dikirim.
   - Untuk IP peer router Amazon, masukkan alamat CIDR IPv4 yang akan digunakan untuk mengirim lalu lintas ke AWS.

   > **Important**
   >
   > Jika Anda membiarkan AWS auto-menetapkan alamat IP, /29 CIDR akan dialokasikan dari 169.254.0.0/16. AWStidak merekomendasikan opsi ini jika Anda berniat menggunakan alamat IP peer router pelanggan sebagai sumber dan tujuan untuk lalu lintas. Sebagai gantinya, Anda harus menggunakan RFC 1918 atau pengalamatan lainnya, dan tentukan sendiri alamatnya. Untuk informasi lebih lanjut tentang RFC 1918 lihat Alokasi Alamat untuk Internet Pribadi.
7. (Antarmuka virtual privat atau publik) Untuk menambahkan peer BGP IPv6, pilih IPv6. Alamat IPv6 peer secara otomatis ditetapkan dari kolam alamat IPv6 Amazon; Anda tidak dapat menentukan alamat IPv6 kustom.
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 Autentikasi BGP, masukkan kunci BGP MD5 Anda.
10. Pilih Tambahkan peering.

Untuk membuat peer BGP menggunakan baris perintah atau API

- create-bgp-peer (AWS CLI)
- CreateBGPPeer (API AWS Direct Connect)

Menghapus peer BGP

Jika antarmuka virtual Anda memiliki sesi peering BGP IPv4 dan IPv6, Anda dapat menghapus salah satu sesi peering BGP (tetapi tidak keduanya).

Untuk menghapus peer BGP

1. Buka konsol AWS Direct Connect 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)
- DeleteBGPPeer (API AWS Direct Connect)

Mengatur MTU jaringan untuk antarmuka virtual privat atau antarmuka virtual transit

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.

Maximum transmission unit (MTU) dari koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang dapat diizinkan yang dapat dilewatkan melalui koneksi. MTU antarmuka privat virtual dapat sebesar 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.

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 instans EC2 tidak mendukung bingkai jumbo, instans akan menjatuhkan jumbo frame dari Direct Connect. Semua jenis instans EC2 mendukung bingkai jumbo kecuali C1, CC1, T1, dan M1. Untuk informasi selengkapnya, lihat Maximum Transmission Unit (MTU) Jaringan untuk Instans EC2 di Panduan Pengguna Amazon EC2 untuk Instans Linux.

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.

Untuk mengatur MTU antarmuka virtual privat

1. Buka konsol AWS Direct Connect 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 MTU Jumbo (MTU ukuran 9001) atau MTU Jumbo (MTU ukuran 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 ConnectAPI)

Menambah atau menghapus tanda antarmuka virtual

Tanda menyediakan cara untuk mengidentifikasi antarmuka virtual. Anda dapat menambahkan atau menghapus tanda jika Anda adalah pemilik akun untuk antarmuka virtual.

Untuk menambah atau menghapus tanda antarmuka virtual

1. Buka konsol AWS Direct Connect 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)

Menghapus antarmuka virtual

Menghapus satu atau lebih antarmuka virtual. Sebelum dapat menghapus koneksi, Anda harus menghapus antarmuka virtualnya. Menghapus antarmuka virtual akan menghentikan biaya transfer data AWS Direct Connect yang terkait dengan antarmuka virtual.

Untuk menghapus antarmuka virtual

1. Buka konsol AWS Direct Connect 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 ConnectAPI)

Membuat antarmuka virtual yang di-host

Anda dapat membuat antarmuka virtual yang di-host publik, transit, atau privat. Sebelum memulai, pastikan Anda telah membaca informasi di Prasyarat untuk antarmuka virtual.

Membuat antarmuka virtual privat yang di-host

Untuk membuat antarmuka virtual privat yang di-host

1. Buka konsol AWS Direct Connect 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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

> **Important**
>
> Jika Anda membiarkan AWS auto-menetapkan alamat IP, /29 CIDR akan dialokasikan dari 169.254.0.0/16. AWStidak merekomendasikan opsi ini jika Anda berniat menggunakan alamat IP peer router pelanggan sebagai sumber dan tujuan untuk lalu lintas. Sebaliknya Anda harus menggunakan RFC 1918 atau pengalamatan lain (non-RFC 1918), dan tentukan sendiri alamatnya. Untuk informasi lebih lanjut tentang RFC 1918 lihat Alokasi Alamat untuk Internet Pribadi.

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

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

c. (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.

7. Setelah antarmuka virtual yang di-host diterima oleh pemilik akun AWS lainnya, Anda dapat 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 ConnectAPI)

Membuat antarmuka virtual publik yang di-host

Untuk membuat antarmuka virtual publik yang di-host

1. Buka konsol AWS Direct Connect 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 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. Untuk mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

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

> **Important**
>
> Jika Anda membiarkan AWS auto-menetapkan alamat IP, /29 CIDR akan dialokasikan dari 169.254.0.0/16. AWStidak merekomendasikan opsi ini jika Anda berniat menggunakan alamat IP peer router pelanggan sebagai sumber dan tujuan untuk lalu lintas. Sebagai gantinya, Anda harus menggunakan RFC 1918 atau pengalamatan lainnya, dan tentukan sendiri alamatnya. Untuk informasi lebih lanjut tentang RFC 1918 lihat Alokasi Alamat untuk Internet Pribadi.

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

7. Untuk mengiklankan prefiks ke Amazon, untuk Prefiks yang ingin Anda iklankan, masukkan alamat tujuan CIDR IPv4 (dipisahkan dengan koma) tempat 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 di-host diterima oleh pemilik akun AWS lainnya, Anda dapat 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 ConnectAPI)

Membuat antarmuka virtual transit yang di-host

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 konsol AWS Direct Connect 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 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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

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

> **Important**
>
> Jika Anda membiarkan AWS auto-menetapkan alamat IP, /29 CIDR akan dialokasikan dari 169.254.0.0/16. AWStidak merekomendasikan opsi ini jika Anda berniat menggunakan alamat IP peer router pelanggan sebagai sumber dan tujuan untuk lalu lintas. Sebagai gantinya, Anda harus menggunakan RFC 1918 atau pengalamatan lainnya, dan tentukan sendiri alamatnya. Untuk informasi lebih lanjut tentang RFC 1918 lihat Alokasi Alamat untuk Internet Pribadi.

[IPv6] Untuk mengonfigurasi peer BGP IPv6, pilih IPv6. Alamat IPv6 peer secara otomatis ditetapkan dari kolam alamat IPv6 Amazon. Anda tidak dapat menentukan alamat IPv6 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 di-host diterima oleh pemilik akun AWS lainnya, Anda dapat 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 ConnectAPI)

Menerima antarmuka virtual yang di-host

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.

Untuk menerima antarmuka virtual yang di-host

1. Buka konsol AWS Direct Connect 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 ConnectAPI)

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

- confirm-public-virtual-interface (AWS CLI)
- ConfirmPublicVirtualInterface(AWS Direct ConnectAPI)

Untuk menerima antarmuka virtual transit yang di-host menggunakan baris perintah atau API

- confirm-transit-virtual-interface (AWS CLI)
- ConfirmTransitVirtualInterface(AWS Direct ConnectAPI)

Memigrasikan antarmuka 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. ID VLAN unik; oleh karena itu, memigrasikan VIF dengan cara ini berarti VLAN 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 konsol AWS Direct Connect 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

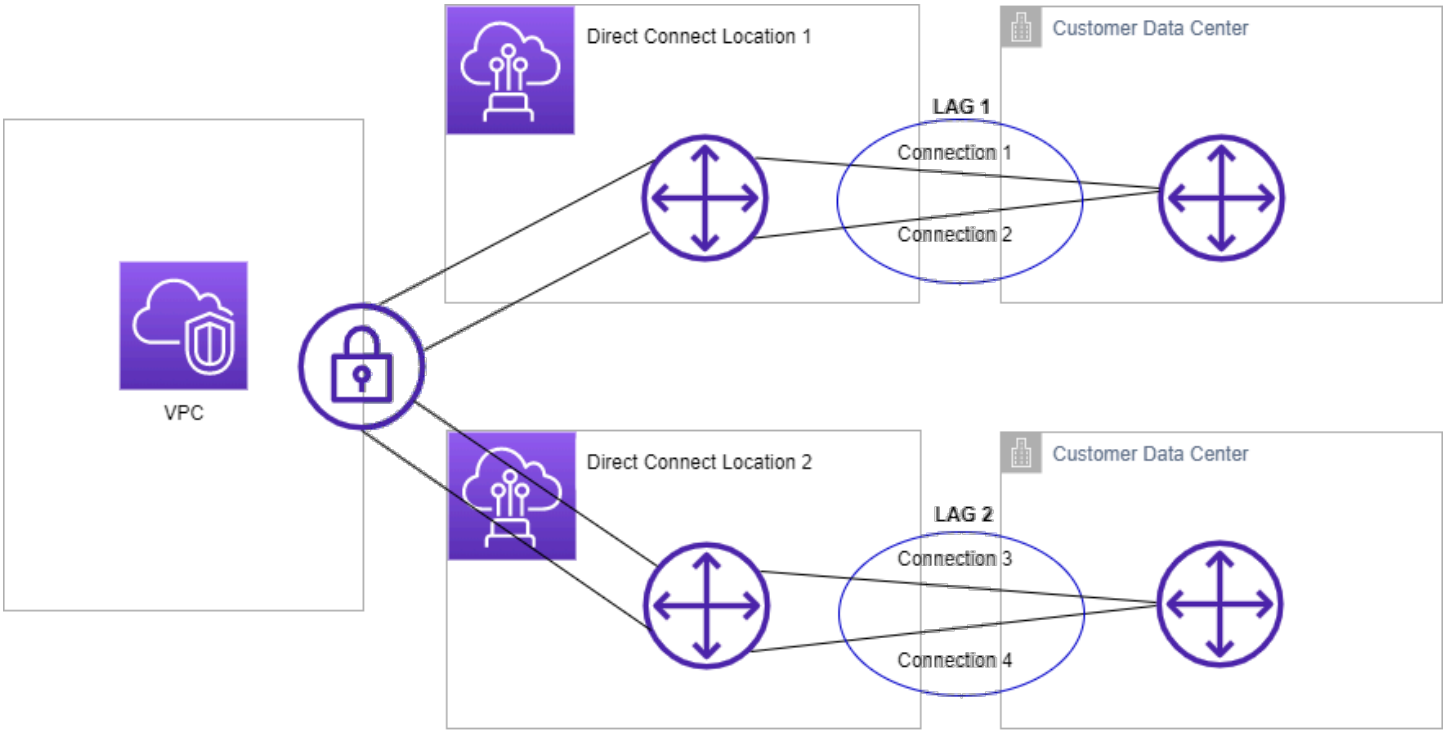
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface(AWS Direct ConnectAPI)

Grup agregasi tautan

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 mengagregat beberapa koneksi di satu titik akhir AWS Direct Connect, memungkinkan Anda memperlakukannya sebagai satu koneksi terkelola. LAG 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 dua LAG 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 berikut berlaku:

- Semua koneksi harus berupa koneksi khusus dan memiliki kecepatan port 1 Gbps, 10 Gbps, atau 100 Gbps.
- Semua koneksi di LAG harus menggunakan bandwidth yang sama.
- Anda dapat memiliki maksimal dua koneksi 100G, atau empat koneksi dengan kecepatan port kurang dari 100G di LAG. Setiap koneksi di LAG dihitung terhadap batas koneksi Anda secara keseluruhan untuk Wilayah.
- Semua koneksi di LAG harus berakhir di titik akhir AWS Direct Connect yang sama.
- LAG didukung untuk semua jenis antarmuka virtual—publik, pribadi, dan transit.

Ketika membuat LAG, Anda dapat mengunduh Letter of Authorization dan Connecting Facility Assignment (LOA-CFA) untuk setiap koneksi fisik baru secara individual dari konsol AWS Direct Connect. Untuk informasi selengkapnya, lihat Unduh LOA-CFA.

Semua LAG memiliki atribut yang menentukan jumlah minimum koneksi di LAG yang harus operasional agar LAG itu sendiri dapat menjadi operasional. Secara default, LAG baru memiliki atribut yang diatur 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**
>
> Ketika Anda membuat LAG atau mengaitkan lebih banyak koneksi dengan LAG, kami mungkin tidak dapat menjamin cukup port tersedia pada titik akhir AWS Direct Connect tertentu.

Pertimbangan MACsec

Pertimbangkan hal berikut ketika Anda ingin mengonfigurasi MACsec pada LAG:

- Ketika Anda membuat LAG dari koneksi yang ada, kami memisahkan semua kunci MACsec dari koneksi. Kemudian kita menambah koneksi ke LAG, dan mengaitkan kunci LAG MACsec dengan koneksi.

- Ketika Anda mengaitkan koneksi yang ada ke LAG, kunci MACsec yang saat ini terkait dengan LAG akan dikaitkan dengan koneksi. Oleh karena itu, kami memisahkan kunci MACsec dari koneksi, menambahkan koneksi ke LAG, lalu mengaitkan kunci LAG MACsec dengan koneksi.

Membuat LAG

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 perangkat AWS yang sama (berakhir di titik akhir AWS Direct Connect 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.

Create a LAG with new connections using the console

Untuk membuat LAG dengan koneksi baru

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAG.
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 100G.

- (Opsional) Mengonfigurasi MAC Security (MACsec) untuk koneksi. Di bawah Pengaturan Tambahan, pilih Minta port berkemampuan MACsec.

  MACsec hanya tersedia pada koneksi khusus.
- (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.

5. Pilih Buat LAG.

Create a LAG with existing connections using the console

Untuk membuat LAG dari koneksi yang ada

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAG.
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 100G.
   - 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.

Command line

Untuk membuat LAG menggunakan baris perintah atau API

- create-lag (AWS CLI)
- CreateLag(AWS Direct ConnectAPI)

Untuk mendeksripsikan LAG menggunakan baris perintah atau API

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

Untuk mengunduh LOA-CFA menggunakan baris perintah atau API

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct ConnectAPI)

Setelah membuat LAG, Anda dapat mengaitkan atau memisahkan koneksi dari LAG. Untuk informasi selengkapnya, lihat Mengaitkan koneksi dengan LAG dan Memisahkan koneksi dari LAG.

Menampilkan detail LAG Anda

Setelah membuat LAG, Anda dapat melihat detailnya.

Console

Untuk melihat informasi tentang LAG Anda

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAG.
3. Pilih LAG dan pilih Lihat detail.
4. Anda dapat melihat informasi tentang LAG, termasuk ID dan titik akhir AWS Direct Connect tempat koneksi berakhir.

Command line

Untuk melihat informasi tentang LAG menggunakan baris perintah atau API

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

Memperbarui LAG

Anda dapat memperbarui atribut grup agregasi tautan (LAG) berikut:

- Nama LAG.
- Nilai minimum dari jumlah koneksi yang harus operasional agar LAG itu sendiri dapat menjadi operasional.
- Mode enkripsi MACsec LAG.

  MACsec hanya tersedia pada koneksi khusus.

  AWS menetapkan nilai ini untuk 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.

Console

Untuk memperbarui LAG

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAG.
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.

Command line

Untuk memperbarui LAG menggunakan baris perintah atau API

- update-lag (AWS CLI)
- UpdateLag(AWS Direct ConnectAPI)

Untuk menambah tanda atau menghapus tanda menggunakan baris perintah

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Mengaitkan koneksi dengan LAG

Anda dapat mengaitkan koneksi yang ada dengan LAG. Koneksi dapat bersifat mandiri, atau dapat berupa bagian dari LAG lain. Koneksi harus berada di perangkat AWS 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 terganggu selama pengaitan.

Console

Untuk mengaitkan koneksi dengan LAG

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAG.
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.

Command line

Untuk mengaitkan koneksi menggunakan baris perintah atau API

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag(AWS Direct ConnectAPI)

Memisahkan koneksi dari LAG

Mengonversi koneksi menjadi mandiri dengan memisahkannya dari LAG. 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 ke AWS terputus selama pemisahan.

Console

Untuk memisahkan koneksi dari LAG

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel sebelah kiri, pilih LAG.
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.

Command line

Untuk memutuskan koneksi menggunakan baris perintah atau API

- disassociate-connection-from-lag (AWS CLI)
- DisassociateConnectionFromLag(AWS Direct ConnectAPI)

Mengaitkan CKN/CAK MACsec dengan LAG

Setelah membuat LAG yang mendukung MACsec, Anda dapat mengaitkan CKN/CAK dengan koneksi.

> **Note**
>
> Anda tidak dapat mengubah kunci rahasia MACsec setelah 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 "Menghapus pengaitan antara semua kunci rahasia MACsec dan LAG.".

Console

Untuk mengaitkan kunci MACsec dengan LAG

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAG.
3. Pilih LAG dan pilih Lihat detail.
4. Pilih Kaitkan kunci.
5. Masukkan kunci MACsec.

   [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.

   [Menggunakan rahasia] Pilih Rahasia Secret Manager yang ada, lalu untuk Rahasia, pilih kunci rahasia MACsec.
6. Pilih Kaitkan kunci.

Command line

Untuk mengaitkan kunci MACsec dengan LAG

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(AWS Direct ConnectAPI)

Menghapus pengaitan antara semua kunci rahasia MACsec dan LAG.

Anda dapat menghapus pengaitan antara LAG dan kunci MACsec.

Console

Untuk menghapus pengaitan antara LAG dan kunci MACsec

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.

2. Di panel navigasi, pilih LAG.
3. Pilih LAG dan pilih Lihat detail.
4. Pilih rahasia MACsec yang ingin dihapus, lalu pilih Pisahkan kunci.
5. Di kotak dialog konfirmasi, masukkan pisahkan, lalu pilihPisahkan.

Command line

Untuk menghapus pengaitan antara LAG dan kunci MACsec

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct ConnectAPI)

Menghapus LAG

Anda dapat menghapus LAG jika tidak lagi membutuhkannya. 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 Hapus koneksi.

Console

Untuk menghapus LAG

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih LAG.
3. Pilih LAG, lalu pilih Hapus.
4. Di kotak dialog konfirmasi, pilih Hapus.

Command line

Untuk menghapus LAG menggunakan baris perintah atau API

- delete-lag (AWS CLI)
- DeleteLag(AWS Direct ConnectAPI)

Bekerja dengan gateway Direct Connect

Anda dapat bekerja dengan AWS Direct Connect gateway menggunakan konsol VPC Amazon atau. AWS CLI

Daftar Isi

Gateway Direct Connect

Gunakan AWS Direct Connect gateway untuk menghubungkan VPC Anda. Anda mengaitkan AWS Direct Connect gateway dengan salah satu gateway berikut:

- Transit gateway saat Anda memiliki beberapa VPC di Wilayah yang sama
- Virtual private gateway

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 China.

Pelanggan yang menggunakan Direct Connect dengan VPC 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 VPC, yang memiliki gateway pribadi virtual (VGW) terlampir yang terkait dengan gateway Direct Connect yang sama dan pada antarmuka virtual yang sama. Dalam hal ini, VPC 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 VPC yang dilampirkan ke gateway Direct Connect (misalnya, 10.0.0.0/24 dan 10.0.1.0/24), dan pada antarmuka virtual yang sama, maka dari jaringan lokal Anda, VPC dapat berkomunikasi satu sama lain.

Jika Anda ingin memblokir komunikasi VPC-ke-VPC dalam gateway Direct Connect, lakukan hal berikut:

1. Siapkan grup keamanan pada instance dan sumber daya lain di VPC untuk memblokir lalu lintas antar VPC, juga menggunakan ini sebagai bagian dari grup keamanan default di VPC.
2. Hindari mengiklankan supernet dari jaringan lokal Anda yang tumpang tindih dengan VPC Anda. Sebagai gantinya, Anda dapat mengiklankan rute yang lebih spesifik dari jaringan lokal Anda yang tidak tumpang tindih dengan VPC Anda.
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 VPC. Misalnya, alih-alih menggunakan satu Direct Connect Gateway untuk pengembangan dan produksi VPC Anda, gunakan Direct Connect Gateways terpisah untuk masing-masing VPC ini.

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 VPC yang terhubung ke gateway transit yang terkait dengan gateway Direct Connect yang sama, VPC dapat berkomunikasi. Untuk mencegah VPC berkomunikasi, kaitkan tabel rute dengan lampiran VPC yang memiliki opsi lubang hitam yang disetel.

Berikut ini menjelaskan skenario di mana Anda dapat menggunakan gateway Direct Connect.

Skenario

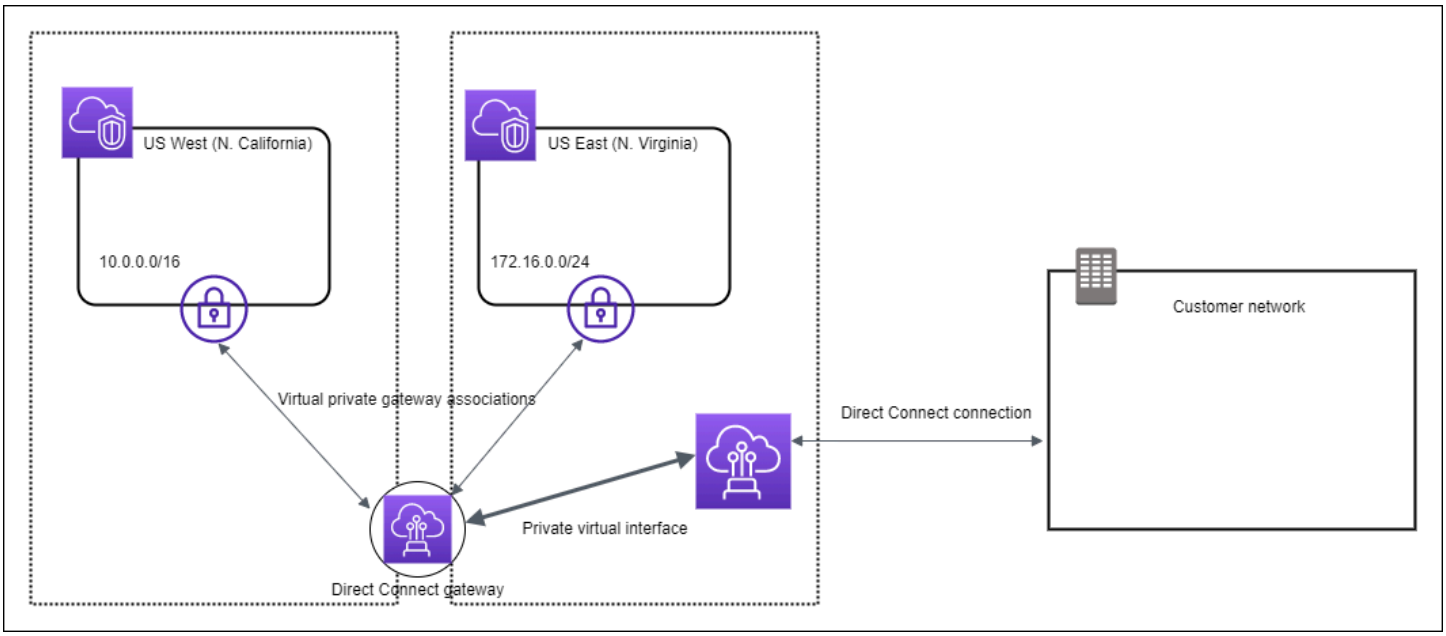
- Keterkaitan virtual private gateway
- Keterkaitan virtual private gateway di seluruh akun
- Keterkaitan transit gateway
- Keterkaitan transit gateway di seluruh akun

- Membuat gateway Direct Connect
- Menghapus gateway Direct Connect
- Bermigrasi dari virtual private gateway ke gateway Direct Connect

Keterkaitan virtual private gateway

Dalam diagram berikut, gateway Direct Connect memungkinkan Anda untuk menggunakan koneksi AWS Direct Connect di Wilayah US East (N. Virginia) untuk mengakses VPC di akun Anda di Wilayah US East (N. Virginia) dan US West (N. California).

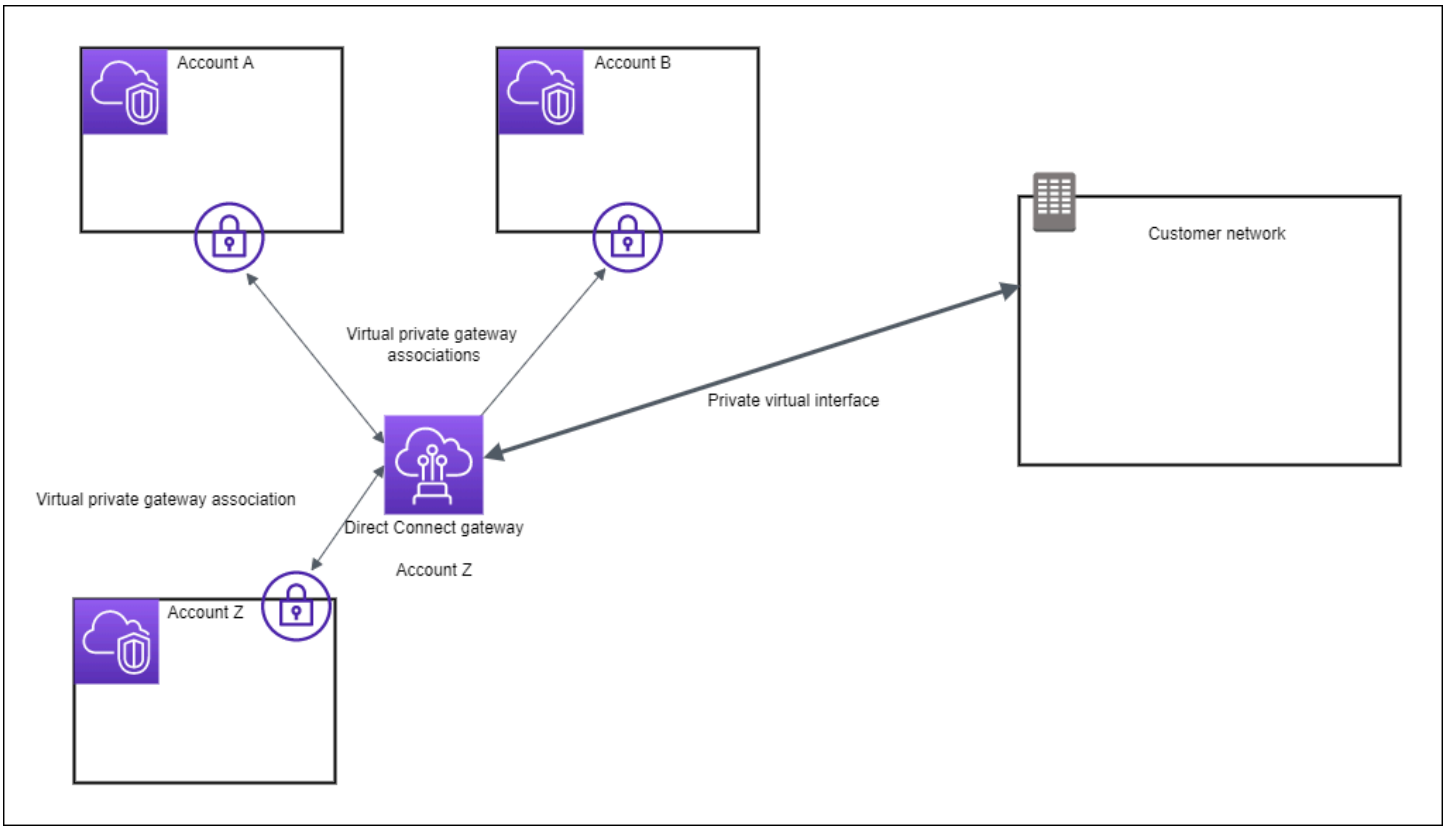
Setiap VPC memiliki virtual private gateway yang terhubung ke gateway Direct Connect menggunakan keterkaitan virtual private gateway. Gateway Direct Connect menggunakan antarmuka virtual pribadi untuk koneksi ke AWS Direct Connect lokasi. Ada koneksi AWS Direct Connect dari lokasi ke pusat data pelanggan.



Keterkaitan virtual private gateway di seluruh akun

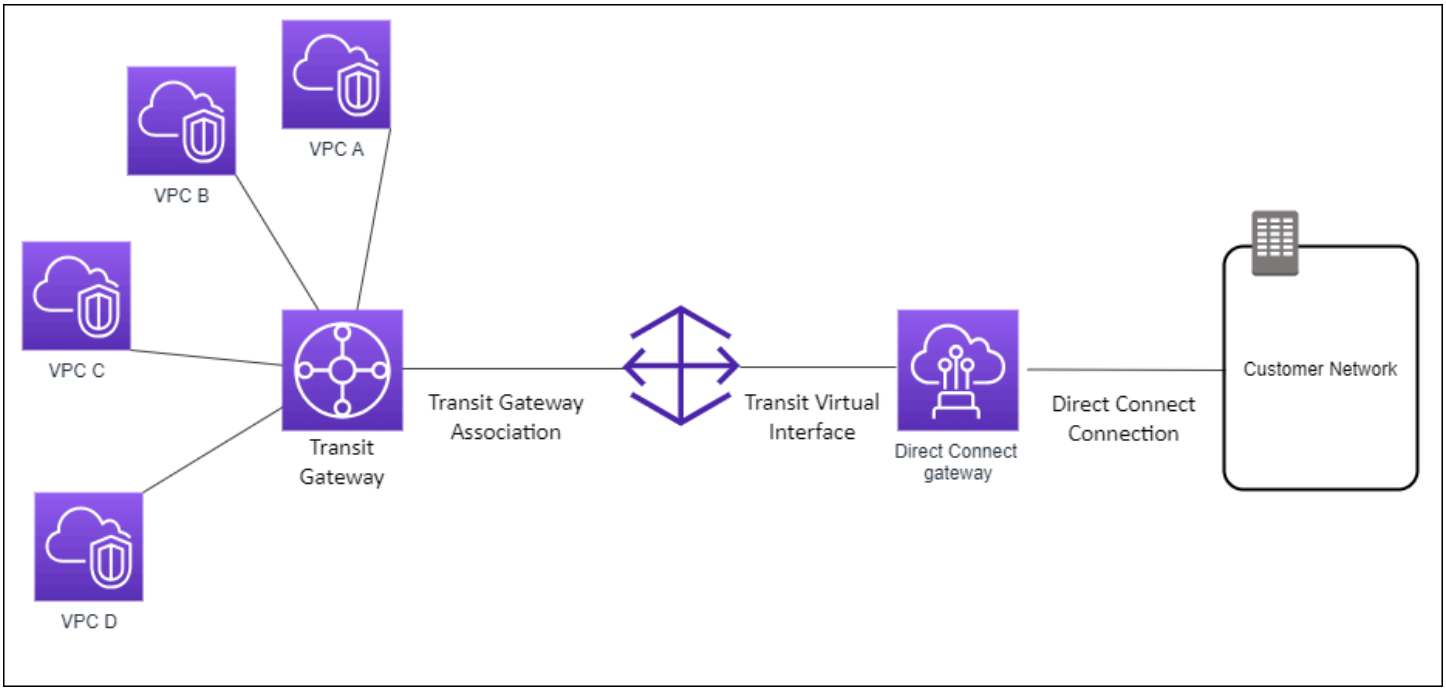
Pertimbangkan skenario pemilik gateway Direct Connect (Akun Z) yang memiliki gateway Direct Connect ini. Akun A dan Akun B ingin menggunakan gateway Direct Connect. Akun A dan Akun B masing-masing mengirim proposal keterkaitan ke Akun Z. Akun Z menerima proposal keterkaitan dan secara opsional dapat 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.



Keterkaitan transit gateway

Diagram berikut menggambarkan bagaimana gateway Direct Connect memungkinkan Anda membuat satu koneksi ke koneksi Direct Connect yang dapat digunakan oleh semua VPC Anda.



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:

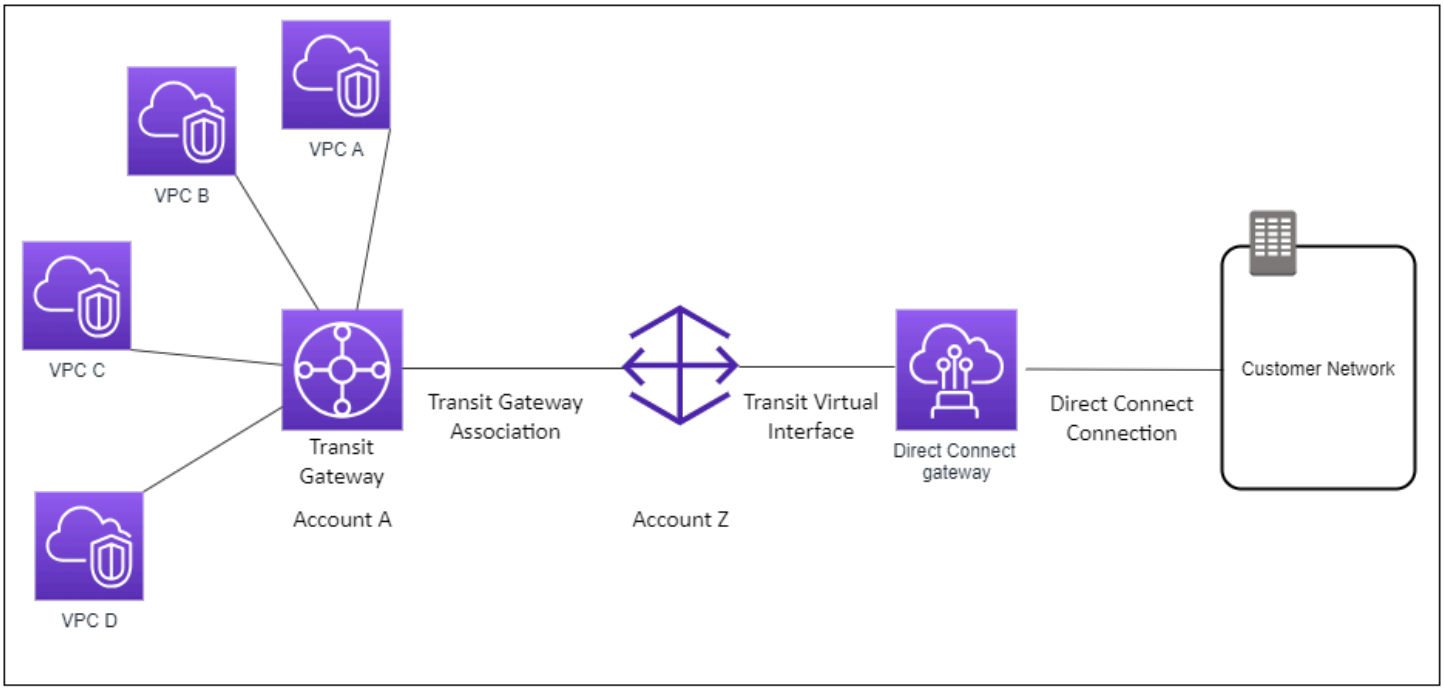
- Mengelola satu koneksi untuk beberapa VPC atau VPN yang berada di Wilayah yang sama.
- Iklankan awalan dari lokal ke AWS dan dari ke lokal. AWS

Untuk informasi tentang mengonfigurasi transit gateway, lihat Bekerja dengan Transit Gateway di Panduan Transit Amazon VPC.

Keterkaitan transit gateway di seluruh 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, VPC yang terlampir pada transit

gateway dapat merutekan lalu lintas dari transit gateway ke gateway Direct Connect. Akun Z juga memiliki perutean ke pelanggan karena Akun Z memiliki gateway.



Daftar Isi

Membuat gateway Direct Connect

Anda dapat membuat gateway Direct Connect di Wilayah yang didukung.

Untuk membuat gateway Direct Connect

1. Buka konsol AWS Direct Connect 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.
- Virtual private gateway: Untuk mengaitkan virtual private gateway, pilih virtual private gateway.

Untuk membuat gateway Direct Connect menggunakan baris perintah atau API

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway(AWS Direct Connect API)

Menghapus gateway Direct Connect

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.

Menghapus gateway Direct Connect

1. Buka konsol AWS Direct Connect 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)

Bermigrasi dari virtual private gateway ke gateway Direct Connect

Jika Anda memiliki virtual private gateway yang terlampir pada antarmuka virtual, dan Anda ingin bermigrasi ke gateway Direct Connect, lakukan langkah-langkah berikut:

Untuk bermigrasi ke gateway Direct Connect

1. Buat gateway Direct Connect. Untuk informasi selengkapnya, lihat the section called “Membuat gateway Direct Connect”.

2. Buat antarmuka virtual untuk gateway Direct Connect. Untuk informasi selengkapnya, lihat the section called “Membuat antarmuka virtual”.
3. Kaitkan virtual private gateway dengan gateway Direct Connect. Untuk informasi selengkapnya, lihat the section called “Mengaitkan dan memisahkan virtual private gateway”.
4. Hapus antarmuka virtual yang dikaitkan dengan virtual private gateway. Untuk informasi selengkapnya, lihat the section called “Menghapus antarmuka virtual”.

Keterkaitan virtual private gateway

Anda dapat menggunakan AWS Direct Connect gateway untuk menghubungkan koneksi AWS Direct Connect melalui antarmuka virtual privat ke satu atau beberapa VPC di setiap akun yang terletak 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.
- Anda tidak dapat melampirkan gateway Direct Connect ke gateway pribadi virtual ketika gateway Direct Connect sudah dikaitkan dengan gateway transit.
- VPC yang Anda terhubung 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 CIDR IPv4 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 VPC 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.

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 AWS Direct Connect.

Daftar Isi

- Membuat antarmuka virtual privat ke gateway Direct Connect
- Mengaitkan virtual private gateway di seluruh akun

Membuat virtual private gateway

Virtual private gateway harus dilampirkan ke VPC yang ingin Anda hubungkan.

> **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 VPC yang terhubung melalui ASN yang ditugaskan untuk itu.

Setelah Anda membuat virtual private gateway, Anda harus melampirkannya ke VPC Anda.

Untuk membuat gateway privat virtual dan melampirkannya ke VPC Anda

1. Buka konsol AWS Direct Connect 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 (Amazon EC2 Query API)

- 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 (Amazon EC2 Query API)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Mengaitkan dan memisahkan virtual private gateway

Anda dapat mengaitkan atau memisahkan virtual private gateway dan gateway Direct Connect. Pemilik akun virtual private gateway melakukan operasi ini.

Untuk mengaitkan virtual private gateway

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.
2. Di panel navigasi, pilih gateway Direct Connect dan kemudian pilih gateway Direct Connect.
3. Pilih View details (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 konsol AWS Direct Connect 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)

Membuat antarmuka virtual privat ke gateway Direct Connect

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.

> **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 konsol AWS Direct Connect 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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

> **Important**
>
> Jika Anda membiarkan AWS auto-menetapkan alamat IPv4, /29 CIDR akan dialokasikan dari 169.254.0.0/16 IPv4 Link-Local menurut RFC 3927 untuk konektivitas. point-to-point AWS tidak merekomendasikan opsi ini jika Anda bermaksud menggunakan alamat IP rekan router pelanggan sebagai sumber dan/atau tujuan untuk lalu lintas VPC. Sebagai gantinya, Anda harus menggunakan RFC 1918 atau pengalamatan lainnya (non-RFC 1918), dan tentukan sendiri alamatnya.
>
> - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.
> - Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat Lokal-Tautan IPv4.

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

Mengaitkan virtual private gateway 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 prefiks bertindak sebagai filter yang mengizinkan CIDR yang sama, atau CIDR yang lebih kecil 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 the section called “Interaksi prefiks yang diizinkan”.

Tugas

- Membuat proposal keterkaitan
- Menerima atau menolak proposal keterkaitan
- Memperbarui prefiks yang diizinkan untuk sebuah keterkaitan
- Menghapus proposal keterkaitan

Membuat proposal keterkaitan

Jika Anda memiliki virtual private gateway, Anda harus membuat proposal keterkaitan. Gateway pribadi virtual harus dilampirkan ke VPC di akun Anda AWS . Pemilik gateway Direct Connect harus membagikan ID gateway Direct Connect dan ID AWS akunnya. Setelah membuat proposal, pemilik gateway Direct Connect harus menerimanya agar Anda dapat memperoleh akses ke jaringan on-premise melalui AWS Direct Connect.

Untuk membuat proposal keterkaitan

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Virtual private gatewaydan pilih virtual private gateway.
3. Pilih Lihat detail.
4. PilihKeterkaitan gateway Direct Connect dan 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 AWS 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 gateway Direct Connect, masukkan ID AWS akun yang memiliki gateway Direct Connect untuk asosiasi tersebut.
   c. (Opsional) Untuk menentukan daftar prefiks yang diizinkan dari virtual private gateway, tambahkan prefiks ke Prefiks yang diizinkan, memisahkannya menggunakan koma, atau memasukkannya ke baris terpisah.
8. Pilih Kaitkan 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 proposal keterkaitan

Jika Anda memiliki gateway Direct Connect, Anda harus menerima proposal keterkaitan untuk membuat keterkaitan. Jika tidak, Anda dapat menolak proposal keterkaitan.

Untuk menerima proposal keterkaitan

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Gateway Direct Connect.
3. Pilih gateway Direct Connect dengan proposal tertunda dan pilih Lihat detail.
4. Pada tab Proposal tertunda, pilih proposal dan pilih Terima proposal.

5. ((Opsional) Untuk menentukan daftar prefiks yang diizinkan dari virtual private 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 konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Gateway Direct Connect.
3. Pilih gateway Direct Connect dengan proposal tertunda dan pilih Lihat detail.
4. Pada tab Proposal tertunda, pilih virtual private gateway dan pilih Tolak proposal.
5. Di kotak dialog Tolak proposal, masukkan Hapus dan 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)

Memperbarui prefiks yang diizinkan untuk sebuah keterkaitan

Anda dapat memperbarui prefiks yang diizinkan dari virtual private gateway melalui gateway Direct Connect.

Jika Anda adalah pemilik virtual private gateway, buat proposal keterkaitan baru untuk gateway Direct Connect dan virtual private gateway yang sama, menentukan prefiks untuk diizinkan.

Jika Anda pemilik gateway Direct Connect, perbarui prefiks yang diizinkan saat menerima proposal keterkaitanatau memperbarui prefiks yang diizinkan untuk keterkaitan yang ada sebagai berikut.

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)

Menghapus proposal keterkaitan

Pemilik virtual private gateway dapat menghapus proposal keterkaitan gateway Direct Connect jika masih menunda penerimaan. Setelah proposal keterkaitan diterima, Anda tidak dapat menghapusnya, tetapi Anda dapat memisahkan virtual private gateway dari gateway Direct Connect. Untuk informasi selengkapnya, lihat the section called “Mengaitkan dan memisahkan virtual private gateway”.

Untuk menghapus proposal keterkaitan

1. Buka konsol AWS Direct Connect di https://console.aws.amazon.com/directconnect/v2/home.
2. Di panel navigasi, pilih Virtual private gatewaydan pilih virtual private gateway.
3. Pilih Lihat detail.
4. Pilih Keterkaitan gateway Direct Connect tertunda, pilih keterkaitan dan pilih Hapus keterkaitan.
5. Di kotak dialog Hapus proposal keterkaitan, masukkan Hapus dan 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)

Keterkaitan transit gateway

Anda dapat menggunakan AWS Direct Connect gateway untuk menghubungkan AWS Direct Connect melalui antarmuka virtual transit ke VPC atau VPN yang terlampir pada transit gateway 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.
- Gateway Direct Connect mendukung komunikasi antara antarmuka virtual transit terlampir dan gateway transit terkait.
- Jika Anda terhubung ke beberapa transit gateway yang berada di Wilayah yang berbeda, gunakan ASN unik untuk setiap transit gateway.
- Antarmuka virtual apa pun di dalam awalan jaringan yang diiklankan melalui Direct Connect hanya disebarkan ke gateway transit di seluruh Wilayah, tetapi tidak dalam Wilayah yang sama

Mengaitkan dan memisahkan transit gateway

Untuk mengaitkan transit gateway

1. Buka konsol AWS Direct Connect 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. the section called “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 konsol AWS Direct Connect 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 konsol AWS Direct Connect 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 modifikasi dan kemudian 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 CIDR VPC Amazon untuk semua gateway pribadi virtual. Untuk informasi selengkapnya tentang awalan yang diizinkan, lihat. the section called “Interaksi prefiks yang diizinkan”
6. Pilih Edit asosiasi.

   Di bagian asosiasi Gateway, Negara menampilkan pemutakhiran. Ketika selesai, Negara berubah menjadi terkait.
7. Pilih Pisahkan.
8. Pilih Disassociate lagi untuk mengonfirmasi bahwa Anda ingin memisahkan gateway.

   Di bagian asosiasi Gateway, Negara menampilkan disassociating. Setelah selesai, pesan konfirmasi akan ditampilkan dan gateway dihapus dari bagian tersebut. 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)

Membuat antarmuka virtual transit ke gateway Direct Connect

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

> **Important**
>
> Jika Anda mengaitkan transit gateway Anda 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 konsol AWS Direct Connect 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 mengonfigurasi BGP IPv4 atau peer IPv6, lakukan hal berikut:

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

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

      > **Important**
      >
      > Jika Anda membiarkan AWS auto-menetapkan alamat IPv4, /29 CIDR akan dialokasikan dari 169.254.0.0/16 IPv4 Link-Local menurut RFC 3927 untuk konektivitas. point-to-point AWS tidak merekomendasikan opsi ini jika Anda bermaksud menggunakan alamat IP rekan router pelanggan sebagai sumber dan/atau tujuan untuk lalu lintas VPC. Sebagai gantinya, Anda harus menggunakan RFC 1918 atau pengalamatan lainnya (non-RFC 1918), dan tentukan sendiri alamatnya.
      >
      > - Untuk informasi lebih lanjut tentang RFC 1918, lihat Alokasi Alamat untuk Internet Pribadi.

- Untuk informasi selengkapnya tentang RFC 3927, lihat Konfigurasi Dinamis Alamat Lokal-Tautan IPv4.

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

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 VPC yang dilampirkan ke gateway transit tidak memiliki CIDR yang ditetapkan. Prefiks dalam daftar prefiks Direct Connect yang diizinkan berasal dari gateway Direct Connect dan diiklankan ke jaringan on-premise. Untuk informasi selengkapnya tentang bagaimana prefiks yang diizinkan berinteraksi dengan transit gateway dan virtual private gateway, lihat the section called “Interaksi prefiks yang diizinkan”.

Tugas

- Membuat proposal keterkaitan transit gateway
- Menerima atau menolak proposal keterkaitan transit gateway
- Memperbarui prefiks yang diizinkan untuk keterkaitan transit gateway
- Menghapus proposal keterkaitan transit gateway

Membuat proposal keterkaitan transit gateway

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.

Untuk membuat proposal keterkaitan

1. Buka konsol AWS Direct Connect 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 proposal keterkaitan transit gateway

Jika Anda memiliki gateway Direct Connect, Anda harus menerima proposal keterkaitan untuk membuat keterkaitan. Anda juga memiliki opsi untuk menolak proposal keterkaitan.

Untuk menerima proposal keterkaitan

1. Buka konsol AWS Direct Connect 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 konsol AWS Direct Connect 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)

Memperbarui prefiks yang diizinkan untuk keterkaitan transit gateway

Anda dapat memperbarui prefiks yang diizinkan dari transit gateway melalui gateway Direct Connect.

Jika Anda adalah pemilik transit gateway, buat proposal keterkaitan baru untuk gateway Direct Connect dan virtual private gateway yang sama, menentukan prefiks untuk yang akan diizinkan.

Jika Anda pemilik gateway Direct Connect, perbarui prefiks yang diizinkan saat menerima proposal keterkaitan atau memperbarui prefiks yang diizinkan untuk keterkaitan yang ada sebagai berikut.

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)

Menghapus proposal keterkaitan transit gateway

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 the section called “Membuat proposal keterkaitan transit gateway”.

Untuk menghapus proposal keterkaitan

1. Buka konsol AWS Direct Connect 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)

Interaksi prefiks yang diizinkan

Pelajari bagaimana prefiks yang diizinkan berinteraksi dengan transit gateway dan virtual private gateway. Untuk informasi selengkapnya, lihat the section called “Kebijakan perutean dan komunitas BGP”.

Keterkaitan virtual private gateway

Daftar prefiks (IPv4 dan IPv6) bertindak sebagai filter yang mengizinkan CIDR yang sama, atau rentang CIDR yang lebih kecil 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` ke`updating`. Memodifikasi awalan yang ada hanya dapat menunda 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 ketika VPC yang dilampirkan ke gateway transit tidak memiliki CIDR yang ditetapkan. 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 CIDR yang sama atau lebih kecil.

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.

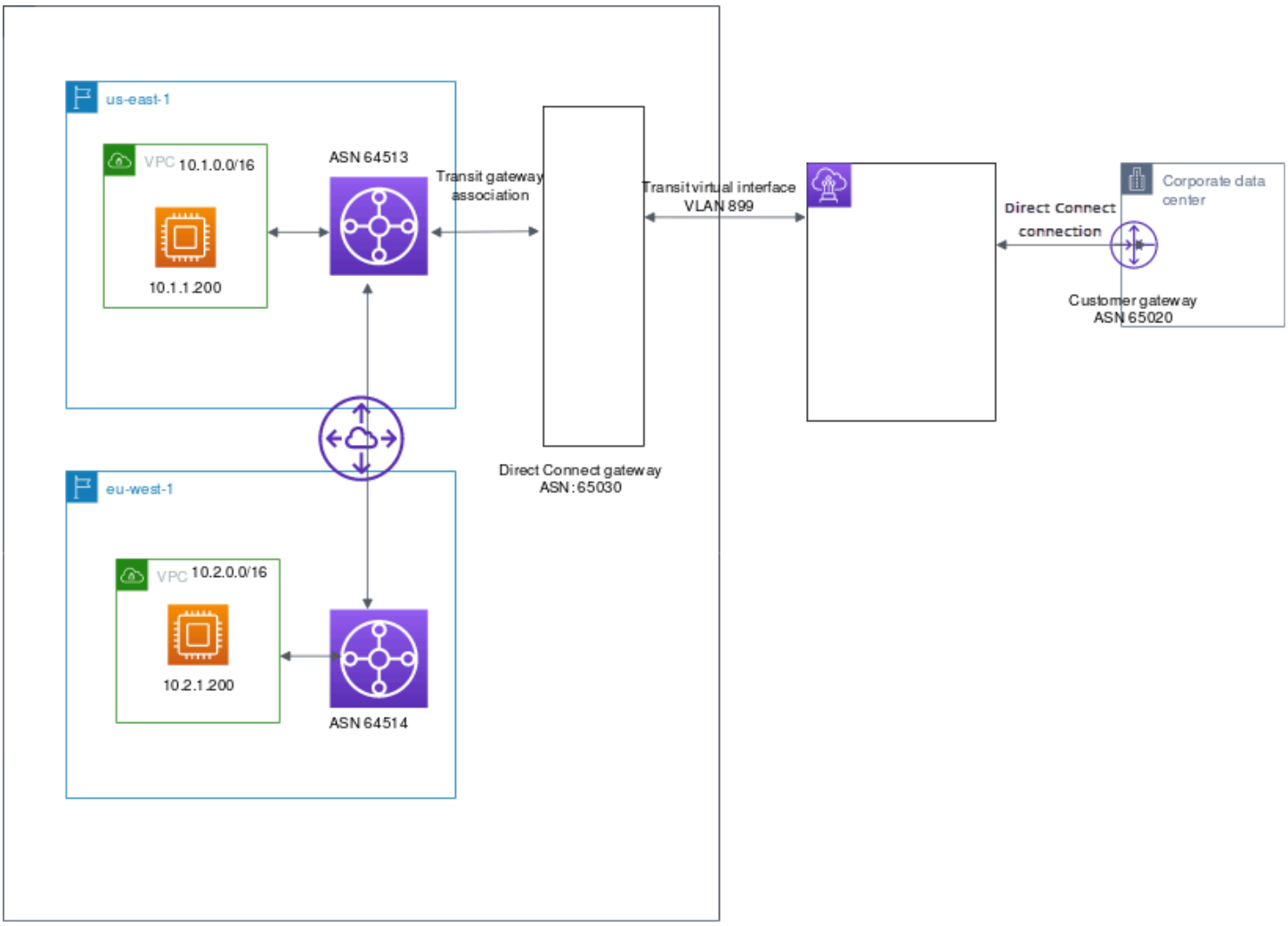
Tumpang tindih awalan yang diizinkan tidak diperbolehkan ketika beberapa gateway transit dikaitkan dengan gateway Direct Connect. Misalnya, jika Anda memiliki gateway transit dengan daftar awalan yang diizinkan yang mencakup 10.1.0.0/16, dan gateway transit kedua dengan daftar awalan yang diizinkan yang 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 mencakup semua jaringan IPv4, 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` ke`updating`. Memodifikasi awalan yang ada hanya dapat menunda 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 the section called “Membuat gateway Direct Connect”.
- Transit antarmuka virtual: Atur VLAN ke 899, dan ASN ke 65020. Untuk informasi selengkapnya, lihat the section called “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 the section called “Mengaitkan dan memisahkan transit gateway”.
- 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.

Penandaan pada sumber daya AWS Direct Connect

Tanda adalah sebuah label yang diberikan oleh pemilik sumber daya kepada mereka sumber daya AWS Direct Connect mereka. Setiap tanda terdiri atas sebuah kunci dan sebuah nilai opsional, yang keduanya Anda tentukan. Tanda memungkinkan pemilik sumber daya untuk mengategorikan sumber daya AWS Direct Connect 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 koneksi AWS Direct Connect 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 serangkaian kunci tanda akan mempermudah Anda dalam mengelola sumber daya Anda. Tanda tidak memiliki makna semantik pada AWS Direct Connect dan diterjemahkan sebagai serangkaian karakter saja. Selain itu, tanda tidak secara otomatis ditetapkan ke sumber daya Anda. Anda dapat mengedit kunci dan nilai tanda, dan Anda dapat membuang tanda dari sumber daya kapan saja. Anda dapat mengatur nilai tanda menjadi sebuah string kosong, tetapi Anda tidak dapat mengatur nilai tanda menjadi nol. Jika Anda

menambahkan tag yang memiliki kunci yang sama dengan tag yang ada pada sumber daya tersebut, nilai yang baru akan menimpa nilai yang lama. Jika Anda menghapus sebuah sumber daya, tanda apa pun untuk sumber daya tersebut juga dihapus.

Anda dapat memberi tanda pada sumber daya berikut AWS Direct Connect menggunakan konsol AWS Direct Connect, API AWS Direct Connect, AWS CLI, AWS Tools for Windows PowerShell, atau SDK AWS. Ketika Anda menggunakan alat ini untuk mengelola tanda, Anda harus menentukan Amazon Resource Name (ARN) untuk sumber daya. Untuk informasi lebih lanjut tentang ARN, lihat Amazon Resource Name (ARN) di Referensi Umum Amazon Web.

Resource	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	Tidak	Tidak	Tidak	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 tanda peka huruf besar dan kecil.
- Prefiks `aws:` dicadangkan untuk penggunaan AWS. 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.
- Tanda alokasi biaya hanya didukung untuk koneksi, anterkoneksi, dan LAG. Untuk informasi tentang cara menggunakan tanda dengan manajemen biaya, lihatMenggunakan Tanda Alokasi Biayadi AWS Billing and Cost ManagementPanduan Pengguna.

Cara menggunakan tanda dengan 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
Hapus satu atau beberapa tanda.	UntagResource	untag-sumber
Penjelasan satu tanda atau lebih	DescribeTags	mendeskripsikan tag

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 merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda akan mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menggambarkan ini sebagai keamanan dari cloud dan keamanan di dalam cloud:

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan AWS di dalam AWS Cloud. AWS juga memberi layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari program kepatuhan AWS. Untuk mempelajari program kepatuhan yang berlaku di AWS Direct Connect, lihat Cakupan Layanan Menurut Program Kepatuhan AWS.
- Keamanan di cloud – Tanggung jawab Anda ditentukan menurut layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku.

Dokumentasi ini akan membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Direct Connect. Topik berikut akan menunjukkan kepada Anda cara membuat konfigurasi AWS Direct Connect untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan layanan AWS lain yang membantu Anda memantau dan mengamankan sumber daya AWS Direct Connect Anda.

Topik

Perlindungan data di AWS Direct Connect

Model tanggung jawab bersama AWS diterapkan untuk perlindungan data AWS Direct Connect. Sebagaimana dijelaskan dalam model ini, AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda harus bertanggung jawab untuk memelihara kendali terhadap konten yang di-hosting pada infrastruktur ini. Anda juga bertanggung jawab atas tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data. Untuk informasi tentang perlindungan data di Eropa, silakan lihat postingan blog Model Tanggung Jawab Bersama AWS dan GDPR di Blog Keamanan AWS.

Untuk tujuan perlindungan data, sebaiknya Anda melindungi kredensial Akun AWS dan menyiapkan AWS IAM Identity Center atau AWS Identity and Access Management (IAM) untuk pengguna individu. Dengan cara seperti itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugas mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan log aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama dengan semua kontrol keamanan default dalam Layanan AWS.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi selengkapnya tentang titik akhir FIPS yang tersedia, silakan lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Sebaiknya Anda tidak memasukkan informasi rahasia atau sensitif, seperti alamat email pelanggan, ke dalam tanda atau bidang teks bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS Direct Connect atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang teks bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau diagnostik. Saat Anda memberikan URL ke server eksternal, sebaiknya Anda tidak menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

Untuk informasi selengkapnya tentang perlindungan data, lihat postingan blog AWS postingan blog Model Tanggung Jawab Bersama dan Peraturan Perlindungan Data Umum (GDPR) di AWSBlog Keamanan.

Topik

Privasi lalu lintas inter-jaringan di AWS Direct Connect

Lalu lintas antara layanan dengan klien dan aplikasi on-premise

Anda memiliki dua opsi konektivitas antara jaringan privat dan AWS:

- Keterkaitan ke AWS Site-to-Site VPN. Untuk informasi selengkapnya, lihat the section called “Keamanan infrastruktur”.
- Keterkaitan ke VPC. Untuk informasi selengkapnya, lihat the section called “Keterkaitan virtual private gateway” dan the section called “Keterkaitan transit gateway”.

Lalu lintas antara sumber daya AWS di Wilayah yang sama

Anda memiliki dua opsi konektivitas:

- Keterkaitan ke AWS Site-to-Site VPN. Untuk informasi selengkapnya, lihat the section called “Keamanan infrastruktur”.
- Keterkaitan ke VPC. Selengkapnya, lihat the section called “Keterkaitan virtual private gateway” dan the section called “Keterkaitan transit gateway”.

Enkripsi dalam AWS Direct Connect

AWS Direct Connecttidak mengenkripsi lalu lintas dalam transit Anda. Untuk mengenkripsi data dalam transit yang melintasi AWS Direct Connect, Anda harus menggunakan opsi enkripsi transit untuk layanan tersebut. Untuk mempelajari enkripsi lalu lintas instans EC2, lihat Enkripsi dalam Transit di Panduan Pengguna Amazon EC2 untuk Instans Linux.

Dengan AWS Direct Connect dan AWS Site-to-Site VPN, Anda dapat menggabungkan satu atau lebih AWS Direct Connect koneksi jaringan khusus dengan VPN Amazon VPC. Kombinasi

ini menyediakan koneksi privat yang dienkripsi IPSEC yang juga mengurangi biaya jaringan, meningkatkan throughput bandwidth, dan memberikan pengalaman jaringan yang lebih konsisten dibandingkan koneksi VPN berbasis internet. Untuk informasi selengkapnya, lihat Opsi Konektivitas Amazon VPC ke Amazon VPC.

MAC Security (MACsec) adalah standar IEEE yang menyediakan kerahasiaan data, integritas data, dan autentisitas asal data. Anda dapat menggunakan AWS Direct Connect yang mendukung MACsec untuk mengenkripsi data Anda dari pusat data perusahaan Anda ke lokasi AWS Direct Connect. Untuk informasi selengkapnya, lihat Keamanan MAC.

Identity and Access Management untuk Direct Connect

(IAM) AWS Identity and Access Management adalah Layanan AWS yang membantu seorang administrator dalam mengendalikan akses ke sumber daya AWS secara aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya Direct Connect. IAM adalah sebuah layanan Layanan AWS yang dapat Anda gunakan tanpa dikenakan biaya tambahan.

Topik

Audiens

Cara menggunakan AWS Identity and Access Management (IAM) beragam, tergantung 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 Anda 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 menggunakan identitas

Autentikasi merupakan cara Anda untuk masuk ke AWS dengan menggunakan kredensial identitas Anda. Anda harus terautentikasi (masuk keAWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk ke AWS sebagai identitas terfederasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Para pengguna (Pusat Identitas IAM), otentikasi sign-on tunggal perusahaan Anda, dan kredensial Google atau Facebook Anda merupakan contoh identitas terfederasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas dengan menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil suatu peran.

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

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 kredensial Anda. Jika Anda tidak menggunakan peralatan AWS,

maka Anda harus menandatangani sendiri permintaan tersebut. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, silakan lihat Menandatangani permintaan API AWS di Panduan Pengguna IAM.

Terlepas dari metode autentikasi yang Anda gunakan, Anda mungkin juga diminta untuk menyediakan informasi keamanan tambahan. Sebagai contoh, AWS menyarankan supaya Anda menggunakan autentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, silakan lihat Autentikasi multi-faktor di Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS di Panduan Pengguna IAM.

Pengguna root Akun AWS

Ketika Anda membuat Akun AWS, Anda memulai dengan satu identitas masuk yang memiliki akses ke semua Layanan AWS dan sumber daya di akun tersebut. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk ke alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan 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, silakan lihat Tugas yang memerlukan kredensial pengguna root di Panduan Pengguna IAM.

Identitas terfederasi

Praktik terbaiknya berupa, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensial temporer.

Identitas terfederasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, dikenal sebagai AWS Directory Service, direktori Pusat Identitas, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas terfederasi mengakses Akun AWS, identitas tersebut mengambil peran, dan peran memberikan kredensial temporer.

Untuk pengelolaan akses terpusat, kami sarankan Anda menggunakanAWS 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 Akun AWS Anda dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, silakan lihat Apakah Pusat Identitas IAM itu? di User Guide AWS IAM Identity Center.

Pengguna dan Grup IAM

Pengguna IAM adalah identitas dalam Akun AWS Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Apabila memungkinkan, kami menyarankan untuk mengandalkan pada kredensial temporer alih-alih membuat pengguna IAM yang memiliki kredensyal jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami menyarankan Anda memutar kunci akses. Untuk informasi selengkapnya, silakan lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang di Panduan Pengguna IAM.

Grup IAM adalah identitas yang menerangkan secara spesifik kumpulan pengguna IAM. Anda tidak dapat masuk sebagai kelompok. Anda dapat menggunakan grup untuk menerangkan secara spesifik izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Sebagai contoh, Anda dapat memiliki grup yang diberi nama AdminIAM 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 tersebut dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial temporer. Untuk mempelajari selengkapnya, silakan lihat Kapan harus membuat pengguna IAM (alih-alih peran) di Panduan Pengguna IAM.

Peran IAM

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

IAM role dengan kredensial temporer berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas terfederasi, Anda harus membuat sebuah peran dan menentukan izin untuk peran tersebut. Ketika identitas gabungan terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran-peran untuk federasi, silakan lihat Membuat sebuah peran untuk Penyedia Identitas pihak ketiga di Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi serangkain izin. Untuk mengontrol apa

yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengkorelasikan izin yang diatur ke peran dalam IAM. Untuk informasi tentang rangkaian izin, silakan lihat Rangkaian izin di Panduan Pengguna AWS IAM Identity Center.

- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM untuk sementara mengambil izin berbeda untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) di akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, pada beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan suatu peran sebagai proksi). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, silakan lihat Bagaimana peran IAM role berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan – Sebagian Layanan AWS menggunakan fitur di Layanan AWS lainnya. Sebagai contoh, ketika Anda melakukan panggilan dalam suatu layanan, lazim pada layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Suatu layanan mungkin melakukan hal tersebut menggunakan izin pengguna utama panggilan, menggunakan peran layanan, atau peran tertaut layanan.
  - Sesi akses maju (FAS) – Ketika Anda menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan-tindakan di AWS, Anda akan dianggap sebagai seorang pengguna utama. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat pengajuan ke layanan hilir. Permintaan FAS hanya diajukan ketika sebuah layanan menerima pengajuan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, silakan lihat Meneruskan sesi akses.
  - Peran layanan – Sebuah peran layanan adalah sebuah peran IAM yang dijalankan oleh suatu layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, silakan lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran tertaut layanan – Peran tertaut layanan adalah tipe peran layanan yang tertaut dengan Layanan AWS. Layanan tersebut dapat menjalankan peran untuk melakukan sebuah tindakan atas nama Anda. Peran tertaut layanan akan muncul di Akun AWS Anda dan dimiliki oleh

layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran tertaut layanan.

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

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, silakan lihat Kapan harus membuat peran IAM (alih-alih pengguna) di Panduan Pengguna IAM.

Mengelola kebijakan menggunakan akses

Anda mengendalikan akses di AWS dengan membuat kebijakan dan melampirkannya ke identitas atau sumber daya AWS. Kebijakan adalah objek di AWS yang, ketika terkait dengan identitas atau sumber daya, akan menentukan izinnya. AWS mengevaluasi kebijakan-kebijakan tersebut ketika seorang pengguna utama (pengguna, root user, atau sesi peran) mengajukan permintaan. Izin dalam kebijakan menentukan apakah permintaan diberikan atau ditolak. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, silakan lihat Gambaran Umum kebijakan JSON di Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

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

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk pengoperasiannya. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole` . Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari AWS Management Console, AWS CLI, atau APIAWS.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, misalnya pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol apa yang pengguna tindakan dan peran dapat kerjakan, pada sumber daya mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, silakan lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline ditanam secara langsung ke pengguna tunggal, grup, atau peran. Kebijakan terkelola adalah kebijakan yang berdiri sendiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran di Akun AWS Anda. Kebijakan terkelola mencakup kebijakan terkelola AWS dan kebijakan terkelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, silakan lihat Memilih antara kebijakan terkelola dan kebijakan inline diPanduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan-kebijakan berbasis sumber daya adalah kebijakan terpercaya 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 yang dilampiri kebijakan, kebijakan tersebut menentkan tindakan apa yang dapat dilakukan oleh pengguna utama yang ditentukan di sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

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

Daftar kontrol akses (ACL)

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

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh-contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat Gambaran umum daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Ringkas Amazon.

Tipe-tipe kebijakan lain

AWS mendukung tipe kebijakan tambahan, yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada 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 batas 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 menindihi izin. Untuk informasi selengkapnya tentang batasan izin, silakan lihat Batasan izin untuk entitas IAM di Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – SCP adalah kebijakan JSON yang menentukan izin maksimum untuk sebuah organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan secara terpusat mengelola beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau ke semua akun Anda. SCP membatasi izin untuk entitas dalam akun anggota, termasuk setiap Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organisasi dan SCP, silakan lihat Cara kerja SCP di Panduan Pengguna AWS Organizations.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah perpotongan kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga dapat berasal dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini menindihi izin. Untuk informasi selengkapnya, silakan lihat Kebijakan sesi di Panduan Pengguna IAM.

Berbagai tipe kebijakan

Ketika beberapa tipe kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan ketika beberapa tipe kebijakan dilibatkan, silakan 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
ACL	Tidak
ABAC (tag dalam kebijakan)	Parsial
Kredensial temporer	Ya
Izin-izin pengguna utama	Ya
Peran layanan	Ya
Peran tertaut layanan	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Direct Connect dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWSlayanan 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, misalnya pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol apa yang pengguna tindakan dan peran dapat kerjakan, pada sumber daya mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, silakan lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta persyaratan yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik pengguna utama dalam sebuah kebijakan berbasis identitas karena pengguna utama berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, silakan 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-kebijakan berbasis sumber daya adalah kebijakan terpercaya 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 yang dilampiri kebijakan, kebijakan tersebut menentkan tindakan apa yang dapat dilakukan oleh pengguna utama yang ditentukan di sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai pengguna utama dalam kebijakan berbasis sumber daya. Menambahkan pengguna utama akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika pengguna utama dan sumber daya berada dalam Akun AWS yang berbeda, Administrator IAM di akun tepercaya juga harus memberikan izin kepada entitas pengguna utama (pengguna atau peran) untuk mengakses sumber daya. Mereka

memberikan izin melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses kepada pengguna utama dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, silakan lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Tindakan kebijakan untuk Direct Connect

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan-tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan-tindakan kebijakan biasanya memiliki nama yang sama sebagaimana operasi API AWS yang dikaitkan padanya. Ada beberapa pengecualian, misalnya tindakan yang memiliki izin saja yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam sebuah kebijakan. Tindakan-tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam suatu kebijakan untuk memberikan izin guna melakukan operasi yang 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-tindakan tersebut dengan koma.

```
"Action": [
      "Direct Connect:action1",
      "Direct Connect:action2"
         ]
```

Sumber daya kebijakan untuk Direct Connect

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen kebijakan JSON `Resource` menentukan objek atau objek-objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan entah elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan-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 mengindikasikan bahwa pernyataan tersebut berlaku bagi semua sumber daya.

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

Untuk melihat daftar tipe resource Direct Connect dan ARNnya, 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-kunci persyaratan kebijakan spesifik layanan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan syarat yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator syarat, misalnya sama dengan atau kurang dari, untuk mencocokkan syarat 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 dengan menggunakan operasi `AND` yang logis. Jika Anda menentukan beberapa niilai untuk satu kunci persyaratan, maka AWS akan mengevaluasi syarat tersebut menggunakan operasi `OR` yang logis. Semua persyaratan harus dipenuhi sebelum izin pernyataan diberikan.

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

AWS mendukung kunci-kunci syarat global dan kunci-kunci syarat spesifik layanan. Untuk melihat semua kunci persyaratan global AWS, silakan lihat kunci konteks syarat global AWS 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.

ACL di Direct Connect

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis

sumber daya, meskipun kebijakan-kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan Direct Connect

Mendukung ABAC (tag dalam kebijakan)	Parsial

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

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi dimana pengelolaan kebijakan menjadi rumit.

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

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

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

Menggunakan kredensial sementara dengan Direct Connect

Mendukung kredensial temporer	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk dengan menggunakan kredensial temporer. Sebagai informasi tambahan, termasuk tentang Layanan AWS mana saja yang berfungsi dengan kredensial temporer, silakan lihat Layanan AWS yang berfungsi dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensial temporer jika Anda masuk ke AWS Management Console dengan menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Sebagai contoh, ketika Anda mengakses AWS dengan menggunakan tautan masuk tunggal (SSO) milik perusahaan Anda, proses itu secara otomatis akan membuat kredensial temporer. Anda juga akan secara otomatis membuat kredensial temporer ketika Anda masuk ke konsol sebagai seorang pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang peralihan peran, silakan lihat Peralihan peran (konsol) di Panduan Pengguna IAM.

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

Izin utama lintas layanan untuk Direct Connect

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna IAM atau peran IAM untuk mengerjakan tindakan di AWS, Anda akan dianggap sebagai pengguna utama. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat pengajuan ke layanan hilir. Permintaan FAS hanya diajukan ketika sebuah layanan menerima pengajuan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, silakan lihat Meneruskan sesi akses.

Peran layanan untuk Direct Connect

Mendukung peran layanan	Ya

Peran layanan adalah sebuah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat 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 yang tertaut dengan layanan	Tidak

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

Untuk detail tentang pembuatan atau pengelolaan peran yang terhubung dengan layanan, lihat Layanan AWS yang bekerja dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Service-linked role (Peran yang terhubung dengan layanan). Pilih tautan Ya untuk melihat dokumentasi peran tertaut 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. Pengguan dan peran tersebut juga tidak dapat melakukan tugas dengan menggunakan API AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS. Untuk mengabulkan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan para pengguna dapat mengambil peran.

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

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Direct Connect, termasuk format ARN 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 mengenakan biaya kepada Anda Akun AWS. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan terkelola AWS dan beralih ke izin dengan hak akses paling rendah – Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan terkelola AWS yang memberikan izin untuk banyak kasus penggunaan umum. Kebijakan tedapat di Akun AWS Anda. Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan AWS yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, silakan lihat kebijakan-kebijakan terkelola AWS atau kebijakan-kebijakan terkelola AWS untuk fungsi tugas di 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 melakukan ini dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan pengguna IAM untuk mengajukan izin, silakan lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan syarat dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu syarat ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan syarat untuk memberi akses ke tindakan layanan jika digunakan melalui Layanan AWS yang spesifk, sepertiAWS CloudFormation. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.

- Gunakan Analizer Akses IAM untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – Analizer Akses IAM memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. Analizer Akses IAM menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, silakan lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.
- Memerlukan autentikasi multi-faktor (MFA) – Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Akun AWS Anda, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan syarat MFA pada kebijakan Anda. Untuk informasi selengkapnya, silakan lihat Mengonfigurasi akses API yang diproteksi MFA di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, silakan lihat Praktik terbaik keamanan di IAM di 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 persyaratan 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 JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan-tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan-tindakan kebijakan biasanya memiliki nama yang sama sebagaimana operasi API AWS yang dikaitkan padanya. Ada beberapa pengecualian, misalnya tindakan yang memiliki izin saja yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam sebuah kebijakan. Tindakan-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 instans Amazon EC2 dengan operasi API `DescribeVpnGateways` Amazon EC2, Anda menyertakan tindakan `ec2:DescribeVpnGateways` 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 JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen kebijakan JSON `Resource` menentukan objek atau objek-objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan entah elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan-tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin tingkat sumber daya, seperti operasi daftar, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan berlaku untuk semua sumber daya.

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

Direct Connect menggunakan ARN berikut:

ARN sumber daya Direct Connect

Jenis Sumber Daya	ARN
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`

Untuk informasi lebih lanjut tentang format ARN, lihat Amazon Resource Name (ARN) dan namespace Layanan AWS.

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 kondisi tersebut, Anda harus menggunakan wildcard (*).

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

Untuk melihat daftar jenis sumber daya Direct Connect dan ARN-nya, 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 URL TINDAKAN-LAYANAN;.

Kunci syarat

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan siapa yang memiliki akses ke hal apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan syarat yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator syarat, misalnya sama dengan atau kurang dari, untuk mencocokkan syarat 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 dengan menggunakan operasi `AND` yang logis. Jika Anda menentukan beberapa niilai untuk satu kunci persyaratan, maka AWS akan mengevaluasi syarat tersebut menggunakan operasi `OR` yang logis. Semua persyaratan harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan syarat. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika

izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan IAM: variabel dan tag di Panduan Pengguna IAM.

AWS mendukung kunci-kunci syarat global dan kunci-kunci syarat spesifik layanan. Untuk melihat semua kunci ketentuan global AWS, lihat kunci konteks ketentuan global AWS dalam Panduan Pengguna IAM.

Direct Connect menentukan set kunci ketentuannya sendiri dan juga mendukung penggunaan beberapa kunci ketentuan global. Untuk melihat semua kunci ketentuan global AWS, lihat Kunci Konteks Ketentuan Global AWS dalam 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 kunci 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 URL TINDAKAN-LAYANAN;.

Menggunakan konsol Direct Connect

Untuk mengakses konsol Direct Connect, Anda harus memiliki rangkaian izin minimum. Izin ini harus memperbolehkan Anda untuk membuat daftar dan melihat perincian tentang sumber daya Direct Connect di akun AWS. 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 kebijakan yang dikelola AWS berikut ini ke entitas. Untuk informasi selengkapnya, lihat Menambahkan Izin ke Pengguna dalam Panduan Pengguna IAM:

```
directconnect
```

Anda tidak perlu mengizinkan konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau API AWS. Alih-alih, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang Anda coba lakukan.

Izinkan para pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara Anda dapat membuat kebijakan yang mengizinkan para pengguna IAM untuk melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka.

Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini pada konsol atau secara terprogram menggunakan AWS CLI atau API 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 ketentuan dalam kebijakan IAM untuk mengontrol pasangan kunci-nilai tanda 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 tertaut layanan untuk AWS Direct Connect

AWS Direct Connect menggunakan peran yang terhubung dengan layanan AWS Identity and Access Management (IAM). Peran yang terkait dengan layanan adalah tipe IAM role unik yang terkait langsung ke layanan. Peran yang terhubung dengan layanan ditentukan sebelumnya oleh AWS

Direct Connect dan mencakup semua izin yang diperlukan layanan untuk menghubungi layanan AWS lainnya atas nama Anda.

Peran yang terhubung dengan layanan memudahkan pengaturan AWS Direct Connect karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS Direct Connect menentukan izin peran yang terhubung dengan layanan, dan kecuali ditentukan sebaliknya, hanya AWS Direct Connect yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran yang terhubung dengan layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya AWS Direct Connect karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran yang terhubung dengan layanan, lihat Layanan AWS yang Berfungsi dengan IAM dan cari layanan yang memiliki Ya di kolom Peran yang Terhubung dengan Layanan. Pilih Ya dengan tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk AWS Direct Connect

AWS Direct Connectmenggunakan peran yang terkait dengan terkait dengan layanan bernama`AWSServiceRoleForDirectConnect`. Hal ini memungkinkanAWS Direct Connect untuk mengambil secretes MacSec disimpan dalamAWS Secrets Manager atas nama Anda.

`AWSServiceRoleForDirectConnect` peran terkait layanan memercayakan layanan berikut untuk menjalankan peran tersebut:

- `directconnect.amazonaws.com`

Peran`AWSServiceRoleForDirectConnect` 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` tertaut layanan berhasil dibuat, identitas IAM yang Anda gunakanAWS Direct Connect dengan harus memiliki 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 yang terkait dengan layanan untuk AWS Direct Connect

Anda tidak perlu membuat peran terkait layanan secara manual. AWS Direct Connectmembuat peran yang terkait dengan terkait dengan layanan untuk Anda. Ketika Anda menjalankan`associate-mac-sec-key` perintah,AWS membuat peran terkait layanan yang memungkinkanAWS Direct Connect untuk mengambil rahasia MacSec yang disimpan dalamAWS Secrets Manager atas nama Anda diAWS Management Console,AWS CLI, atauAWS API.

> **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 selengkapnya, lihat Peran Baru Muncul di Akun IAM Saya.

Jika Anda menghapus peran yang terhubung dengan layanan ini, lalu ingin membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran tersebut di akun Anda. AWS Direct Connect membuat lagi peran yang terhubung dengan layanan untuk Anda.

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaanAWS Direct Connect. Di AWS CLI atau API AWS, buat peran yang terhubung dengan layanan dengan nama layanan `directconnect.amazonaws.com`. Untuk informasi lebih lanjut, lihat Membuat peran terkait layanan dalam Panduan Pengguna IAM. Jika Anda menghapus peran yang terhubung dengan layanan ini, Anda dapat menggunakan proses yang sama untuk membuat ulang peran tersebut.

Mengedit peran terkait layanan untuk AWS Direct Connect

AWS Direct Connect tidak mengizinkan Anda untuk mengedit peran terkait layanan `AWSServiceRoleForDirectConnect`. 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 lebih lanjut, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk AWS Direct Connect

Anda tidak perlu menghapus peran `AWSServiceRoleForDirectConnect` secara manual. Ketika Anda menghapus peran terkait layanan, Anda harus menghapus semua sumber daya terkait yang disimpan dalam layananAWS Secrets Manager web. APIAWS CLI, atauAWS API,AWS Direct Connect membersihkan sumber daya dan menghapus peran terkait layanan untuk Anda.AWS Management Console

Anda juga dapat menggunakan konsol IAM untuk menghapus peran tertaut layanan. Untuk melakukannya, pertama-tama Anda harus membersihkan secara manual sumber daya untuk peran tertaut layanan, lalu Anda dapat menghapusnya.

> **Note**
>
> JikaAWS Direct Connect layanan menggunakan peran tersebut ketika Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika ini terjadi, tunggu beberapa menit, lalu coba lagi operasi.

Untuk menghapus sumber daya AWS Direct Connect yang digunakan oleh **`AWSServiceRoleForDirectConnect`**

1. Menghapus hubungan antara semua kunci MACsec dan koneksi. Untuk informasi selengkapnya, lihat the section called “Hapus keterkaitan antara kunci rahasia MACsec dan koneksi”

2. Menghapus hubungan antara semua kunci MACsec dan LAG. Untuk informasi selengkapnya, lihat the section called “Menghapus pengaitan antara semua kunci rahasia MACsec dan LAG.”

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

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

Wilayah yang didukung untuk peran yang terhubung dengan layanan AWS Direct Connect

AWS Direct Connectmendukung penggunaan peran yang terkait dengan terkait dengan layanan di semuaWilayah AWS tempat fitur Keamanan MAC tersedia. Untuk informasi selengkapnya, lihat AWS Direct ConnectLokasi.

Kebijakan terkelola AWS untuk AWS Direct Connect

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

Perlu diingat bahwa kebijakan terkelola AWS mungkin tidak memberikan izin hak akses paling rendah untuk kasus penggunaan khusus 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 ada dalam kebijakan-kebijakan terkelola AWS. Jika AWS memperbarui izin yang ditentukan dalam sebuah kebijakan terkelola AWS, maka pembaruan itu akan mempengaruhi semua identitas pengguna utama (pengguna, grup, dan peran) yang terkait dengan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan terkelola AWS saat sebuah Layanan AWS baru diluncurkan atau operasi API baru tersedia untuk layanan yang sudah ada.

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

AWSkebijakan terkelola: AWSDirectConnectFullAccess

Anda dapat melampirkan kebijakan `AWSDirectConnectFullAccess` ke identitas IAM. Kebijakan ini memberikan izin yang memungkinkan akses penuh ke AWS Direct Connect.

Untuk menampilkan izin untuk kebijakan ini, lihat AWSDirectConnectFullAccess di AWS Management Console.

AWSkebijakan terkelola: AWSDirectConnectReadOnlyAccess

Anda dapat melampirkan kebijakan `AWSDirectConnectReadOnlyAccess` ke identitas IAM. Kebijakan ini memberikan izin yang mengizinkan akses hanya baca ke AWS Direct Connect.

Untuk menampilkan izin untuk kebijakan ini, lihat AWSDirectConnectReadOnlyAccess di AWS Management Console.

AWSkebijakan terkelola: AWSDirectConnectServiceRolePolicy

Kebijakan ini dilampirkan ke peran terkait layanan yang diberi nama AWSServiceRoleForDirectConnectAWS Direct Connectuntuk memungkinkan mengambil rahasia Keamanan MAC atas nama Anda. Untuk informasi selengkapnya, lihat the section called “Peran tertaut layanan”.

Untuk menampilkan izin untuk kebijakan ini, lihat AWSDirectConnectServiceRolePolicy di AWS Management Console.

AWS Direct Connect memperbarui pada kebijakan terkelola AWS

Lihat detail tentang pembaruan terhadap kebijakan terkelola AWS untuk AWS Direct Connect sejak layanan ini mulai melacak perubahan-perubahan tersebut. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat dokumen AWS Direct Connect.

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 Connectmulai 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

Jika Anda menerima pesan galat bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh galat 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 membutuhkan bantuan, hubungi administrator AWS Anda. Administrator Anda adalah orang yang memberikan kredensial masuk Anda.

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.

Sebagian Layanan AWS mengizinkan Anda untuk memberikan peran yang sudah ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran tertaut-layanan. Untuk melakukan tindakan tersebut, Anda harus memiliki izin untuk memberikan peran pada layanan tersebut.

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 membutuhkan bantuan, hubungi administrator AWS Anda. Administrator Anda adalah orang yang memberikan kredensial masuk Anda.

Saya ingin mengizinkan orang di luar saya Akun AWS mengakses sumber daya Direct Connect saya

Anda dapat membuat peran yang dapat digunakan para pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi akses kepada orang ke sumber daya Anda.

Untuk mempelajari selengkapnya, lihat hal berikut:

- Untuk mempelajari apakah Direct Connect mendukung fitur berikut, lihat Cara Direct Connect berfungsi dengan IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya di seluruh Akun AWS yang Anda miliki, silakan lihat Menyediakan akses ke pengguna IAM di Akun AWS lainnya yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke pihak ketiga Akun AWS, silakan lihat Menyediakan akses ke akun Akun AWS yang dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, silakan lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) di Panduan Pengguna IAM .
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan IAM role dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Pencatatan dan pemantauan di AWS Direct Connect

Anda dapat menggunakan alat pemantauan otomatis berikut untuk melihat AWS Direct Connect dan melaporkan saat terjadi kesalahan:

- Alarm Amazon CloudWatch – Lihat satu metrik selama periode waktu yang Anda tentukan. Lakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas selama periode waktu tertentu. Tindakan ini adalah pemberitahuan yang dikirim ke topik Amazon SNS. Alarm CloudWatch tidak akan mengambil tindakan hanya karena status tertentu; status harus berubah dan dipertahankan selama beberapa periode tertentu. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.
- Pemantauan Log AWS CloudTrail – Membagikan berkas log antara akun dan memantau berkas log CloudTrail secara waktu nyata dengan mengirimkannya ke CloudWatch Logs. Anda juga dapat menulis aplikasi pemrosesan log di Java dan memvalidasi bahwa berkas log Anda tidak berubah setelah pengiriman oleh CloudTrail. Untuk informasi selengkapnya, lihat Pembuatan log panggilan API AWS Direct Connect menggunakan AWS CloudTrail dan Bekerja dengan Berkas Log CloudTrail di Panduan Pengguna AWS CloudTrail.

Untuk informasi selengkapnya, lihat Pemantauan.

Validasi kepatuhan untuk AWS Direct Connect

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan khusus, lihat Layanan AWS di Scope oleh Program Program Kepatuhan yang Anda minati. Untuk informasi umum, silakan lihat Program Kepatuhan AWS .

Anda bisa 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, serta hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Quick Start Keamanan dan Kepatuhan – Panduan Quick Start Keamanan dan Kepatuhan – Panduan deployment ini membahas pertimbangan arsitektur dan menyediakan langkah-langkah untuk melakukan deployment terhadap lingkungan dasar di AWS yang menjadi fokus keamanan dan kepatuhan.

- Merancang Keamanan dan Kepatuhan HIPAA di Amazon Web Services – Laporan resmi ini menjelaskan cara perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

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

- Sumber Daya Kepatuhan AWS – Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- Panduan Kepatuhan Pelanggan AWS – Pahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan kontrol keamanan di banyak kerangka kerja (termasuk National Institute of Standards and Technology (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan di Panduan Developer AWS Config – Layanan AWS Config menilai seberapa baik konfigurasi sumber daya Anda dalam mematuhi praktik-praktik internal, pedoman industri, dan regulasi internal.
- AWS Security Hub – Layanan AWS ini memberikan pandangan komprehensif tentang status keamanan Anda di dadlam AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda dan untuk memeriksa kepatuhan terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- AWS Audit Manager – Layanan AWS ini akan membantu Anda untuk terus-menerus mengaudit penggunaan AWS untuk menyederhanakan bagaimana Anda mengelola risiko dan kepatuhan terhadap regulasi dan standar industri.

Ketahanan di AWS Direct Connect

Infrastruktur global AWS dibangun di sekitar Wilayah dan Availability Zone AWS. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah dan terisolasi secara fisik, yang terhubung dengan jaringan yang memiliki latensi rendah, throughput tinggi, dan sangat berkelebihan. Dengan Availability Zone, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara Availability Zone tanpa gangguan. Availability Zone memiliki ketersediaan yang lebih baik, menoleransi kegagalan, dan dapat diskalakan dibandingkan satu atau beberapa infrastruktur pusat data tradisional.

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

Selain infrastruktur global AWS, AWS Direct Connect menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan pencadangan Anda.

Untuk informasi tentang cara menggunakan VPN dengan AWS Direct Connect, lihat AWSDirect Connect Plus VPN.

Failover

Kit Alat Ketahanan AWS Direct Connect menyediakan wizard koneksi dengan beberapa model ketahanan yang membantu Anda memesan koneksi khusus untuk mencapai tujuan SLA Anda. Anda memilih model ketahanan, kemudian AWS Direct Connect Kit Alat Ketahanan akan 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 dapat mencapai ketahanan pengembangan dan pengujian untuk beban kerja 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 Menggunakan Kit Alat Ketahanan AWS Direct Connect untuk memulai.

Keamanan infrastruktur dalam AWS Direct Connect

Sebagai layanan terkelola,AWS Direct Connect dilindungi oleh prosedur keamanan jaringanAWS global. Anda menggunakan panggilan API AWS yang 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 suite cipher 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 access key ID dan secret access key yang terkait dengan principal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara untuk menandatangani permintaan.

Anda dapat menghubungi 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 kebijakan AWS Direct Connect untuk mengontrol akses dari titik akhir Amazon Virtual Private Cloud (Amazon VPC) tertentu atau VPC tertentu. Secara efektif, ini mengisolasi akses jaringan ke sumber daya AWS Direct Connect yang diberikan hanya dari VPC tertentu dalam jaringan AWS. Misalnya, lihatthe section called “Contoh kebijakan berbasis identitas”.

Border Gateway Protocol (BGP) keamanan

Internet sebagian besar bergantung pada BGP untuk merutekan informasi antar sistem jaringan. Perutean BGP beberapa kali dapat rentan terhadap serangan berbahaya, atau pembajakan BGP. Untuk memahami caraAWS kerjanya agar lebih aman melindungi jaringan Anda dari pembajakan BGP, lihat CaraAWS membantu mengamankan perutean internet.

Menggunakan metode AWS CLI

Anda dapat menggunakan AWS CLI untuk membuat dan bekerja dengan sumber daya AWS Direct Connect.

Contoh berikut menggunakan perintah AWS CLI untuk membuat koneksi AWS Direct Connect. 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, lihat Panduan Pengguna AWS Command Line Interface.

Isi

Langkah 1: Buat koneksi

Langkah pertama adalah mengirimkan permintaan koneksi. Pastikan Anda mengetahui kecepatan port yang Anda butuhkan dan lokasi AWS Direct Connect. Untuk informasi selengkapnya, lihat AWS Direct Connect koneksi.

Untuk membuat permintaan koneksi

1. Jelaskan lokasi AWS Direct Connect 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 diekstrak 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 telah menempatkan pesanan untuk koneksi AWS Direct Connect, 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 layanan AWS yang tidak ada dalam VPC. Anda dapat membuat antarmuka virtual yang mendukung lau lintas IPv4 atau IPv6.

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

Ketika Anda membuat antarmuka virtual menggunakan AWS CLI, output menyertakan informasi konfigurasi router umum. Untuk membuat konfigurasi router yang spesifik untuk perangkat Anda, gunakan konsol AWS Direct Connect. 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 lalu lintas IPv4, Anda perlu alamat IPv4 privat untuk setiap akhir sesi peering BGP. Anda dapat menentukan alamat IPv4 Anda sendiri, atau Anda dapat membiarkan Amazon menghasilkan alamat untuk Anda. Pada contoh berikut, alamat IPv4 dihasilkan 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 privat yang mendukung lalu lintas IPv6, gunakan perintah yang sama seperti di atas dan tentukan parameter `ipv6` untuk `addressFamily`. Anda tidak dapat menentukan alamat IPv6 Anda sendiri untuk sesi peering BGP; Amazon mengalokasikan alamat IPv6 Anda.

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 lalu lintas IPv4, Anda juga harus menentukan alamat IPv4 publik untuk setiap akhir sesi peering BGP, dan rute IPv4 publik yang akan Anda iklankan beriklan melalui BGP. Contoh berikut membuat antarmuka virtual publik untuk lalu lintas IPv4.

```
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 lalu lintas IPv6, Anda dapat menentukan rute IPv6 yang akan Anda iklankan melalui BGP. Anda tidak dapat menentukan alamat IPv6 untuk sesi peering; Amazon mengalokasikan alamat IPv6 untuk Anda. Contoh berikut membuat antarmuka virtual publik untuk lalu lintas IPv6.

```
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>
```

Pembuatan log panggilan API AWS Direct Connect menggunakan AWS CloudTrail

AWS Direct Connectterintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauAWS layanan diAWS Direct Connect. CloudTrail menangkap semua panggilan API untukAWS Direct Connect sebagai kejadian. Panggilan yang direkam mencakup panggilan dari AWS Direct Connect konsol dan panggilan kode ke operasi API AWS Direct Connect ini. Jika membuat jejak, Anda dapat mengaktifkan pengiriman tindakan CloudTrail berkelanjutan ke bucket Amazon S3, termasuk kejadian untukAWS Direct Connect. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat kejadian terbaru di CloudTrail konsol di Riwayat. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat, alamat IP asal permintaan tersebut dibuatAWS Direct Connect, siapa yang membuat permintaan, kapan permintaan dibuat, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail lainnya.

Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

AWS Direct Connectinformasi dalam CloudTrail

CloudTrail diaktifkan diAWS akun Anda saat Anda membuat akun. Saat aktivitas terjadi diAWS Direct Connect, aktivitas tersebut dicatat dalam CloudTrail peristiwa bersama peristiwaAWS layanan lainnya di Riwayat. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat Kejadian dengan Riwayat CloudTrail Kejadian.

Untuk catatan berkelanjutan tentang peristiwa di akun AWS Anda, termasuk peristiwa untuk AWS Direct Connect, buat jejak. Jejak memungkinkan CloudTrail untuk mengirim berkas log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasiAWS layanan lainnya untuk dianalisis lebih lanjut dan bertindak berdasarkan data kejadian yang dikumpulkan di CloudTrail log. Untuk informasi selengkapnya, lihat yang berikut:

- Ikhtisar untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail

- Menerima Berkas CloudTrail Log dari Beberapa Wilayah dan Menerima Berkas CloudTrail Log dari Beberapa Akun

SemuaAWS Direct Connect tindakan dicatat oleh CloudTrail dan didokumentasikan dalam ReferensiAWS Direct Connect API. Misalnya, panggilan untuk`CreateConnection` dan`CreatePrivateVirtualInterface` tindakan menghasilkan entri di berkas CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Jika permintaan tersebut dibuat dengan kredensi root atauAWS Identity and Access Management (IAM pengguna).
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan.
- Bahwa permintaan dibuat oleh layanan AWS lain.

Untuk informasi selengkapnya, lihat CloudTrail `userIdentity` Elemen.

Memahami entri file log AWS Direct Connect

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang Anda tentukan. CloudTrail berkas log berisi satu atau beberapa entri log. Sebuah peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail berkas log bukan merupakan jejak tumpukan terurut dari panggilan API publik, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

Berikut ini adalah contoh catatan CloudTrail log untukAWS 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
    },
    ...
  ]
}
```

Memantau 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 sajakah sasaran 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-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 Pemantauan CloudWatch dengan Amazon.
- 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 Pembuatan log panggilan API AWS Direct Connect menggunakan AWS CloudTrail dan Bekerja dengan File CloudTrail Log di Panduan AWS CloudTrail Pengguna.

Alat-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.
- Membuat dan mengedit alarm agar diberi tahu tentang masalah.

Pemantauan CloudWatch dengan Amazon

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.

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: Boolean
`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”. Untuk informasi selengkapnya tentang mendapatkan statistik penjumlahan, lihat Mendapatkan Statistik untuk Metrik di Panduan CloudWatch Pengguna Amazon. Nilai metrik diatur ke 0 ketika kesalahan pada antarmuka berhenti. **Note** Metrik ini menggantikan `ConnectionCRCErrorCount` , yang tidak lagi digunakan. Unit: Hitungan
`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 the section called “AWS Direct Connect dimensi yang tersedia”. 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 the section called “AWS Direct Connect dimensi yang tersedia”. 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.

Melihat 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**
>
> Jika Anda menetapkan interval 1 menit, Direct Connect akan melakukan upaya terbaik untuk menulis metrik untuk CloudWatch menggunakan interval ini, tetapi tidak selalu dapat dijamin.

Anda dapat menggunakan prosedur berikut untuk melihat metrik koneksi Direct Connect.

Untuk melihat metrik menggunakan konsol CloudWatch

Metrik dikelompokkan berdasarkan ruang nama layanan dahulu, lalu berdasarkan berbagai kombinasi dimensi dalam setiap ruang nama. 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 konsol AWS Direct Connect di https://console.aws.amazon.com/ec2spot/home/fleet.
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"
```

Membuat CloudWatch alarm 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	4	Batas ini tidak dapat dinaikkan.
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)	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 LAG. Jumlah antarmuka virtual transit yang diizinkan sekarang empat

Komponen	Kuota	Komentar
		(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 TURUN.	100 masing-masing untuk IPv4 dan IPv6	Batas ini tidak dapat dinaikkan.
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	
Grup agregasi tautan (LAG) 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.

Komponen	Kuota	Komentar
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.
Antarmuka virtual (pribadi atau transit) per gateway AWS Direct Connect	30	Batas ini tidak dapat dinaikkan.
Jumlah awalan per AWS Transit Gateway dari AWS ke on-premise pada antarmuka virtual transit	200 total gabungan untuk IPv4 dan IPv6	Batas ini tidak dapat dinaikkan.
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) dan 100Gbps: 100GBASE-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 penyeimbangan beban dengan beberapa VIF publik, semua VIF 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

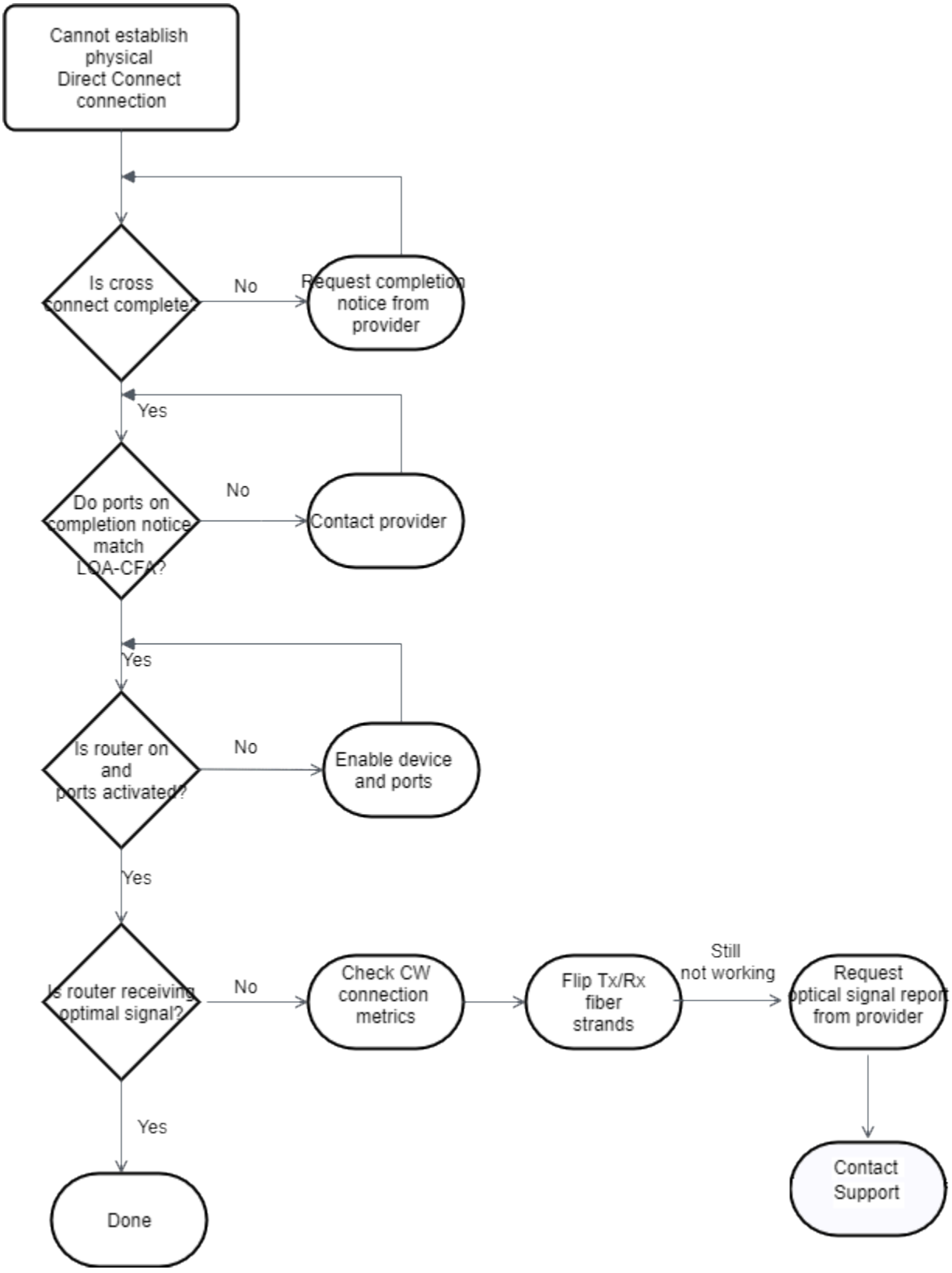
Pemecahan masalah lapisan 1 (fisik)

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).
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 Support 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.

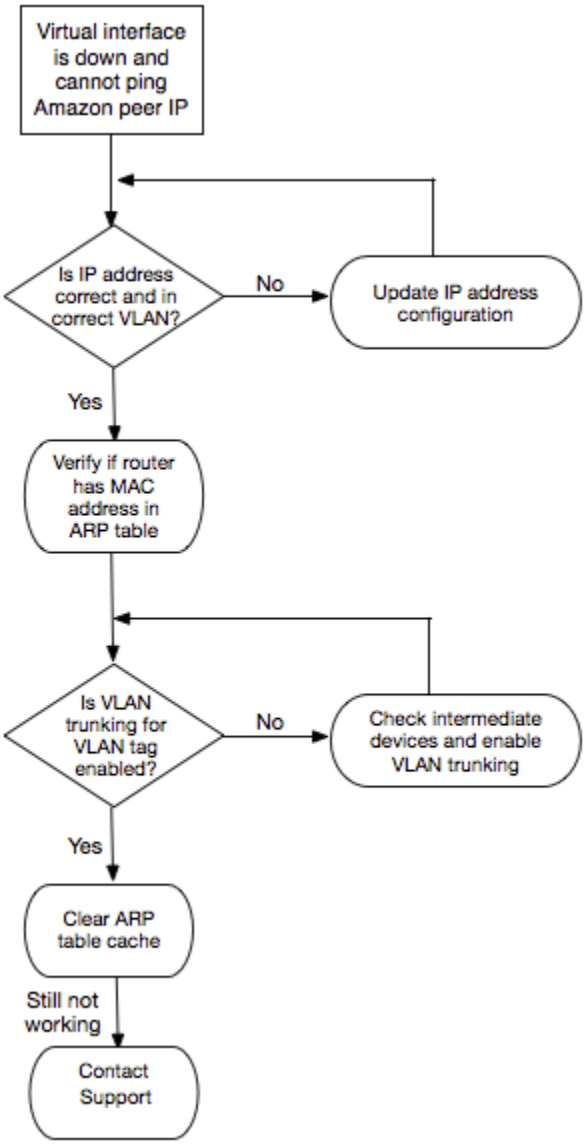

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check 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 bahwa 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.

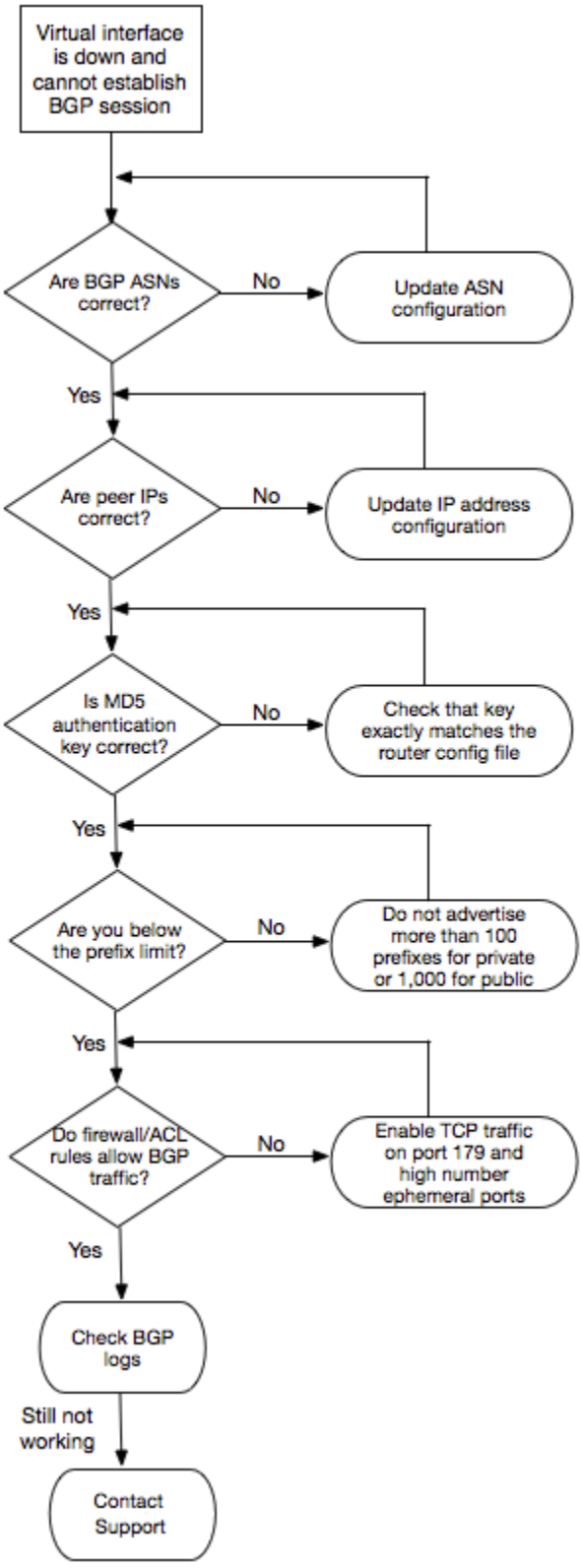
Pemecahan masalah lapisan 3/4 (Jaringan/Transportasi)

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 tidak 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 IP untuk kedua sisi sesi peering BGP dikonfigurasi dengan benar.
3. Pastikan bahwa kunci autentikasi MD5 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.



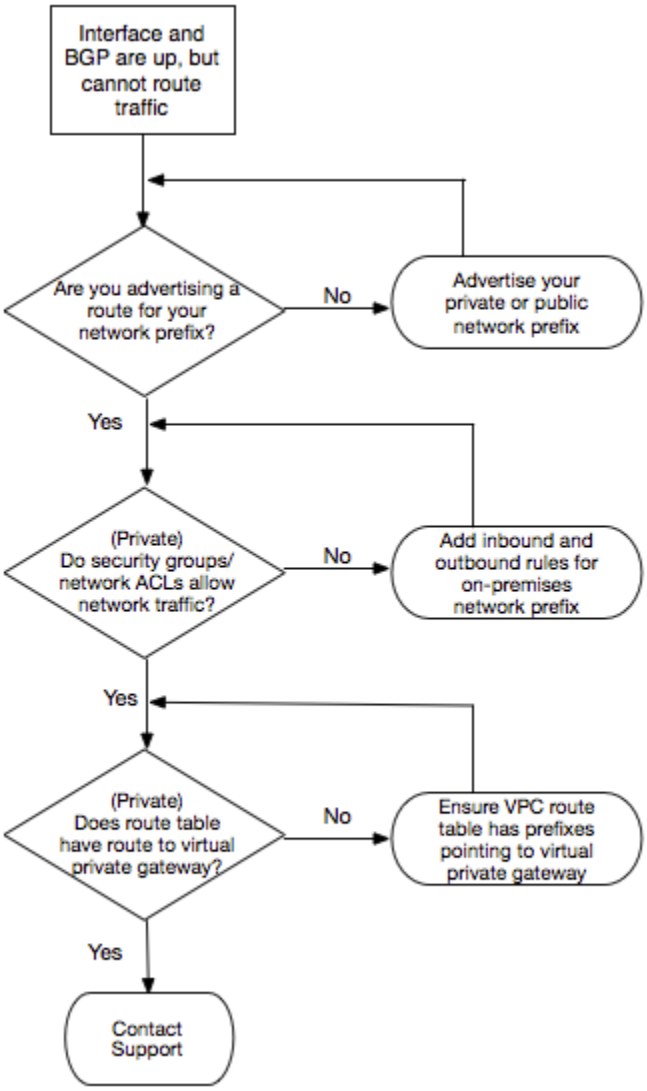
Jika sesi peering BGP dibuat tetapi Anda mengalami masalah perutean, lihat Masalah perutean pemecahan masalah.

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 privat, pastikan bahwa grup keamanan VPC dan ACL jaringan memungkinkan lalu lintas masuk dan keluar untuk prefiks jaringan lokal Anda. Untuk informasi selengkapnya, lihat Grup Keamanan dan ACL Jaringan 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 menguraikan rilis untuk AWS Direct Connect.

Fitur	Deskripsi	Tanggal
Support untuk SiteLink	Anda dapat membuat antarmuka pribadi virtual yang memungkinkan konektivitas antara dua titik Direct Connect dari presence (PoPs) di AWS Region yang sama. Untuk informasi selengkapnya, lihat Antarmuka virtual yang di-host.	2021-12-01
Mendukung MAC Security	Anda dapat menggunakan AWS Direct Connect yang mendukung MACsec untuk mengenkripsi data Anda dari pusat data perusahaan Anda ke lokasi AWS Direct Connect. Untuk informasi selengkapnya, lihat Keamanan MAC.	2021-03-31
Dukungan untuk 100G	Topik yang diperbarui untuk menyertakan dukungan untuk koneksi khusus 100G.	2021-02-12
Lokasi baru di Italia	Topik yang diperbarui untuk memasukkan penambahan lokasi baru di Italia. Untuk informasi selengkapnya, lihat the section called “Eropa (Milan)”.	2021-01-22
Lokasi baru di Israel	Topik diperbarui untuk memasukkan penambahan lokasi baru di Israel. Untuk informasi selengkapnya, lihat the section called “Israel (Tel Aviv)”.	2020-07-07
Dukungan Pengujian Failover Kit Alat Ketahanan	Gunakan fitur Pengujian Failover Kit Alat Ketahanan untuk menguji ketahanan koneksi Anda. Untuk informasi selengkapnya, lihat the section called “Pengujian Failover AWS Direct Connect”.	2020-06-03
CloudWatch Dukungan metrik VIF	Anda dapat memantau AWS Direct Connect koneksi fisik, dan antarmuka virtual, menggunakan CloudWatch. Untuk informasi selengkapnya, lihat the section called “Pemantauan CloudWatch dengan Amazon”.	2020-05-11

Fitur	Deskripsi	Tanggal
AWS Direct Connect Kit Alat Ketahanan	AWS Direct Connect Kit Alat Ketahanan menyediakan wizard koneksi dengan beberapa model ketahanan yang akan membantu Anda memesan koneksi khusus untuk mencapai tujuan SLA Anda. Untuk informasi selengkapnya, lihat Menggunakan Kit Alat Ketahanan AWS Direct Connect untuk memulai.	2019-10-07
Dukungan Wilayah Tambahan untuk Dukungan untuk AWS Transit Gateway di seluruh akun	Untuk informasi, lihat the section called “Keterkaitan transit gateway”.	2019-09-30
AWS Direct Connect Dukungan untuk AWS Transit Gateway	Anda dapat menggunakan AWS Direct Connectgateway untuk menghubungkan AWS Direct Connect melalui antarmuka virtual transit ke VPC atau VPN yang terlampir pada transit gateway Anda. Anda mengaitkan gateway Direct Connect dengan transit gateway Kemudian, buat antarmuka virtual transit untuk koneksi AWS Direct Connect ke gateway Direct Connect. Untuk informasi, lihat the section called “Keterkaitan transit gateway”.	2019-03-27
Dukungan bingkai jumbo	Anda dapat mengirim bingkai jumbo (9001 MTU) melalui AWS Direct Connect. Untuk informasi selengkapnya, lihat Mengatur MTU jaringan untuk antarmuka virtual privat atau antarmuka virtual transit.	2018-10-11
Komunitas BGP preferensi lokal	Anda dapat menggunakan tanda komunitas BGP preferensi lokal untuk mendapatkan penyeimbangan beban dan preferens i rute untuk lalu lintas masuk ke jaringan Anda. Untuk informasi selengkapnya, lihat Komunitas BGP preferensi lokal.	2018-02-06

Fitur	Deskripsi	Tanggal
Gateway AWS Direct Connect	Anda dapat menggunakan gateway Direct Connect untuk menghubungkan koneksi AWS Direct Connect Anda ke VPC di Wilayah jarak jauh. Untuk informasi selengkapnya, lihat Bekerja dengan gateway Direct Connect.	2017-11-01
CloudWatch Metrik Amazon	Anda dapat melihat CloudWatch metrik untuk AWS Direct Connect koneksi Anda. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.	2017-06-29
Link aggregation group (Grup agregasi tautan)	Anda dapat membuat grup agregasi tautan (LAG) untuk mengaregatkan beberapa koneksi AWS Direct Connect. Untuk informasi selengkapnya, lihat Grup agregasi tautan.	2017-02-13
Dukungan IPv6	Antarmuka virtual Anda sekarang dapat mendukung sesi peering IPv6 BGP. Untuk informasi selengkapnya, lihat Menambahkan atau menghapus peer BGP.	2016-12-01
Dukungan penandaan	Sekarang Anda dapat menandai sumber daya AWS Direct Connect. Untuk informasi selengkapnya, lihat Penandaan pada sumber daya AWS Direct Connect.	2016-11-04
LOA-CFA layanan mandiri	Sekarang Anda dapat mengunduh Letter of Authorization and Connecting Facility Assignment (LOA-CFA) menggunakan konsol atau API AWS Direct Connect.	2016-06-22
Lokasi baru di Silicon Valley	Topik yang diperbarui untuk menyertakan penambahan lokasi Silicon Valley baru di Wilayah US West (N. California).	2016-06-03
Lokasi baru di Amsterdam	Topik yang diperbarui untuk menyertakan penambahan lokasi Amsterdam baru di Wilayah Eropa (Frankfurt).	2016-05-19

Fitur	Deskripsi	Tanggal
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).	2016-04-27
Lokasi baru di Sao Paulo, Brasil	Topik yang diperbarui untuk untuk menyertakan penambahan lokasi Sao Paulo baru di Wilayah South America (São Paulo).	2015-12-09
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 Mumbai (Wilayah Asia Pasifik (Singapura)).	2015-11-27
Lokasi baru di Wilayah China (Beijing)	Topik terbaru untuk menyertakan penambahan lokasi Beijing baru di Wilayah China (Beijing).	2015-04-14
Lokasi Las Vegas baru di Wilayah US West (Oregon).	Topik yang diperbarui untuk menyertakan penambahan lokasi Las vegas AWS Direct Connect baru di Wilayah US West (Oregon).	2014-11-10
Wilayah EU (Frankfurt) baru	Topik yang diperbarui untuk menyertakan penambahan lokasi AWS Direct Connect baru yang melayani Wilayah EU (Frankfurt).	2014-10-23
Lokasi baru di Wilayah Asia Pacific (Sydney)	Topik yang diperbarui untuk menyertakan penambahan lokasi AWS Direct Connect baru yang melayani Wilayah Asia Pacific (Sydney).	2014-07-14

Fitur	Deskripsi	Tanggal
Dukungan untuk AWS CloudTrail	Menambahkan topik baru untuk menjelaskan bagaimana Anda dapat menggunakan CloudTrail untuk login aktivitasAWS Direct Connect. Untuk informasi selengkapnya, lihat Pembuatan log panggilan API AWS Direct Connect menggunakan AWS CloudTrail.	2014-04-04
Dukungan untuk mengakses Wilayah AWS jarak jauh	Penambahan topik baru untuk menjelaskan bagaimana Anda dapat mengakses sumber daya publik di Wilayah jarak jauh. Untuk informasi selengkapnya, lihat Mengakses Wilayah AWS jarak jauh.	2013-12-19
Dukungan untuk koneksi yang di-host	Topik yang diperbarui untuk menyertakan dukungan untuk koneksi yang di-host.	2013-10-22
Lokasi baru di Wilayah EU (Ireland)	Topik yang diperbarui untuk menyertakan penambahan lokasi AWS Direct Connect baru yang melayani Wilayah EU (Ireland).	2013-06-24
Lokasi Seattle baru di Wilayah US West (Oregon)	Topik yang diperbarui untuk menyertakan penambahan lokasi AWS Direct Connect baru di Seattle melayani Wilayah US West (Oregon).	2013-05-08
Dukungan untuk menggunakan IAM dengan AWS Direct Connect	Penambahan topik tentang menggunakan AWS Identity and Access Management dengan AWS Direct Connect. Untuk informasi selengkapnya, lihat the section called “Pengelolaan Identitas dan Akses”.	2012-12-21

Fitur	Deskripsi	Tanggal
Wilayah Asia Pacific (Sydney)	Topik yang diperbarui untuk menyertakan penambahan lokasi AWS Direct Connect baru yang melayani Wilayah Asia Pacific (Sydney).	2012-12-14
Konsol AWS Direct Connect baru, dan Wilayah US East (N. Virginia) dan South America (Sao Paulo)	Mengganti AWS Direct ConnectPanduan Memulai dengan AWS Direct Connect Panduan Pengguna. Penambahan topik baru untuk membahas konsol AWS Direct Connect baru, menambahk an topik penagihan, menambahkan informasi konfigurasi router, dan topik terbaru untuk menyertakan dua lokasi AWS Direct Connect baru yang melayani Wilayah US East (N. Virginia) dan South America (Sao Paulo).	2012-08-13
Dukungan untuk Wilayah EU (Ireland), Asia Pacific (Singapor e), dan Asia Pacific (Tokyo)	Penambahan bagian pemecahan masalah baru dan topik yang diperbarui untuk menyertakan penambahan empat lokasi AWS Direct Connect baru yang melayani Wilayah US West (Northern California), EU (Ireland), Asia Pacific (Singapore), dan Asia Pacific (Tokyo).	2012-01-10
Dukungan untuk Wilayah US West (Northern California)	Topik terbaru untuk menyertakan penambahan Wilayah US West (Northern California).	2011-09-08
Rilis publik	Rilis pertama AWS Direct Connect.	2011-08-03

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