Panduan Pengguna untuk rak Outposts

AWS Outposts

AWS Outposts: Panduan Pengguna untuk rak Outposts

Table of Contents

Apa itu AWS Outposts?

AWS Outposts adalah layanan yang dikelola sepenuhnya yang memperluas AWS infrastruktur, layanan APIs, dan alat ke tempat pelanggan. Dengan menyediakan akses lokal ke infrastruktur AWS terkelola, AWS Outposts memungkinkan pelanggan untuk membangun dan menjalankan aplikasi di tempat menggunakan antarmuka pemrograman yang sama seperti di AWS Wilayah, sambil menggunakan sumber daya komputasi dan penyimpanan lokal untuk latensi yang lebih rendah dan kebutuhan pemrosesan data lokal.

Outpost adalah kumpulan kapasitas AWS komputasi dan penyimpanan yang digunakan di situs pelanggan. AWS mengoperasikan, memantau, dan mengelola kapasitas ini sebagai bagian dari suatu AWS Wilayah. Anda dapat membuat subnet di Outpost dan menentukannya saat Anda membuat AWS sumber daya seperti EC2 instance, volume EBS, kluster ECS, dan instans RDS. Instance dalam subnet Outpost berkomunikasi dengan instans lain di AWS Wilayah menggunakan alamat IP pribadi, semuanya dalam VPC yang sama.

> **Note**
>
> Anda tidak dapat menghubungkan Outpost ke Outpost atau Local Zone lain yang berada dalam VPC yang sama.

Untuk informasi lebih lanjut, lihat halaman AWS Outposts produk.

Konsep utama

Ini adalah konsep kunci untuk AWS Outposts.

- Situs pos terdepan — Bangunan fisik yang dikelola pelanggan tempat AWS akan memasang Pos Luar Anda. Sebuah situs harus memenuhi fasilitas, jaringan, dan persyaratan daya untuk Outpost Anda.
- Kapasitas pos terdepan — Sumber daya komputasi dan penyimpanan yang tersedia di Outpost. Anda dapat melihat dan mengelola kapasitas untuk Outpost Anda dari AWS Outposts konsol. AWS Outposts mendukung manajemen kapasitas swalayan yang dapat Anda tentukan di tingkat Outposts untuk mengkonfigurasi ulang semua aset di Outposts atau khusus untuk setiap aset individu. Aset Outpost dapat berupa server tunggal dalam rak Outposts atau server Outposts.

- Peralatan pos terdepan — Perangkat keras fisik yang menyediakan akses ke AWS Outposts layanan. Perangkat keras termasuk rak, server, sakelar, dan kabel yang dimiliki dan dikelola oleh. AWS
- Rak Outposts — Faktor bentuk Outpost yang merupakan rak 42U standar industri. Rak Outposts termasuk server yang dapat dipasang di rak, sakelar, panel patch jaringan, rak daya, dan panel kosong.
- Outposts ACE racks — Rak Aggregation, Core, Edge (ACE) bertindak sebagai titik agregasi jaringan untuk penyebaran Outpost multi-rak. Rak ACE mengurangi jumlah port jaringan fisik dan persyaratan antarmuka logis dengan menyediakan konektivitas antara beberapa rak komputasi Outpost di Outposts logis Anda dan jaringan on-premise Anda.

  Anda harus memasang rak ACE jika Anda memiliki empat atau lebih rak komputasi. Jika Anda memiliki kurang dari empat rak komputasi tetapi berencana untuk memperluas ke empat atau lebih rak di masa depan, kami sarankan Anda memasang rak ACE paling awal.

  Untuk informasi tambahan tentang rak ACE, lihat Menskalakan penyebaran AWS Outposts rak dengan rak ACE.
- Server Outposts - Faktor bentuk Outpost yang merupakan server 1U atau 2U standar industri, yang dapat dipasang di rak 4 pos standar yang sesuai dengan EIA-310D 19. Server Outposts menyediakan layanan komputasi dan jaringan lokal ke situs yang memiliki ruang terbatas atau persyaratan kapasitas yang lebih kecil.
- Pemilik pos terdepan — Pemilik akun untuk akun yang AWS Outposts melakukan pemesanan. Setelah AWS terlibat dengan pelanggan, pemilik dapat menyertakan titik kontak tambahan. AWS akan berkomunikasi dengan kontak untuk mengklarifikasi pesanan, janji pemasangan, dan pemeliharaan dan penggantian perangkat keras. Contact AWS Dukungan Center jika informasi kontak berubah.
- Tautan layanan — Rute jaringan yang memungkinkan komunikasi antara Outpost Anda dan AWS Wilayah terkaitnya. Setiap Pos Luar adalah perpanjangan dari Availability Zone dan Wilayah terkaitnya.
- Local Gateway (LGW) — Router virtual interkoneksi logis yang memungkinkan komunikasi antara rak Outposts dan jaringan lokal Anda.
- Antarmuka jaringan lokal — Antarmuka jaringan yang memungkinkan komunikasi dari server Outposts dan jaringan lokal Anda.

AWS sumber daya di Outposts

Anda dapat membuat sumber daya berikut di Outpost untuk mendukung beban kerja latensi rendah yang harus berjalan di dekat data dan aplikasi lokal:

Komputasi

Jenis sumber daya	Rak	Peladen
EC2 Contoh Amazon	Y	Ya
Cluster Amazon ECS	Y	Ya
Node Amazon EKS	Y	Tidak

Database dan analitik

Jenis sumber daya	Rak	Peladen
ElastiCacheNode Amazon (kluster Redis, kluster Memcached)	Y	Tidak
Cluster EMR Amazon	Y	Tidak
Instans Amazon RDS DB	Y	Tidak

Jaringan

Jenis sumber daya	Rak	Peladen
Proksi Utusan App Mesh	 Y	 Ya
Penyeimbang Beban Aplikasi	 Y	 Tidak
Amazon VPC subnet	 Y	 Ya
Rute Amazon 53	 Y	 Tidak

Penyimpanan

Jenis sumber daya	Rak	Peladen
Volume Amazon EBS	 Y	 Tidak
Ember Amazon S3	 Y	 Tidak

Lainnya Layanan AWS

Layanan	Rak	Peladen
AWS IoT Greengrass	 Y	 Ya

Harga

Harga didasarkan pada detail pesanan Anda. Saat melakukan pemesanan, Anda dapat memilih dari berbagai konfigurasi Outpost, masing-masing menyediakan kombinasi jenis EC2 instans Amazon dan opsi penyimpanan. Anda juga memilih jangka waktu kontrak dan opsi pembayaran. Harga termasuk yang berikut:

- Rak Outposts - Pengiriman, instalasi, pemeliharaan layanan infrastruktur, tambalan dan peningkatan perangkat lunak, dan penghapusan rak.
- Server Outposts - Pengiriman, pemeliharaan layanan infrastruktur, dan tambalan dan peningkatan perangkat lunak. Anda bertanggung jawab atas instalasi dan pengepakan server untuk pengembalian.

Anda ditagih untuk sumber daya bersama dan transfer data apa pun dari AWS Wilayah ke Pos Luar. Anda juga ditagih untuk transfer data yang AWS berfungsi untuk menjaga ketersediaan dan keamanan.

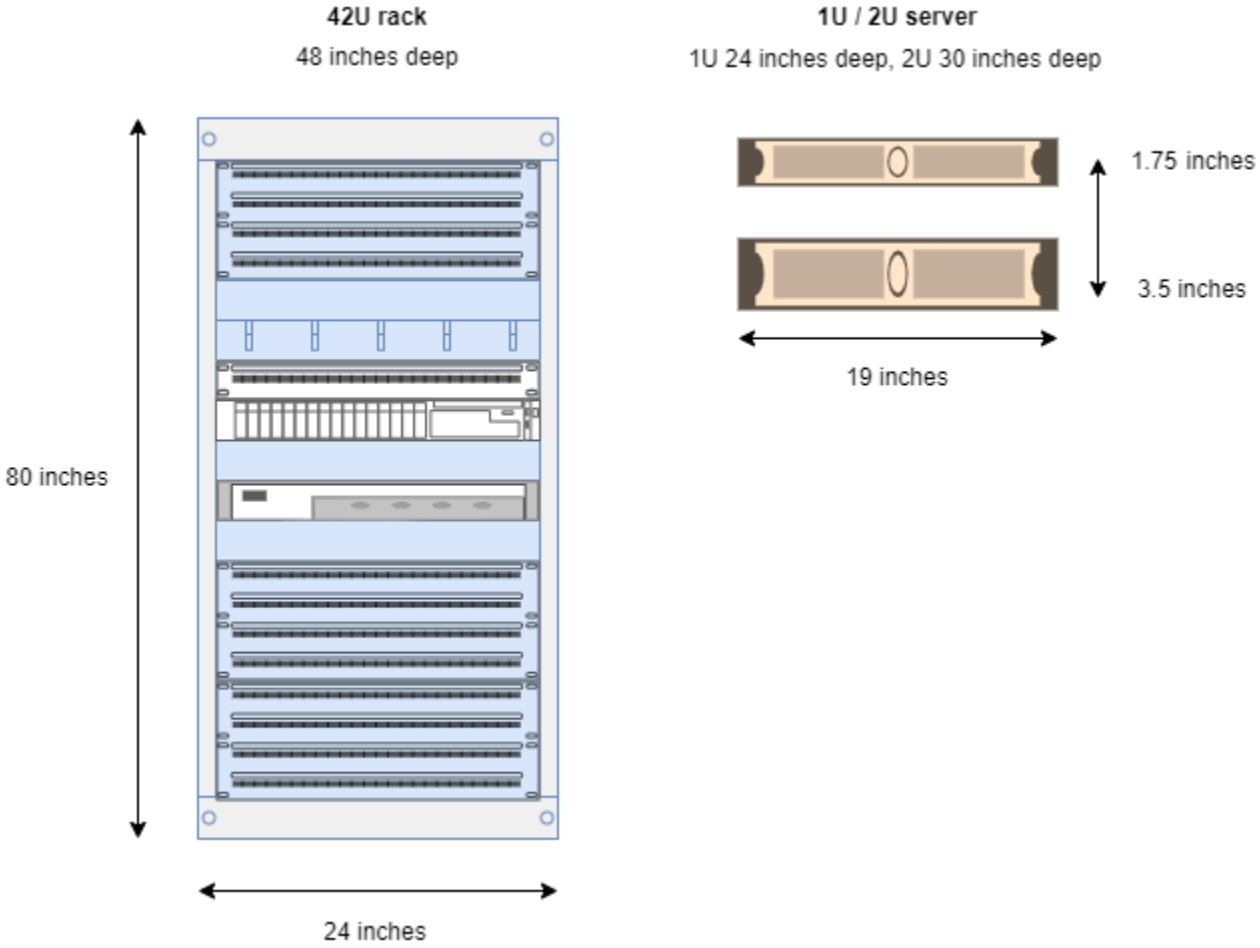
Untuk harga berdasarkan lokasi, konfigurasi, dan opsi pembayaran, lihat:

- Harga rak Outposts
- Harga server Outposts

Bagaimana cara AWS Outposts kerja

AWS Outposts dirancang untuk beroperasi dengan koneksi yang konstan dan konsisten antara Pos Luar Anda dan AWS Wilayah. Untuk mencapai koneksi ini ke Wilayah, dan ke beban kerja lokal di lingkungan lokal, Anda harus menghubungkan Outpost ke jaringan lokal. Jaringan lokal Anda harus menyediakan akses jaringan area luas (WAN) kembali ke Wilayah. Ini juga harus menyediakan akses LAN atau WAN ke jaringan lokal tempat beban kerja atau aplikasi lokal Anda berada.

Diagram berikut menggambarkan kedua faktor bentuk Outpost.



Daftar Isi

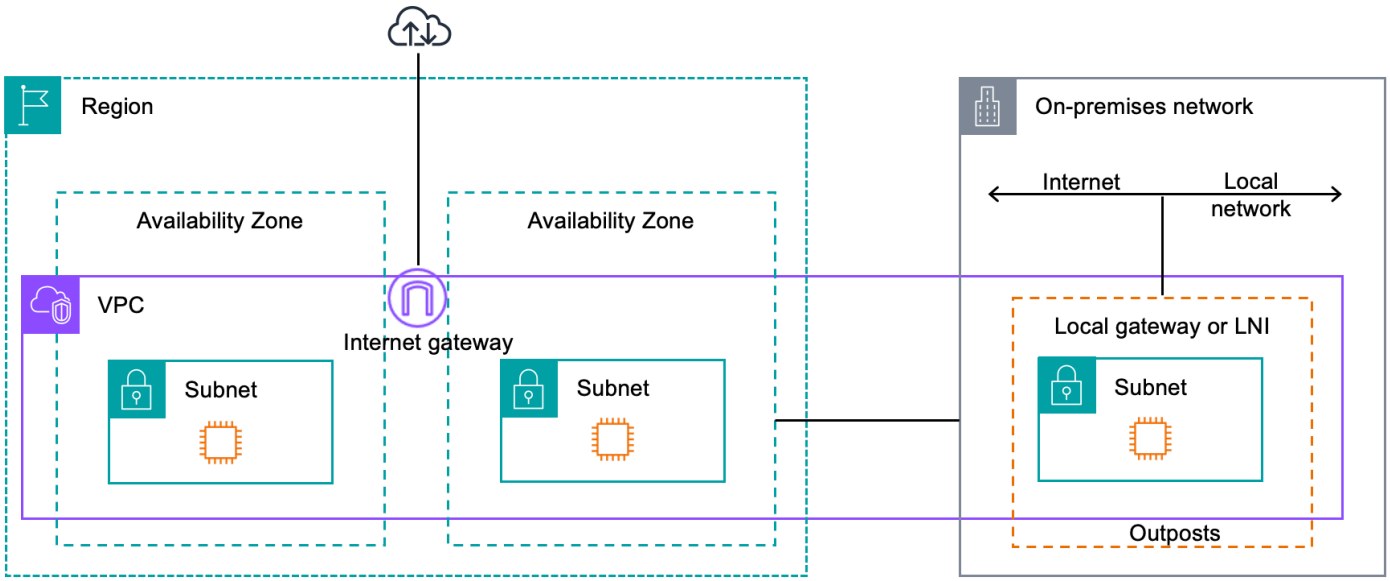
- Tautan layanan
- Gerbang lokal
- Antarmuka jaringan lokal

Komponen jaringan

AWS Outposts memperluas VPC Amazon dari AWS Wilayah ke Pos Luar dengan komponen VPC yang dapat diakses di Wilayah, termasuk gateway internet, gateway pribadi virtual, Gateway Transit VPC Amazon, dan titik akhir VPC. Pos Luar ditempatkan ke Availability Zone di Region dan merupakan perpanjangan dari Availability Zone yang dapat Anda gunakan untuk ketahanan.

Diagram berikut menunjukkan komponen jaringan untuk Outpost Anda.

- Sebuah Wilayah AWS dan jaringan lokal
- VPC dengan beberapa subnet di Wilayah
- Pos terdepan di jaringan lokal
- Konektivitas antara Outpost dan jaringan lokal yang disediakan:
  - Untuk rak Outposts: gerbang lokal
  - Untuk server Outposts: antarmuka jaringan lokal (LNI)



VPCs dan subnet

Virtual Private Cloud (VPC) mencakup semua Availability Zone di Wilayahnya. AWS Anda dapat memperpanjang VPC di Wilayah ke Outpost Anda dengan menambahkan subnet Outpost. Untuk menambahkan subnet Outpost ke VPC, tentukan Amazon Resource Name (ARN) Outpost saat Anda membuat subnet.

Outposts mendukung beberapa subnet. Anda dapat menentukan subnet EC2 instance saat meluncurkan EC2 instance di Outpost Anda. Anda tidak dapat menentukan perangkat keras yang mendasari tempat instance digunakan, karena Outpost adalah kumpulan kapasitas AWS komputasi dan penyimpanan.

Setiap Outpost dapat mendukung beberapa VPCs yang dapat memiliki satu atau lebih subnet Outpost. Untuk informasi tentang kuota VPC, lihat Kuota VPC Amazon di Panduan Pengguna Amazon VPC.

Anda membuat subnet Outpost dari rentang VPC CIDR dari VPC tempat Anda membuat Outpost. Anda dapat menggunakan rentang alamat Outpost untuk sumber daya, seperti EC2 instance yang berada di subnet Outpost.

Perutean

Secara default, setiap subnet Outpost mewarisi tabel rute utama dari VPC-nya. Anda dapat membuat tabel rute khusus dan mengaitkannya dengan subnet Outpost.

Tabel rute untuk subnet Outpost berfungsi seperti yang mereka lakukan untuk subnet Availability Zone. Anda dapat menentukan alamat IP, gateway internet, gateway lokal, gateway pribadi virtual, dan koneksi peering sebagai tujuan. Misalnya, setiap subnet Outpost, baik melalui tabel rute utama yang diwarisi, atau tabel kustom, mewarisi rute lokal VPC. Ini berarti bahwa semua lalu lintas di VPC, termasuk subnet Outpost dengan tujuan di CIDR VPC tetap dirutekan di VPC.

Tabel rute subnet pos terdepan dapat mencakup tujuan berikut:

- Rentang VPC CIDR - AWS mendefinisikan ini saat instalasi. Ini adalah rute lokal dan berlaku untuk semua perutean VPC, termasuk lalu lintas antara instance Outpost di VPC yang sama.
- AWS Tujuan wilayah - Ini termasuk daftar awalan untuk Amazon Simple Storage Service (Amazon S3), titik akhir gateway Amazon DynamoDB, s, gateway pribadi virtual, gateway internet AWS Transit Gateway, dan peering VPC.

Jika Anda memiliki koneksi peering dengan beberapa VPCs di Outpost yang sama, lalu lintas antara VPCs sisa-sisa di Outpost dan tidak menggunakan tautan layanan kembali ke Wilayah.

- Komunikasi intra-VPC di seluruh Outposts dengan gateway lokal - Anda dapat membangun komunikasi antar subnet dalam VPC yang sama di berbagai Outposts dengan gateway lokal menggunakan routing VPC langsung. Untuk informasi selengkapnya, lihat:
  - Perutean VPC langsung
  - Routing ke gateway AWS Outposts lokal

DNS

Untuk antarmuka jaringan yang terhubung ke VPC EC2 , instance di subnet Outposts dapat menggunakan Layanan DNS Amazon Route 53 untuk menyelesaikan nama domain ke alamat IP. Route 53 mendukung fitur DNS, seperti pendaftaran domain, perutean DNS, dan pemeriksaan kesehatan untuk instance yang berjalan di Outpost Anda. Zona Ketersediaan yang dihosting publik dan pribadi didukung untuk merutekan lalu lintas ke domain tertentu. Resolver Route 53 diselenggarakan di Wilayah. AWS Oleh karena itu, konektivitas tautan layanan dari Outpost kembali ke AWS Wilayah harus aktif dan berjalan agar fitur DNS ini berfungsi.

Anda mungkin menemukan waktu resolusi DNS yang lebih lama dengan Route 53, tergantung pada latensi jalur antara Pos Luar dan Wilayah. AWS Dalam kasus tersebut, Anda dapat menggunakan server DNS yang diinstal secara titik waktu di lingkungan on-premise Anda. Untuk menggunakan server DNS Anda sendiri, Anda harus membuat set opsi DHCP untuk server DNS lokal dan mengaitkannya dengan VPC. Anda juga harus memastikan bahwa ada konektivitas IP ke server DNS ini. Anda mungkin juga perlu menambahkan rute ke tabel perutean gateway lokal untuk jangkauan tetapi ini hanya opsi untuk rak Outposts dengan gateway lokal. Karena set opsi DHCP memiliki cakupan VPC, instance di subnet Outpost dan subnet Availability Zone untuk VPC akan mencoba menggunakan server DNS yang ditentukan untuk resolusi nama DNS.

Pencatatan kueri tidak didukung untuk kueri DNS yang berasal dari Outpost.

Tautan layanan

Tautan layanan adalah koneksi dari Pos Luar Anda kembali ke AWS Wilayah atau Wilayah rumah Outposts pilihan Anda. Tautan layanan adalah seperangkat koneksi VPN terenkripsi yang digunakan setiap kali Outpost berkomunikasi dengan Wilayah asal pilihan Anda. Anda menggunakan LAN virtual (VLAN) untuk menyegmentasikan lalu lintas pada tautan layanan. Tautan layanan VLAN

memungkinkan komunikasi antara Pos Luar dan AWS Wilayah untuk pengelolaan lalu lintas Outpost dan intra-VPC antara Wilayah dan Pos Luar. AWS

Tautan layanan Anda dibuat saat Outpost Anda disediakan. Jika Anda memiliki faktor bentuk server, Anda membuat koneksi. Jika Anda memiliki rak, AWS buat tautan layanan. Untuk informasi selengkapnya, lihat:

- AWS Outposts konektivitas ke Wilayah AWS
- Perutean aplikasi/beban kerja dalam Whitepaper Pertimbangan Desain dan AWS Outposts Arsitektur Ketersediaan Tinggi AWS

Gerbang lokal

Rak Outposts menyertakan gateway lokal untuk menyediakan konektivitas ke jaringan lokal Anda. Jika Anda memiliki rak Outposts, Anda dapat menyertakan gateway lokal sebagai target di mana tujuannya adalah jaringan lokal Anda. Gateway lokal hanya tersedia untuk rak Outposts dan hanya dapat digunakan di VPC dan tabel rute subnet yang terkait dengan rak Outposts. Untuk informasi selengkapnya, lihat:

- Gerbang lokal untuk rak Outposts Anda
- Perutean aplikasi/beban kerja dalam Whitepaper Pertimbangan Desain dan AWS Outposts Arsitektur Ketersediaan Tinggi AWS

Antarmuka jaringan lokal

Server Outposts menyertakan antarmuka jaringan lokal untuk menyediakan konektivitas ke jaringan lokal Anda. Antarmuka jaringan lokal hanya tersedia untuk server Outposts yang berjalan di subnet Outpost. Anda tidak dapat menggunakan antarmuka jaringan lokal dari EC2 instance di rak Outposts atau di Region. AWS Antarmuka jaringan lokal dimaksudkan hanya untuk lokasi lokal. Untuk informasi selengkapnya, lihat Antarmuka jaringan lokal di Panduan AWS Outposts Pengguna untuk server Outposts.

Persyaratan situs untuk rak Outposts

Situs Outpost adalah lokasi fisik tempat Outpost Anda beroperasi. Situs hanya tersedia di negara dan wilayah tertentu. Untuk informasi lebih lanjut, lihat, AWS Outposts rak FAQs. Lihat pertanyaan: Di negara dan wilayah mana rak Outposts tersedia?

Halaman ini mencakup persyaratan untuk rak Outposts. Jika Anda memasang rak Agregasi, Inti, Edge (ACE), situs Anda juga harus memenuhi persyaratan yang tercantum diPersyaratan situs untuk rak Outpost ACE.

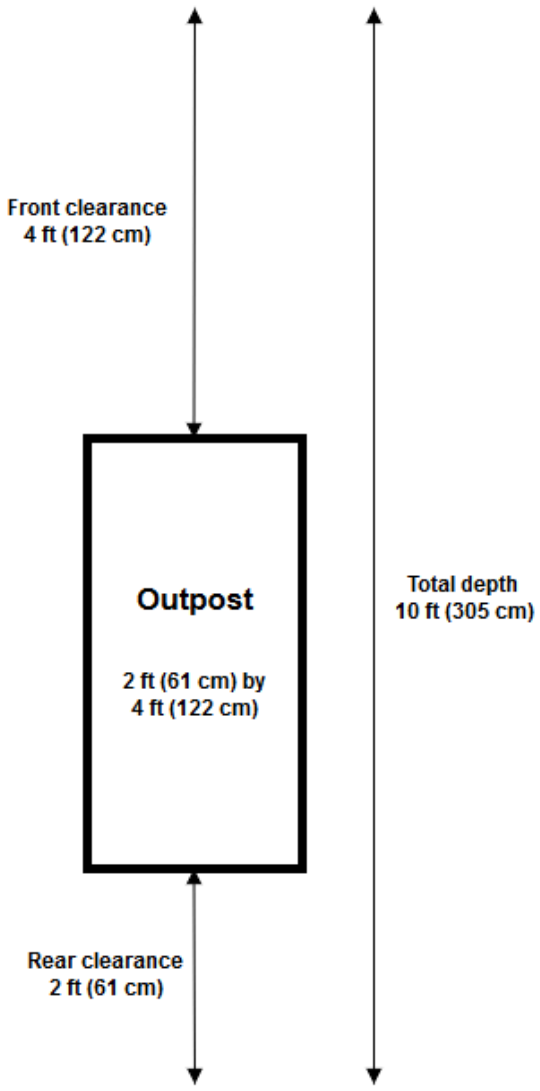
Untuk persyaratan server Outposts, lihat Persyaratan situs untuk server Outposts di AWS Outposts Panduan Pengguna untuk server Outposts.

Fasilitas

Ini adalah persyaratan fasilitas untuk rak.

- Suhu dan kelembaban — Suhu sekitar harus antara 41° F (5° C) dan 95° F (35° C). Kelembaban relatif harus antara 8 persen dan 80 persen tanpa kondensasi.
- Aliran Udara - Rak menarik udara dingin dari lorong depan dan mengalirkan udara panas ke lorong belakang. Posisi rak harus menyediakan setidaknya 145,8 kali kVA aliran udara kaki kubik per menit (CFM).
- Dermaga pemuatan - Dermaga pemuatan Anda harus menampung peti rak yang tingginya 94 inci (239 cm) kali lebar 54 inci (138 cm) kali kedalaman 51 inci (130 cm).
- Dukungan berat - Berat bervariasi berdasarkan konfigurasi. Anda dapat menemukan bobot untuk konfigurasi Anda yang ditentukan dalam ringkasan pesanan pada beban titik rak. Lokasi di mana rak dipasang dan jalur ke lokasi itu harus mendukung berat yang ditentukan. Ini termasuk angkutan dan lift standar di sepanjang jalan.
- Clearance - Rak memiliki tinggi 80 inci (203 cm) kali lebar 24 inci (61 cm) kali kedalaman 48 inci (122 cm). Setiap pintu, lorong, belokan, landai, dan lift harus memberikan izin yang cukup. Pada posisi istirahat akhir, harus ada area selebar 24 inci (61 cm) kali 48 inci (122 cm) untuk Outpost, dengan tambahan jarak depan 48 inci (122 cm) dan jarak bebas belakang 24 inci (61 cm). Total area minimum yang diperlukan untuk Pos Luar adalah lebar 24 inci (61 cm) dengan kedalaman 10 kaki (305 cm).

  Diagram berikut menunjukkan total area minimum yang diperlukan untuk Pos Luar, termasuk izin.



- Penguat seismik — Sejauh yang disyaratkan oleh peraturan atau kode, Anda akan memasang dan memelihara jangkar dan penyangga seismik yang sesuai untuk rak saat berada di fasilitas Anda. AWS menyediakan braket lantai yang memberikan perlindungan hingga 2.0G aktivitas seismik dengan semua rak Outposts.
- Titik ikatan - Kami menyarankan Anda memberikan ikatan wire/point pada posisi rak sehingga teknisi listrik Anda dapat mengikat rak selama pemasangan yang akan divalidasi oleh teknisi bersertifikat. AWS
- Akses fasilitas — Anda tidak akan mengubah fasilitas dengan cara yang berdampak negatif pada kemampuan AWS mengakses, melayani, atau menghapus Outpost.
- Ketinggian - Ketinggian ruangan tempat rak dipasang harus di bawah 10.005 kaki (3.050 meter).

Jaringan

Ini adalah persyaratan jaringan untuk rak.

- Menyediakan uplink dengan kecepatan 1 Gbps, 10 Gbps, 40 Gbps, atau 100 Gbps.

  Untuk rekomendasi bandwidth untuk koneksi tautan layanan, lihat Rekomendasi bandwidth.
- Sediakan serat mode tunggal (SMF) dengan Lucent Connector (LC), serat multimode (MMF), atau MMF dengan LC. OM4
- Sediakan satu atau dua perangkat hulu, yang dapat berupa sakelar atau router. Kami merekomendasikan dua perangkat untuk menyediakan ketersediaan tinggi.

Daftar periksa kesiapan jaringan

Gunakan daftar periksa ini saat Anda mengumpulkan informasi untuk konfigurasi Outpost Anda. Ini termasuk LAN, WAN, dan perangkat apa pun antara Outpost dan tujuan lalu lintas lokal, dan tujuan di AWS Wilayah.

Kecepatan uplink, port, dan serat

Kecepatan dan port uplink

Sebuah Outpost memiliki dua perangkat jaringan Outpost yang terhubung ke jaringan lokal Anda. Jumlah uplink yang dapat didukung setiap perangkat tergantung pada kebutuhan bandwidth Anda dan apa yang dapat didukung router Anda. Untuk informasi selengkapnya, lihat Konektivitas fisik.

Daftar berikut menunjukkan berapa banyak port uplink yang didukung untuk setiap perangkat jaringan Outpost, berdasarkan kecepatan uplink.

1 Gbps

1, 2, 4, 6, atau 8 uplink

10 Gbps

1, 2, 4, 8, 12, atau 16 uplink

40 Gbps atau 100 Gbps

1, 2, atau 4 uplink

Serat

Jenis serat berikut didukung:

- Serat mode tunggal (SMF) dengan Lucent Connector (LC)
- Serat multi-mode (MMF) atau OM4 MMF dengan LC

Tergantung pada kecepatan uplink dan jenis serat yang Anda pilih, standar optik berikut didukung.

Kecepatan uplink	Jenis serat	Standar optik
1 Gbps	SMF	- 1000Base-LX
1 Gbps	MMF	— 1000Base-SX
10 Gbps	SMF	— 10GBASE-IR — 10GBASE-LR
10 Gbps	MMF	— 10GBASE-SR
40 Gbps	SMF	- 40GBASE- IR4 (LR4L) - 40GBASE- LR4
Aplikasi breakout 4 x 10 Gbps	MMF	- 40GBASE- ESR4 - 40GBASE- SR4
100 Gbps	SMF	— 100G PSM4 MSA - 100GBASE- CWDM4 - 100GBASE- LR4
Aplikasi breakout 4 x 25 Gbps	MMF	- 100GBASE- SR4

Agregasi tautan pos terdepan dan VLANs

Link aggregation control protocol (LACP) diperlukan antara Outpost dan jaringan Anda. Anda harus menggunakan LAG dinamis dengan LACP.

VLANs Berikut ini diperlukan untuk setiap perangkat jaringan Outpost. Untuk informasi selengkapnya, lihat Virtual LANs.

Perangkat jaringan pos terdepan	Tautan layanan VLAN	VLAN gerbang lokal
#1	Nilai yang valid: 1-4094	Nilai yang valid: 1-4094
#2	Nilai yang valid: 1-4094	Nilai yang valid: 1-4094

Untuk setiap perangkat jaringan Outpost, Anda dapat memilih apakah akan menggunakan yang sama VLANs atau berbeda VLANs untuk tautan layanan dan gateway lokal. Namun, kami menyarankan agar setiap perangkat jaringan Outpost memiliki VLAN yang berbeda dari perangkat jaringan Outpost lainnya. Untuk informasi selengkapnya, lihat Agregasi tautan dan Virtual LANs.

Kami juga merekomendasikan konektivitas lapisan 2 redundan. LACP digunakan untuk agregasi tautan dan tidak digunakan untuk ketersediaan tinggi. LACP antara perangkat jaringan Outpost tidak didukung.

Konektivitas IP perangkat jaringan pos terdepan

Masing-masing dari dua perangkat jaringan Outpost memerlukan CIDR dan alamat IP untuk tautan layanan dan gateway lokal. VLANs Kami merekomendasikan mengalokasikan subnet khusus untuk setiap perangkat jaringan dengan /30 atau /31 CIDR. Tentukan subnet dan alamat IP dari subnet untuk Outpost yang akan digunakan. Untuk informasi selengkapnya, lihat Konektivitas lapisan jaringan.

Perangkat jaringan pos terdepan	Persyaratan tautan layanan	Persyaratan gateway lokal
#1	— Tautan layanan CIDR (/30 atau/31) — Alamat IP tautan layanan	— Gerbang lokal CIDR (/30 atau/31) — Alamat IP gateway lokal

Perangkat jaringan pos terdepan	Persyaratan tautan layanan	Persyaratan gateway lokal
#2	— Tautan layanan CIDR (/30 atau/31) — Alamat IP tautan layanan	— Gerbang lokal CIDR (/30 atau/31) — Alamat IP gateway lokal

Unit transmisi maksimum tautan layanan (MTU)

Jaringan harus mendukung 1500-byte MTU antara Outpost dan titik akhir tautan layanan di Wilayah induk. AWS Untuk informasi selengkapnya tentang tautan layanan, lihatAWS Outposts konektivitas ke AWS Wilayah.

Tautan layanan Border Gateway Protocol

Outpost menetapkan sesi peering BGP (eBGP) eksternal antara setiap perangkat jaringan Outpost dan perangkat jaringan lokal Anda untuk konektivitas tautan layanan melalui tautan layanan VLAN. Untuk informasi selengkapnya, lihat Tautan layanan konektivitas BGP.

Pos terdepan	Persyaratan BGP tautan layanan
Pos Terdepan Anda	— Nomor Sistem Otonomi BGP Outpost (ASN). 2-byte (16-bit) atau 4-byte (32-bit). Dari rentang ASN pribadi Anda (64512-65534 atau 4200000000-4294967294). — Infrastruktur CIDR (/26 diperlukan, diiklankan sebagai dua bersebelahan/27 detik).

Perangkat jaringan lokal	Persyaratan BGP tautan layanan
#1	— Tautan layanan alamat IP peer BGP. — Layanan link BGP peer ASN. 2-byte (16-bit) atau 4-byte (32-bit).
#2	— Tautan layanan alamat IP peer BGP.

Perangkat jaringan lokal	Persyaratan BGP tautan layanan
	— Layanan link BGP peer ASN. 2-byte (16-bit) atau 4-byte (32-bit).

Firewall tautan layanan

UDP dan TCP 443 harus terdaftar secara statis di firewall.

Protokol	Port Sumber	Alamat Sumber	Pelabuhan Tujuan	Alamat Tujuan
UDP	443	Tautan layanan pos terdepan /26	443	Rute umum Outpost Region
TCP	1025-65535	Tautan layanan pos terdepan /26	443	Rute umum Outpost Region

Anda dapat menggunakan AWS Direct Connect koneksi atau koneksi internet publik untuk menghubungkan Outpost kembali ke AWS Wilayah. Untuk konektivitas tautan layanan Outpost, Anda dapat menggunakan NAT atau PAT di firewall atau router tepi Anda. Pembentukan tautan layanan selalu dimulai dari Outpost.

Untuk informasi selengkapnya tentang persyaratan tautan layanan, seperti latensi MTU dan 175 ms, lihat Konektivitas melalui tautan layanan.

Protokol Gerbang Perbatasan gerbang lokal

Outpost menetapkan sesi peering eBGP dari setiap perangkat jaringan Outpost ke perangkat jaringan lokal untuk konektivitas dari jaringan lokal Anda ke gateway lokal. Untuk informasi selengkapnya, lihat Konektivitas BGP gateway lokal.

Pos terdepan	Persyaratan BGP gateway lokal
Pos Terdepan Anda	— Nomor Sistem Otonomi BGP Outpost (ASN). 2-byte (16-bit) atau 4-byte (32-bit). Dari rentang ASN pribadi Anda (64512-65534 atau 4200000000-4294967294).

Pos terdepan	Persyaratan BGP gateway lokal
	— CoIP CIDR untuk beriklan (publik atau pribadi, /26 minimum).

Perangkat jaringan lokal	Persyaratan BGP gateway lokal
#1	— Alamat IP peer BGP gateway lokal. — Gateway lokal BGP peer ASN. 2-byte (16-bit) atau 4-byte (32-bit).
#2	— Alamat IP peer BGP gateway lokal. — Gateway lokal BGP peer ASN. 2-byte (16-bit) atau 4-byte (32-bit).

Daya

Rak daya Outposts mendukung tiga konfigurasi daya: 5 kVA, 10 kVA, atau 15 kVA. Konfigurasi rak daya tergantung pada penarikan daya total kapasitas Outpost. Misalnya, jika sumber daya Outpost Anda memiliki daya tarik maksimum 9,7 kVA, Anda harus menyediakan konfigurasi daya untuk 10 kVA: 4 x L6-30P atau IEC3 09, 2 tetes ke S1, dan 2 tetes ke S2 untuk daya fase tunggal yang berlebihan. Tiga konfigurasi daya dijelaskan dalam tabel kedua berikut.

Untuk melihat persyaratan penarikan daya untuk sumber daya Outpost yang berbeda, pilih Jelajahi katalog di AWS Outposts konsol di https://console.aws.amazon.com/outposts/.

Persyaratan	Spesifikasi
Tegangan saluran AC	Fase tunggal 208 hingga 277 VAC; 50 atau 60 Hz Tiga fase: • 208 hingga 250 VAC (Delta); 50 hingga 60 Hz • 346 hingga 480 VAC (Wye); 50 hingga 60 Hz

Persyaratan	Spesifikasi
Konsumsi daya	5 kVA (4 kW), 10 kVA (9 kW), atau 15 kVA (13 kW)
Perlindungan AC (pemutus daya hulu)	Untuk input 1N (non-redundan) dan input 2N (redundan): 30 A, 32 A, atau 50 A dengan pemutus sirkuit kurva D atau kurva K. Untuk input 2N (redundan) saja: C-curve, D-curve, atau K-curve circuit breaker. Kurva B atau lebih rendah tidak didukung.
Jenis saluran masuk AC (wadah)	Colokan 3xL6-30P, P+P+E, 30A atau 3x 0309 P+N+E,, 32A fase tunggal IEC6 IP67 Tiga fase, Wye 1x IEC6 0309, 3P+N+E,, posisi jam 7, steker 30A atau IEC6 1x 0309 IP67, 3P+N+E,, posisi jam 6, steker 32A IP67 Tiga fase, Delta 1xNon-NEMA twistlock Hubbell CS8365 C, 3P +E, ground tengah, steker 50A **Note** Praktik terbaik adalah mengawinkan IP67 steker dengan IP67 stopkontak. Jika itu tidak memungkinkan, IP67 steker akan kawin dengan IP44 stopkontak. Peringkat steker dan soket gabungan akan menjadi peringkat yang lebih rendah (IP44).
Panjang cambuk	10.25 kaki (3 m)
Masukan kabel Whip - Rack	Dari atas atau di bawah rak

Rak daya memiliki dua input, S1 dan S2, yang dapat dikonfigurasi sebagai berikut.

	Redundan, fase tunggal	Redundan, tiga fase	Fase tunggal	Tiga fase
5 kVA	2 x L6-30P atau IEC3 09; 1 tetes ke S1 dan 1 tetes ke S2	2 x AH53 0P7W, AH532 P6W, atau CS8365 C; 1 drop ke S1 dan 1 drop ke S2	Tidak ditawarkan	1 x AH53 0P7W, AH532 P6W atau CS8365 C; 1 tetes ke S1
10 kVA	4 x L6-30P atau IEC3 09; 2 tetes ke S1 dan 2 tetes ke S2		2 x L6-30P atau IEC3 09; 2 tetes ke S1	
15 kVA	6 x L6-30P atau IEC3 09; 3 tetes ke S1 dan 3 tetes ke S2		3 x L6-30P atau IEC3 09; 3 tetes ke S1	

Jika cambuk AC yang AWS menyediakan seperti yang dijelaskan sebelumnya harus dilengkapi dengan steker listrik alternatif, pertimbangkan hal berikut:

- Hanya teknisi listrik bersertifikat yang disediakan pelanggan yang harus memodifikasi cambuk AC agar sesuai dengan jenis steker baru.
- Instalasi harus mematuhi semua persyaratan keselamatan nasional, negara bagian, dan lokal yang berlaku, dan diperiksa sebagaimana diperlukan untuk keselamatan listrik.
- Anda, pelanggan, harus memberi tahu AWS perwakilan Anda tentang modifikasi pada steker cambuk AC. Atas permintaan, Anda akan memberikan informasi tentang modifikasi AWS. Anda juga akan menyertakan catatan inspeksi keselamatan yang dikeluarkan oleh otoritas yang memiliki yurisdiksi. Ini adalah persyaratan untuk memvalidasi keamanan instalasi sebelum meminta AWS karyawan melakukan pekerjaan pada peralatan.

Pemenuhan pesanan

Untuk memenuhi pesanan, AWS akan menjadwalkan tanggal dan waktu dengan Anda. Anda juga akan menerima daftar periksa item untuk diverifikasi atau diberikan sebelum instalasi.

Tim AWS instalasi akan tiba di situs Anda pada tanggal dan waktu yang dijadwalkan. Mereka akan menempatkan rak pada posisi yang diidentifikasi. Anda dan tukang listrik Anda bertanggung jawab untuk melakukan sambungan listrik dan pemasangan ke rak.

Anda harus memastikan bahwa instalasi listrik, dan setiap perubahan pada instalasi tersebut, dilakukan oleh teknisi listrik bersertifikat sesuai dengan semua hukum, kode, dan praktik terbaik yang berlaku. Anda harus mendapatkan persetujuan dari AWS secara tertulis sebelum membuat perubahan apa pun pada perangkat keras Outpost atau instalasi listrik. Anda setuju untuk memberikan AWS dokumentasi yang memverifikasi kepatuhan dan keamanan setiap perubahan. AWS tidak bertanggung jawab atas risiko apa pun yang ditimbulkan oleh instalasi listrik Outpost atau kabel listrik fasilitas atau perubahan apa pun. Anda tidak boleh membuat perubahan lain pada perangkat keras Outposts.

Tim akan membangun konektivitas jaringan untuk rak Outposts di atas uplink yang Anda berikan, dan akan mengkonfigurasi kapasitas rak.

Instalasi selesai ketika Anda mengonfirmasi bahwa kapasitas Amazon EC2 dan Amazon EBS untuk rak Outposts Anda tersedia dari Anda. Akun AWS

Persyaratan situs untuk rak Outpost ACE

> **Note**
>
> Berlaku hanya jika Anda membutuhkan rak ACE.

Rak Agregasi, Inti, Edge (ACE) bertindak sebagai titik agregasi jaringan untuk penyebaran Outpost multi-rak. Anda harus memasang rak ACE jika Anda memiliki empat atau lebih rak komputasi. Jika Anda memiliki kurang dari empat rak komputasi tetapi berencana untuk memperluas ke empat atau lebih rak di masa depan, kami sarankan Anda memasang rak ACE.

Untuk memasang rak ACE, Anda harus memenuhi persyaratan di bagian ini selain persyaratan yang tercantum dalamPersyaratan situs untuk rak Outposts.

> **Note**
>
> Rak ACE tidak sepenuhnya tertutup dan tidak termasuk pintu depan atau pintu belakang.

Fasilitas

Ini adalah persyaratan fasilitas untuk rak ACE.

- Daya - Semua rak ACE dikirim dengan fase tunggal 10kVA (tipe konektor AA+BB; IEC6 0309 atau L6-30P Whip).
- Dukungan berat - Rak ACE memiliki berat 705 lbs (320 kg).
- Dimensi jarak bebas/ukuran - Rak ACE memiliki tinggi 80 inci (203 cm), lebar 24 inci (61 cm), dan kedalaman 42 inci (107 cm).

  Jika rak ACE memiliki lengan manajemen kabel, maka lebar rak adalah 36 inci (91,5 cm).

Jaringan

Ini adalah persyaratan jaringan untuk rak ACE. Untuk memahami bagaimana rak ACE menghubungkan perangkat jaringan Outposts, perangkat jaringan lokal, dan rak Outposts, lihat. Konektivitas rak ACE

- Persyaratan jaringan rak - Pastikan Anda memenuhi persyaratan yang tercantum dalam Daftar periksa kesiapan jaringan dan Konektivitas jaringan lokal untuk rak Outposts bagian kecuali untuk perubahan berikut:
  - Rak ACE memiliki empat perangkat jaringan yang terhubung ke perangkat hulu, bukan dua seperti dalam kasus rak Outposts tunggal.
  - Rak ACE tidak mendukung uplink 1 Gbps.
- Kecepatan uplink - Menyediakan uplink dengan kecepatan 10 Gbps, 40 Gbps, atau 100 Gbps. Untuk rekomendasi bandwidth untuk koneksi tautan layanan,Rekomendasi bandwidth tautan layanan.

> **Important**
>
> Rak ACE tidak mendukung uplink 1 Gbps.

- Serat - Menyediakan serat mode tunggal (SMF) dengan Lucent Connector (LC), atau serat multi-mode (MMF) dengan Lucent Connector (LC). Untuk daftar lengkap jenis serat dan standar optik yang didukung, lihatKecepatan uplink, port, dan serat.
- Perangkat hulu - Menyediakan dua atau empat perangkat hulu, yang dapat berupa sakelar atau router.
- Layanan VLAN dan VLAN Gateway Lokal — Untuk masing-masing dari empat perangkat jaringan ACE Anda harus menyediakan VLAN Layanan dan VLAN Gateway Lokal yang berbeda. Anda dapat memilih untuk menyediakan hanya dua yang berbeda VLANs, satu untuk VLAN Layanan dan satu untuk VLAN gateway Lokal, atau memiliki yang berbeda VLANs di setiap perangkat jaringan ACE untuk VLAN Layanan dan LGW VLAN dengan total 8 berbeda. VLANs Untuk informasi lebih lanjut tentang bagaimana grup agregasi tautan (LAGs) dan VLAN digunakan, lihat Agregasi tautan dan. Virtual LANs
- CIDR dan alamat IP untuk tautan layanan dan gateway lokal VLANs - Kami merekomendasikan mengalokasikan subnet khusus untuk setiap perangkat jaringan ACE dengan CIDR /30 atau/31. Atau, dimungkinkan untuk mengalokasikan subnet /29 tunggal di setiap Layanan dan VLAN Gateway Lokal. Dalam kedua kasus, Anda harus menentukan alamat IP untuk perangkat jaringan ACE untuk digunakan. Untuk informasi selengkapnya, lihat Konektivitas lapisan jaringan.
- Customer and Outpost BGP Autonomous System Number (ASN) untuk link layanan VLAN dan Local Gateway VLAN — The Outpost menetapkan sesi peering BGP (eBGP) eksternal antara setiap perangkat rak ACE dan perangkat jaringan lokal Anda untuk konektivitas tautan layanan melalui tautan layanan VLAN. Selain itu, ia menetapkan sesi peering eBGP dari setiap perangkat jaringan ACE ke perangkat jaringan lokal untuk konektivitas dari jaringan lokal Anda ke gateway

lokal. Untuk informasi selengkapnya, lihat Tautan layanan konektivitas BGP dan Konektivitas BGP gateway lokal.

> **Important**
>
> Subnet infrastruktur tautan layanan - Subnet infrastruktur tautan layanan (harus /26) diperlukan untuk setiap rak komputasi yang disertakan dalam instalasi Outposts Anda.

Daya

Ini adalah kebutuhan daya untuk rak ACE.

Persyaratan	Spesifikasi
Tegangan saluran AC	Fase tunggal 200 hingga 240 VAC; 50 atau 60 Hz
Konsumsi daya	10 kVA fase tunggal (AA+BB)
Perlindungan AC (pemutus daya hulu)	Untuk input 2N (redundan) saja: C-curve, D-curve, atau K-curve circuit breaker. Kurva B atau lebih rendah tidak didukung.
Jenis saluran masuk AC (wadah)	IEC6Jenis konektor cambuk 0309 atau L6-30P.

Pesan rak Outposts untuk memulai. Setelah menginstal peralatan Outpost Anda, luncurkan EC2 instans Amazon dan konfigurasikan konektivitas ke jaringan lokal Anda.

Tugas

- Buat pesanan untuk rak Outposts
- Luncurkan instance di rak Outposts Anda
- Optimalkan Amazon EC2 untuk AWS Outposts

Buat pesanan untuk rak Outposts

Untuk mulai menggunakan AWS Outposts, Anda harus membuat Outpost dan memesan kapasitas Outpost.

Prasyarat

- Tinjau konfigurasi yang tersedia untuk rak Outposts Anda.
- Situs Outpost adalah lokasi fisik untuk peralatan Outpost Anda. Sebelum memesan kapasitas, verifikasi bahwa situs Anda memenuhi persyaratan. Untuk informasi selengkapnya, lihat Persyaratan situs untuk rak Outposts.
- Anda harus memiliki paket AWS Enterprise Support atau paket AWS Enterprise On-Ramp Support.
- Tentukan mana yang akan Akun AWS Anda gunakan untuk membuat situs Outposts, membuat Outpost, dan melakukan pemesanan. Pantau email yang terkait dengan akun ini untuk informasi dari AWS.

Tugas

- Langkah 1: Buat situs
- Langkah 2: Buat Pos Terdepan
- Langkah 3: Tempatkan pesanan
- Langkah 4: Ubah kapasitas instance
- Langkah selanjutnya

Langkah 1: Buat situs

Buat situs untuk menentukan alamat operasi. Alamat operasi adalah lokasi fisik untuk rak Outposts Anda.

Prasyarat

- Tentukan alamat operasi.

Untuk membuat situs

1. Masuk ke AWS.
2. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
3. Untuk memilih induk Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
4. Di panel navigasi, pilih Situs.
5. Pilih Buat situs.
6. Untuk jenis perangkat keras yang didukung, pilih Rak dan server.
7. Masukkan nama, deskripsi, dan alamat operasi untuk situs Anda.
8. Untuk detail Situs, berikan informasi yang diminta tentang situs.
    - Berat maksimum - Berat rak maksimum yang dapat didukung situs ini, dalam lbs.
    - Power draw — Power draw tersedia pada posisi penempatan perangkat keras untuk rak, dalam kVA.
    - Opsi daya — Opsi daya yang dapat Anda sediakan untuk perangkat keras.
    - Konektor daya — Konektor daya yang AWS harus direncanakan untuk menyediakan koneksi ke perangkat keras.
    - Penurunan umpan daya - Tunjukkan apakah umpan daya berada di atas atau di bawah rak.
    - Kecepatan uplink - Kecepatan uplink yang harus didukung rak untuk koneksi ke Wilayah, dalam Gbps.
    - Jumlah uplink — Jumlah uplink untuk setiap perangkat jaringan Outpost yang ingin Anda gunakan untuk menghubungkan rak ke jaringan Anda.
    - Jenis serat — Jenis serat yang akan Anda gunakan untuk memasang rak ke jaringan Anda.
    - Standar optik — Jenis standar optik yang akan Anda gunakan untuk memasang rak ke jaringan Anda.

9. (Opsional) Untuk catatan Situs, masukkan informasi lain yang mungkin berguna AWS untuk mengetahui tentang situs.
10. Baca persyaratan fasilitas, lalu pilih Saya telah membaca persyaratan fasilitas.
11. Pilih Buat situs.

Langkah 2: Buat Pos Terdepan

Buat Pos Terdepan untuk rak Anda. Kemudian, tentukan Outpost ini saat Anda melakukan pemesanan.

Prasyarat

- Tentukan AWS Availability Zone untuk dikaitkan dengan situs Anda.

Untuk membuat Outpost

1. Di panel navigasi, pilih Outposts.
2. Pilih Buat Pos Terdepan.
3. Pilih Rak.
4. Masukkan nama dan deskripsi untuk Outpost Anda.
5. Pilih Availability Zone untuk Outpost Anda.
6. (Opsional) Untuk mengonfigurasi konektivitas pribadi, pilih Gunakan konektivitas pribadi. Pilih VPC dan subnet di Availability Zone yang sama Akun AWS dan Availability Zone sebagai Outpost Anda. Untuk informasi selengkapnya, lihat the section called “Prasyarat”.

   > **Note**
   >
   > Jika Anda perlu menghapus konektivitas pribadi untuk Outpost Anda, Anda harus menghubungi AWS Dukungan Center.

7. Untuk ID Situs, pilih situs Anda.
8. Pilih Buat Pos Terdepan.

Langkah 3: Tempatkan pesanan

Tempatkan pesanan untuk rak Outposts yang Anda butuhkan.

> **Important**
>
> Anda tidak dapat mengedit pesanan setelah mengirimkannya, jadi tinjau semua detail dengan cermat sebelum mengirimkan. Jika Anda perlu mengubah pesanan, hubungi Manajer AWS Akun Anda.

Prasyarat

- Tentukan bagaimana Anda akan membayar pesanan. Anda dapat membayar semua di muka, sebagian di muka, atau tidak ada di muka. Jika Anda tidak memilih untuk membayar semua di muka, Anda akan membayar biaya bulanan selama jangka waktu kontrak.

  Harga termasuk pengiriman, instalasi, pemeliharaan layanan infrastruktur, dan patch dan upgrade perangkat lunak.
- Tentukan apakah alamat pengiriman berbeda dari alamat operasi yang Anda tentukan untuk situs.

Untuk melakukan pemesanan

1. Di panel navigasi, pilih Pesanan.
2. Pilih Tempatkan pesanan.
3. Untuk jenis perangkat keras yang didukung, pilih Rak.
4. Untuk menambah kapasitas, pilih konfigurasi. Jika konfigurasi yang tersedia tidak memenuhi kebutuhan Anda, hubungi AWS Dukungan Pusat untuk meminta konfigurasi kapasitas khusus.
5. Pilih Berikutnya.
6. Pilih Gunakan Outpost yang ada dan pilih Outpost Anda.
7. Pilih Berikutnya.
8. Pilih jangka waktu kontrak dan opsi pembayaran.
9. Tentukan alamat pengiriman. Anda dapat menentukan alamat baru atau memilih alamat operasi situs. Jika Anda memilih alamat operasi, ketahuilah bahwa perubahan masa depan pada alamat operasi situs tidak akan menyebar ke pesanan yang ada. Jika Anda perlu mengubah nama dan alamat lokasi pengiriman pada pesanan yang ada, hubungi Manajer AWS Akun Anda.
10. Pilih Berikutnya.
11. Pada halaman Tinjauan dan pemesanan, verifikasi bahwa informasi Anda benar dan edit sesuai kebutuhan. Anda tidak akan dapat mengedit pesanan setelah Anda mengirimkannya.

12. Pilih Tempatkan pesanan.

Langkah 4: Ubah kapasitas instance

Pos Luar menyediakan kumpulan kapasitas AWS komputasi dan penyimpanan di situs Anda sebagai perpanjangan pribadi dari Availability Zone di suatu AWS Wilayah. Karena kapasitas komputasi dan penyimpanan yang tersedia di Outpost terbatas dan ditentukan oleh ukuran dan jumlah rak yang AWS dipasang di situs Anda, Anda dapat memutuskan berapa banyak Amazon, Amazon EBS, dan Amazon S3 AWS Outposts pada kapasitas yang Anda butuhkan untuk menjalankan beban kerja awal Anda, mengakomodasi pertumbuhan masa depan, dan untuk menyediakan kapasitas ekstra untuk mengurangi kegagalan server dan peristiwa pemeliharaan. EC2

Kapasitas setiap pesanan Outpost baru dikonfigurasi dengan konfigurasi kapasitas default. Anda dapat mengonversi konfigurasi default untuk membuat berbagai instance untuk memenuhi kebutuhan bisnis Anda. Untuk melakukannya, Anda membuat tugas kapasitas, menentukan ukuran dan kuantitas instance, dan menjalankan tugas kapasitas untuk mengimplementasikan perubahan.

> **Note**
>
> - Anda dapat mengubah jumlah ukuran instans setelah Anda melakukan pemesanan untuk Outposts Anda.
> - Ukuran dan kuantitas contoh ditentukan pada tingkat Outpost.
> - Instans ditempatkan secara otomatis berdasarkan praktik terbaik.

Untuk memodifikasi kapasitas instance

1. Dari panel navigasi kiri AWS Outposts konsol, pilih Tugas kapasitas.
2. Pada halaman tugas Kapasitas, pilih Buat tugas kapasitas.
3. Pada halaman Memulai, pilih pesanan.
4. Untuk mengubah kapasitas, Anda dapat menggunakan langkah-langkah di konsol atau mengunggah file JSON.

Console steps

1. Pilih Ubah konfigurasi kapasitas Outpost.

2. Pilih Berikutnya.
3. Pada halaman Configure instance capacity, setiap tipe instance menampilkan satu ukuran instans dengan jumlah maksimum yang telah dipilih sebelumnya. Untuk menambahkan lebih banyak ukuran instance, pilih Tambahkan ukuran instans.
4. Tentukan kuantitas instance dan catat kapasitas yang ditampilkan untuk ukuran instance tersebut.
5. Lihat pesan di akhir setiap bagian tipe instans yang memberi tahu Anda jika Anda berada di atas atau di bawah kapasitas. Lakukan penyesuaian pada ukuran instans atau tingkat kuantitas untuk mengoptimalkan total kapasitas yang tersedia.
6. Anda juga dapat meminta AWS Outposts untuk mengoptimalkan kuantitas instans untuk ukuran instans tertentu. Untuk melakukannya:

   a. Pilih ukuran instans.

   b. Pilih Saldo otomatis di akhir bagian tipe instans terkait.
7. Untuk setiap jenis instance, pastikan bahwa kuantitas instance ditentukan untuk setidaknya satu ukuran instance.
8. Pilih Berikutnya.
9. Pada halaman Tinjau dan buat, verifikasi pembaruan yang Anda minta.
10. Pilih Buat. AWS Outposts menciptakan tugas kapasitas.
11. Pada halaman tugas kapasitas, pantau status tugas.

> **Note**
>
> - AWS Outposts mungkin meminta Anda untuk menghentikan satu atau beberapa instance yang berjalan untuk mengaktifkan menjalankan tugas kapasitas. Setelah Anda menghentikan instance ini, AWS Outposts akan menjalankan tugas.
> - Jika Anda perlu mengubah kapasitas setelah menyelesaikan pesanan, hubungi AWS Dukungan Pusat untuk melakukan perubahan.

Upload a JSON file

1. Pilih Unggah konfigurasi kapasitas.
2. Pilih Berikutnya.

3. Pada halaman Paket konfigurasi kapasitas Unggah, unggah file JSON yang menentukan jenis, ukuran, dan kuantitas instans.

   Example

   Contoh file JSON:

```
{
    "InstancePools": [
        {
            "InstanceType": "c5.24xlarge",
            "Count": 1
        },
        {
            "InstanceType": "m5.24xlarge",
            "Count": 2
        }
    ]
}
```

4. Tinjau isi file JSON di bagian Paket konfigurasi Kapasitas.
5. Pilih Berikutnya.
6. Pada halaman Tinjau dan buat, verifikasi pembaruan yang Anda minta.
7. Pilih Buat. AWS Outposts menciptakan tugas kapasitas.
8. Pada halaman tugas kapasitas, pantau status tugas.

> **Note**
>
> - AWS Outposts mungkin meminta Anda untuk menghentikan satu atau beberapa instance yang berjalan untuk mengaktifkan menjalankan tugas kapasitas. Setelah Anda menghentikan instance ini, AWS Outposts akan menjalankan tugas.
> - Jika Anda perlu mengubah kapasitas setelah menyelesaikan pesanan, hubungi AWS Dukungan Pusat untuk melakukan perubahan.
> - Untuk memecahkan masalah, lihat Memecahkan masalah tugas kapasitas.

Langkah selanjutnya

Anda dapat melihat status pesanan Anda menggunakan AWS Outposts konsol. Status awal pesanan Anda adalah Pesanan diterima. Jika Anda memiliki pertanyaan tentang pesanan Anda, hubungi AWS Dukungan Pusat.

Untuk memenuhi pesanan, AWS akan menjadwalkan tanggal dan waktu dengan Anda.

Anda juga akan menerima daftar periksa item untuk diverifikasi atau diberikan sebelum instalasi. Tim AWS instalasi akan tiba di situs Anda pada tanggal dan waktu yang dijadwalkan. Tim akan menggulung rak ke posisi yang diidentifikasi dan tukang listrik Anda dapat memberi daya pada rak. Tim akan membangun konektivitas jaringan untuk rak di atas uplink yang Anda sediakan, dan akan mengkonfigurasi kapasitas rak. Instalasi selesai ketika Anda mengonfirmasi bahwa kapasitas Amazon EC2 dan Amazon EBS untuk Outpost Anda tersedia dari akun Anda AWS .

Luncurkan instance di rak Outposts Anda

Setelah Outpost Anda diinstal dan kapasitas komputasi dan penyimpanan tersedia untuk digunakan, Anda dapat memulai dengan membuat sumber daya. Luncurkan EC2 instans Amazon dan buat volume Amazon EBS di Outpost Anda menggunakan subnet Outpost. Anda juga dapat membuat snapshot volume Amazon EBS di Outpost Anda. Untuk informasi selengkapnya, lihat snapshot lokal Amazon EBS AWS Outposts di Panduan Pengguna Amazon EBS.

Prasyarat

Anda harus menginstal Outpost di situs Anda. Untuk informasi selengkapnya, lihat Membuat pesanan untuk rak Outposts.

Tugas

- Langkah 1: Buat VPC
- Langkah 2: Buat tabel rute subnet dan kustom
- Langkah 3: Konfigurasikan konektivitas gateway lokal
- Langkah 4: Konfigurasikan jaringan lokal
- Langkah 5: Luncurkan instance di Outpost
- Langkah 6: Uji konektivitas

Langkah 1: Buat VPC

Anda dapat memperluas VPC apa pun di AWS Wilayah ke Pos Luar Anda. Lewati langkah ini jika Anda sudah memiliki VPC yang dapat Anda gunakan.

Untuk membuat VPC untuk Outpost Anda

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pilih Wilayah yang sama dengan rak Outposts.
3. Pada panel navigasi, pilih Your VPCs dan kemudian pilih Create VPC.
4. Pilih VPC saja.
5. (Opsional) untuk tag Nama masukkan nama untuk VPC.
6. Untuk blok IPv4 CIDR, pilih input manual IPv4 CIDR dan masukkan rentang IPv4 alamat untuk VPC di kotak teks CIDR. IPv4

   > **Note**
   >
   > Jika Anda ingin menggunakan perutean VPC Langsung, tentukan rentang CIDR yang tidak tumpang tindih dengan rentang IP yang Anda gunakan di jaringan lokal.

7. Untuk blok IPv6 CIDR, pilih No IPv6 CIDR block.
8. Untuk Tenancy, pilih Default.
9. (Opsional) Untuk menambahkan tag ke VPC Anda, pilih Tambahkan tag, dan masukkan kunci dan nilai.
10. Pilih Buat VPC.

Langkah 2: Buat tabel rute subnet dan kustom

Anda dapat membuat dan menambahkan subnet Outpost ke VPC mana pun di AWS Wilayah tempat Pos Luar berada. Ketika Anda melakukannya, VPC menyertakan Outpost. Untuk informasi selengkapnya, lihat Komponen jaringan.

> **Note**
>
> Jika Anda meluncurkan instance di subnet Outpost yang telah dibagikan dengan Anda oleh orang lain Akun AWS, lewati ke Langkah 5: Luncurkan instance di Outpost.

2a: Buat subnet Outpost

Untuk membuat subnet Outpost

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Pada panel navigasi, pilih Outposts.
3. Pilih Outpost, lalu pilih Actions, Create subnet. Anda diarahkan untuk membuat subnet di konsol VPC Amazon. Kami memilih Outpost untuk Anda dan Availability Zone tempat Outpost berada.
4. Pilih VPC.
5. Dalam pengaturan Subnet, beri nama subnet Anda secara opsional dan tentukan rentang alamat IP untuk subnet.
6. Pilih Buat subnet.
7. (Opsional) Untuk mempermudah identifikasi subnet Outpost, aktifkan kolom Outpost ID pada halaman Subnet. Untuk mengaktifkan kolom, pilih ikon Preferensi, pilih Outpost ID, dan pilih Konfirmasi.

2b: Buat tabel rute khusus

Gunakan prosedur berikut untuk membuat tabel rute kustom dengan rute ke gateway lokal. Anda tidak dapat menggunakan tabel rute yang sama dengan subnet Availability Zone.

Untuk membuat tabel rute kustom

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel rute.
3. Pilih Buat tabel rute.
4. (Opsional) Untuk Nama, masukkan nama untuk tabel rute Anda.
5. Untuk VPC, pilih VPC Anda.
6. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
7. Pilih Buat tabel rute.

2c: Kaitkan subnet Outpost dan tabel rute khusus

Agar tabel rute mengarah ke subnet khusus, Anda harus mengaitkan tabel rute dengan subnet. Sebuah tabel rute dapat dikaitkan dengan beberapa subnet. Namun, subnet hanya dapat dikaitkan

dengan satu tabel rute pada satu waktu. Setiap subnet tidak secara eksplisit dikaitkan dengan tabel yang secara implisit dikaitkan dengan tabel rute utama secara default.

Untuk mengaitkan subnet Outpost dan tabel rute kustom

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Dari panel navigasi, pilih Tabel rute.
3. Pada tab Pengaitan subnet, pilih Sunting pengaitan subnet.
4. Pilih kotak centang untuk subnet untuk dikaitkan dengan tabel rute.
5. Pilih Simpan pengaitan.

Langkah 3: Konfigurasikan konektivitas gateway lokal

Lokal gateway (LGW) memungkinkan konektivitas antara subnet Outpost Anda dan jaringan lokal Anda.

Untuk informasi lebih lanjut tentang LGW, lihat Gerbang lokal.

Untuk menyediakan konektivitas antara instance di subnet Outposts dan jaringan lokal Anda, Anda harus menyelesaikan tugas-tugas berikut.

3a. Buat tabel rute gateway lokal kustom

Gunakan prosedur berikut untuk membuat tabel rute khusus untuk gateway lokal Anda.

Untuk membuat tabel rute gateway lokal kustom

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Pada panel navigasi, pilih Tabel rute gateway lokal.
4. Pilih Buat tabel rute gateway lokal.
5. (Opsional) Untuk Nama, masukkan nama untuk tabel rute Anda.
6. Untuk gateway lokal, pilih gateway lokal Anda.
7. Untuk Mode, pilih mode komunikasi dengan jaringan lokal Anda.
   - Pilih perutean VPC Langsung untuk menggunakan alamat IP pribadi instans Anda.
   - Pilih CoIP untuk menggunakan alamat dari kumpulan alamat IP milik pelanggan Anda. Untuk informasi selengkapnya, lihat Membuat kumpulan CoIP.

8. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
9. Pilih Buat tabel rute gateway lokal.

3b: Kaitkan VPC dengan tabel rute khusus

Gunakan prosedur berikut untuk mengaitkan VPC dengan tabel rute gateway lokal Anda. Mereka tidak terkait secara default.

Untuk mengaitkan VPC dengan tabel rute gateway lokal kustom

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Pada panel navigasi, pilih Tabel rute gateway lokal.
4. Pilih tabel rute, lalu pilih Actions, Associate VPC.
5. Untuk ID VPC, pilih VPC yang akan dikaitkan dengan tabel rute gateway lokal.
6. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
7. Pilih Kaitkan VPC.

3c: Tambahkan entri rute di tabel rute subnet Outpost

Tambahkan entri rute di tabel rute subnet Outpost untuk mengaktifkan lalu lintas antara subnet Outpost dan gateway lokal.

Subnet pos terdepan dalam VPC, yang dikaitkan dengan tabel rute gateway lokal, dapat memiliki jenis target tambahan dari ID gateway Outpost Local untuk tabel rute mereka. Pertimbangkan kasus di mana Anda ingin rute lalu lintas dengan alamat tujuan 172.16.100.0/24 ke jaringan pelanggan melalui gateway lokal. Untuk melakukan ini, edit tabel rute subnet Outpost dan tambahkan rute berikut dengan jaringan tujuan dan target gateway lokal.

Tujuan	Target
172.16.100.0/24	`lgw-id`

Untuk menambahkan entri rute dengan gateway lokal sebagai target dalam tabel rute subnet

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Tabel rute, dan pilih tabel rute yang Anda buat. 2b: Buat tabel rute khusus
3. Pilih Tindakan dan kemudian Edit rute.
4. Untuk menambahkan rute, pilih Tambah rute.
5. Untuk Tujuan masukkan blok CIDR tujuan ke jaringan pelanggan.
6. Untuk Target, pilih Outpost local gateway ID.
7. Pilih Simpan perubahan.

3d: Buat domain perutean gateway lokal dengan mengaitkan tabel rute khusus dengan grup VIF

Grup VIF adalah pengelompokan logis dari antarmuka virtual (). VIFs Kaitkan tabel rute gateway lokal dengan grup VIF untuk membuat domain perutean gateway lokal.

Untuk mengaitkan tabel rute kustom dengan grup VIF

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Pada panel navigasi, pilih Networking dan kemudian domain routing LGW.
4. Pilih Buat domain perutean LGW.
5. Masukkan nama untuk domain routing gateway lokal.
6. Pilih gateway lokal, grup VIF gateway lokal, dan tabel rute gateway lokal.
7. Pilih Buat domain perutean LGW.

3e: Tambahkan entri rute di tabel rute

Edit tabel rute gateway lokal untuk menambahkan rute statis yang memiliki Grup VIF sebagai target dan rentang CIDR subnet lokal Anda (atau 0.0.0.0/0) sebagai tujuan.

Tujuan	Target
172.16.100.0/24	`VIF-Group-ID`

Untuk menambahkan entri rute di tabel rute LGW

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Pada panel navigasi, pilih Tabel rute gateway lokal.
3. Pilih tabel rute gateway lokal, lalu pilih Tindakan, Edit rute.
4. Pilih Tambahkan rute.
5. Untuk Tujuan, masukkan blok CIDR tujuan, satu alamat IP, atau ID daftar awalan.
6. Untuk Target, pilih ID gateway lokal.
7. Pilih Simpan rute.

3f: (Opsional) Tetapkan alamat IP milik pelanggan ke instance

Jika Anda mengonfigurasi Outposts Anda 3a. Buat tabel rute gateway lokal kustom untuk menggunakan kumpulan alamat IP (CoIP) milik pelanggan, Anda harus mengalokasikan alamat IP Elastis dari kumpulan alamat CoIP dan mengaitkan alamat IP Elastis dengan instans. Untuk informasi selengkapnya, lihat Alamat IP milik pelanggan.

Jika Anda mengonfigurasi Outposts untuk menggunakan Direct VPC routing (DVR), lewati langkah ini.

Kumpulan alamat IP milik pelanggan bersama

Jika Anda ingin menggunakan kumpulan alamat IP milik pelanggan bersama, kumpulan harus dibagikan sebelum Anda memulai konfigurasi. Untuk informasi tentang cara membagikan IPv4 alamat milik pelanggan, lihat. the section called “Berbagi sumber daya Outpost”

Langkah 4: Konfigurasikan jaringan lokal

Outpost menetapkan BGP eksternal yang mengintip dari setiap Outpost Networking Device (OND) ke Perangkat Jaringan Lokal Pelanggan (CND) untuk mengirim dan menerima lalu lintas dari jaringan lokal Anda ke Outposts.

Untuk informasi selengkapnya, lihat Konektivitas BGP gateway lokal.

Untuk mengirim dan menerima lalu lintas dari jaringan lokal Anda ke Outpost, pastikan bahwa:

- Pada perangkat jaringan pelanggan Anda, sesi BGP di VLAN gateway lokal berada dalam status AKTIF dari perangkat jaringan Anda.

- Untuk lalu lintas dari lokal ke Outposts, pastikan Anda menerima iklan BGP dari Outposts di CND Anda. Iklan BGP ini berisi rute yang harus digunakan jaringan lokal Anda untuk merutekan lalu lintas dari lokal ke Outpost. Oleh karena itu, pastikan bahwa jaringan Anda memiliki routing yang tepat antara Outposts dan sumber daya on-prem.
- Untuk lalu lintas dari Outposts ke jaringan lokal, pastikan Anda CNDs mengirimkan iklan rute BGP subnet jaringan lokal ke Outposts (atau 0.0.0.0/0). Sebagai alternatif, Anda dapat mengiklankan rute default (misalnya 0.0.0.0/0) ke Outposts. Subnet lokal yang diiklankan oleh CNDs harus memiliki rentang CIDR yang sama dengan atau termasuk dalam rentang CIDR yang Anda konfigurasikan. 3e: Tambahkan entri rute di tabel rute

Contoh: Iklan BGP dalam mode VPC Langsung

Pertimbangkan skenario di mana Anda memiliki Outpost, dikonfigurasi dalam mode VPC Langsung, dengan dua perangkat jaringan rak Outposts yang dihubungkan oleh VLAN gateway lokal ke dua perangkat jaringan lokal pelanggan. Berikut ini dikonfigurasi:

- VPC dengan blok CIDR 10.0.0.0/16.
- Subnet Outpost di VPC dengan blok CIDR 10.0.3.0/24.
- Subnet di jaringan lokal dengan blok CIDR 172.16.100.0/24
- Outposts menggunakan alamat IP pribadi dari instans pada subnet Outpost, misalnya 10.0.3.0/24, untuk berkomunikasi dengan jaringan lokal Anda.

Dalam skenario ini, rute yang diiklankan oleh:

- Gateway lokal ke perangkat pelanggan Anda adalah 10.0.3.0/24.
- Perangkat pelanggan Anda ke gateway lokal Outpost adalah 172.16.100.0/24.

Akibatnya, gateway lokal akan mengirim lalu lintas keluar dengan jaringan tujuan 172.16.100.0/24 ke perangkat pelanggan Anda. Pastikan jaringan Anda memiliki konfigurasi routing yang benar untuk mengirimkan lalu lintas ke host tujuan dalam jaringan Anda.

Untuk perintah dan konfigurasi spesifik yang diperlukan untuk memeriksa status sesi BGP dan rute yang diiklankan dalam sesi tersebut, lihat dokumentasi dari vendor jaringan Anda.

Untuk pemecahan masalah, lihat daftar periksa pemecahan masalah jaringan AWS Outposts rak.

Contoh: Iklan BGP dalam mode CoIP

Pertimbangkan skenario di mana Anda memiliki Outpost dengan dua perangkat jaringan rak Outposts yang terhubung oleh VLAN gateway lokal ke dua perangkat jaringan lokal pelanggan. Berikut ini dikonfigurasi:

- VPC dengan blok CIDR 10.0.0.0/16.
- Subnet di VPC dengan blok CIDR 10.0.3.0/24.
- Kumpulan IP milik pelanggan (10.1.0.0/26).
- Asosiasi alamat IP Elastis yang mengaitkan 10.0.3.112 ke 10.1.0.2.
- Subnet di jaringan lokal dengan blok CIDR 172.16.100.0/24
- Komunikasi antara Outpost dan jaringan lokal Anda akan menggunakan CoIP Elastic IPs untuk menangani instance di Outpost, rentang CIDR VPC tidak digunakan.

Dalam skenario ini rute yang diiklankan oleh:

- Gateway lokal ke perangkat pelanggan Anda adalah 10.1.0.0/26.
- Perangkat pelanggan Anda ke gateway lokal Outpost adalah 172.16.100.0/24.

Akibatnya gateway lokal akan mengirim lalu lintas keluar dengan jaringan tujuan 172.16.100.0/24 ke perangkat pelanggan Anda. Pastikan jaringan Anda memiliki konfigurasi routing yang tepat untuk mengirimkan lalu lintas ke host tujuan dalam jaringan Anda.

Untuk perintah dan konfigurasi spesifik yang diperlukan untuk memeriksa status sesi BGP dan rute yang diiklankan dalam sesi tersebut, lihat dokumentasi dari vendor jaringan Anda.

Untuk pemecahan masalah, lihat daftar periksa pemecahan masalah jaringan AWS Outposts rak.

Untuk pemecahan masalah, lihat daftar periksa pemecahan masalah jaringan AWS Outposts rak.

Langkah 5: Luncurkan instance di Outpost

Anda dapat meluncurkan EC2 instance di subnet Outpost yang Anda buat, atau di subnet Outpost yang telah dibagikan dengan Anda. Grup keamanan mengontrol lalu lintas VPC masuk dan keluar untuk instance di subnet Outpost, seperti yang mereka lakukan untuk instance di subnet Availability Zone. Untuk menyambung ke EC2 instance di subnet Outpost, Anda dapat menentukan key pair saat meluncurkan instance, seperti yang Anda lakukan untuk instance di subnet Availability Zone.

Pertimbangan

- Jika Anda melampirkan volume data blok yang didukung oleh sistem penyimpanan blok pihak ketiga yang kompatibel selama proses peluncuran instans di Outpost, lihat posting blog ini Menyederhanakan penggunaan penyimpanan blok pihak ketiga dengan. AWS Outposts
- Anda dapat membuat grup penempatan untuk memengaruhi cara Amazon EC2 mencoba menempatkan grup instance yang saling bergantung pada perangkat keras Outposts. Anda dapat memilih strategi grup penempatan yang memenuhi kebutuhan beban kerja Anda.
- Jika Outpost Anda telah dikonfigurasi untuk menggunakan kumpulan alamat IP (CoIP) milik pelanggan, Anda harus menetapkan alamat IP milik pelanggan untuk setiap instance yang Anda luncurkan.

Untuk meluncurkan instans di subnet Outpost Anda

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Pada panel navigasi, pilih Outposts.
3. Pilih Outpost, lalu pilih Actions, View details.
4. Pada halaman ringkasan Outpost, pilih Launch instance. Anda dialihkan ke wizard peluncuran instans di EC2 konsol Amazon. Kami memilih subnet Outpost untuk Anda, dan hanya menampilkan jenis instance yang didukung oleh rak Outposts Anda.
5. Pilih jenis instans yang didukung oleh rak Outposts Anda. Perhatikan bahwa instance yang tampak berwarna abu-abu tidak tersedia.
6. (Opsional) Untuk meluncurkan instance ke grup penempatan, perluas Detail lanjutan dan gulir ke grup Penempatan. Anda dapat memilih grup penempatan yang ada atau membuat grup penempatan baru.
7. Selesaikan wizard untuk meluncurkan instance di subnet Outpost Anda. Untuk informasi selengkapnya, lihat Meluncurkan EC2 instance di Panduan EC2 Pengguna Amazon:

> **Note**
>
> Jika Anda menambahkan volume Amazon EBS, Anda harus menggunakan tipe volume gp2.

Langkah 6: Uji konektivitas

Anda dapat menguji konektivitas dengan menggunakan kasus penggunaan yang sesuai.

Uji konektivitas dari jaringan lokal Anda ke Outpost

Dari komputer di jaringan lokal Anda, jalankan `ping` perintah ke alamat IP pribadi instans Outpost.

```
ping 10.0.3.128
```

Berikut ini adalah output contoh.

```
Pinging 10.0.3.128

Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.3.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Uji konektivitas dari instans Outpost ke jaringan lokal Anda

Tergantung pada sistem operasi Anda, gunakan ssh atau rdp untuk terhubung ke alamat IP pribadi dari instance Outpost Anda. Untuk informasi tentang menghubungkan ke instance Linux, lihat Connect ke EC2 instans Anda di Panduan EC2 Pengguna Amazon.

Setelah instance berjalan, jalankan `ping` perintah ke alamat IP komputer di jaringan lokal Anda. Dalam contoh berikut, alamat IP adalah 172.16.0.130.

```
ping 172.16.0.130
```

Berikut ini adalah output contoh.

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
```

```
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Uji konektivitas antara AWS Wilayah dan Pos Terdepan

Luncurkan instance di subnet di AWS Wilayah. Misalnya, gunakan perintah run-instance.

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

Setelah instance berjalan, lakukan operasi berikut:

1. Dapatkan alamat IP pribadi dari instance di AWS Wilayah. Informasi ini tersedia di EC2 konsol Amazon di halaman detail instance.
2. Bergantung pada sistem operasi Anda, gunakan ssh atau sambungkan rdp ke alamat IP pribadi instans Outpost Anda.
3. Jalankan ping perintah dari instance Outpost Anda, tentukan alamat IP instance di Region. AWS

   ```
   ping 10.0.1.5
   ```

   Berikut ini adalah output contoh.

   ```
   Pinging 10.0.1.5

   Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128

   Ping statistics for 10.0.1.5
   Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

   Approximate round trip time in milliseconds
   ```

```
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Contoh konektivitas alamat IP milik pelanggan

Uji konektivitas dari jaringan lokal Anda ke Outpost

Dari komputer di jaringan lokal Anda, jalankan `ping` perintah ke alamat IP milik pelanggan Outpost.

```
ping 172.16.0.128
```

Berikut ini adalah output contoh.

```
Pinging 172.16.0.128

Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Uji konektivitas dari instans Outpost ke jaringan lokal Anda

Tergantung pada sistem operasi Anda, gunakan ssh atau rdp untuk terhubung ke alamat IP pribadi dari instance Outpost Anda. Untuk selengkapnya, lihat Connect ke EC2 instans Anda di Panduan EC2 Pengguna Amazon.

Setelah instance Outpost berjalan, jalankan `ping` perintah ke alamat IP komputer di jaringan lokal Anda.

```
ping 172.16.0.130
```

Berikut ini adalah output contoh.

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
```

```
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Uji konektivitas antara AWS Wilayah dan Pos Terdepan

Luncurkan instance di subnet di AWS Wilayah. Misalnya, gunakan perintah run-instance.

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

Setelah instance berjalan, lakukan operasi berikut:

1. Dapatkan alamat IP pribadi instance AWS Region, misalnya 10.0.0.5. Informasi ini tersedia di EC2 konsol Amazon di halaman detail instance.
2. Tergantung pada sistem operasi Anda, gunakan ssh atau rdp untuk terhubung ke alamat IP pribadi dari instance Outpost Anda.
3. Jalankan `ping` perintah dari instance Outpost Anda ke alamat IP instance AWS Region.

   ```
   ping 10.0.0.5
   ```

   Berikut ini adalah output contoh.

   ```
   Pinging 10.0.0.5

   Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128

   Ping statistics for 10.0.0.5
   Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

   Approximate round trip time in milliseconds
   ```

```
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Optimalkan Amazon EC2 untuk AWS Outposts

Berbeda dengan Wilayah AWS, kapasitas Amazon Elastic Compute Cloud (Amazon EC2) di Outpost terbatas. Anda dibatasi oleh total volume kapasitas komputasi yang Anda pesan. Topik ini menawarkan praktik terbaik dan strategi pengoptimalan untuk membantu Anda memaksimalkan EC2 kapasitas Amazon Anda AWS Outposts.

Daftar Isi

Host Khusus di Outposts

Host EC2 Khusus Amazon adalah server fisik dengan kapasitas EC2 instans yang sepenuhnya didedikasikan untuk penggunaan Anda. Outpost Anda sudah memberi Anda perangkat keras khusus, tetapi Host Khusus memungkinkan Anda untuk menggunakan lisensi perangkat lunak yang ada dengan pembatasan lisensi per soket, per-inti, atau per-VM terhadap satu host. Untuk informasi selengkapnya, lihat Host Khusus AWS Outposts di Panduan EC2 Pengguna Amazon.

Selain lisensi, pemilik Outpost dapat menggunakan Host Khusus untuk mengoptimalkan server dalam penyebaran Outpost mereka dengan dua cara:

- Mengubah tata letak kapasitas server
- Kontrol penempatan instance di tingkat perangkat keras

Mengubah tata letak kapasitas server

Host Khusus menawarkan kemampuan untuk mengubah tata letak server dalam penyebaran Outpost Anda tanpa menghubungi. Dukungan Ketika Anda membeli kapasitas untuk Outpost Anda, Anda menentukan tata letak EC2 kapasitas yang disediakan setiap server. Setiap server mendukung satu keluarga tipe instance. Tata letak dapat menawarkan satu jenis instans atau beberapa jenis instance. Host Khusus memungkinkan Anda mengubah apa pun yang Anda pilih untuk tata letak awal itu. Jika Anda mengalokasikan host untuk mendukung satu jenis instans untuk seluruh kapasitas, Anda

hanya dapat meluncurkan satu jenis instance dari host tersebut. Ilustrasi berikut menyajikan server m5.24xlarge dengan tata letak homogen:

Anda dapat mengalokasikan kapasitas yang sama untuk beberapa jenis instans. Ketika Anda mengalokasikan host untuk mendukung beberapa jenis instans, Anda mendapatkan tata letak heterogen yang tidak memerlukan tata letak kapasitas eksplisit. Ilustrasi berikut menyajikan server m5.24xlarge dengan tata letak heterogen pada kapasitas penuh:

Untuk informasi selengkapnya, lihat Mengalokasikan Host Khusus di Panduan EC2 Pengguna Amazon.

Kontrol penempatan instance di tingkat perangkat keras

Anda dapat menggunakan Host Khusus untuk mengontrol penempatan instans di tingkat perangkat keras. Gunakan penempatan otomatis untuk Host Khusus untuk mengelola apakah instance yang Anda luncurkan diluncurkan ke host tertentu, atau ke host yang tersedia yang memiliki konfigurasi yang cocok. Gunakan afinitas host untuk membangun hubungan antara instans dan Host Khusus. Jika Anda memiliki rak Outposts, Anda dapat menggunakan fitur Host Khusus ini untuk meminimalkan dampak kegagalan perangkat keras yang berkorelasi. Untuk informasi selengkapnya tentang pemulihan instans, lihat Penempatan otomatis Host Khusus dan afinitas host di EC2 Panduan Pengguna Amazon.

Anda dapat berbagi Host Khusus menggunakan AWS Resource Access Manager. Berbagi Host Khusus memungkinkan Anda untuk mendistribusikan host dalam penyebaran Outpost di seluruh. Akun AWS Untuk informasi selengkapnya, lihat Sumber Daya Bersama.

Mengatur pemulihan instance

Instance di Outpost Anda yang masuk ke keadaan tidak sehat karena kegagalan perangkat keras harus dimigrasikan ke host yang sehat. Anda dapat mengatur pemulihan otomatis agar migrasi ini dilakukan secara otomatis berdasarkan pemeriksaan status instans. Untuk informasi selengkapnya, lihat Ketahanan instans.

Grup penempatan di Outposts

AWS Outposts mendukung kelompok penempatan. Gunakan grup penempatan untuk memengaruhi cara Amazon EC2 mencoba menempatkan grup instance yang saling bergantung yang Anda luncurkan pada perangkat keras yang mendasarinya. Anda dapat menggunakan strategi yang

berbeda (cluster, partisi, atau spread) untuk memenuhi kebutuhan beban kerja yang berbeda. Jika Anda memiliki Outpost rak tunggal, Anda dapat menggunakan strategi penyebaran untuk menempatkan instance di seluruh host alih-alih rak.

Grup penempatan tersebar

Gunakan grup penempatan spread untuk mendistribusikan satu instance di perangkat keras yang berbeda. Peluncuran instance dalam grup penempatan spread mengurangi risiko kegagalan simultan yang mungkin terjadi ketika instance berbagi peralatan yang sama. Grup penempatan dapat menyebarkan instans di seluruh rak atau host. Anda dapat menggunakan grup penempatan spread level host hanya dengan AWS Outposts.

Grup penempatan tingkat sebaran rak

Grup penempatan level spread rak Anda dapat menampung sebanyak mungkin instance karena Anda memiliki rak di penyebaran Outpost Anda. Ilustrasi berikut menunjukkan penerapan Outpost tiga rak yang menjalankan tiga instance dalam grup penempatan level spread rak.

Grup penempatan tingkat penyebaran tuan rumah

Grup penempatan level spread host Anda dapat menampung instance sebanyak yang Anda miliki di penyebaran Outpost Anda. Ilustrasi berikut menunjukkan penyebaran Outpost rak tunggal yang menjalankan tiga instance dalam grup penempatan tingkat penyebaran host.

Grup penempatan partisi

Gunakan grup penempatan partisi untuk mendistribusikan beberapa instance di seluruh rak dengan partisi. Setiap partisi dapat menampung beberapa instance. Anda dapat menggunakan distribusi otomatis untuk menyebarkan instance di seluruh partisi atau menyebarkan instance ke partisi target. Ilustrasi berikut menunjukkan grup penempatan partisi dengan distribusi otomatis.

Anda juga dapat menyebarkan instance ke partisi target. Ilustrasi berikut menunjukkan kelompok penempatan partisi dengan distribusi yang ditargetkan.

Untuk informasi selengkapnya tentang bekerja dengan grup penempatan, lihat Grup penempatan dan Grup penempatan AWS Outposts di Panduan EC2 Pengguna Amazon.

Untuk informasi selengkapnya tentang ketersediaan AWS Outposts tinggi, lihat Pertimbangan Desain dan Arsitektur Ketersediaan AWS Outposts Tinggi.

AWS Outposts konektivitas ke AWS Wilayah

AWS Outposts mendukung konektivitas jaringan area luas (WAN) melalui koneksi tautan layanan.

Daftar Isi

Konektivitas melalui tautan layanan

Tautan layanan adalah koneksi yang diperlukan antara Outposts Anda dan AWS Wilayah (atau Wilayah asal). Hal ini memungkinkan untuk pengelolaan Outposts dan pertukaran lalu lintas ke dan dari Wilayah. AWS Tautan layanan memanfaatkan serangkaian koneksi VPN terenkripsi untuk berkomunikasi dengan Wilayah asal.

Setelah koneksi link layanan dibuat, Outpost Anda menjadi operasional dan dikelola oleh AWS. Tautan layanan memfasilitasi lalu lintas berikut:

- Lalu lintas VPC pelanggan antara Outpost dan yang terkait. VPCs
- Lalu lintas manajemen Outposts, seperti manajemen sumber daya, pemantauan sumber daya, dan pembaruan firmware dan perangkat lunak.

Persyaratan unit transmisi maksimum (MTU) tautan layanan

Maximum transmission unit (MTU) dari koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang dapat diizinkan yang dapat dilewatkan melalui koneksi. Jaringan harus mendukung 1500-byte MTU antara Outpost dan titik akhir tautan layanan di Wilayah induk. AWS

Lalu lintas yang bergerak dari instans di Outposts ke instans di Wilayah memiliki MTU sebesar 1300.

Rekomendasi bandwidth tautan layanan

Untuk pengalaman dan ketahanan yang optimal, AWS Anda harus menggunakan konektivitas redundan minimal 500 Mbps untuk setiap rak komputasi dan latensi pulang-pergi maksimum 175 ms untuk koneksi tautan layanan ke Wilayah. AWS Anda dapat menggunakan AWS Direct Connect atau koneksi internet untuk tautan layanan. Persyaratan minimum 500 Mbps dan waktu pulang pergi maksimum untuk koneksi tautan layanan memungkinkan Anda meluncurkan EC2 instans Amazon, melampirkan volume Amazon EBS, dan mengakses AWS layanan, seperti Amazon EKS, Amazon EMR, dan CloudWatch metrik dengan kinerja optimal.

Persyaratan bandwidth tautan layanan Outposts Anda bervariasi tergantung pada karakteristik berikut:

- Jumlah AWS Outposts rak dan konfigurasi kapasitas
- Karakteristik beban kerja, seperti ukuran AMI, elastisitas aplikasi, kebutuhan kecepatan burst, dan lalu lintas Amazon VPC ke Wilayah

Untuk menerima rekomendasi khusus tentang bandwidth tautan layanan yang diperlukan untuk kebutuhan Anda, hubungi perwakilan AWS penjualan atau mitra APN Anda.

Koneksi internet redundan

Saat Anda membangun konektivitas dari Pos Luar ke AWS Wilayah, kami sarankan Anda membuat beberapa koneksi untuk ketersediaan dan ketahanan yang lebih tinggi. Untuk informasi lebih lanjut, lihat Rekomendasi AWS Direct Connect Ketahanan.

Jika Anda memerlukan konektivitas ke internet publik, Anda dapat menggunakan koneksi internet yang berlebihan dan beragam penyedia internet, seperti yang Anda lakukan dengan beban kerja lokal yang ada.

Siapkan tautan layanan Anda

Langkah-langkah berikut menjelaskan proses penyiapan tautan layanan.

1. Pilih opsi koneksi antara Outposts Anda dan Wilayah asal AWS . Anda dapat memilih koneksi publik atau pribadi.
2. Setelah Anda memesan rak Outposts Anda, AWS hubungi Anda untuk mengumpulkan VLAN, IP, BGP, dan subnet infrastruktur. IPs Untuk informasi selengkapnya, lihat Konektivitas jaringan lokal.
3. Selama instalasi, AWS konfigurasikan tautan layanan di Outpost berdasarkan informasi yang Anda berikan.

4. Anda mengonfigurasi perangkat jaringan lokal Anda, seperti router, untuk terhubung ke setiap perangkat jaringan Outpost melalui konektivitas BGP. Untuk informasi tentang tautan layanan VLAN, IP, dan konektivitas BGP, lihat. Jaringan
5. Anda mengonfigurasi perangkat jaringan Anda, seperti firewall, untuk mengaktifkan Outposts Anda mengakses Wilayah atau AWS Wilayah asal. AWS Outposts memanfaatkan subnet infrastruktur tautan layanan IPs untuk mengatur koneksi VPN dan kontrol pertukaran dan lalu lintas data dengan Wilayah. Pembentukan tautan layanan selalu dimulai dari Outpost.

> **Note**
>
> Anda tidak akan dapat mengubah konfigurasi tautan layanan setelah menyelesaikan pesanan.

Opsi konektivitas publik tautan layanan

Anda dapat mengonfigurasi tautan layanan dengan koneksi publik untuk lalu lintas antara Outposts dan Home AWS Region. Anda dapat memilih untuk menggunakan internet publik atau AWS Direct Connect publik VIFs.

Jika Anda berencana hanya mengizinkan daftar AWS Wilayah publik IPs (bukan 0.0.0.0/0) di firewall Anda, Anda harus memastikan bahwa aturan firewall Anda sesuai dengan rentang alamat IP saat ini up-to-date. Untuk informasi selengkapnya, lihat rentang alamat AWS IP di Panduan Pengguna Amazon VPC.

Gambar berikut menunjukkan kedua opsi untuk membuat koneksi publik tautan layanan antara Outposts Anda dan Wilayah: AWS

Opsi 1. Konektivitas publik melalui internet

Opsi ini memerlukan subnet infrastruktur tautan AWS Outposts layanan IPs untuk memiliki akses ke rentang IP publik AWS Wilayah atau Wilayah asal Anda. Anda harus mengizinkan daftar AWS Wilayah publik IPs atau 0.0.0.0/0 pada perangkat jaringan seperti firewall Anda.

Opsi 2. Konektivitas publik melalui AWS Direct Connect publik VIFs

Opsi ini memerlukan subnet infrastruktur tautan AWS Outposts layanan IPs untuk memiliki akses ke rentang IP publik AWS Wilayah atau Wilayah asal Anda melalui layanan DX. Anda harus mengizinkan daftar AWS Wilayah publik IPs atau 0.0.0.0/0 pada perangkat jaringan seperti firewall Anda.

Opsi konektivitas pribadi tautan layanan

Anda dapat mengonfigurasi tautan layanan dengan koneksi pribadi untuk lalu lintas antara Outposts dan Home AWS Region. Anda dapat memilih untuk menggunakan AWS Direct Connect pribadi atau transit VIFs.

Pilih opsi konektivitas pribadi saat Anda membuat Outpost di AWS Outposts konsol. Untuk petunjuk, lihat Membuat Pos Terdepan.

Ketika Anda memilih opsi konektivitas pribadi, koneksi VPN tautan layanan dibuat setelah Outpost diinstal, menggunakan VPC dan subnet yang Anda tentukan. Hal ini memungkinkan konektivitas pribadi melalui VPC dan meminimalkan eksposur internet publik.

Gambar berikut menunjukkan kedua opsi untuk membuat tautan layanan koneksi pribadi VPN antara Outposts Anda dan Wilayah: AWS

Prasyarat

Prasyarat berikut diperlukan sebelum Anda dapat mengonfigurasi konektivitas pribadi untuk Outpost Anda:

- Anda harus mengonfigurasi izin untuk entitas IAM (pengguna atau peran) untuk memungkinkan pengguna atau peran membuat peran terkait layanan untuk konektivitas pribadi. Entitas IAM memerlukan izin untuk mengakses tindakan berikut:
  - `iam:CreateServiceLinkedRole` pada `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
  - `iam:PutRolePolicy` pada `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
  - `ec2:DescribeVpcs`

- `ec2:DescribeSubnets`

Untuk informasi lebih lanjut, lihat AWS Identity and Access Management untuk AWS Outposts

- Di AWS akun dan Availability Zone yang sama dengan Outpost Anda, buat VPC untuk tujuan tunggal konektivitas pribadi Outpost dengan subnet /25 atau lebih besar yang tidak bertentangan dengan 10.1.0.0/16. Misalnya, Anda mungkin menggunakan 10.3.0.0/16.
- Konfigurasikan grup keamanan subnet untuk memungkinkan lalu lintas untuk arah masuk dan keluar UDP 443.
- Iklankan CIDR subnet ke jaringan lokal Anda. Anda dapat menggunakannya AWS Direct Connect untuk melakukannya. Untuk informasi selengkapnya, lihat antarmuka AWS Direct Connect virtual dan Bekerja dengan AWS Direct Connect gateway di Panduan Pengguna.AWS Direct Connect

> **Note**
>
> Untuk memilih opsi konektivitas pribadi saat Outpost Anda dalam status PENDING, pilih Outposts dari AWS Outposts konsol dan pilih Outpost Anda. Pilih Tindakan, Tambahkan konektivitas pribadi dan ikuti langkah-langkahnya.

Setelah Anda memilih opsi konektivitas pribadi untuk Outpost Anda, AWS Outposts secara otomatis membuat peran terkait layanan di akun Anda yang memungkinkannya menyelesaikan tugas-tugas berikut atas nama Anda:

- Membuat antarmuka jaringan di subnet dan VPC yang Anda tentukan, dan membuat grup keamanan untuk antarmuka jaringan.
- Memberikan izin ke AWS Outposts layanan untuk melampirkan antarmuka jaringan ke instance titik akhir tautan layanan di akun.
- Melampirkan antarmuka jaringan ke instance titik akhir tautan layanan dari akun.

> **Important**
>
> Setelah Outpost Anda diinstal, konfirmasikan konektivitas ke pribadi IPs di subnet Anda dari Outpost Anda.

Opsi 1. Konektivitas pribadi melalui AWS Direct Connect pribadi VIFs

Buat AWS Direct Connect koneksi, antarmuka virtual pribadi, dan gateway pribadi virtual untuk memungkinkan Outpost lokal Anda mengakses VPC.

Untuk informasi selengkapnya, lihat bagian berikut di Panduan AWS Direct Connect Pengguna:

- Koneksi khusus dan host
- Buat antarmuka virtual pribadi
- Asosiasi gateway pribadi virtual

Jika AWS Direct Connect koneksi berada di AWS akun yang berbeda dari VPC Anda, lihat Mengaitkan gateway pribadi virtual di seluruh akun di Panduan Pengguna.AWS Direct Connect

Opsi 2. Konektivitas pribadi melalui AWS Direct Connect transit VIFs

Buat AWS Direct Connect koneksi, antarmuka virtual transit, dan gateway transit untuk memungkinkan Outpost lokal Anda mengakses VPC.

Untuk informasi selengkapnya, lihat bagian berikut di Panduan AWS Direct Connect Pengguna:

- Koneksi khusus dan host
- Buat antarmuka virtual transit ke gateway Direct Connect
- Asosiasi gerbang transit

Firewall dan tautan layanan

Bagian ini membahas konfigurasi firewall dan koneksi link layanan.

Dalam diagram berikut, konfigurasi memperluas VPC Amazon dari Wilayah ke AWS Pos Luar. Antarmuka virtual AWS Direct Connect publik adalah koneksi tautan layanan. Lalu lintas berikut melewati tautan layanan dan AWS Direct Connect koneksi:

- Manajemen lalu lintas ke Pos Terdepan melalui tautan layanan
- Lalu lintas antara Outpost dan yang terkait VPCs

Jika Anda menggunakan firewall stateful dengan koneksi internet Anda untuk membatasi konektivitas dari internet publik ke tautan layanan VLAN, Anda dapat memblokir semua koneksi masuk yang dimulai dari internet. Ini karena tautan layanan VPN hanya dimulai dari Pos Luar ke Wilayah, bukan dari Wilayah ke Pos Luar.

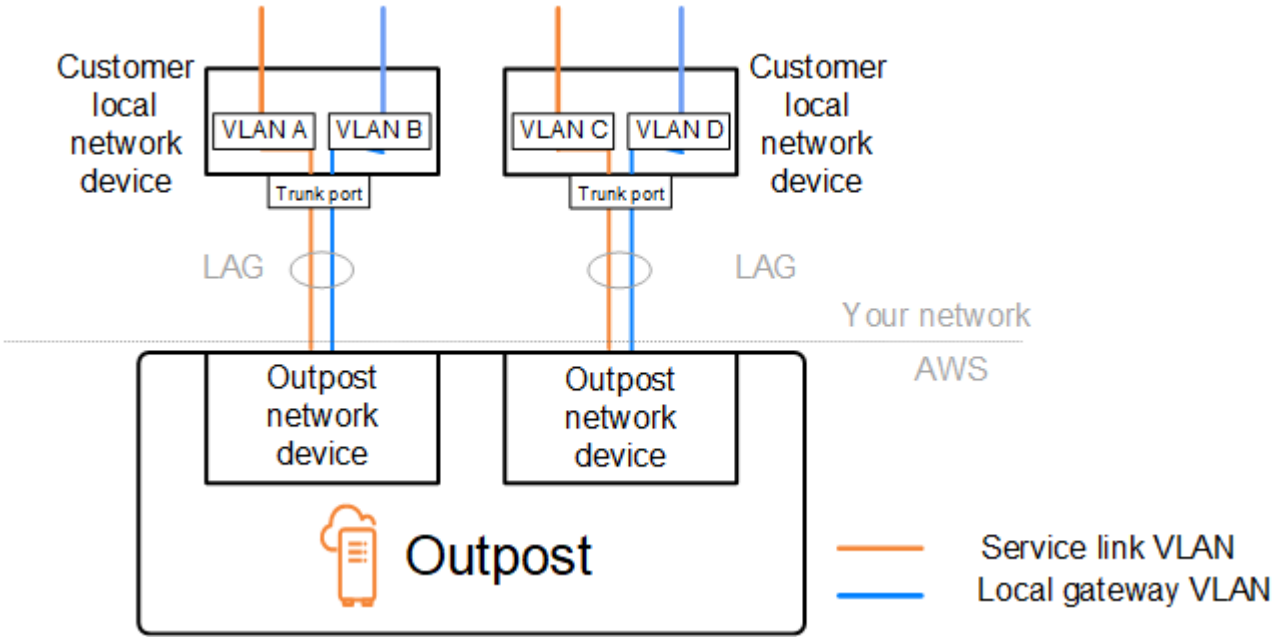
Jika Anda menggunakan firewall untuk membatasi konektivitas dari tautan layanan VLAN, Anda dapat memblokir semua koneksi masuk. Anda harus mengizinkan koneksi keluar kembali ke Pos Luar dari AWS Wilayah sesuai tabel berikut. Jika firewall stateful, koneksi keluar dari Outpost yang diizinkan, yang berarti bahwa mereka dimulai dari Outpost, harus diizinkan kembali masuk.

Protokol	Port Sumber	Alamat Sumber	Pelabuhan Tujuan	Alamat Tujuan
UDP	443	AWS Outposts tautan layanan /26	443	AWS Outposts Publik wilayah IPs
TCP	1025-65535	AWS Outposts tautan layanan /26	443	AWS Outposts Publik wilayah IPs

> **Note**
>
> Instance di Outpost tidak dapat menggunakan link layanan untuk berkomunikasi dengan instance di Outposts lain. Manfaatkan routing melalui gateway lokal atau antarmuka jaringan lokal untuk berkomunikasi antara Outposts.
> AWS Outposts Rak juga dirancang dengan daya redundan dan peralatan jaringan, termasuk komponen gateway lokal. Untuk informasi lebih lanjut, lihat Ketahanan di. AWS Outposts

Daftar periksa pemecahan masalah jaringan rak Outposts

Gunakan daftar periksa ini untuk membantu memecahkan masalah tautan layanan yang berstatus. `DOWN`



Konektivitas dengan perangkat jaringan Outpost

Periksa status peering BGP pada perangkat jaringan lokal pelanggan yang terhubung ke perangkat jaringan Outpost. Jika status peering BGP adalah`DOWN`, ikuti langkah-langkah berikut:

1. Ping alamat IP peer jarak jauh pada perangkat jaringan Outpost dari perangkat pelanggan. Anda dapat menemukan alamat IP rekan dalam konfigurasi BGP perangkat Anda. Anda juga dapat merujuk ke yang Daftar periksa kesiapan jaringan diberikan kepada Anda pada saat instalasi.
2. Jika ping tidak berhasil, periksa koneksi fisik dan pastikan status konektivitas. `UP`
   a. Konfirmasikan status LACP perangkat jaringan lokal pelanggan.
   b. Periksa status antarmuka pada perangkat. Jika statusnya`UP`, lewati ke langkah 3.
   c. Periksa perangkat jaringan lokal pelanggan dan konfirmasikan bahwa modul optik berfungsi.
   d. Ganti serat yang rusak dan pastikan lampu (Tx/Rx) berada dalam kisaran yang dapat diterima.
3. Jika ping berhasil, periksa perangkat jaringan lokal pelanggan dan pastikan bahwa konfigurasi BGP berikut sudah benar.
   a. Konfirmasikan bahwa Nomor Sistem Otonomi lokal (ASN Pelanggan) dikonfigurasi dengan benar.
   b. Konfirmasikan bahwa Nomor Sistem Otonom jarak jauh (Outpost ASN) dikonfigurasi dengan benar.
   c. Konfirmasikan bahwa IP antarmuka dan alamat IP rekan jarak jauh dikonfigurasi dengan benar.
   d. Konfirmasikan bahwa rute yang diiklankan dan diterima sudah benar.

4. Jika sesi BGP Anda mengepak antara status aktif dan terhubung, verifikasi bahwa port TCP 179 dan port fana lain yang relevan tidak diblokir pada perangkat jaringan lokal pelanggan.
5. Jika Anda perlu memecahkan masalah lebih lanjut, periksa hal berikut di perangkat jaringan lokal pelanggan:
   a. Log debug BGP dan TCP
   b. Log BGP
   c. Penangkapan paket
6. Jika masalah berlanjut, lakukan tangkapan MTR/traceroute/packet dari router yang terhubung Outpost Anda ke alamat IP peer perangkat jaringan Outpost. Bagikan hasil pengujian dengan AWS Support, menggunakan paket dukungan Enterprise Anda.

Jika status peering BGP adalah `UP` antara perangkat jaringan lokal pelanggan dan perangkat jaringan Outpost, tetapi tautan layanan masih`DOWN`, Anda dapat memecahkan masalah lebih lanjut dengan memeriksa perangkat berikut di perangkat jaringan lokal pelanggan Anda. Gunakan salah satu daftar periksa berikut, tergantung pada bagaimana konektivitas tautan layanan Anda disediakan.

- Router tepi terhubung dengan AWS Direct Connect - Antarmuka virtual publik yang digunakan untuk konektivitas tautan layanan. Untuk informasi selengkapnya, lihat AWS Direct Connect konektivitas antarmuka virtual publik ke AWS Wilayah.
- Router tepi terhubung dengan AWS Direct Connect - Antarmuka virtual pribadi digunakan untuk konektivitas tautan layanan. Untuk informasi selengkapnya, lihat AWS Direct Connect konektivitas antarmuka virtual pribadi ke AWS Wilayah.
- Router Edge terhubung dengan Penyedia Layanan Internet (ISPs) — Internet publik digunakan untuk konektivitas tautan layanan. Untuk informasi selengkapnya, lihat Konektivitas internet publik ISP ke Wilayah AWS.

AWS Direct Connect konektivitas antarmuka virtual publik ke AWS Wilayah

Gunakan daftar periksa berikut untuk memecahkan masalah router tepi yang terhubung AWS Direct Connect saat antarmuka virtual publik digunakan untuk konektivitas tautan layanan.

1. Konfirmasikan bahwa perangkat yang terhubung langsung dengan perangkat jaringan Outpost menerima rentang alamat IP tautan layanan melalui BGP.
   a. Konfirmasikan rute yang diterima melalui BGP dari perangkat Anda.

b. Periksa tabel rute tautan layanan Virtual Routing and Forwarding instance (VRF). Ini harus menunjukkan bahwa itu menggunakan rentang alamat IP.

2. Untuk memastikan konektivitas Wilayah, periksa tabel rute untuk tautan layanan VRF. Ini harus mencakup rentang alamat IP AWS Publik atau rute default.
3. Jika Anda tidak menerima rentang alamat IP AWS publik di tautan layanan VRF, periksa item berikut.

   a. Periksa status AWS Direct Connect tautan dari router tepi atau AWS Management Console.

   b. Jika tautan fisiknyaUP, periksa status peering BGP dari router tepi.

   c. Jika status peering BGP adalahDOWN, ping alamat AWS IP peer dan periksa konfigurasi BGP di router tepi. Untuk informasi selengkapnya, lihat Pemecahan masalah AWS Direct Connect di Panduan AWS Direct Connect Pengguna dan Status BGP antarmuka virtual saya tidak aktif di konsol. AWS Apa yang harus saya lakukan? .

   d. Jika BGP dibuat dan Anda tidak melihat rute default atau rentang alamat IP AWS publik di VRF, hubungi Support, menggunakan paket AWS dukungan Enterprise Anda.

4. Jika Anda memiliki firewall lokal, periksa item berikut.

   a. Konfirmasikan bahwa port yang diperlukan untuk konektivitas tautan layanan diizinkan di firewall jaringan. Gunakan traceroute pada port 443 atau alat pemecahan masalah jaringan lainnya untuk mengonfirmasi konektivitas melalui firewall dan perangkat jaringan Anda. Port berikut harus dikonfigurasi dalam kebijakan firewall untuk konektivitas tautan layanan.

      - Protokol TCP - Port sumber: TCP 1025-65535, Port tujuan: 443.
      - Protokol UDP - Port sumber: TCP 1025-65535, Port tujuan: 443.

   b. Jika firewall stateful, pastikan bahwa aturan keluar memungkinkan jangkauan alamat IP tautan layanan Outpost ke rentang alamat IP AWS publik. Untuk informasi selengkapnya, lihat AWS Outposts konektivitas ke AWS Wilayah.

   c. Jika firewall tidak stateful, pastikan untuk mengizinkan aliran masuk juga (dari rentang alamat IP AWS publik ke rentang alamat IP tautan layanan).

   d. Jika Anda telah mengkonfigurasi router virtual di firewall, pastikan bahwa routing yang sesuai dikonfigurasi untuk lalu lintas antara Outpost dan Region. AWS

5. Jika Anda telah mengonfigurasi NAT di jaringan lokal untuk menerjemahkan rentang alamat IP tautan layanan Outpost ke alamat IP publik Anda sendiri, periksa item berikut.

   a. Konfirmasikan bahwa perangkat NAT tidak kelebihan beban dan memiliki port gratis untuk dialokasikan untuk sesi baru.

b. Konfirmasikan bahwa perangkat NAT dikonfigurasi dengan benar untuk melakukan terjemahan alamat.

6. Jika masalah berlanjut, lakukan tangkapan MTR/traceroute/packet dari router edge Anda ke alamat IP peer. AWS Direct Connect Bagikan hasil pengujian dengan AWS Support, menggunakan paket dukungan Enterprise Anda.

AWS Direct Connect konektivitas antarmuka virtual pribadi ke AWS Wilayah

Gunakan daftar periksa berikut untuk memecahkan masalah router tepi yang terhubung AWS Direct Connect saat antarmuka virtual pribadi digunakan untuk konektivitas tautan layanan.

1. Jika konektivitas antara rak Outposts dan AWS Region menggunakan fitur konektivitas AWS Outposts pribadi, periksa item berikut.
   a. Ping alamat AWS IP peering jarak jauh dari router tepi dan konfirmasikan status peering BGP.
   b. Pastikan BGP mengintip antarmuka virtual AWS Direct Connect pribadi antara VPC titik akhir tautan layanan Anda dan Pos Luar yang diinstal di tempat Anda. UP Untuk informasi selengkapnya, lihat Pemecahan masalah AWS Direct Connect di Panduan AWS Direct Connect Pengguna, Status BGP antarmuka virtual saya tidak aktif di konsol. AWS Apa yang harus saya lakukan? , dan Bagaimana saya bisa memecahkan masalah koneksi BGP melalui Direct Connect? .
   c. Antarmuka virtual AWS Direct Connect pribadi adalah koneksi pribadi ke router tepi Anda di AWS Direct Connect lokasi yang Anda pilih, dan menggunakan BGP untuk bertukar rute. Rentang CIDR cloud pribadi virtual (VPC) pribadi Anda diiklankan melalui sesi BGP ini ke router tepi Anda. Demikian pula, rentang alamat IP untuk tautan layanan Outpost diiklankan ke wilayah tersebut melalui BGP dari router tepi Anda.
   d. Konfirmasikan bahwa jaringan ACLs yang terkait dengan titik akhir pribadi tautan layanan di VPC Anda memungkinkan lalu lintas yang relevan. Untuk informasi selengkapnya, lihat Daftar periksa kesiapan jaringan.
   e. Jika Anda memiliki firewall lokal, pastikan firewall memiliki aturan keluar yang memungkinkan rentang alamat IP tautan layanan dan titik akhir layanan Outpost (alamat IP antarmuka jaringan) yang terletak di VPC atau CIDR VPC. Pastikan port TCP 1025-65535 dan UDP 443 tidak diblokir. Untuk informasi selengkapnya, lihat Memperkenalkan konektivitas AWS Outposts pribadi.
   f. Jika firewall tidak stateful, pastikan firewall memiliki aturan dan kebijakan untuk mengizinkan lalu lintas masuk ke Outpost dari titik akhir layanan Outpost di VPC.

2. Jika Anda memiliki lebih dari 100 jaringan di jaringan lokal, Anda dapat mengiklankan rute default melalui sesi BGP ke AWS antarmuka virtual pribadi Anda. Jika Anda tidak ingin mengiklankan rute default, rangkum rute sehingga jumlah rute yang diiklankan kurang dari 100.
3. Jika masalah berlanjut, lakukan tangkapan MTR/traceroute/packet dari router edge Anda ke alamat IP peer. AWS Direct Connect Bagikan hasil pengujian dengan AWS Support, menggunakan paket dukungan Enterprise Anda.

Konektivitas internet publik ISP ke Wilayah AWS

Gunakan daftar periksa berikut untuk memecahkan masalah router tepi yang terhubung melalui ISP saat menggunakan internet publik untuk konektivitas tautan layanan.

- Konfirmasikan bahwa tautan internet sudah aktif.
- Konfirmasikan bahwa server publik dapat diakses dari perangkat edge Anda yang terhubung melalui ISP.

Jika internet atau server publik tidak dapat diakses melalui tautan ISP, selesaikan langkah-langkah berikut.

1. Periksa apakah status peering BGP dengan router ISP ditetapkan.
   a. Konfirmasikan bahwa BGP tidak mengepak.
   b. Konfirmasikan bahwa BGP menerima dan mengiklankan rute yang diperlukan dari ISP.
2. Dalam hal konfigurasi rute statis, periksa apakah rute default dikonfigurasi dengan benar pada perangkat edge.
3. Konfirmasikan apakah Anda dapat menjangkau internet menggunakan koneksi ISP lain.
4. Jika masalah berlanjut, lakukan tangkapan MTR/traceroute/packet di router tepi Anda. Bagikan hasilnya dengan tim dukungan teknis ISP Anda untuk pemecahan masalah lebih lanjut.

Jika internet dan server publik dapat diakses melalui tautan ISP, selesaikan langkah-langkah berikut.

1. Konfirmasikan apakah EC2 instans atau penyeimbang beban Anda yang dapat diakses publik di Wilayah Outpost home dapat diakses dari perangkat edge Anda. Anda dapat menggunakan ping atau telnet untuk mengonfirmasi konektivitas, dan kemudian menggunakan traceroute untuk mengonfirmasi jalur jaringan.

2. Jika Anda menggunakan VRFs untuk memisahkan lalu lintas di jaringan Anda, konfirmasikan bahwa tautan layanan VRF memiliki rute atau kebijakan yang mengarahkan lalu lintas ke dan dari ISP (internet) dan VRF. Lihat pos pemeriksaan berikut.
   a. Router tepi terhubung dengan ISP. Periksa tabel rute ISP VRF router edge untuk mengonfirmasi bahwa rentang alamat IP tautan layanan ada.
   b. Perangkat jaringan lokal pelanggan yang terhubung dengan Outpost. Periksa konfigurasi VRFs dan pastikan bahwa perutean dan kebijakan yang diperlukan untuk konektivitas antara tautan layanan VRF dan ISP VRF dikonfigurasi dengan benar. Biasanya, rute default dikirim dari ISP VRF ke tautan layanan VRF untuk lalu lintas ke internet.
   c. Jika Anda mengonfigurasi perutean berbasis sumber di router yang terhubung ke Outpost Anda, konfirmasikan bahwa konfigurasi sudah benar.
3. Pastikan firewall lokal dikonfigurasi untuk memungkinkan konektivitas keluar (port TCP 1025-65535 dan UDP 443) dari rentang alamat IP tautan layanan Outpost ke rentang alamat IP publik. AWS Jika firewall tidak stateful, pastikan konektivitas masuk ke Outpost juga dikonfigurasi.
4. Pastikan NAT dikonfigurasi di jaringan lokal untuk menerjemahkan rentang alamat IP tautan layanan Outpost ke alamat IP publik. Selain itu, konfirmasikan item berikut.
   a. Perangkat NAT tidak kelebihan beban dan memiliki port gratis untuk dialokasikan untuk sesi baru.
   b. Perangkat NAT dikonfigurasi dengan benar untuk melakukan terjemahan alamat.

Jika masalah berlanjut, lakukan tangkapan MTR/traceroute/packet.

- Jika hasilnya menunjukkan bahwa paket dijatuhkan atau diblokir di jaringan lokal, tanyakan kepada jaringan atau tim teknis Anda untuk panduan tambahan.
- Jika hasilnya menunjukkan bahwa paket jatuh atau diblokir di jaringan ISP, hubungi tim dukungan teknis ISP.
- Jika hasilnya tidak menunjukkan masalah, kumpulkan hasil dari semua pengujian (seperti MTR, telnet, traceroute, packet captures, dan log BGP) dan hubungi Support menggunakan paket dukungan Enterprise Anda. AWS

Outposts berada di belakang dua perangkat firewall

Jika Anda telah menempatkan Outpost Anda di belakang sepasang firewall yang disinkronkan dengan ketersediaan tinggi atau dua firewall yang berdiri sendiri, perutean asimetris dari tautan

layanan mungkin terjadi. Ini berarti bahwa lalu lintas masuk dapat melewati firewall-1, sementara lalu lintas keluar melewati firewall-2. Gunakan daftar periksa berikut untuk mengidentifikasi potensi perutean asimetris dari tautan layanan terutama jika itu berfungsi dengan benar sebelumnya.

- Verifikasi apakah ada perubahan terbaru atau pemeliharaan berkelanjutan dalam pengaturan perutean jaringan perusahaan Anda yang mungkin menyebabkan perutean tautan layanan asimetris melalui firewall.
  - Gunakan grafik lalu lintas firewall untuk memeriksa perubahan pola lalu lintas yang sejalan dengan dimulainya masalah tautan layanan.
  - Periksa kegagalan firewall sebagian atau skenario pasangan firewall berotak terpisah yang mungkin menyebabkan firewall Anda tidak lagi menyinkronkan tabel koneksi mereka satu sama lain.
  - Periksa tautan ke bawah atau perubahan terbaru pada perutean (perubahan OSPF/ISIS/EIGRP metrik, perubahan peta rute BGP) di jaringan perusahaan Anda yang sejalan dengan dimulainya masalah tautan layanan.
- Jika Anda menggunakan konektivitas Internet publik untuk tautan layanan ke wilayah asal, pemeliharaan penyedia layanan dapat memunculkan perutean asimetris dari tautan layanan melalui firewall.
  - Periksa grafik lalu lintas untuk tautan ke ISP Anda untuk perubahan pola lalu lintas yang sejalan dengan dimulainya masalah tautan layanan.
- Jika Anda menggunakan AWS Direct Connect konektivitas untuk tautan layanan, ada kemungkinan pemeliharaan yang AWS direncanakan memicu perutean tautan layanan asimetris.
  - Periksa pemberitahuan pemeliharaan yang direncanakan pada AWS Direct Connect layanan Anda.
  - Perhatikan bahwa jika Anda memiliki AWS Direct Connect layanan redundan, Anda dapat secara proaktif menguji perutean tautan layanan Outposts melalui setiap jalur jaringan yang mungkin dalam kondisi pemeliharaan. Ini memungkinkan Anda untuk menguji apakah gangguan pada salah satu AWS Direct Connect layanan Anda dapat menyebabkan perutean tautan layanan asimetris. Ketahanan AWS Direct Connect bagian konektivitas end-to-end jaringan dapat diuji oleh Resiliency with AWS Direct Connect Resiliency Toolkit. Untuk informasi selengkapnya, lihat Menguji AWS Direct Connect Ketahanan dengan Toolkit Ketahanan - Pengujian Failover.

Setelah Anda melalui daftar periksa sebelumnya dan menunjuk perutean asimetris tautan layanan sebagai penyebab utama yang mungkin, ada sejumlah tindakan lebih lanjut yang dapat Anda ambil:

- Kembalikan perutean simetris dengan mengembalikan perubahan jaringan perusahaan atau menunggu pemeliharaan yang direncanakan penyedia selesai.
- Masuk ke salah satu atau kedua firewall dan hapus semua informasi status aliran untuk semua aliran dari baris perintah (jika didukung oleh vendor firewall).
- Saring sementara pengumuman BGP melalui salah satu firewall atau tutup antarmuka pada satu firewall untuk memaksa perutean simetris melalui firewall lainnya.
- Reboot setiap firewall pada gilirannya untuk menghilangkan potensi korupsi dalam pelacakan status aliran lalu lintas tautan layanan di memori firewall.
- Libatkan vendor firewall Anda untuk memverifikasi atau melonggarkan pelacakan status aliran UDP untuk koneksi UDP yang bersumber pada port 443 dan ditujukan untuk port 443.

Gerbang lokal untuk rak Outposts Anda

Gerbang lokal adalah komponen inti dari arsitektur untuk rak Outposts Anda. Gateway lokal memungkinkan konektivitas antara subnet Outpost Anda dan jaringan lokal Anda. Jika infrastruktur on-premise menyediakan akses internet, beban kerja yang berjalan di rak Outposts juga dapat memanfaatkan gateway lokal untuk berkomunikasi dengan layanan regional atau beban kerja regional. Konektivitas ini dapat dicapai baik dengan menggunakan koneksi publik (internet) atau menggunakan AWS Direct Connect. Untuk informasi selengkapnya, lihat AWS Outposts konektivitas ke AWS Wilayah.

Daftar Isi

Dasar-dasar gateway lokal

AWS membuat gateway lokal untuk setiap rak Outposts sebagai bagian dari proses instalasi. Rak Outposts mendukung satu gateway lokal. Gerbang lokal dimiliki oleh yang Akun AWS terkait dengan rak Outposts.

> **Note**
>
> Untuk memahami batasan bandwidth instance untuk lalu lintas yang melalui gateway lokal, lihat Bandwidth jaringan EC2 instans Amazon di Panduan EC2 Pengguna Amazon.

Sebuah gateway lokal memiliki komponen-komponen berikut:

- Tabel rute - Hanya pemilik gateway lokal yang dapat membuat tabel rute gateway lokal. Untuk informasi selengkapnya, lihat the section called “Tabel rute”.

- Kumpulan CoIP — (Opsional) Anda dapat menggunakan rentang alamat IP yang Anda miliki untuk memfasilitasi komunikasi antara jaringan lokal dan instance di VPC Anda. Untuk informasi selengkapnya, lihat the section called “Alamat IP milik pelanggan”.
- Virtual interface (VIFs) — Local gateway VIFs (Virtual Interface) adalah komponen antarmuka logis dari rak Outposts yang mengatur konektivitas VLAN, IP, dan BGP antara perangkat jaringan Outposts dan perangkat jaringan on-premise untuk konektivitas gateway lokal. AWS membuat satu VIF untuk setiap LAG dan menambahkan keduanya VIFs ke grup VIF. Tabel rute gateway lokal harus memiliki rute default ke keduanya VIFs untuk konektivitas jaringan lokal. Untuk informasi selengkapnya, lihat Konektivitas jaringan lokal.
- Grup VIF — AWS menambahkan yang VIFs dibuat ke grup VIF. Kelompok VIF adalah pengelompokan logis dari. VIFs
- Tabel rute gateway lokal dan asosiasi VPC — Tabel rute gateway lokal dan asosiasi VPC memungkinkan Anda untuk menghubungkan ke tabel rute gateway lokal. VPCs Dengan asosiasi ini, Anda dapat menambahkan rute yang ditargetkan ke gateway lokal dalam tabel rute subnet Outposts Anda. Hal ini memungkinkan komunikasi antara sumber daya subnet Outposts Anda dan jaringan lokal Anda melalui gateway lokal.
- Domain routing gateway lokal — Domain routing gateway lokal adalah asosiasi tabel rute gateway lokal dan grup VIF gateway lokal. Dengan asosiasi ini, Anda dapat menambahkan rute yang ditargetkan ke grup VIF gateway lokal dalam tabel rute gateway lokal Anda. Ini memungkinkan komunikasi antara sumber daya subnet Outposts Anda dan jaringan lokal Anda melalui grup VIF yang dipilih.

Saat AWS menyediakan rak Outposts Anda, kami membuat beberapa komponen dan Anda bertanggung jawab untuk membuat yang lain.

AWS tanggung jawab

- Memberikan perangkat keras.
- Membuat gateway lokal.
- Membuat antarmuka virtual (VIFs) dan grup VIF.

Tanggung jawab Anda

- Buat tabel rute gateway lokal.
- Kaitkan VPC dengan tabel rute gateway lokal.

- Kaitkan grup VIF dengan tabel rute gateway lokal untuk membuat domain perutean gateway lokal.

Perutean gateway lokal

Instans di subnet Outpost Anda dapat menggunakan salah satu opsi berikut untuk komunikasi dengan jaringan lokal Anda melalui gateway lokal:

- Alamat IP pribadi — Gateway lokal menggunakan alamat IP pribadi dari instans di subnet Outpost Anda untuk memfasilitasi komunikasi dengan jaringan lokal Anda. Ini adalah opsi default.
- Alamat IP milik pelanggan — Gateway lokal melakukan terjemahan alamat jaringan (NAT) untuk alamat IP milik pelanggan yang Anda tetapkan ke instance di subnet Outpost. Opsi ini mendukung rentang CIDR yang tumpang tindih dan topologi jaringan lainnya.

Untuk informasi selengkapnya, lihat the section called “Tabel rute”.

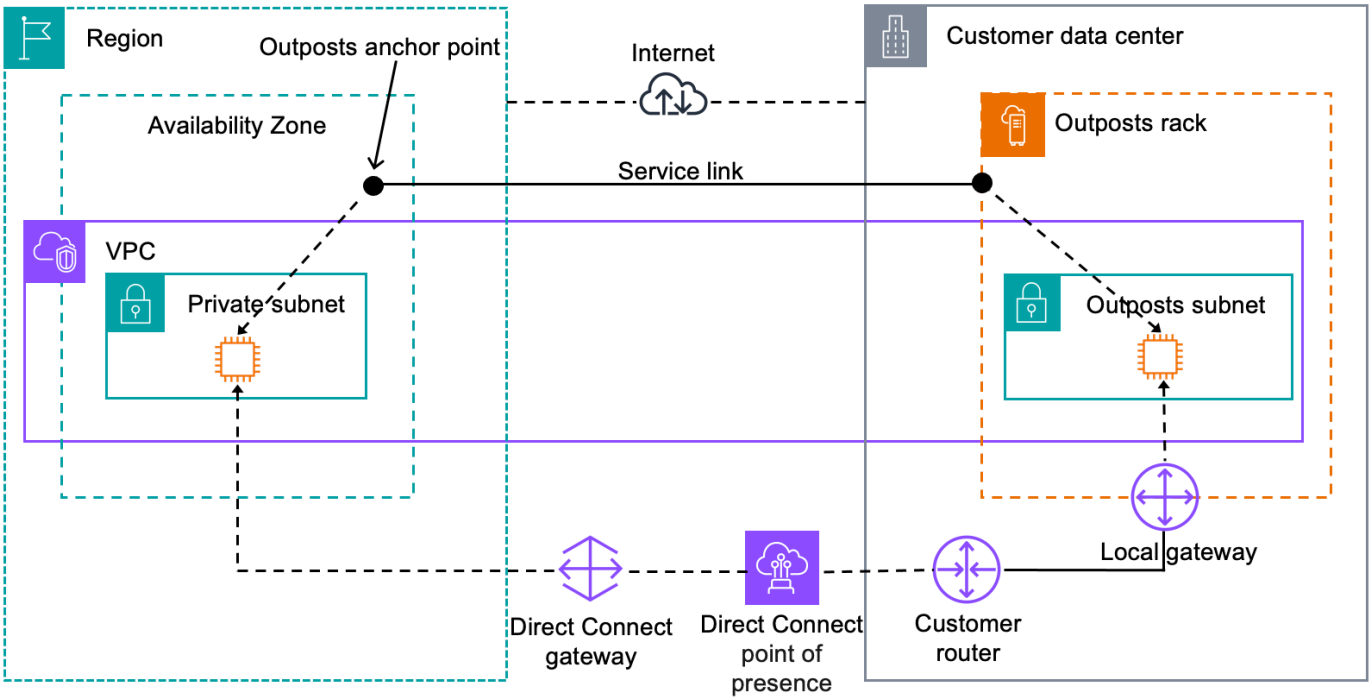
Konektivitas melalui gateway lokal

Peran utama gateway lokal adalah menyediakan konektivitas dari Outpost ke jaringan lokal lokal Anda. Ini juga menyediakan konektivitas ke internet melalui jaringan lokal Anda. Sebagai contoh, lihat the section called “Perutean VPC langsung” dan the section called “Alamat IP milik pelanggan”.

Gateway lokal juga dapat menyediakan jalur pesawat data kembali ke AWS Wilayah. Jalur pesawat data untuk gateway lokal melintasi dari Outpost, melalui gateway lokal, dan ke segmen LAN gateway lokal pribadi Anda. Itu kemudian akan mengikuti jalur pribadi kembali ke titik akhir AWS layanan di Wilayah. Perhatikan bahwa jalur bidang kontrol selalu menggunakan konektivitas tautan layanan, terlepas dari jalur bidang data yang Anda gunakan.

Anda dapat menghubungkan infrastruktur Outposts lokal Anda Layanan AWS ke Wilayah secara pribadi. AWS Direct Connect Untuk informasi selengkapnya, lihat konektivitas AWS Outposts pribadi.

Gambar berikut menunjukkan konektivitas melalui gateway lokal:



Tabel rute gateway lokal

Sebagai bagian dari instalasi rak, AWS membuat gateway lokal, mengkonfigurasi VIFs dan grup VIF. Gateway lokal dimiliki oleh AWS akun yang terkait dengan Outpost. Anda membuat tabel rute gateway lokal. Tabel rute gateway lokal harus memiliki asosiasi ke grup VIF dan VPC. Anda membuat dan mengelola asosiasi grup VIF dan VPC. Hanya pemilik gateway lokal yang dapat memodifikasi tabel rute gateway lokal.

Tabel rute subnet pos terdepan dapat menyertakan rute ke grup VIF gateway lokal untuk menyediakan konektivitas ke jaringan lokal Anda.

Tabel rute gateway lokal memiliki mode yang menentukan cara instance di subnet Outposts berkomunikasi dengan jaringan lokal Anda. Opsi default adalah perutean VPC langsung, yang menggunakan alamat IP pribadi dari instance. Pilihan lainnya adalah menggunakan alamat dari kumpulan alamat IP milik pelanggan (CoIP) yang Anda berikan. Direct VPC routing dan CoIP adalah opsi yang saling eksklusif yang mengontrol cara kerja routing. Untuk menentukan opsi terbaik untuk Outpost Anda, lihat Cara memilih antara mode perutean CoIP dan Direct VPC di rak Outposts. AWS

Anda dapat membagikan tabel rute gateway lokal dengan AWS akun lain atau unit organisasi menggunakan AWS Resource Access Manager. Untuk informasi selengkapnya, lihat Bekerja dengan AWS Outposts sumber daya bersama.

Daftar Isi

Perutean VPC langsung

Perutean VPC langsung menggunakan alamat IP pribadi instans di VPC Anda untuk memfasilitasi komunikasi dengan jaringan lokal Anda. Alamat ini diiklankan ke jaringan lokal Anda dengan BGP. Iklan ke BGP hanya untuk alamat IP pribadi yang termasuk dalam subnet di rak Outposts Anda. Jenis routing ini adalah mode default untuk Outposts. Dalam mode ini, gateway lokal tidak melakukan NAT untuk instance, dan Anda tidak perlu menetapkan alamat IP Elastis ke instance Anda. EC2 Anda memiliki opsi untuk menggunakan ruang alamat Anda sendiri alih-alih mode perutean VPC langsung. Untuk informasi selengkapnya, lihat Alamat IP milik pelanggan.

Mode perutean VPC langsung tidak mendukung rentang CIDR yang tumpang tindih.

Perutean VPC langsung hanya didukung untuk antarmuka jaringan misalnya. Dengan antarmuka jaringan yang AWS dibuat atas nama Anda (dikenal sebagai antarmuka jaringan yang dikelola pemohon), alamat IP pribadinya tidak dapat dijangkau dari jaringan lokal Anda. Misalnya, titik akhir VPC tidak dapat dijangkau secara langsung dari jaringan lokal Anda.

Contoh berikut menggambarkan routing VPC langsung.

Contoh

Contoh: Konektivitas internet melalui VPC

Contoh di subnet Outpost dapat mengakses internet melalui gateway internet yang terpasang ke VPC.

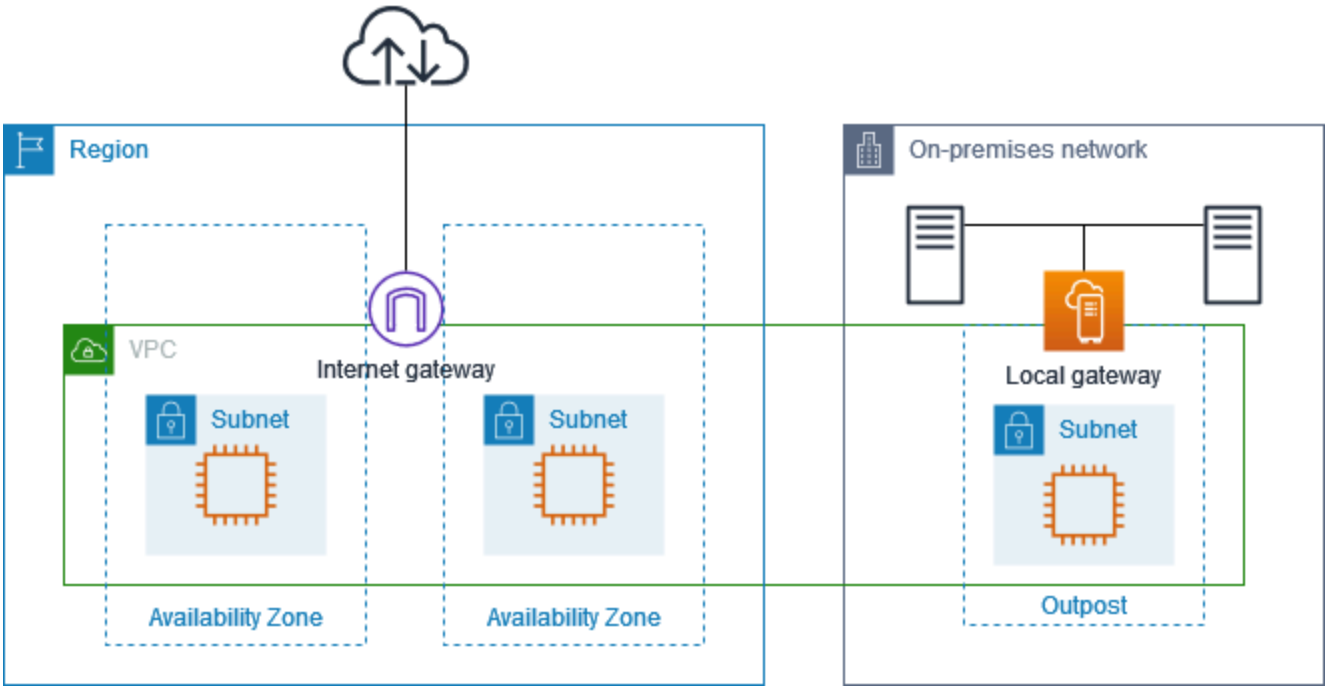
Pertimbangkan konfigurasi berikut:

- VPC induk mencakup dua Availability Zone dan memiliki subnet di setiap Availability Zone.
- Outpost memiliki satu subnet.

- Setiap subnet memiliki EC2 instance.
- Gateway lokal menggunakan iklan BGP untuk mengiklankan alamat IP pribadi subnet Outpost ke jaringan lokal.

> **Note**
>
> Iklan BGP hanya didukung untuk subnet di Outpost yang memiliki rute dengan gateway lokal sebagai tujuan. Subnet lainnya tidak diiklankan melalui BGP.

Dalam diagram berikut, lalu lintas dari instance di subnet Outpost dapat menggunakan gateway internet untuk VPC untuk mengakses internet.



Untuk mencapai konektivitas internet melalui Wilayah induk, tabel rute untuk subnet Outpost harus memiliki rute berikut.

Tujuan	Target	Komentar
VPC CIDR	Lokal:	Menyediakan konektivitas antara subnet di VPC.

Tujuan	Target	Komentar
0.0.0.0	*internet-gateway-id*	Mengirim lalu lintas yang ditujukan untuk internet ke gateway internet.
on-premises network CIDR	*local-gateway-id*	Mengirim lalu lintas yang ditujukan untuk jaringan lokal ke gateway lokal.

Contoh: Konektivitas internet melalui jaringan lokal

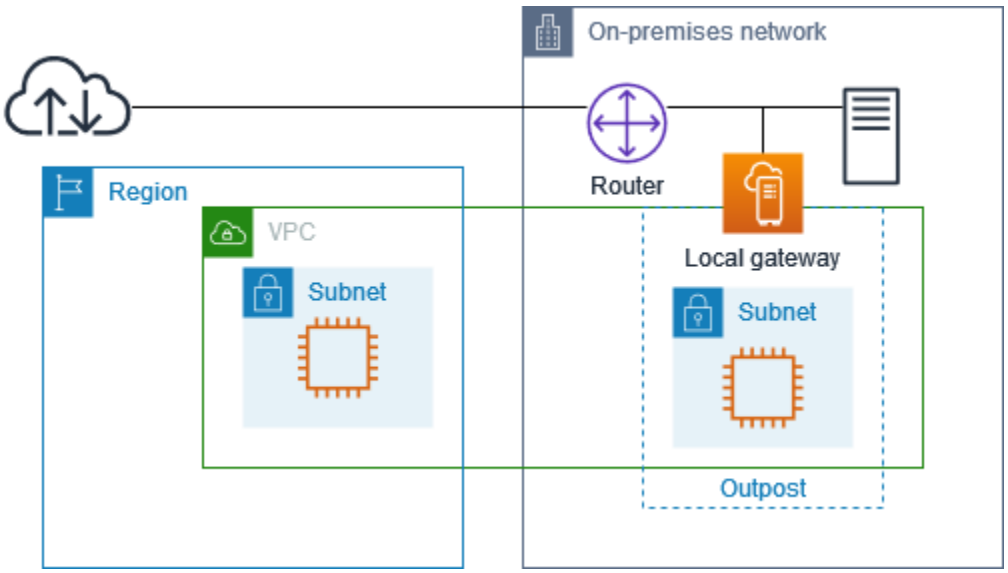
Instans di subnet Outpost dapat mengakses internet melalui jaringan lokal. Contoh di subnet Outpost tidak memerlukan alamat IP publik atau alamat IP Elastis.

Pertimbangkan konfigurasi berikut:

- Subnet Outpost memiliki instance EC2 .
- Router di jaringan lokal melakukan terjemahan alamat jaringan (NAT).
- Gateway lokal menggunakan iklan BGP untuk mengiklankan alamat IP pribadi subnet Outpost ke jaringan lokal.

> **Note**
>
> Iklan BGP hanya didukung untuk subnet di Outpost yang memiliki rute dengan gateway lokal sebagai tujuan. Subnet lainnya tidak diiklankan melalui BGP.

Dalam diagram berikut, lalu lintas dari instance di subnet Outpost dapat menggunakan gateway lokal untuk mengakses internet atau jaringan lokal. Lalu lintas dari jaringan lokal menggunakan gateway lokal untuk mengakses instans di subnet Outpost.



Untuk mencapai konektivitas internet melalui jaringan lokal, tabel rute untuk subnet Outpost harus memiliki rute berikut.

Tujuan	Target	Komentar
VPC CIDR	Lokal:	Menyediakan konektivitas antara subnet di VPC.
0.0.0.0/0	*local-gateway-id*	Mengirim lalu lintas yang ditujukan untuk internet ke gateway lokal.

Akses keluar ke internet

Lalu lintas yang dimulai dari instance di subnet Outpost dengan tujuan internet menggunakan rute untuk 0.0.0.0/0 untuk merutekan lalu lintas ke gateway lokal. Gateway lokal mengirimkan lalu lintas ke router. Router menggunakan NAT untuk menerjemahkan alamat IP pribadi ke alamat IP publik pada router, dan kemudian mengirimkan lalu lintas ke tujuan.

Akses keluar ke jaringan lokal

Lalu lintas yang dimulai dari instance di subnet Outpost dengan tujuan jaringan lokal menggunakan rute untuk 0.0.0.0/0 untuk merutekan lalu lintas ke gateway lokal. Gateway lokal mengirimkan lalu lintas ke tujuan di jaringan lokal.

Akses masuk dari jaringan lokal

Lalu lintas dari jaringan lokal dengan tujuan instans di subnet Outpost menggunakan alamat IP pribadi instans. Ketika lalu lintas mencapai gateway lokal, gateway lokal mengirimkan lalu lintas ke tujuan di VPC.

Alamat IP milik pelanggan

Secara default, gateway lokal menggunakan alamat IP pribadi instance di VPC Anda untuk memfasilitasi komunikasi dengan jaringan lokal Anda. Namun, Anda dapat memberikan rentang alamat, yang dikenal sebagai kumpulan alamat IP milik pelanggan (CoIP), yang mendukung rentang CIDR yang tumpang tindih dan topologi jaringan lainnya.

Jika Anda memilih CoIP, Anda harus membuat kumpulan alamat, menetapkannya ke tabel rute gateway lokal, dan mengiklankan alamat ini kembali ke jaringan pelanggan Anda melalui BGP. Alamat IP milik pelanggan yang terkait dengan tabel rute gateway lokal Anda ditampilkan dalam tabel rute sebagai rute yang disebarkan.

Alamat IP milik pelanggan menyediakan konektivitas lokal atau eksternal ke sumber daya di jaringan lokal Anda. Anda dapat menetapkan alamat IP ini ke sumber daya di Outpost Anda, seperti EC2 instance, dengan mengalokasikan alamat IP Elastis baru dari kumpulan IP milik pelanggan, dan kemudian menetapkannya ke sumber daya Anda. Untuk informasi selengkapnya, lihat Kolam CoIP.

> **Note**
>
> Untuk kumpulan alamat IP milik pelanggan, Anda harus dapat merutekan alamat di jaringan Anda.

Ketika Anda mengalokasikan alamat IP Elastis dari kumpulan alamat IP milik pelanggan Anda, Anda terus memiliki alamat IP di kumpulan alamat IP milik pelanggan Anda. Anda bertanggung jawab untuk mengiklankannya sesuai kebutuhan di jaringan internal atau WAN Anda.

Anda dapat secara opsional membagikan kumpulan milik pelanggan Anda dengan beberapa Akun AWS di organisasi Anda menggunakan. AWS Resource Access Manager Setelah Anda berbagi pool, peserta dapat mengalokasikan alamat IP Elastis dari kumpulan alamat IP milik pelanggan, dan kemudian menetapkannya ke EC2 instance di Outpost. Untuk informasi selengkapnya, lihat Sumber Daya Bersama.

Contoh

- Contoh: Konektivitas internet melalui VPC

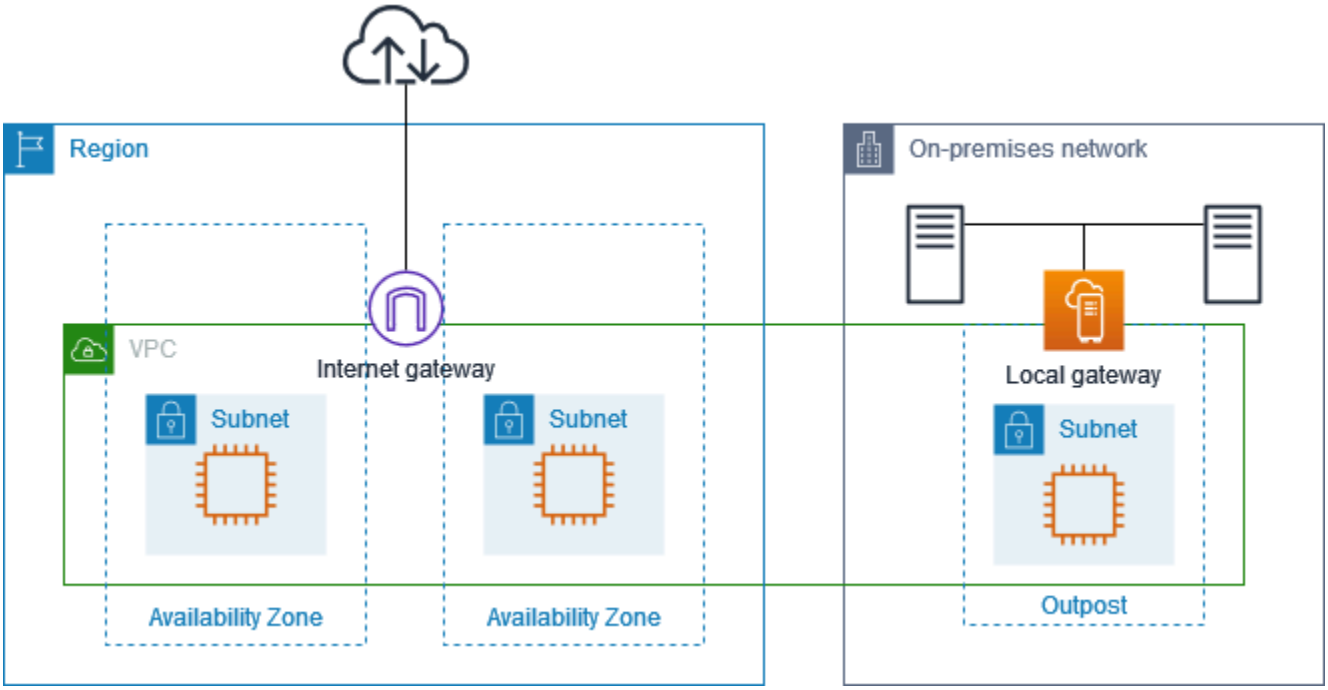
- Contoh: Konektivitas internet melalui jaringan lokal

Contoh: Konektivitas internet melalui VPC

Contoh di subnet Outpost dapat mengakses internet melalui gateway internet yang terpasang ke VPC.

Pertimbangkan konfigurasi berikut:

- VPC induk mencakup dua Availability Zone dan memiliki subnet di setiap Availability Zone.
- Outpost memiliki satu subnet.
- Setiap subnet memiliki EC2 instance.
- Ada kumpulan alamat IP milik pelanggan.
- Instance di subnet Outpost memiliki alamat IP Elastis dari kumpulan alamat IP milik pelanggan.
- Gateway lokal menggunakan iklan BGP untuk mengiklankan kumpulan alamat IP milik pelanggan ke jaringan lokal.



Untuk mencapai konektivitas internet melalui Wilayah, tabel rute untuk subnet Outpost harus memiliki rute berikut.

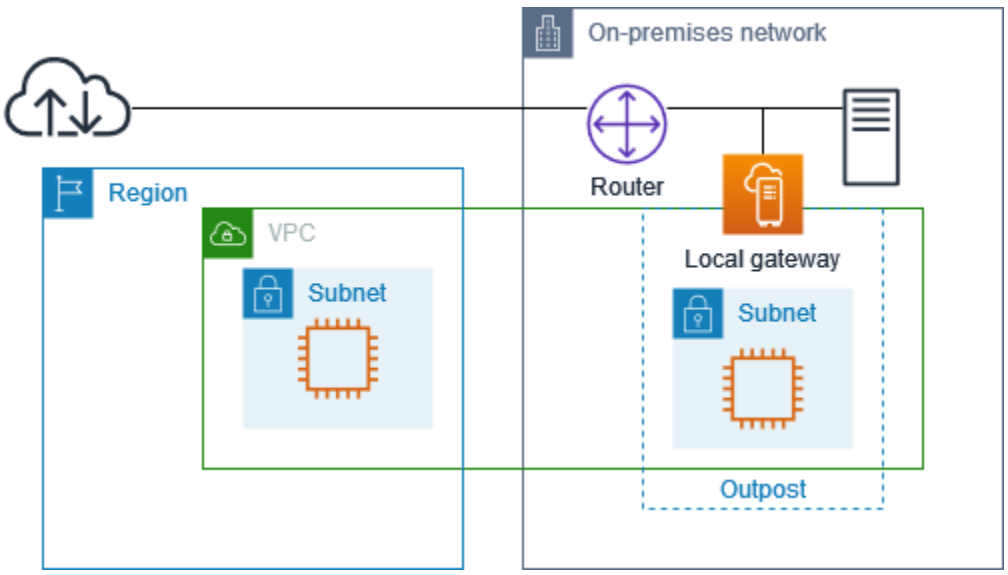
Tujuan	Target	Komentar
VPC CIDR	Lokal:	Menyediakan konektivitas antara subnet di VPC.
0.0.0.0	*internet-gateway-id*	Mengirim lalu lintas yang ditujukan untuk internet publik ke gateway internet.
On-premises network CIDR	*local-gateway-id*	Mengirim lalu lintas yang ditujukan untuk jaringan lokal ke gateway lokal.

Contoh: Konektivitas internet melalui jaringan lokal

Instans di subnet Outpost dapat mengakses internet melalui jaringan lokal.

Pertimbangkan konfigurasi berikut:

- Subnet Outpost memiliki instance EC2 .
- Ada kumpulan alamat IP milik pelanggan.
- Gateway lokal menggunakan iklan BGP untuk mengiklankan kumpulan alamat IP milik pelanggan ke jaringan lokal.
- Asosiasi alamat IP Elastis yang memetakan 10.0.3.112 ke 10.1.0.2.
- Router di jaringan lokal pelanggan melakukan NAT.



Untuk mencapai konektivitas internet melalui gateway lokal, tabel rute untuk subnet Outpost harus memiliki rute berikut.

Tujuan	Target	Komentar
VPC CIDR	Lokal:	Menyediakan konektivitas antara subnet di VPC.
0.0.0.0/0	*local-gateway-id*	Mengirim lalu lintas yang ditujukan untuk internet ke gateway lokal.

Akses keluar ke internet

Lalu lintas yang dimulai dari EC2 instance di subnet Outpost dengan tujuan internet menggunakan rute untuk 0.0.0.0/0 untuk merutekan lalu lintas ke gateway lokal. Gateway lokal memetakan alamat IP pribadi instance ke alamat IP milik pelanggan, dan kemudian mengirimkan lalu lintas ke router. Router menggunakan NAT untuk menerjemahkan alamat IP milik pelanggan ke alamat IP publik di router, dan kemudian mengirimkan lalu lintas ke tujuan.

Akses keluar ke jaringan lokal

Lalu lintas yang dimulai dari EC2 instance di subnet Outpost dengan tujuan jaringan lokal menggunakan rute untuk 0.0.0.0/0 untuk merutekan lalu lintas ke gateway lokal. Gateway lokal menerjemahkan alamat IP EC2 instance ke alamat IP milik pelanggan (alamat IP elastis), dan kemudian mengirimkan lalu lintas ke tujuan.

Akses masuk dari jaringan lokal

Lalu lintas dari jaringan lokal dengan tujuan instans di subnet Outpost menggunakan alamat IP milik pelanggan (alamat IP Elastis) instans. Ketika lalu lintas mencapai gateway lokal, gateway lokal memetakan alamat IP milik pelanggan (alamat IP elastis) ke alamat IP instance, dan kemudian mengirimkan lalu lintas ke tujuan di VPC. Selain itu, tabel rute gateway lokal mengevaluasi setiap rute yang menargetkan antarmuka jaringan elastis. Jika alamat tujuan cocok dengan CIDR tujuan rute statis, lalu lintas dikirim ke elastic network interface tersebut. Ketika lalu lintas mengikuti rute statis ke elastic network interface, alamat tujuan dipertahankan dan tidak diterjemahkan ke alamat IP pribadi antarmuka jaringan.

Tabel rute kustom

Anda dapat membuat tabel rute khusus untuk gateway lokal Anda. Tabel rute gateway lokal harus memiliki asosiasi ke grup VIF dan VPC. Untuk step-by-step petunjuk arah, lihat Mengkonfigurasi konektivitas gateway lokal.

Rute tabel rute gateway lokal

Anda dapat membuat tabel rute gateway lokal dan rute masuk ke antarmuka jaringan di Outpost Anda. Anda juga dapat memodifikasi rute masuk gateway lokal yang ada untuk mengubah antarmuka jaringan target.

Rute berada dalam status aktif hanya ketika antarmuka jaringan targetnya dilampirkan ke instance yang sedang berjalan. Jika instance dihentikan atau antarmuka terlepas, status rute berubah dari aktif menjadi lubang hitam.

Daftar Isi

Persyaratan dan pembatasan

Persyaratan dan batasan berikut berlaku:

- Antarmuka jaringan target harus milik subnet di Outpost Anda dan harus dilampirkan ke instance di Outpost itu. Rute gateway lokal tidak dapat menargetkan EC2 instans Amazon di Outpost yang berbeda atau di induk Wilayah AWS.
- Subnet harus milik VPC yang terkait dengan tabel rute gateway lokal.
- Anda tidak boleh melebihi lebih dari 100 rute antarmuka jaringan dalam tabel rute yang sama.
- AWS memprioritaskan rute yang paling spesifik, dan jika rute cocok, kami memprioritaskan rute statis daripada rute yang disebarkan.
- Titik akhir VPC antarmuka tidak didukung.
- Iklan BGP hanya untuk subnet di Outpost yang memiliki rute di tabel rute yang menargetkan gateway lokal. Jika subnet tidak memiliki rute dalam tabel rute yang menargetkan gateway lokal, maka subnet tersebut tidak diiklankan dengan BGP.

- Hanya antarmuka jaringan yang dilampirkan ke instance Outpost yang dapat berkomunikasi melalui gateway lokal untuk Outpost tersebut. Antarmuka jaringan yang termasuk dalam subnet Outpost tetapi dilampirkan ke instance di Wilayah tidak dapat berkomunikasi melalui gateway lokal untuk Outpost tersebut.
- Antarmuka yang dikelola pemohon, seperti yang dibuat untuk titik akhir VPC, tidak dapat dijangkau dari jaringan lokal melalui gateway lokal. Mereka hanya dapat dihubungi dari contoh yang ada di subnet Outpost.

Pertimbangan NAT berikut berlaku:

- Gateway lokal tidak melakukan NAT pada lalu lintas yang cocok dengan rute antarmuka jaringan. Sebaliknya, alamat IP tujuan dipertahankan.
- Matikan pemeriksaan sumber/tujuan untuk antarmuka jaringan target. Untuk informasi selengkapnya, lihat Konsep antarmuka jaringan di Panduan EC2 Pengguna Amazon.
- Konfigurasikan sistem operasi untuk memungkinkan lalu lintas dari CIDR tujuan diterima di antarmuka jaringan.

Buat tabel rute gateway lokal kustom

Anda dapat membuat tabel rute khusus untuk gateway lokal Anda menggunakan AWS Outposts konsol.

Untuk membuat tabel rute gateway lokal kustom menggunakan konsol

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Pada panel navigasi, pilih Tabel rute gateway lokal.
4. Pilih Buat tabel rute gateway lokal.
5. (Opsional) Untuk Nama, masukkan nama untuk tabel rute gateway lokal Anda.
6. Untuk gateway lokal, pilih gateway lokal Anda.
7. (Opsional) Pilih grup VIF Rekanan dan pilih grup VIF Anda.

   Edit tabel rute gateway lokal untuk menambahkan rute statis yang memiliki Grup VIF sebagai target.
8. Untuk Mode, pilih mode komunikasi dengan jaringan lokal Anda.

- Pilih perutean VPC Langsung untuk menggunakan alamat IP pribadi sebuah instans.
- Pilih CoIP untuk menggunakan alamat IP milik pelanggan.
  - (Opsional) Tambahkan atau hapus kumpulan CoIP dan blok CIDR tambahan

    [Tambahkan kumpulan CoIP] Pilih Tambahkan kolam baru dan lakukan hal berikut:

    - Untuk Nama, masukkan nama untuk kumpulan CoIP Anda.
    - Untuk CIDR, masukkan blok CIDR alamat IP milik pelanggan.
  - [Tambahkan blok CIDR] Pilih Tambahkan CIDR baru dan masukkan berbagai alamat IP milik pelanggan.
  - [Hapus kumpulan CoIP atau blok CIDR tambahan] Pilih Hapus di sebelah kanan blok CIDR atau di bawah kumpulan CoIP.

    Anda dapat menentukan hingga 10 kumpulan CoIP dan 100 blok CIDR.

9. (Opsional) Tambahkan atau hapus tanda.

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

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

   [Hapus tag] Pilih Hapus di sebelah kanan kunci dan nilai tag.
10. Pilih Buat tabel rute gateway lokal.

Ganti mode tabel rute gateway lokal atau hapus tabel rute gateway lokal

Anda harus menghapus dan membuat ulang tabel rute gateway lokal untuk beralih mode. Menghapus tabel rute gateway lokal menyebabkan gangguan lalu lintas jaringan.

Untuk beralih mode atau menghapus tabel rute gateway lokal

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Verifikasi bahwa Anda berada di tempat yang benar Wilayah AWS.

   Untuk mengubah Region, gunakan pemilih Region di pojok kanan atas halaman.
3. Pada panel navigasi, pilih Tabel rute gateway lokal.

4. Verifikasi apakah tabel rute gateway lokal dikaitkan dengan grup VIF. Jika dikaitkan, Anda harus menghapus asosiasi antara tabel rute gateway lokal dan grup VIF.

   a. Pilih ID dari tabel rute gateway lokal.
   b. Pilih tab asosiasi grup VIF.
   c. Jika satu atau beberapa grup VIF dikaitkan dengan tabel rute gateway lokal, pilih Edit asosiasi grup VIF.
   d. Kosongkan kotak centang grup VIF Associate.
   e. Pilih Simpan perubahan.
5. Pilih Hapus tabel rute gateway lokal.
6. Di kotak dialog konfirmasi, ketik **`delete`** lalu pilih Hapus.
7. (Opsional) Buat tabel rute gateway lokal dengan mode baru.

   a. Pada panel navigasi, pilih Tabel rute gateway lokal.
   b. Pilih Buat tabel rute gateway lokal.
   c. Konfigurasikan tabel rute gateway lokal menggunakan mode baru. Untuk informasi selengkapnya, lihat Membuat tabel rute gateway lokal kustom.

Buat kolam CoIP

Anda dapat memberikan rentang alamat IP untuk memfasilitasi komunikasi antara jaringan lokal dan instans di VPC Anda. Untuk informasi selengkapnya, lihat Alamat IP milik pelanggan.

Kolam IP milik pelanggan tersedia untuk tabel rute gateway lokal dalam mode CoIP.

Gunakan prosedur berikut untuk membuat kolam CoIP.

Console

Untuk membuat kolam CoIP menggunakan konsol

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Pada panel navigasi, pilih Tabel rute gateway lokal.
4. Pilih tabel rute.
5. Pilih tab CoIP pool di panel detail, lalu pilih Create CoIP pool.

6. (Opsional) Untuk Nama, masukkan nama untuk kumpulan CoIP Anda.
7. Pilih Tambahkan CIDR baru dan masukkan berbagai alamat IP milik pelanggan.
8. (Opsional) Untuk menambahkan blok CIDR, pilih Tambahkan CIDR baru dan masukkan berbagai alamat IP milik pelanggan.
9. Pilih Buat kolam CoIP.

AWS CLI

Untuk membuat kolam CoIP menggunakan AWS CLI

1. Gunakan create-coip-poolperintah untuk membuat kumpulan alamat CoIP untuk tabel rute gateway lokal yang ditentukan.

```
aws ec2 create-coip-pool --local-gateway-route-table-id lgw-rtb-
abcdefg1234567890
```

Berikut ini adalah output contoh.

```
{
    "CoipPool": {
        "PoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890",
        "PoolArn": "arn:aws:ec2:us-west-2:123456789012:coip-pool/ipv4pool-
coip-1234567890abcdefg"
    }
}
```

2. Gunakan create-coip-cidrperintah untuk membuat berbagai alamat CoIP di kolam CoIP yang ditentukan.

```
aws ec2 create-coip-cidr --cidr 15.0.0.0/24 --coip-pool-id ipv4pool-
coip-1234567890abcdefg
```

Berikut ini adalah output contoh.

```
{
    "CoipCidr": {
        "Cidr": "15.0.0.0/24",
        "CoipPoolId": "ipv4pool-coip-1234567890abcdefg",
```

```
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890"
    }
}
```

Setelah Anda membuat kumpulan CoIP, gunakan prosedur berikut untuk menetapkan alamat ke instans Anda.

Console

Untuk menetapkan alamat CoIP ke instance menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Elastic IPs.
3. Pilih Alokasi alamat IP elastis.
4. Untuk Network Border Group, pilih lokasi dari mana alamat IP diiklankan.
5. Untuk kumpulan IPv4 alamat Publik, pilih kumpulan IPv4 alamat milik Pelanggan.
6. Untuk kumpulan IPv4 alamat milik Pelanggan, pilih kumpulan yang Anda konfigurasikan.
7. Pilih Alokasikan.
8. Pilih alamat IP Elastis, dan pilih Actions, Associate Elastic IP address.
9. Pilih instance dari Instance, lalu pilih Associate.

AWS CLI

Untuk menetapkan alamat CoIP ke instance menggunakan AWS CLI

1. Gunakan describe-coip-poolsperintah untuk mengambil informasi tentang kumpulan alamat milik pelanggan Anda.

   ```
   aws ec2 describe-coip-pools
   ```

   Berikut ini adalah output contoh.

   ```
   {
       "CoipPools": [
           {
               "PoolId": "ipv4pool-coip-0abcdef0123456789",
               "PoolCidrs":  [
   ```

```
                "192.168.0.0/16"
            ],
            "LocalGatewayRouteTableId": "lgw-rtb-0abcdef0123456789"
        }
    ]
}
```

2. Gunakan perintah allocate-address untuk mengalokasikan alamat IP Elastis. Gunakan ID pool yang dikembalikan pada langkah sebelumnya.

```
aws ec2 allocate-address--address 192.0.2.128 --customer-owned-ipv4-
pool ipv4pool-coip-0abcdef0123456789
```

Berikut ini adalah output contoh.

```
{
    "CustomerOwnedIp": "192.0.2.128",
    "AllocationId": "eipalloc-02463d08ceEXAMPLE",
    "CustomerOwnedIpv4Pool": "ipv4pool-coip-0abcdef0123456789",
}
```

3. Gunakan perintah associate-address untuk mengaitkan alamat IP Elastic dengan instance Outpost. Gunakan ID alokasi yang dikembalikan pada langkah sebelumnya.

```
aws ec2 associate-address --allocation-id eipalloc-02463d08ceEXAMPLE --network-
interface-id eni-1a2b3c4d
```

Berikut ini adalah output contoh.

```
{
    "AssociationId": "eipassoc-02463d08ceEXAMPLE",
}
```

Konektivitas jaringan lokal untuk rak Outposts

Anda memerlukan komponen berikut untuk menghubungkan rak Outposts Anda ke jaringan lokal Anda:

- Konektivitas fisik dari panel patch Outpost ke perangkat jaringan lokal pelanggan Anda.
- Link Aggregation Control Protocol (LACP) untuk membuat dua koneksi link aggregation group (LAG) ke perangkat jaringan Outpost Anda dan ke perangkat jaringan lokal Anda.
- Konektivitas Virtual LAN (VLAN) antara Outpost dan perangkat jaringan lokal pelanggan Anda.
- point-to-pointKonektivitas lapisan 3 untuk setiap VLAN.
- Border Gateway Protocol (BGP) untuk iklan rute antara Outpost dan tautan layanan lokal Anda.
- BGP untuk iklan rute antara Outpost dan perangkat jaringan lokal lokal Anda untuk konektivitas ke gateway lokal.

Daftar Isi

Konektivitas fisik

Rak Outposts memiliki dua perangkat jaringan fisik yang terhubung ke jaringan lokal Anda.

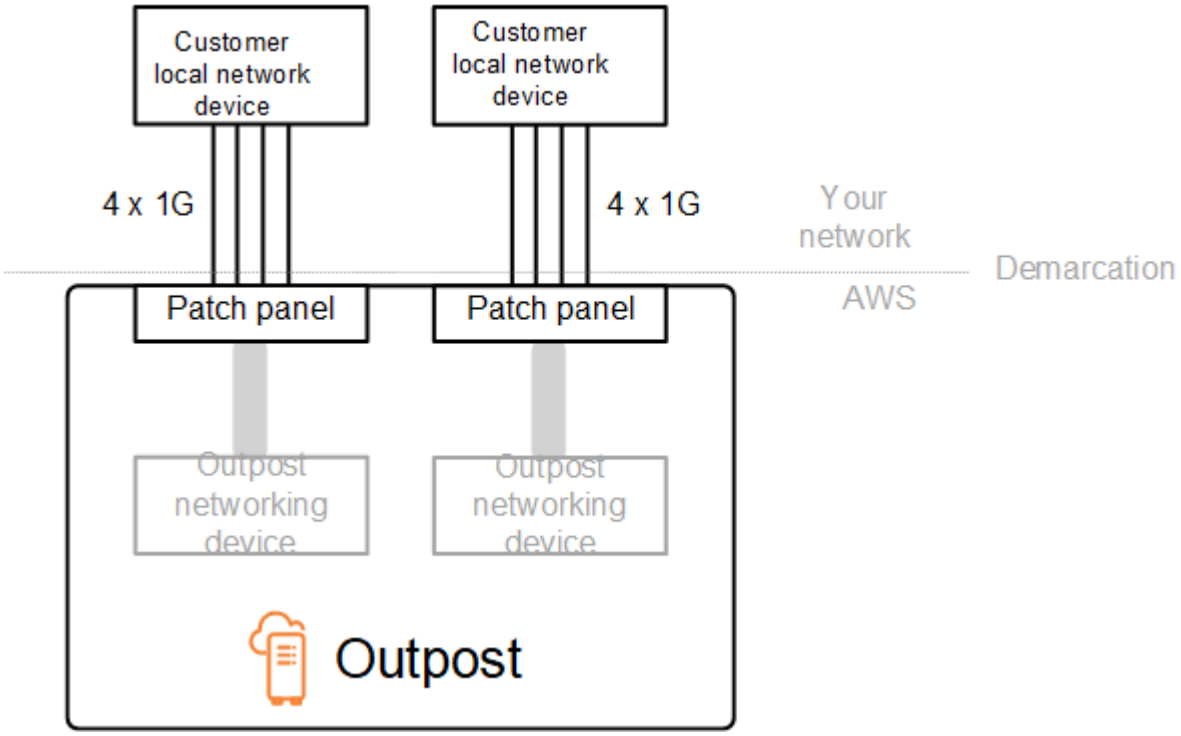
Pos Luar memerlukan minimal dua tautan fisik antara perangkat jaringan Outpost ini dan perangkat jaringan lokal Anda. Outpost mendukung kecepatan dan kuantitas uplink berikut untuk setiap perangkat jaringan Outpost.

Kecepatan uplink	Jumlah uplink
1 Gbps	1, 2, 4, 6, atau 8
10 Gbps	1, 2, 4, 8, 12, atau 16
40 Gbps atau 100 Gbps	1, 2, atau 4

Kecepatan dan kuantitas uplink simetris pada setiap perangkat jaringan Outpost. Jika Anda menggunakan 100 Gbps sebagai kecepatan uplink, Anda harus mengonfigurasi tautan dengan koreksi kesalahan maju (FEC). CL91

Rak Outposts dapat mendukung serat mode tunggal (SMF) dengan Lucent Connector (LC), serat multimode (MMF), atau MMF dengan LC. OM4 AWS menyediakan optik yang kompatibel dengan serat yang Anda berikan pada posisi rak.

Dalam diagram berikut, demarkasi fisik adalah panel patch serat di setiap Pos Luar. Anda menyediakan kabel serat yang diperlukan untuk menghubungkan Outpost ke panel patch.



Agregasi tautan

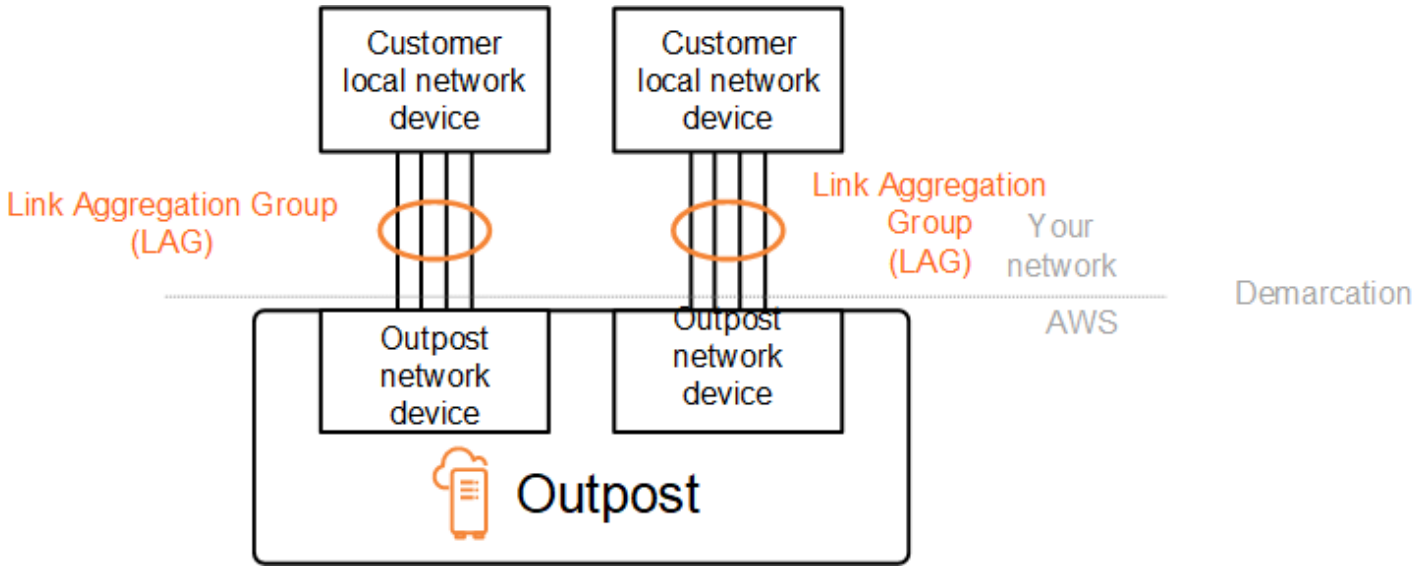
AWS Outposts menggunakan Link Aggregation Control Protocol (LACP) untuk membuat koneksi grup agregasi tautan (LAG) antara perangkat jaringan Outpost Anda dan perangkat jaringan lokal Anda. Tautan dari setiap perangkat jaringan Outpost digabungkan ke dalam Ethernet LAG untuk mewakili koneksi jaringan tunggal. Ini LAGs menggunakan LACP dengan pengatur waktu cepat standar. Anda tidak dapat mengonfigurasi LAGs untuk menggunakan pengatur waktu lambat.

Untuk mengaktifkan instalasi Outpost di situs Anda, Anda harus mengonfigurasi sisi koneksi LAG pada perangkat jaringan Anda.

Dari perspektif logis, abaikan panel patch Outpost sebagai titik demarkasi dan gunakan perangkat jaringan Outpost.

Untuk penerapan yang memiliki beberapa rak, Outpost harus memiliki empat LAGs antara lapisan agregasi perangkat jaringan Outpost dan perangkat jaringan lokal Anda.

Diagram berikut menunjukkan empat koneksi fisik antara setiap perangkat jaringan Outpost dan perangkat jaringan lokal yang terhubung. Kami menggunakan Ethernet LAGs untuk menggabungkan tautan fisik yang menghubungkan perangkat jaringan Outpost dan perangkat jaringan lokal pelanggan.



Virtual LANs

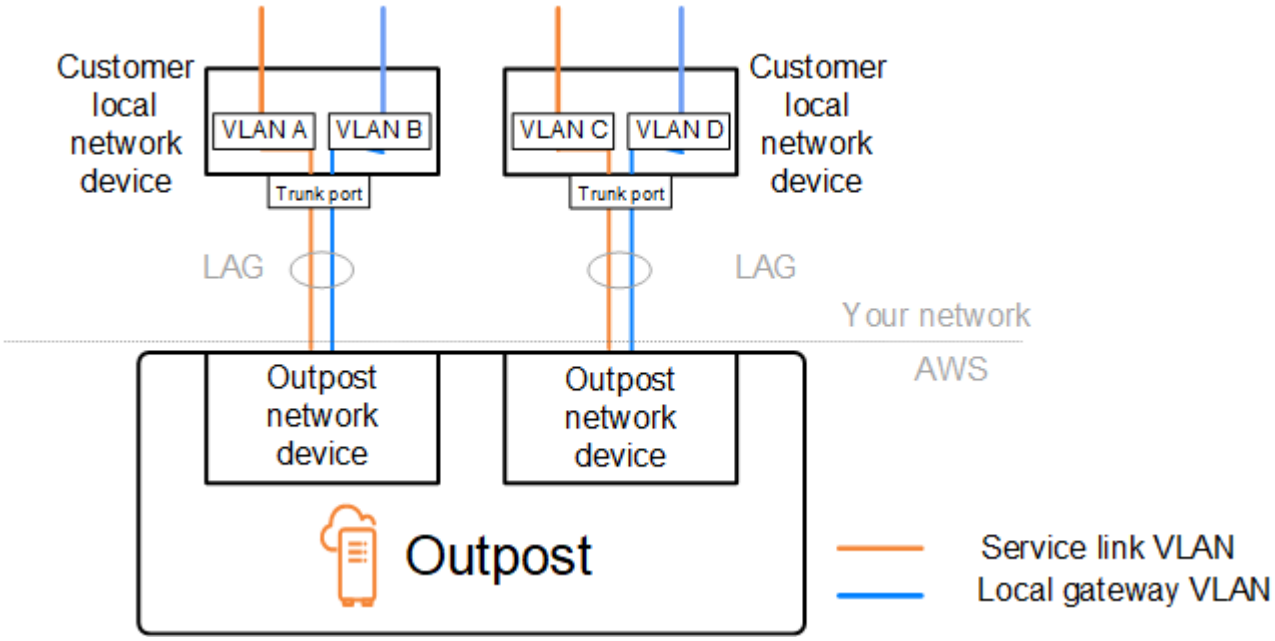
Setiap LAG antara perangkat jaringan Outpost dan perangkat jaringan lokal harus dikonfigurasi sebagai trunk Ethernet IEEE 802.1q. Hal ini memungkinkan penggunaan beberapa VLANs untuk segregasi jaringan antara jalur data.

Setiap Outpost memiliki hal-hal berikut VLANs untuk berkomunikasi dengan perangkat jaringan lokal Anda:

- Service link VLAN - Memungkinkan komunikasi antara Outpost Anda dan perangkat jaringan lokal Anda untuk membuat jalur tautan layanan untuk konektivitas tautan layanan. Untuk informasi selengkapnya, lihat AWS Outposts konektivitas ke AWS Wilayah.
- VLAN gateway lokal - Memungkinkan komunikasi antara Outpost Anda dan perangkat jaringan lokal Anda untuk membuat jalur gateway lokal untuk menghubungkan subnet Outpost Anda dan jaringan area lokal Anda. Outpost local gateway memanfaatkan VLAN ini untuk menyediakan instans Anda konektivitas ke jaringan lokal Anda, yang mungkin termasuk akses internet melalui jaringan Anda. Untuk informasi selengkapnya, lihat Gateway lokal.

Anda dapat mengonfigurasi tautan layanan VLAN dan VLAN gateway lokal hanya antara Outpost dan perangkat jaringan lokal pelanggan Anda.

Outpost dirancang untuk memisahkan link layanan dan jalur data gateway lokal menjadi dua jaringan terisolasi. Ini memungkinkan Anda untuk memilih jaringan mana yang dapat berkomunikasi dengan layanan yang berjalan di Outpost. Hal ini juga memungkinkan Anda untuk membuat link layanan jaringan terisolasi dari jaringan gateway lokal dengan menggunakan beberapa tabel rute pada perangkat jaringan lokal pelanggan Anda, umumnya dikenal sebagai Virtual Routing and Forwarding instance (VRF). Garis demarkasi ada di port perangkat jaringan Outpost. AWS mengelola infrastruktur apa pun di AWS sisi koneksi, dan Anda mengelola infrastruktur apa pun di sisi Anda.



Untuk mengintegrasikan Outpost Anda dengan jaringan lokal selama instalasi dan operasi yang sedang berlangsung, Anda harus mengalokasikan yang VLANs digunakan antara perangkat jaringan Outpost dan perangkat jaringan lokal pelanggan. Anda perlu memberikan informasi ini AWS sebelum instalasi. Untuk informasi selengkapnya, lihat the section called “Daftar periksa kesiapan jaringan”.

Konektivitas lapisan jaringan

Untuk membangun konektivitas lapisan jaringan, setiap perangkat jaringan Outpost dikonfigurasi dengan Virtual Interfaces (VIFs) yang menyertakan alamat IP untuk setiap VLAN. Melalui ini VIFs, perangkat AWS Outposts jaringan dapat mengatur konektivitas IP dan sesi BGP dengan peralatan jaringan lokal Anda.

Sebaiknya lakukan hal berikut:

- Gunakan subnet khusus, dengan /30 atau /31 CIDR, untuk mewakili konektivitas logis ini. point-to-point
- Jangan menjembatani VLANs antara perangkat jaringan lokal Anda.

Untuk konektivitas lapisan jaringan, Anda harus membuat dua jalur:

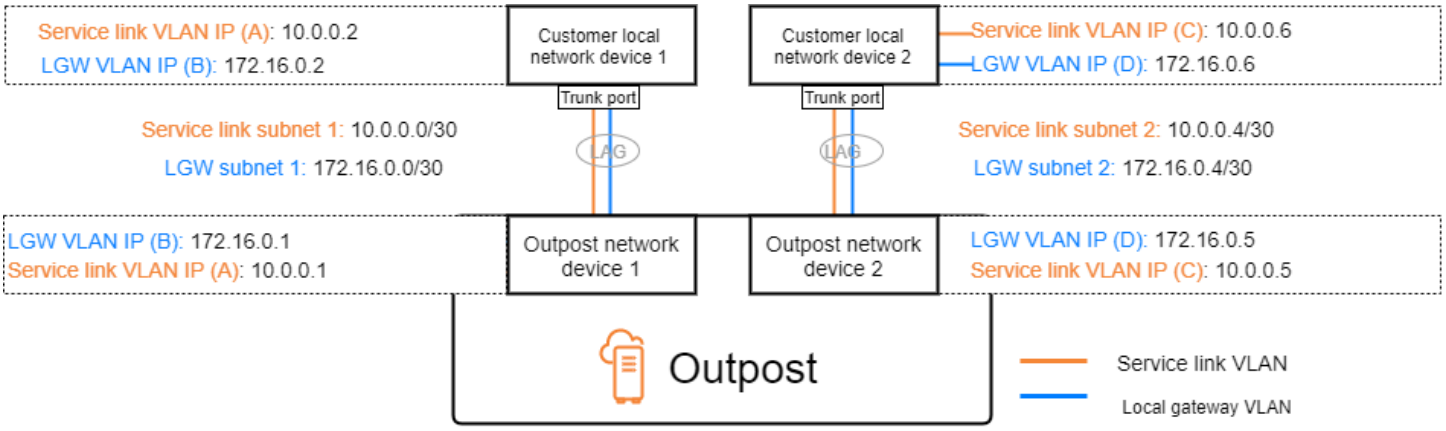
- Jalur tautan layanan - Untuk menetapkan jalur ini, tentukan subnet VLAN dengan kisaran /30 atau /31 dan alamat IP untuk setiap tautan layanan VLAN pada perangkat jaringan. AWS Outposts Tautan layanan Virtual Interfaces (VIFs) digunakan untuk jalur ini untuk membangun konektivitas

IP dan sesi BGP antara Outpost Anda dan perangkat jaringan lokal Anda untuk konektivitas tautan layanan. Untuk informasi selengkapnya, lihat AWS Outposts konektivitas ke AWS Wilayah.

- Jalur gateway lokal - Untuk menetapkan jalur ini, tentukan subnet VLAN dengan kisaran /30 atau /31 dan alamat IP untuk VLAN gateway lokal pada perangkat jaringan. AWS Outposts Gateway lokal VIFs digunakan pada jalur ini untuk membangun konektivitas IP dan sesi BGP antara Outpost Anda dan perangkat jaringan lokal Anda untuk konektivitas sumber daya lokal Anda.

Diagram berikut menunjukkan koneksi dari setiap perangkat jaringan Outpost ke perangkat jaringan lokal pelanggan untuk jalur tautan layanan dan jalur gateway lokal. Ada empat VLANs untuk contoh ini:

- VLAN A adalah untuk jalur tautan layanan yang menghubungkan perangkat jaringan Outpost 1 dengan perangkat jaringan lokal pelanggan 1.
- VLAN B adalah untuk jalur gateway lokal yang menghubungkan perangkat jaringan Outpost 1 dengan perangkat jaringan lokal pelanggan 1.
- VLAN C adalah untuk jalur tautan layanan yang menghubungkan perangkat jaringan Outpost 2 dengan perangkat jaringan lokal pelanggan 2.
- VLAN D adalah untuk jalur gateway lokal yang menghubungkan perangkat jaringan Outpost 2 dengan perangkat jaringan lokal pelanggan 2.



Tabel berikut menunjukkan contoh nilai untuk subnet yang menghubungkan perangkat jaringan Outpost 1 dengan perangkat jaringan lokal pelanggan 1.

VLAN	Subnet	Perangkat Pelanggan 1 IP	AWS OND 1 IP
A	10.0.0.0/30	10.0.0.2	10.0.0.1
B	172.16.0.0/30	172.16.0.2	172.16.0.1

Tabel berikut menunjukkan nilai contoh untuk subnet yang menghubungkan perangkat jaringan Outpost 2 dengan perangkat jaringan lokal pelanggan 2.

VLAN	Subnet	Perangkat Pelanggan 2 IP	AWS OND 2 IP
C	10.0.0.4/30	10.0.0.6	10.0.0.5
D	172.16.0.4/30	172.16.0.6	172.16.0.5

Konektivitas rak ACE

> **Note**
>
> Lewati bagian ini jika Anda tidak membutuhkan rak ACE.

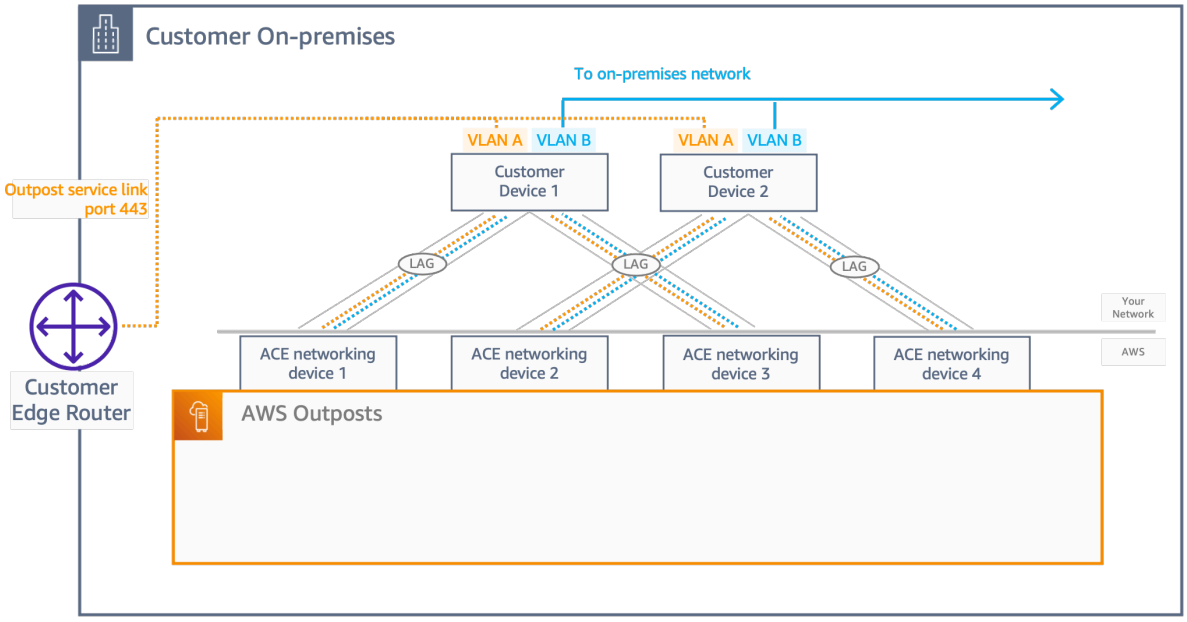
Rak Agregasi, Inti, Edge (ACE) bertindak sebagai titik agregasi jaringan untuk penyebaran Outpost multi-rak. Anda harus menggunakan rak ACE jika Anda memiliki empat atau lebih rak komputasi. Jika Anda memiliki kurang dari empat rak komputasi tetapi berencana untuk memperluas ke empat atau lebih rak di masa depan, kami sarankan Anda memasang rak ACE paling awal.

Dengan rak ACE, perangkat jaringan Outposts tidak lagi terhubung langsung ke perangkat jaringan lokal Anda. Sebaliknya, mereka terhubung ke rak ACE, yang menyediakan konektivitas ke rak Outposts. Dalam topologi ini, AWS memiliki alokasi antarmuka VLAN dan konfigurasi antara perangkat jaringan Outposts dan perangkat jaringan ACE.

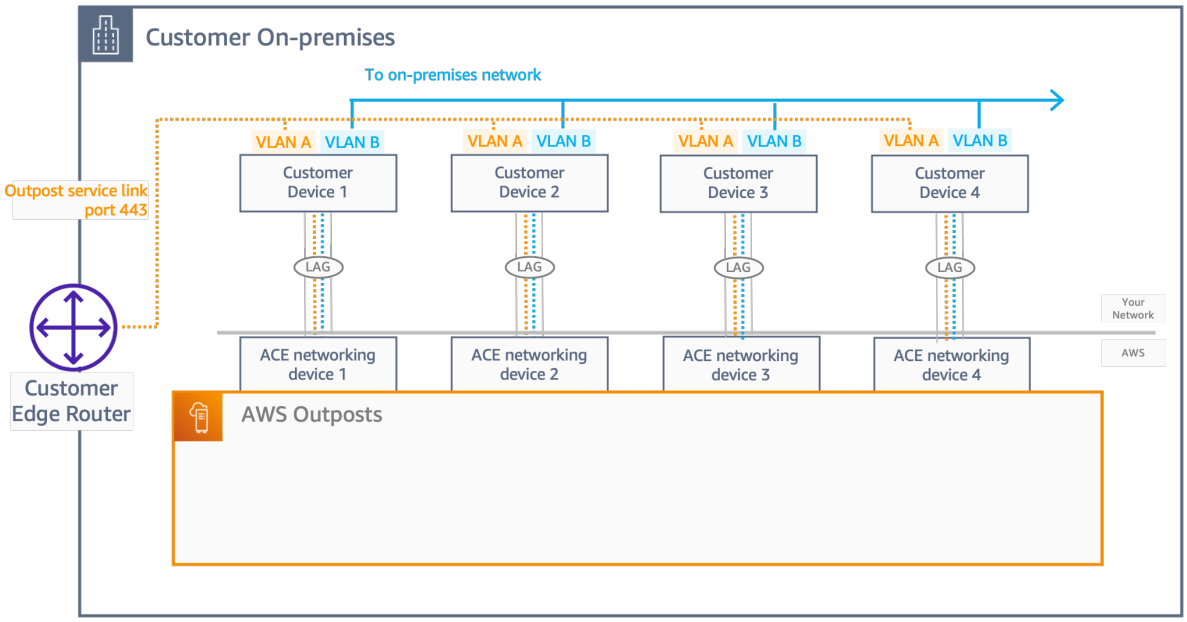
Rak ACE mencakup empat perangkat jaringan yang dapat dihubungkan ke dua perangkat pelanggan hulu dalam jaringan pelanggan lokal atau empat perangkat pelanggan hulu untuk ketahanan maksimum.

Gambar berikut menunjukkan dua topologi jaringan.

Gambar berikut menunjukkan empat perangkat jaringan ACE dari rak ACE yang terhubung ke dua perangkat pelanggan hulu:



Gambar berikut menunjukkan empat perangkat jaringan ACE dari rak ACE yang terhubung ke empat perangkat pelanggan hulu:

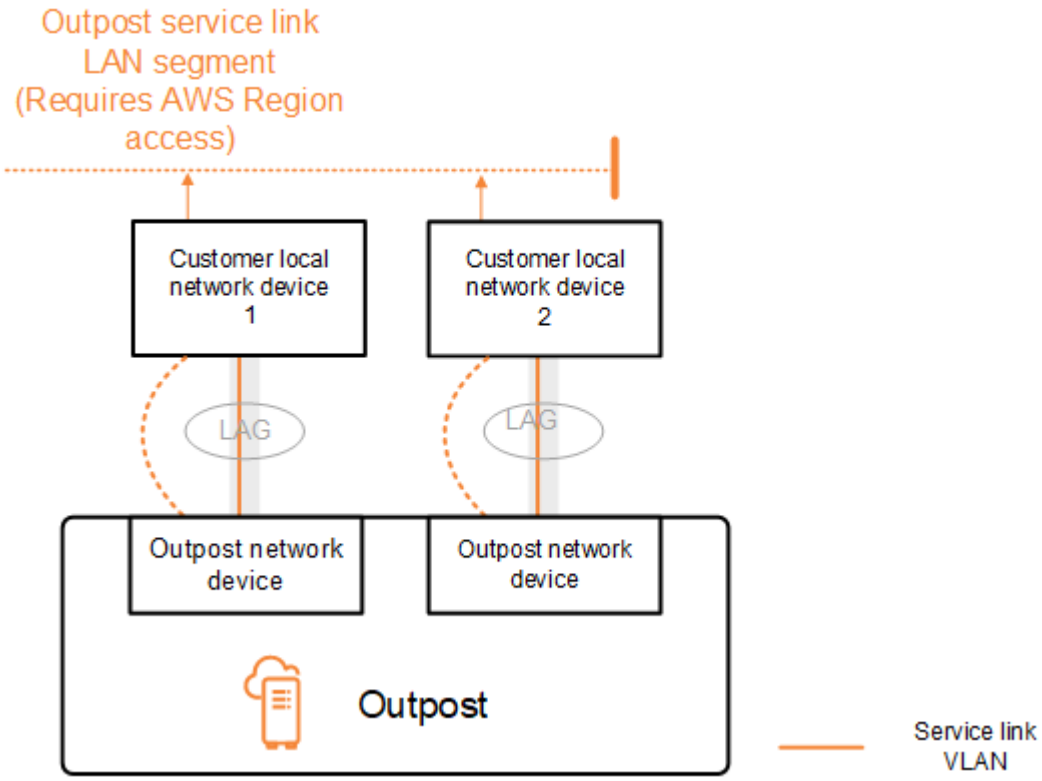


Tautan layanan konektivitas BGP

Outpost menetapkan sesi peering BGP eksternal antara setiap perangkat jaringan Outpost dan perangkat jaringan lokal pelanggan untuk konektivitas tautan layanan melalui tautan layanan VLAN. Sesi peering BGP dibuat antara alamat IP /30 atau/31 yang disediakan untuk VLAN. point-to-point Setiap sesi peering BGP menggunakan Autonomous System Number (ASN) pribadi pada perangkat jaringan Outpost dan ASN yang Anda pilih untuk perangkat jaringan lokal pelanggan Anda. Sebagai bagian dari proses instalasi, AWS mengkonfigurasi atribut yang Anda berikan..

Pertimbangkan skenario di mana Anda memiliki Outpost dengan dua perangkat jaringan Outpost yang terhubung oleh tautan layanan VLAN ke dua perangkat jaringan lokal pelanggan. Anda mengonfigurasi infrastruktur berikut, dan atribut BGP ASN perangkat jaringan lokal pelanggan untuk setiap tautan layanan:

- Layanan link BGP ASN. 2-byte (16-bit) atau 4-byte (32-bit). Nilai yang valid adalah 64512-65535 atau 4200000000-4294967294.
- Infrastruktur CIDR. Ini harus berupa /26 CIDR per rak.
- Perangkat jaringan lokal pelanggan 1 layanan menautkan alamat IP peer BGP.
- Pelanggan jaringan lokal perangkat 1 layanan link BGP peer ASN. Nilai yang valid adalah 1-4294967294.
- Perangkat jaringan lokal pelanggan 2 layanan tautan alamat IP peer BGP.
- Pelanggan jaringan lokal perangkat 2 layanan link BGP peer ASN. Nilai yang valid adalah 1-4294967294. Untuk informasi selengkapnya, lihat RFC4893.



Outpost menetapkan sesi peering BGP eksternal melalui tautan layanan VLAN menggunakan proses berikut:

1. Setiap perangkat jaringan Outpost menggunakan ASN untuk membuat sesi peering BGP dengan perangkat jaringan lokal yang terhubung.
2. Perangkat jaringan pos terdepan mengiklankan rentang CIDR /26 sebagai dua rentang CIDR /27 untuk mendukung kegagalan tautan dan perangkat. Setiap OND mengiklankan awalan /27 sendiri dengan panjang AS-path 1, ditambah awalan /27 dari semua yang lain ONDs dengan panjang AS-path 4 sebagai cadangan.
3. Subnet digunakan untuk konektivitas dari Outpost ke Region. AWS

Kami menyarankan Anda mengonfigurasi peralatan jaringan pelanggan untuk menerima iklan BGP dari Outposts tanpa mengubah atribut BGP. Jaringan pelanggan harus memilih rute dari Outposts dengan panjang AS-path 1 daripada rute dengan panjang AS-path 4.

Jaringan pelanggan harus mengiklankan awalan BGP yang sama dengan atribut yang sama untuk semua. ONDs Beban jaringan Outpost menyeimbangkan lalu lintas keluar antara semua uplink secara default. Kebijakan routing digunakan di sisi Outpost untuk mengalihkan lalu lintas dari OND jika pemeliharaan diperlukan. Pergeseran lalu lintas ini membutuhkan awalan BGP yang sama dari

sisi pelanggan. ONDs Jika pemeliharaan diperlukan pada jaringan pelanggan, kami sarankan Anda menggunakan AS-path prepending untuk sementara mengalihkan array lalu lintas dari uplink tertentu.

Iklan subnet infrastruktur tautan layanan dan rentang IP

Anda menyediakan rentang CIDR /26 selama proses pra-instalasi untuk subnet infrastruktur tautan layanan. Infrastruktur Outpost menggunakan jangkauan ini untuk membangun konektivitas ke Wilayah melalui tautan layanan. Subnet link layanan adalah sumber Outpost, yang memulai konektivitas.

Perangkat jaringan pos terdepan mengiklankan rentang CIDR /26 sebagai dua/27 blok CIDR untuk mendukung kegagalan tautan dan perangkat.

Anda harus menyediakan link layanan BGP ASN dan subnet infrastruktur CIDR (/26) untuk Outpost. Untuk setiap perangkat jaringan Outpost, berikan alamat IP peering BGP pada VLAN perangkat jaringan lokal dan BGP ASN dari perangkat jaringan lokal.

Jika Anda memiliki penerapan beberapa rak, Anda harus memiliki 1/26 subnet per rak.

Konektivitas BGP gateway lokal

Outpost menggunakan Nomor Sistem Otonomi pribadi (ASN) yang Anda tetapkan untuk menetapkan sesi BGP eksternal. Setiap perangkat jaringan Outpost memiliki BGP eksternal tunggal yang mengintip ke perangkat jaringan lokal menggunakan VLAN gateway lokalnya.

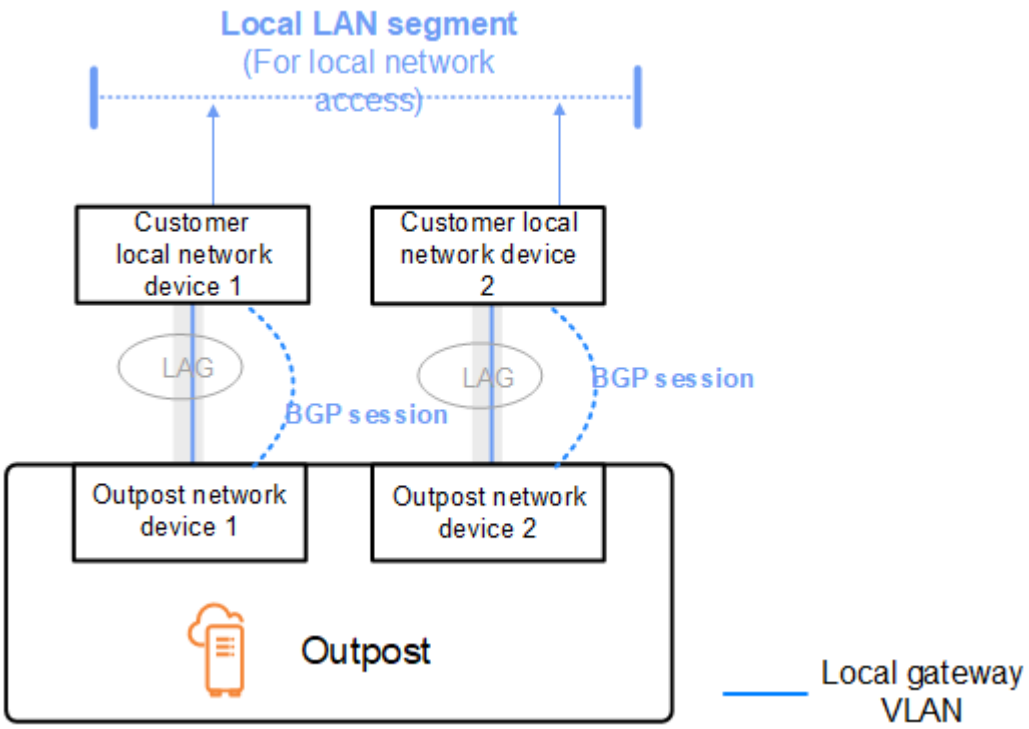
Outpost menetapkan sesi peering BGP eksternal melalui VLAN gateway lokal antara setiap perangkat jaringan Outpost dan perangkat jaringan lokal pelanggan yang terhubung. Sesi peering dibuat antara /30 atau /31 IPs yang Anda berikan saat Anda mengatur konektivitas jaringan dan menggunakan point-to-point konektivitas antara perangkat jaringan Outpost dan perangkat jaringan lokal pelanggan. Untuk informasi selengkapnya, lihat the section called “Konektivitas lapisan jaringan”.

Setiap sesi BGP menggunakan ASN pribadi di sisi perangkat jaringan Outpost, dan ASN yang Anda pilih di sisi perangkat jaringan lokal pelanggan. AWS mengkonfigurasi atribut sebagai bagian dari proses pra-instalasi.

Pertimbangkan skenario di mana Anda memiliki Outpost dengan dua perangkat jaringan Outpost yang terhubung oleh tautan layanan VLAN ke dua perangkat jaringan lokal pelanggan. Anda

mengonfigurasi atribut BGP ASN gateway lokal dan perangkat jaringan lokal pelanggan berikut untuk setiap tautan layanan:

- Pelanggan menyediakan gateway lokal BGP ASN. 2-byte (16-bit) atau 4-byte (32-bit). Nilai yang valid adalah 64512-65535 atau 4200000000-4294967294.
- (Opsional) Anda menyediakan CIDR milik pelanggan yang diiklankan (publik atau pribadi, /26 minimum).
- Anda memberikan pelanggan perangkat jaringan lokal 1 gateway lokal BGP alamat IP peer.
- Anda menyediakan perangkat jaringan lokal pelanggan 1 gateway lokal BGP peer ASN. Nilai yang valid adalah 1-4294967294. Untuk informasi selengkapnya, lihat RFC4893.
- Anda memberikan pelanggan perangkat jaringan lokal 2 gateway lokal BGP alamat IP peer.
- Anda menyediakan perangkat jaringan lokal pelanggan 2 gateway lokal BGP peer ASN. Nilai yang valid adalah 1-4294967294. Untuk informasi selengkapnya, lihat RFC4893.



Kami menyarankan Anda mengonfigurasi peralatan jaringan pelanggan untuk menerima iklan BGP dari Outposts tanpa mengubah atribut BGP, dan mengaktifkan BGP multipath/load balancing untuk mencapai arus lalu lintas masuk yang optimal. As-path prepending digunakan untuk awalan gateway lokal untuk mengalihkan lalu lintas dari ONDs jika pemeliharaan diperlukan. Jaringan pelanggan

harus memilih rute dari Outposts dengan panjang AS-path 1 daripada rute dengan panjang AS-path 4.

Jaringan pelanggan harus mengiklankan awalan BGP yang sama dengan atribut yang sama untuk semua. ONDs Beban jaringan Outpost menyeimbangkan lalu lintas keluar antara semua uplink secara default. Kebijakan routing digunakan di sisi Outpost untuk mengalihkan lalu lintas dari OND jika pemeliharaan diperlukan. Pergeseran lalu lintas ini membutuhkan awalan BGP yang sama dari sisi pelanggan. ONDs Jika pemeliharaan diperlukan pada jaringan pelanggan, kami sarankan Anda menggunakan AS-path prepending untuk sementara mengalihkan array lalu lintas dari uplink tertentu.

Iklan subnet IP milik pelanggan gateway lokal

Secara default, gateway lokal menggunakan alamat IP pribadi instance di VPC Anda (lihat perutean VPC Langsung) untuk memfasilitasi komunikasi dengan jaringan lokal Anda. Namun, Anda dapat menyediakan kumpulan alamat IP milik pelanggan (CoIP).

Anda dapat membuat alamat IP Elastis dari kumpulan ini, dan kemudian menetapkan alamat ke sumber daya di Outpost Anda, seperti EC2 instance.

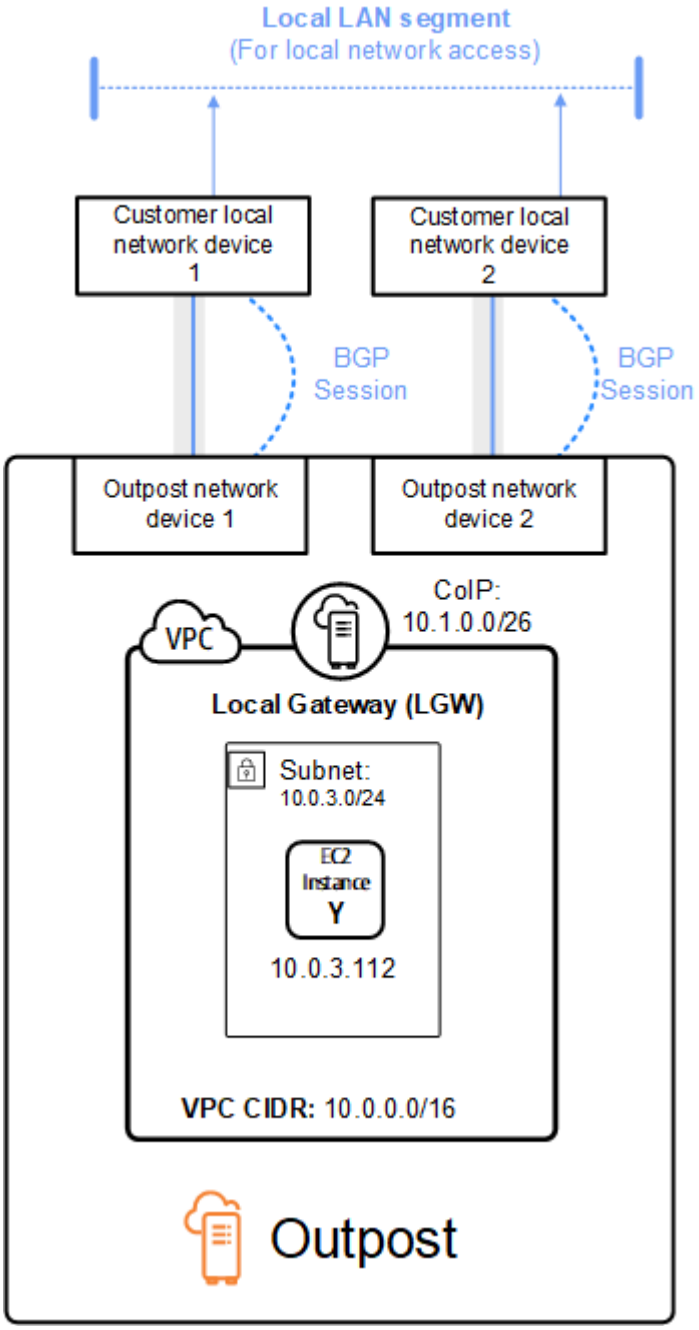
Gateway lokal menerjemahkan alamat IP Elastis ke alamat di kolam milik pelanggan. Gateway lokal mengiklankan alamat yang diterjemahkan ke jaringan lokal Anda, dan jaringan lain yang berkomunikasi dengan Outpost. Alamat diiklankan di kedua sesi BGP gateway lokal ke perangkat jaringan lokal.

> **Tip**
>
> Jika Anda tidak menggunakan CoIP, maka BGP mengiklankan alamat IP pribadi dari setiap subnet di Outpost Anda yang memiliki rute di tabel rute yang menargetkan gateway lokal.

Pertimbangkan skenario di mana Anda memiliki Outpost dengan dua perangkat jaringan Outpost yang terhubung oleh tautan layanan VLAN ke dua perangkat jaringan lokal pelanggan. Berikut ini dikonfigurasi:

- VPC dengan blok CIDR 10.0.0.0/16.
- Subnet di VPC dengan blok CIDR 10.0.3.0/24.
- Sebuah EC2 instance di subnet dengan alamat IP pribadi 10.0.3.112.
- Kumpulan IP milik pelanggan (10.1.0.0/26).

- Asosiasi alamat IP Elastis yang mengaitkan 10.0.3.112 ke 10.1.0.2.
- Gateway lokal yang menggunakan BGP untuk mengiklankan 10.1.0.0/26 ke jaringan lokal melalui perangkat lokal.
- Komunikasi antara Outpost dan jaringan lokal Anda akan menggunakan CoIP Elastic IPs untuk menangani instance di Outpost, rentang CIDR VPC tidak digunakan.



Manajemen kapasitas untuk AWS Outposts

Pos Luar menyediakan kumpulan kapasitas AWS komputasi dan penyimpanan di situs Anda sebagai perpanjangan pribadi dari Availability Zone di suatu AWS Wilayah. Karena kapasitas komputasi dan penyimpanan yang tersedia di Outpost terbatas dan ditentukan oleh ukuran dan jumlah aset yang AWS diinstal di situs Anda, Anda dapat memutuskan berapa banyak Amazon, Amazon EBS, EC2 dan Amazon S3 pada AWS Outposts kapasitas yang Anda butuhkan untuk menjalankan beban kerja awal Anda, mengakomodasi pertumbuhan masa depan, dan untuk menyediakan kapasitas ekstra untuk mengurangi kegagalan server dan peristiwa pemeliharaan.

Topik

Lihat AWS Outposts kapasitas

Anda dapat melihat konfigurasi kapasitas pada tingkat instans atau Outpost.

Untuk melihat konfigurasi kapasitas untuk Outpost Anda menggunakan konsol

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Dari panel navigasi kiri, pilih Outposts.
3. Pilih pos terdepan.
4. Pada halaman Detail Outpost pilih tampilan Instance atau tampilan Rack.

    - Tampilan instance - Menyediakan informasi tentang instance yang dikonfigurasi di Outposts dan distribusi instance berdasarkan ukuran dan keluarga.
    - Tampilan rak - Menyediakan visualisasi instans pada setiap aset dalam setiap Pos Luar dan memungkinkan Anda memilih Ubah kapasitas instans untuk membuat perubahan pada kapasitas instans.

Memodifikasi kapasitas AWS Outposts instans

Kapasitas setiap pesanan Outpost baru dikonfigurasi dengan konfigurasi kapasitas default. Anda dapat mengonversi konfigurasi default untuk membuat berbagai instance untuk memenuhi kebutuhan bisnis Anda. Untuk melakukannya, Anda membuat tugas kapasitas, memilih Outposts atau aset tunggal, menentukan ukuran dan kuantitas instans, dan menjalankan tugas kapasitas untuk mengimplementasikan perubahan.

Pertimbangan

Pertimbangkan hal berikut sebelum memodifikasi kapasitas instance:

- Tugas kapasitas hanya dapat dijalankan oleh AWS akun yang memiliki sumber daya Outpost (pemilik). Konsumen tidak dapat menjalankan tugas kapasitas. Untuk informasi selengkapnya tentang pemilik dan konsumen, lihat Berbagi AWS Outposts sumber daya Anda.
- Ukuran dan kuantitas instans dapat didefinisikan di tingkat Outpost atau pada tingkat aset individu.
- Kapasitas dikonfigurasi secara otomatis di seluruh aset atau semua aset di Pos Luar berdasarkan kemungkinan konfigurasi dan praktik terbaik.
- Saat tugas kapasitas sedang berjalan, aset yang terkait dengan pos terdepan yang dipilih dapat diisolasi. Untuk alasan ini, kami menyarankan untuk membuat tugas kapasitas hanya jika Anda tidak berharap untuk meluncurkan instance baru di Outposts Anda.
- Anda dapat memilih untuk menjalankan tugas kapasitas secara instan atau terus mencoba secara berkala selama 48 jam ke depan. Memilih untuk menjalankan secara instan membutuhkan lebih sedikit waktu isolasi aset, tetapi tugas mungkin gagal jika instance perlu dihentikan untuk menjalankan tugas. Memilih untuk menjalankan secara berkala memungkinkan lebih banyak waktu untuk menghentikan instance sebelum tugas gagal, tetapi aset dapat diisolasi lebih lama.
- Dimungkinkan untuk konfigurasi kapasitas yang valid untuk tidak menggunakan semua vCPU yang tersedia pada suatu aset. Ketika ini terjadi, pesan di akhir bagian Jenis instans akan memberi tahu Anda bahwa Anda berada di bawah kapasitas, tetapi akan memungkinkan konfigurasi diterapkan seperti yang diminta.
- Saat Anda memodifikasi Outpost di konsol, tidak semua instance yang didukung ditampilkan karena mencampur instance yang didukung disk dengan non-disk-backed instance tidak sepenuhnya didukung di konsol. Untuk mengakses semua instance yang mungkin, gunakan API. StartCapacityTask
- Saat menentukan kapasitas untuk Pos Luar, semua keluarga dan tipe instans akan disertakan dalam konfigurasi ulang kecuali mereka terdaftar sebagai instance yang harus dihindari.

- Anda hanya dapat mengubah konfigurasi kapasitas Outposts yang ada untuk menggunakan ukuran EC2 instans Amazon yang valid dari keluarga instans yang didukung pada model aset masing-masing.
- Jika Anda memiliki instans yang berjalan di Outpost yang tidak ingin dihentikan untuk menjalankan tugas kapasitas, pilih ID Instance masing-masing di bawah bagian Instans untuk tetap apa adanya — opsional dan pastikan untuk mempertahankan jumlah yang diperlukan dari ukuran instans ini dalam konfigurasi kapasitas yang diperbarui. Ini akan mempertahankan instance yang digunakan untuk mendukung beban kerja produksi saat tugas kapasitas berjalan.
- Saat mengonfigurasi aset dengan beberapa ukuran instans dalam keluarga instans, gunakan Saldo otomatis untuk memastikan Anda tidak mencoba terlalu banyak atau kurang menyediakan droplet Anda. Penyediaan berlebih tidak didukung, dan akan menyebabkan kegagalan tugas kapasitas.
- Jika Anda ingin mengkonfigurasi ulang keluarga instans di Outpost tanpa mempertahankan ukuran instans apa pun dari konfigurasi kapasitas asli, Anda harus menghentikan semua instance yang sedang berjalan dari keluarga tersebut di Outpost sebelum menjalankan tugas kapasitas. Jika instance dimiliki oleh akun lain atau digunakan oleh layanan berlapis yang berjalan di Outpost, Anda harus menggunakan akun pemilik instance untuk menghentikan instance atau instance layanan.
- Beberapa tugas kapasitas dapat berjalan secara paralel selama mereka berlaku untuk set IDs Aset yang saling eksklusif. Misalnya, Anda dapat membuat beberapa tugas kapasitas tingkat aset untuk Aset yang berbeda secara IDs bersamaan. Namun, jika ada tugas OutPost-level yang sedang berjalan, Anda tidak dapat membuat tugas Outpost atau tingkat aset lainnya secara bersamaan. Demikian pula, jika ada tugas tingkat aset yang berjalan, Anda tidak dapat membuat tugas OutPost-level atau tugas tingkat aset pada AsseID yang sama pada saat yang bersamaan.

Untuk mengubah konfigurasi kapasitas untuk Outpost Anda menggunakan konsol

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Dari panel navigasi kiri, pilih Tugas kapasitas.
3. Pada halaman tugas Kapasitas, pilih Buat tugas kapasitas.
4. Pada halaman Memulai, pilih pesanan, Outpost, atau aset yang akan dikonfigurasi.
5. Untuk mengubah kapasitas, tentukan opsi untuk Metode modifikasi: e langkah di konsol atau unggah file JSON.

    - Ubah paket konfigurasi kapasitas untuk menggunakan langkah-langkah di konsol

- Unggah paket konfigurasi kapasitas untuk mengunggah file JSON

> **Note**
>
> - Untuk mencegah manajemen kapasitas merekomendasikan instans tertentu agar berhenti, tentukan instance yang tidak boleh dihentikan. Instance ini akan dikecualikan dari daftar instance yang akan dihentikan.

Console steps

1. Pilih Tampilan Instance atau Tampilan rak.
2. Pilih Ubah konfigurasi kapasitas Outpost atau Ubah pada satu aset.
3. Pilih Outpost atau aset jika berbeda dari pilihan saat ini.
4. Pilih untuk menjalankan tugas kapasitas ini segera atau secara berkala selama 48 jam.
5. Pilih Berikutnya.
6. Pada halaman Configure instance capacity, setiap tipe instance menampilkan satu ukuran instans dengan jumlah maksimum yang telah dipilih sebelumnya. Untuk menambahkan lebih banyak ukuran instance, pilih Tambahkan ukuran instans.
7. Tentukan kuantitas instance dan catat kapasitas yang ditampilkan untuk ukuran instance tersebut.
8. Lihat pesan di akhir setiap bagian tipe instans yang memberi tahu Anda jika Anda berada di atas atau di bawah kapasitas. Lakukan penyesuaian pada ukuran instans atau tingkat kuantitas untuk mengoptimalkan total kapasitas yang tersedia.
9. Anda juga dapat meminta AWS Outposts untuk mengoptimalkan kuantitas instans untuk ukuran instans tertentu. Untuk melakukannya:

    a. Pilih ukuran instans.

    b. Pilih Saldo otomatis di akhir bagian tipe instans terkait.
10. Untuk setiap jenis instance, pastikan bahwa kuantitas instance ditentukan untuk setidaknya satu ukuran instance.
11. Secara opsional, pilih instance untuk tetap apa adanya.
12. Pilih Berikutnya.
13. Pada halaman Tinjau dan buat, verifikasi pembaruan yang Anda minta.

14. Pilih Buat. AWS Outposts menciptakan tugas kapasitas.
15. Pada halaman tugas kapasitas, pantau status tugas.

Upload a JSON file

1. Pilih Unggah konfigurasi kapasitas.
2. Pilih Berikutnya.
3. Pada halaman Paket konfigurasi kapasitas Unggah, unggah file JSON yang menentukan jenis, ukuran, dan kuantitas instans. Secara opsional, Anda dapat menentukan InstancesToExclude, dan TaskActionOnBlockingInstancesparameter dalam file JSON.

   Example

   Contoh file JSON:

```
{
  "InstancePools": [
    {
      "InstanceType": "c5.24xlarge",
      "Count": 1
    },
    {
      "InstanceType": "m5.24xlarge",
      "Count": 2
    }
  ],
  "InstancesToExclude": {
    "AccountIds": [
      "111122223333"
    ],
    "Instances": [
      "i-1234567890abcdef0"
    ],
    "Services": [
      "ALB"
    ]
  },
  "TaskActionOnBlockingInstances": "WAIT_FOR_EVACUATION"
}
```

4. Tinjau isi file JSON di bagian Paket konfigurasi Kapasitas.

5. Pilih Berikutnya.
6. Pada halaman Tinjau dan buat, verifikasi pembaruan yang Anda minta.
7. Pilih Buat. AWS Outposts menciptakan tugas kapasitas.
8. Pada halaman tugas kapasitas, pantau status tugas.

Memecahkan masalah tugas kapasitas

Tinjau masalah yang diketahui berikut untuk menyelesaikan masalah yang terkait dengan manajemen kapasitas dalam orde baru. Jika Anda tidak melihat masalah Anda terdaftar, hubungi Dukungan.

Pesanan *oo-xxxxxx* tidak terkait dengan Outpost ID *op-xxxxx*

Masalah ini terjadi ketika Anda menggunakan AWS CLI atau API untuk menjalankan `StartCapacityTask`dan ID Outpost dalam permintaan tidak cocok dengan ID Outpost dalam urutan.

Untuk menyelesaikan masalah ini:

1. Masuk ke AWS.
2. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
3. Dari panel navigasi, pilih Pesanan.
4. Pilih pesanan dan verifikasi bahwa status pesanan adalah salah satu dari yang berikut:`PREPARING`,`IN_PROGRESS`, atau`ACTIVE`.
5. Perhatikan ID Pos Luar dalam urutan.
6. Masukkan ID Outpost yang benar dalam permintaan `StartCapacityTask` API.

Paket kapasitas mencakup jenis instans yang tidak didukung

Masalah ini terjadi saat Anda menggunakan API AWS CLI atau untuk membuat atau memodifikasi tugas kapasitas dan permintaan berisi tipe instance yang tidak didukung.

Untuk mengatasi masalah ini, gunakan konsol atau CLI.

Gunakan konsol

1. Masuk ke AWS.

2. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
3. Dari panel navigasi, pilih Tugas kapasitas.
4. Gunakan opsi Unggah konfigurasi kapasitas untuk mengunggah JSON dengan daftar jenis instans yang sama.
5. Konsol menampilkan pesan kesalahan dengan daftar jenis instans yang didukung.
6. Perbaiki permintaan untuk menghapus jenis instance yang tidak didukung.
7. Buat atau ubah tugas kapasitas di konsol menggunakan JSON yang dikoreksi atau gunakan CLI atau API dengan daftar jenis instance yang dikoreksi ini.

Gunakan CLI

1. Gunakan GetOutpostSupportedInstanceTypesperintah untuk melihat daftar jenis instans yang didukung.
2. Membuat atau memodifikasi tugas kapasitas dengan daftar jenis instance yang benar.

Tidak ada pos terdepan dengan Outpost ID *op-xxxxx*

Masalah ini terjadi ketika Anda menggunakan API AWS CLI atau untuk menjalankan `StartCapacityTask`dan permintaan berisi ID Outpost yang tidak valid karena salah satu alasan berikut:

- Pos terdepan berada di AWS wilayah yang berbeda.
- Anda tidak memiliki izin untuk Outpost ini.
- Outpost ID tidak benar.

Untuk menyelesaikan masalah ini:

1. Perhatikan AWS Wilayah yang Anda gunakan dalam permintaan `StartCapacityTask` API.
2. Gunakan aksi `ListOutposts`API untuk mendapatkan daftar Outposts yang Anda miliki di Region. AWS
3. Periksa apakah Outpost ID terdaftar.
4. Masukkan ID Outpost yang benar dalam `StartCapacityTask` permintaan.
5. Jika Anda tidak menemukan ID Outpost, gunakan tindakan `ListOutposts` API lagi untuk memeriksa apakah Outpost ada di Region yang berbeda AWS .

CapacityTaskTutup aktif- *XXXX* sudah ditemukan untuk Outpost op- *XXXX*

Masalah ini terjadi saat Anda menggunakan AWS Outposts konsol atau API untuk berjalan StartCapacityTaskdi Outpost dan sudah ada tugas kapasitas yang berjalan untuk Outpost. Tugas kapasitas dianggap berjalan jika memiliki salah satu status berikut:`REQUESTED`,, `IN_PROGRESS`,`WAITING_FOR_EVACUATION`, atau`CANCELLATION_IN_PROGRESS`.

Untuk mengatasi masalah ini, gunakan AWS Outposts konsol atau CLI.

Gunakan konsol

1. Masuk ke AWS.
2. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
3. Dari panel navigasi, pilih Tugas kapasitas.
4. Pastikan bahwa tidak ada tugas kapasitas berjalan untuk OutpostId.
5. Jika ada tugas kapasitas berjalan untuk OutpostId, tunggu sampai mereka berakhir, atau batalkan jika diinginkan.
6. Ketika tidak ada tugas kapasitas berjalan untuk yang diminta OutpostId, coba lagi permintaan Anda untuk membuat tugas kapasitas.

Gunakan CLI

1. Gunakan ListCapacityTasksperintah untuk menemukan tugas kapasitas berjalan untuk Outpost.
2. Tunggu hingga semua tugas kapasitas berjalan dihentikan, atau batalkan jika diinginkan.
3. Ketika tidak ada tugas kapasitas berjalan untuk yang diminta OutpostId, coba lagi permintaan Anda untuk membuat tugas kapasitas.

CapacityTaskCap aktif- *XXXX* sudah ditemukan untuk Aset *XXXX* di Outpost OP-XXXX

Masalah ini terjadi saat Anda menggunakan AWS Outposts konsol atau API untuk menjalankan StartCapacityTaskaset dan sudah ada tugas kapasitas berjalan untuk aset tersebut. Tugas kapasitas dianggap berjalan jika memiliki salah satu status berikut:`REQUESTED`,, `IN_PROGRESS`,`WAITING_FOR_EVACUATION`, atau`CANCELLATION_IN_PROGRESS`.

Untuk mengatasi masalah ini, gunakan AWS Outposts konsol atau CLI.

Gunakan konsol

1. Masuk ke AWS.
2. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
3. Dari panel navigasi, pilih Tugas kapasitas.
4. Pastikan bahwa tidak ada tugas kapasitas berjalan untuk OutpostId dan tidak ada Tugas kapasitas tingkat aset yang sedang berjalan untuk. AssetId
5. Jika ada tugas kapasitas yang sedang berjalan, tunggu sampai selesai, atau batalkan jika diinginkan.
6. Bila tidak ada tugas kapasitas berjalan, coba lagi permintaan Anda untuk membuat tugas kapasitas.

Gunakan CLI

1. Gunakan ListCapacityTasksperintah untuk menemukan tugas kapasitas berjalan untuk outPostID dan AsseID.
2. Pastikan bahwa tidak ada tugas kapasitas OutPost-level yang berjalan untuk OutpostId, dan tidak ada Tugas kapasitas tingkat aset yang menjalankan untuk. AssetId
3. Jika ada tugas kapasitas yang sedang berjalan, tunggu sampai selesai, atau batalkan jika diinginkan.
4. Coba lagi permintaan Anda untuk membuat tugas kapasitas.

AssetId= tidak *XXXX* valid untuk outPost=op- *XXXX*

Masalah ini terjadi saat Anda menggunakan AWS Outposts konsol atau API untuk menjalankan StartCapacityTaskaset dan AsseID tidak valid karena salah satu alasan berikut:

- Aset tidak terkait dengan Outpost.
- Aset terisolasi.

Untuk mengatasi masalah ini, gunakan AWS Outposts konsol atau CLI.

Gunakan konsol

1. Masuk ke AWS.

2. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
3. Pilih Tampilan rak untuk Pos Terdepan.
4. Verifikasi AssetId bahwa permintaan terkait dengan Outpost, dan tidak ditandai sebagai Host Terisolasi.

    a. Jika Aset diisolasi, ini mungkin karena tugas kapasitas berjalan di atasnya. Anda dapat menavigasi ke panel tugas kapasitas dan memeriksa apakah ada tugas Outpost atau tingkat aset yang sedang berjalan untuk dan. OutpostId AssetId Jika ada, maka tunggu tugas berakhir dan aset tersedia lagi.

    b. Jika tidak ada tugas kapasitas berjalan untuk aset yang terisolasi, maka aset tersebut dapat terdegradasi.
5. Setelah Anda memverifikasi bahwa aset tersebut ada dan dalam status valid, coba lagi permintaan Anda untuk membuat tugas kapasitas.

Gunakan CLI

1. Gunakan ListAssetsperintah untuk menemukan aset yang terkait dengan Outpostid.
2. Verifikasi bahwa AssetId yang diminta terkait dengan Pos Terdepan, dan bahwa Negaranya adalah`ACTIVE`.

    a. Jika Negara aset tidak AKTIF, ini mungkin karena tugas kapasitas berjalan di atasnya. Gunakan ListCapacityTasksperintah untuk menentukan apakah ada tugas Outpost atau tingkat aset yang sedang berjalan untuk dan. OutpostId AssetId Jika ada, maka tunggu tugas berakhir dan aset menjadi AKTIF lagi.

    b. Jika tidak ada tugas kapasitas berjalan untuk aset yang terisolasi, maka aset tersebut dapat terdegradasi.
3. Setelah Anda memverifikasi bahwa aset tersebut ada dan dalam status valid, coba lagi permintaan Anda untuk membuat tugas kapasitas.

Bagikan AWS Outposts sumber daya Anda

Dengan berbagi Outpost, pemilik Outpost dapat berbagi sumber daya Outpost dan Outpost mereka, termasuk situs Outpost dan subnet, dengan akun lain di bawah organisasi yang sama. AWS AWS Sebagai pemilik Outpost, Anda dapat membuat dan mengelola sumber daya Outpost secara terpusat, dan berbagi sumber daya di beberapa AWS akun dalam organisasi Anda. AWS Hal ini memungkinkan konsumen lain untuk menggunakan situs Outpost, mengkonfigurasi VPCs, dan meluncurkan dan menjalankan instance di Outpost bersama.

Dalam model ini, AWS akun yang memiliki sumber daya Outpost (pemilik) berbagi sumber daya dengan AWS akun lain (konsumen) di organisasi yang sama. Konsumen dapat membuat sumber daya di Outposts yang dibagikan dengan mereka dengan cara yang sama seperti mereka akan membuat sumber daya di Outposts yang mereka buat di akun mereka sendiri. Pemilik bertanggung jawab untuk mengelola Pos Luar dan sumber daya yang mereka buat di dalamnya. Pemilik dapat mengubah atau mencabut akses bersama kapan saja. Dengan pengecualian instance yang menggunakan Reservasi Kapasitas, pemilik juga dapat melihat, memodifikasi, dan menghapus sumber daya yang dibuat konsumen di Outposts bersama. Pemilik tidak dapat mengubah instance yang diluncurkan konsumen ke Reservasi Kapasitas yang telah mereka bagikan.

Konsumen bertanggung jawab untuk mengelola sumber daya yang mereka buat di Outposts yang dibagikan dengan mereka, termasuk sumber daya apa pun yang menggunakan Reservasi Kapasitas. Konsumen tidak dapat melihat atau memodifikasi sumber daya yang dimiliki oleh konsumen lain atau oleh pemilik Outpost. Mereka juga tidak dapat memodifikasi Outposts yang dibagikan dengan mereka.

Pemilik Outpost dapat berbagi sumber daya Outpost dengan:

- AWS Akun spesifik di dalam organisasinya di AWS Organizations.
- Unit organisasi di dalam organisasinya di AWS Organizations.
- Seluruh organisasinya di AWS Organizations.

Daftar Isi

Sumber daya Outpost yang dapat dibagikan

Pemilik Outpost dapat membagikan sumber daya Outpost yang tercantum di bagian ini dengan konsumen.

- Host Khusus yang Dialokasikan — Konsumen yang memiliki akses ke sumber daya ini dapat:
  - Luncurkan dan jalankan EC2 instance di Host Khusus.
- Reservasi Kapasitas — Konsumen yang memiliki akses ke sumber daya ini dapat:
  - Identifikasi Reservasi Kapasitas yang dibagikan dengan mereka.
  - Luncurkan dan kelola instans yang menggunakan Reservasi Kapasitas.
- Kumpulan alamat IP milik pelanggan (CoIP) — Konsumen yang memiliki akses ke sumber daya ini dapat:
  - Alokasikan dan kaitkan alamat IP milik pelanggan dengan instance.
- Tabel rute gateway lokal — Konsumen yang memiliki akses ke sumber daya ini dapat:
  - Buat dan kelola asosiasi VPC ke gateway lokal.
  - Lihat konfigurasi tabel rute gateway lokal dan antarmuka virtual.
- Outposts — Konsumen dengan akses ke sumber daya ini dapat:
  - Buat dan kelola subnet di Outpost.
  - Buat dan kelola volume EBS di Outpost.
  - Gunakan AWS Outposts API untuk melihat informasi tentang Outpost.
- S3 di Outposts — Konsumen dengan akses ke sumber daya ini dapat:
  - Buat dan kelola bucket S3, titik akses, dan titik akhir di Outpost.
- Situs — Konsumen dengan akses ke sumber daya ini dapat:
  - Buat, kelola, dan kendalikan Outpost di situs.

- Subnet — Konsumen dengan akses ke sumber daya ini dapat:
  - Lihat informasi tentang subnet.
  - Luncurkan dan jalankan EC2 instance di subnet.

  Gunakan konsol Amazon VPC untuk berbagi subnet Outpost. Untuk informasi selengkapnya, lihat Berbagi subnet di Panduan Pengguna Amazon VPC.

Prasyarat untuk berbagi sumber daya Outposts

- Untuk berbagi sumber daya Outpost dengan organisasi Anda atau unit organisasi di AWS Organizations, Anda harus mengaktifkan berbagi dengan AWS Organizations. Untuk informasi selengkapnya, lihat Mengaktifkan Berbagi dengan AWS Organizations di Panduan AWS RAM Pengguna.
- Untuk membagikan sumber daya Outpost, Anda harus memilikinya di AWS akun Anda. Anda tidak dapat membagikan sumber daya Outpost yang telah dibagikan kepada Anda.
- Untuk membagikan sumber daya Outpost, Anda harus membagikannya dengan akun yang ada di dalam organisasi Anda.

Layanan terkait

Berbagi sumber daya pos terdepan terintegrasi dengan AWS Resource Access Manager ()AWS RAM. AWS RAM adalah layanan yang memungkinkan Anda untuk berbagi AWS sumber daya Anda dengan AWS akun apa pun atau melalui AWS Organizations. Dengan AWS RAM, Anda dapat berbagi sumber daya yang Anda miliki dengan membuat berbagi sumber daya. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan dibagikan. Konsumen dapat berupa AWS akun individu, unit organisasi, atau seluruh organisasi di dalamnya AWS Organizations.

Untuk informasi selengkapnya AWS RAM, lihat Panduan AWS RAM Pengguna.

Berbagi di seluruh Availability Zone

Untuk memastikan bahwa sumber daya didistribusikan di seluruh Availability Zone untuk suatu Wilayah, kami secara independen memetakan Availability Zone ke nama untuk setiap akun. Hal ini dapat menyebabkan perbedaan penamaan Zona Ketersediaan di seluruh akun. Misalnya, Availability

Zone `us-east-1a` untuk AWS akun Anda mungkin tidak memiliki lokasi yang sama dengan AWS akun lain. `us-east-1a`

Untuk mengidentifikasi lokasi sumber daya Outpost relatif terhadap akun Anda, Anda harus menggunakan ID Availability Zone (ID AZ). ID AZ adalah pengidentifikasi unik dan konsisten untuk Availability Zone di semua AWS akun. Misalnya, `use1-az1` adalah ID AZ untuk `us-east-1` Wilayah dan itu adalah lokasi yang sama di setiap AWS akun.

Untuk melihat Availability Zone di akun Anda IDs

1. Arahkan ke AWS RAM konsol di AWS RAM konsol.
2. AZ IDs untuk Wilayah saat ini ditampilkan di panel ID AZ Anda di sisi kanan layar.

> **Note**
>
> Tabel rute gateway lokal berada di AZ yang sama dengan Outpost mereka, jadi Anda tidak perlu menentukan ID AZ untuk tabel rute.

Berbagi sumber daya Outpost

Ketika seorang pemilik berbagi Outpost dengan konsumen, konsumen dapat membuat sumber daya di Outpost dengan cara yang sama seperti mereka akan membuat sumber daya di Outposts yang mereka buat di akun mereka sendiri. Konsumen yang memiliki akses ke tabel rute gateway lokal bersama dapat membuat dan mengelola asosiasi VPC. Untuk informasi selengkapnya, lihat Sumber daya Outpost yang dapat dibagikan.

Untuk membagikan sumber daya Outpost, Anda harus menambahkannya ke pembagian sumber daya. Berbagi sumber daya adalah AWS RAM sumber daya yang memungkinkan Anda berbagi sumber daya di seluruh AWS akun. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan berbagi dengan mereka. Saat membagikan sumber daya Outpost menggunakan AWS Outposts konsol, Anda menambahkannya ke pembagian sumber daya yang ada. Untuk menambahkan sumber daya Outpost ke pembagian sumber daya baru, Anda harus terlebih dahulu membuat pembagian sumber daya menggunakan AWS RAM konsol.

Jika Anda adalah bagian dari organisasi AWS Organizations dan berbagi dalam organisasi Anda diaktifkan, Anda dapat memberikan konsumen di organisasi Anda akses dari AWS RAM konsol ke sumber daya Outpost bersama. Jika tidak, konsumen menerima undangan untuk bergabung dengan

pembagian sumber daya dan diberikan akses ke sumber daya Outpost bersama setelah menerima undangan.

Anda dapat membagikan sumber daya Outpost yang Anda miliki menggunakan AWS Outposts konsol, AWS RAM konsol, atau. AWS CLI

Untuk berbagi Outpost yang Anda miliki menggunakan konsol AWS Outposts

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Pada panel navigasi, pilih Outposts.
3. Pilih Outpost, lalu pilih Actions, View details.
4. Pada halaman ringkasan Outpost, pilih Pembagian sumber daya.
5. Pilih Buat berbagi sumber daya.

Anda diarahkan ke AWS RAM konsol untuk menyelesaikan berbagi Outpost menggunakan prosedur berikut. Untuk berbagi tabel rute gateway lokal yang Anda miliki, gunakan prosedur berikut juga.

Untuk membagikan tabel rute Outpost atau gateway lokal yang Anda miliki menggunakan konsol AWS RAM

Lihat Membuat Sumber Daya Bersama di Panduan Pengguna AWS RAM .

Untuk membagikan tabel rute Outpost atau gateway lokal yang Anda miliki menggunakan AWS CLI

Gunakan perintah create-resource-share.

Membatalkan berbagi sumber daya Outpost bersama

Ketika Anda membatalkan pembagian Outpost Anda dengan konsumen, konsumen tidak dapat lagi melakukan hal berikut:

- Lihat Outpost di AWS Outposts konsol.
- Buat subnet baru di Outpost.
- Buat volume Amazon EBS baru di Outpost.
- Lihat detail Outpost dan jenis instance menggunakan AWS Outposts konsol atau file. AWS CLI

Subnet, volume, atau instance yang dibuat konsumen selama periode bersama tidak dihapus dan konsumen dapat terus melakukan hal berikut:

- Akses dan modifikasi sumber daya ini.
- Luncurkan instance baru pada subnet yang sudah ada yang dibuat konsumen.

Untuk mencegah konsumen mengakses sumber daya mereka dan meluncurkan instans baru di Outpost Anda, minta konsumen menghapus sumber daya mereka.

Ketika tabel rute gateway lokal bersama tidak dibagikan, konsumen tidak dapat lagi membuat asosiasi VPC baru untuknya. Setiap asosiasi VPC yang ada yang dibuat konsumen tetap terkait dengan tabel rute. Sumber daya di dalamnya VPCs dapat terus mengarahkan lalu lintas ke gateway lokal. Untuk mencegah hal ini, minta konsumen menghapus asosiasi VPC.

Untuk membatalkan pembagian sumber daya Outpost bersama yang Anda miliki, Anda harus menghapusnya dari pembagian sumber daya. Anda dapat melakukan ini menggunakan AWS RAM konsol atau AWS CLI.

Untuk membatalkan pembagian sumber daya Outpost bersama yang Anda miliki menggunakan konsol AWS RAM

Lihat Memperbarui Sumber Daya Bersama di Panduan Pengguna AWS RAM .

Untuk membatalkan pembagian sumber daya Outpost bersama yang Anda miliki menggunakan AWS CLI

Gunakan perintah disassociate-resource-share.

Mengidentifikasi sumber daya Outpost bersama

Pemilik dan konsumen dapat mengidentifikasi Outposts bersama menggunakan AWS Outposts konsol dan. AWS CLI Mereka dapat mengidentifikasi tabel rute gateway lokal bersama menggunakan AWS CLI.

Untuk mengidentifikasi Outpost bersama menggunakan konsol AWS Outposts

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Pada panel navigasi, pilih Outposts.
3. Pilih Outpost, lalu pilih Actions, View details.
4. Pada halaman ringkasan Outpost, lihat ID Pemilik untuk mengidentifikasi ID AWS akun pemilik Outpost.

Untuk mengidentifikasi sumber daya Outpost bersama menggunakan AWS CLI

Gunakan perintah list-outposts dan describe-local-gateway-route -tables. Perintah ini mengembalikan sumber daya Outpost yang Anda miliki dan sumber daya Outpost yang dibagikan dengan Anda. `OwnerId`menunjukkan ID AWS akun pemilik sumber daya Outpost.

Izin sumber daya Pos Luar Bersama

Izin untuk pemilik

Pemilik bertanggung jawab untuk mengelola Outpost dan sumber daya yang mereka buat di dalamnya. Pemilik dapat mengubah atau mencabut akses bersama kapan saja. Mereka dapat digunakan AWS Organizations untuk melihat, memodifikasi, dan menghapus sumber daya yang dibuat konsumen di Outposts bersama.

Izin untuk konsumen

Konsumen dapat membuat sumber daya di Outposts yang dibagikan dengan mereka dengan cara yang sama seperti mereka akan membuat sumber daya di Outposts yang mereka buat di akun mereka sendiri. Konsumen bertanggung jawab untuk mengelola sumber daya yang mereka luncurkan ke Outposts yang dibagikan dengan mereka. Konsumen tidak dapat melihat atau memodifikasi sumber daya yang dimiliki oleh konsumen lain atau oleh pemilik Outpost, dan mereka tidak dapat memodifikasi Outpost yang dibagikan dengan mereka.

Tagihan dan pengukuran

Pemilik ditagih untuk sumber daya Outposts dan Outpost yang mereka bagikan. Mereka juga ditagih untuk biaya transfer data apa pun yang terkait dengan lalu lintas VPN tautan layanan Outpost mereka dari Wilayah. AWS

Tidak ada biaya tambahan untuk berbagi tabel rute gateway lokal. Untuk subnet bersama, pemilik VPC ditagih untuk sumber daya tingkat VPC AWS Direct Connect seperti dan koneksi VPN, gateway NAT, dan koneksi Private Link.

Konsumen ditagih untuk sumber daya aplikasi yang mereka buat di Outposts bersama, seperti load balancer dan database Amazon RDS. Konsumen juga ditagih untuk transfer data yang dikenakan biaya dari Wilayah. AWS

Batasan

Batasan berikut berlaku untuk bekerja dengan AWS Outposts berbagi:

- Batasan untuk subnet bersama berlaku untuk bekerja dengan AWS Outposts berbagi. Untuk informasi selengkapnya tentang batas berbagi VPC, lihat Batasan di Panduan Pengguna Amazon Virtual Private Cloud.
- Service quotas berlaku per akun individu.

Keamanan di AWS Outposts

Keamanan di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku AWS Outposts, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Untuk informasi selengkapnya tentang keamanan dan kepatuhan AWS Outposts, lihat FAQ rak.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Outposts. Ini menunjukkan kepada Anda bagaimana memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Anda.

Daftar Isi

Perlindungan data di AWS Outposts

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Outposts. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Konten ini mencakup konfigurasi keamanan dan tugas manajemen untuk Layanan AWS yang Anda gunakan.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya.

Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Enkripsi diam

Dengan AWS Outposts, semua data dienkripsi saat istirahat. Bahan kunci dibungkus ke kunci eksternal yang disimpan dalam perangkat yang dapat dilepas, Nitro Security Key (NSK).

Anda dapat menggunakan enkripsi Amazon EBS untuk volume dan snapshot EBS Anda. Enkripsi Amazon EBS menggunakan AWS Key Management Service (AWS KMS) dan kunci KMS. Untuk informasi selengkapnya, lihat Enkripsi Amazon EBS di Panduan Pengguna Amazon EBS.

Enkripsi bergerak

AWS mengenkripsi data dalam perjalanan antara Outpost Anda dan Wilayahnya. AWS Untuk informasi selengkapnya, lihat Konektivitas melalui tautan layanan.

Anda dapat menggunakan protokol enkripsi, seperti Transport Layer Security (TLS), untuk mengenkripsi data sensitif dalam perjalanan melalui gateway lokal ke jaringan lokal Anda.

Penghapusan data

Ketika Anda menghentikan atau menghentikan sebuah EC2 instance, memori yang dialokasikan untuk itu akan digosok (disetel ke nol) oleh hypervisor sebelum dialokasikan ke instance baru, dan setiap blok penyimpanan diatur ulang.

Menghancurkan Kunci Keamanan Nitro secara kriptografis menghancurkan data di Pos Luar Anda.

Manajemen identitas dan akses (IAM) untuk AWS Outposts

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

Daftar Isi

Bagaimana AWS Outposts bekerja dengan IAM

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

Fitur IAM	AWS Dukungan Outposts
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin principal	Ya

Fitur IAM	AWS Dukungan Outposts
Peran layanan	Tidak
Peran terkait layanan	Ya

Kebijakan berbasis identitas untuk Outposts AWS

Mendukung kebijakan berbasis identitas: Ya

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

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

Contoh kebijakan berbasis identitas untuk Outposts AWS

Untuk melihat contoh kebijakan berbasis identitas AWS Outposts, lihat. AWS Contoh kebijakan Outposts

Tindakan kebijakan untuk AWS Outposts

Mendukung tindakan kebijakan: Ya

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

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki

nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

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

Untuk melihat daftar tindakan AWS Outposts, lihat Tindakan yang ditentukan oleh AWS Outposts dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di AWS Outposts menggunakan awalan berikut sebelum tindakan:

```
outposts
```

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

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

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

```
"Action": "outposts:List*"
```

Sumber daya kebijakan untuk AWS Outposts

Mendukung sumber daya kebijakan: Ya

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

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

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Beberapa tindakan API AWS Outposts mendukung beberapa sumber daya. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARNs dengan koma.

```
"Resource": [
    "resource1",
    "resource2"
]
```

Untuk melihat daftar jenis sumber daya AWS Outposts dan jenisnya ARNs, lihat Jenis sumber daya yang ditentukan oleh AWS Outposts dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang ditentukan oleh AWS Outposts.

Kunci kondisi kebijakan untuk AWS Outposts

Mendukung kunci kondisi kebijakan khusus layanan: Yes

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

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

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

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

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

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

Untuk melihat daftar kunci kondisi AWS Outposts, lihat Kunci kondisi untuk AWS Outposts Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS Outposts.

Untuk melihat contoh kebijakan berbasis identitas AWS Outposts, lihat. AWS Contoh kebijakan Outposts

ABAC dengan Outposts AWS

Mendukung ABAC (tanda dalam kebijakan): Ya

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

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

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

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

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensil sementara dengan Outposts AWS

Mendukung kredensial sementara: Ya

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

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

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

Izin utama lintas layanan untuk Outposts AWS

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran terkait layanan untuk Outposts AWS

Mendukung peran terkait layanan: Ya

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

Untuk detail tentang membuat atau mengelola peran terkait layanan AWS Outposts, lihat. Peran terkait layanan untuk AWS Outposts

AWS Contoh kebijakan Outposts

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

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

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

Daftar Isi

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya AWS Outposts di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Contoh: Menggunakan izin tingkat sumber daya

Contoh berikut menggunakan izin tingkat sumber daya untuk memberikan izin untuk mendapatkan informasi tentang Outpost yang ditentukan.

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

```
    {
      "Effect": "Allow",
      "Action": "outposts:GetOutpost",
      "Resource": "arn:aws:outposts:region:12345678012:outpost/op-1234567890abcdef0"
    }
  ]
}
```

Contoh berikut menggunakan izin tingkat sumber daya untuk memberikan izin untuk mendapatkan informasi tentang situs yang ditentukan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetSite",
      "Resource": "arn:aws:outposts:region:12345678012:site/os-0abcdef1234567890"
    }
  ]
}
```

Peran terkait layanan untuk AWS Outposts

AWS Outposts menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis peran layanan yang ditautkan langsung ke. AWS Outposts AWS Outposts mendefinisikan peran terkait layanan dan mencakup semua izin yang diperlukan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Anda AWS Outposts lebih efisien karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS Outposts mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS Outposts dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi AWS Outposts sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Izin peran terkait layanan untuk AWS Outposts

AWS Outposts menggunakan peran terkait layanan bernama AWSService RoleForOutposts _. ***OutpostID*** Peran ini memberikan izin Outposts untuk mengelola sumber daya jaringan guna mengaktifkan konektivitas pribadi atas nama Anda. Peran ini juga memungkinkan Outposts untuk membuat dan mengonfigurasi antarmuka jaringan, mengelola grup keamanan, dan melampirkan antarmuka ke instance titik akhir tautan layanan. Izin ini diperlukan untuk membangun dan memelihara koneksi pribadi yang aman antara Pos Luar dan AWS layanan lokal Anda, memastikan pengoperasian penyebaran Outpost Anda yang andal.

Peran *OutpostID* terkait layanan AWSService RoleForOutposts _ mempercayai layanan berikut untuk mengambil peran:

- `outposts.amazonaws.com`

Kebijakan peran terkait layanan

*OutpostID*Peran terkait layanan AWSService RoleForOutposts _ mencakup kebijakan berikut:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_*OutpostID*

AWSOutpostsServiceRolePolicy

`AWSOutpostsServiceRolePolicy`Kebijakan ini memungkinkan akses ke AWS sumber daya yang dikelola oleh AWS Outposts.

Kebijakan ini memungkinkan AWS Outposts untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `ec2:DescribeNetworkInterfaces` pada semua AWS sumber daya
- Tindakan: `ec2:DescribeSecurityGroups` pada semua AWS sumber daya
- Tindakan: `ec2:DescribeSubnets` pada semua AWS sumber daya
- Tindakan: `ec2:DescribeVpcEndpoints` pada semua AWS sumber daya
- Tindakan: `ec2:CreateNetworkInterface` pada AWS sumber daya berikut:

```
"arn:*:ec2:*:*:vpc/*",
"arn:*:ec2:*:*:subnet/*",
```

```
"arn:*:ec2:*:*:security-group/*"
```

- Tindakan: `ec2:CreateNetworkInterface` pada AWS sumber daya `"arn:*:ec2:*:*:network-interface/*"` yang cocok dengan kondisi berikut:

```
"ForAnyValue:StringEquals" : { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

- Tindakan: `ec2:CreateSecurityGroup` pada AWS sumber daya berikut:

```
"arn:*:ec2:*:*:vpc/*"
```

- Tindakan: `ec2:CreateSecurityGroup` pada AWS sumber daya `"arn:*:ec2:*:*:security-group/*"` yang cocok dengan kondisi berikut:

```
"ForAnyValue:StringEquals": { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

AWSOutpostsPrivateConnectivityPolicy_OutpostID

`AWSOutpostsPrivateConnectivityPolicy_OutpostID`Kebijakan ini memungkinkan AWS Outposts untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `ec2:AuthorizeSecurityGroupIngress` pada semua AWS sumber daya yang cocok dengan kondisi berikut:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Tindakan: `ec2:AuthorizeSecurityGroupEgress` pada semua AWS sumber daya yang cocok dengan kondisi berikut:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Tindakan: `ec2:CreateNetworkInterfacePermission` pada semua AWS sumber daya yang cocok dengan kondisi berikut:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Tindakan: `ec2:CreateTags` pada semua AWS sumber daya yang cocok dengan kondisi berikut:

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}},
"StringEquals": {"ec2:CreateAction" : ["CreateSecurityGroup",
 "CreateNetworkInterface"]}
```

- Tindakan: `ec2:RevokeSecurityGroupIngress` pada semua AWS sumber daya yang cocok dengan kondisi berikut:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Tindakan: `ec2:RevokeSecurityGroupEgress` pada semua AWS sumber daya yang cocok dengan kondisi berikut:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Tindakan: `ec2:DeleteNetworkInterface` pada semua AWS sumber daya yang cocok dengan kondisi berikut:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Tindakan: `ec2:DeleteSecurityGroup` pada semua AWS sumber daya yang cocok dengan kondisi berikut:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Buat peran terkait layanan untuk AWS Outposts

Anda tidak perlu membuat peran tertaut layanan secara manual. Saat Anda mengonfigurasi konektivitas pribadi untuk Outpost Anda di AWS Management Console, AWS Outposts buat peran terkait layanan untuk Anda.

Untuk informasi selengkapnya, lihat Opsi konektivitas pribadi tautan layanan.

Mengedit peran terkait layanan untuk AWS Outposts

AWS Outposts tidak mengizinkan Anda mengedit peran *OutpostID* terkait layanan AWSService RoleForOutposts _. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Memperbarui peran terkait layanan di Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk AWS Outposts

Jika Anda tidak lagi memerlukan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan demikian, Anda menghindari memiliki entitas tidak terpakai yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran terkait layanan sebelum menghapusnya secara manual.

Jika AWS Outposts layanan menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Anda harus menghapus Outpost Anda sebelum dapat menghapus peran *OutpostID* terkait layanan AWSService RoleForOutposts _.

Sebelum memulai, pastikan Outpost Anda tidak dibagikan menggunakan AWS Resource Access Manager (AWS RAM). Untuk informasi selengkapnya, lihat Membatalkan berbagi sumber daya Outpost bersama.

Untuk menghapus AWS Outposts sumber daya yang digunakan oleh AWSService RoleForOutposts _ ***OutpostID***

Hubungi AWS Enterprise Support untuk menghapus Outpost Anda.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk AWS Outposts peran terkait layanan

AWS Outposts mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat rak FAQs untuk Outposts.

AWS kebijakan terkelola untuk AWS Outposts

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

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

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

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

AWS kebijakan terkelola: AWSOutposts ServiceRolePolicy

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan AWS Outposts melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Peran terkait layanan.

AWS Update Outposts ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk AWS Outposts sejak layanan ini mulai melacak perubahan ini.

Perubahan	Deskripsi	Tanggal
Pembaruan untuk peran AWS Identity and Access Management terkait layanan _ AWSService RoleForOutposts *OutpostID*	Izin peran *OutpostID* terkait layanan AWSServic eRoleForOutposts_ diperbaru i untuk menyempurnakan cara AWS Outposts mengelola sumber daya jaringan untuk konektivitas pribadi, dengan kontrol yang lebih tepat atas antarmuka jaringan dan	April 18, 2025

Perubahan	Deskripsi	Tanggal
	operasi grup keamanan yang diperlukan untuk instance titik akhir tautan layanan.	
AWS Outposts mulai melacak perubahan	AWS Outposts mulai melacak perubahan untuk kebijakan yang AWS dikelola.	Desember 03, 2019

Keamanan infrastruktur di AWS Outposts

Sebagai layanan terkelola, AWS Outposts dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS Outposts melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Untuk informasi selengkapnya tentang keamanan infrastruktur yang disediakan untuk EC2 instans dan volume EBS yang berjalan di Pos Luar Anda, lihat Keamanan Infrastruktur di Amazon. EC2

VPC Flow Logs berfungsi dengan cara yang sama seperti yang mereka lakukan di Region. AWS Ini berarti bahwa mereka dapat dipublikasikan ke CloudWatch Log, Amazon S3, atau ke Amazon GuardDuty untuk analisis. Data perlu dikirim kembali ke Wilayah untuk dipublikasikan ke layanan ini, sehingga tidak terlihat dari CloudWatch atau layanan lain ketika Pos Luar dalam keadaan terputus.

Pemantauan tamper pada peralatan AWS Outposts

Pastikan tidak ada yang memodifikasi, mengubah, merekayasa balik, atau merusak peralatan. AWS Outposts AWS Outposts peralatan dapat dilengkapi dengan pemantauan tamper untuk memastikan kepatuhan terhadap Ketentuan AWS Layanan.

Ketahanan di AWS Outposts

AWS Outposts dirancang agar sangat tersedia. Rak Outposts dirancang dengan kekuatan redundan dan peralatan jaringan. Untuk ketahanan tambahan, kami menyarankan Anda menyediakan sumber daya ganda dan konektivitas jaringan redundan untuk Outpost Anda.

Untuk ketersediaan tinggi, Anda dapat menyediakan tambahan kapasitas built-in dan selalu aktif pada Outposts rack tambahan. Konfigurasi kapasitas pos terdepan dirancang untuk beroperasi di lingkungan produksi, dan mendukung instans N+1 untuk setiap rangkaian instans saat Anda menyediakan kapasitas untuk melakukannya. AWS merekomendasikan agar Anda mengalokasikan kapasitas tambahan yang cukup untuk aplikasi penting misi Anda untuk mengaktifkan pemulihan dan failover jika ada masalah host yang mendasarinya. Anda dapat menggunakan metrik ketersediaan CloudWatch kapasitas Amazon dan mengatur alarm untuk memantau kesehatan aplikasi Anda, membuat CloudWatch tindakan untuk mengonfigurasi opsi pemulihan otomatis, dan memantau pemanfaatan kapasitas Outposts Anda dari waktu ke waktu.

Saat Anda membuat Outpost, Anda memilih Availability Zone dari AWS Region. Availability Zone ini mendukung operasi bidang kontrol seperti menanggapi panggilan API, memantau Outpost, dan memperbarui Outpost. Untuk mendapatkan manfaat dari ketahanan yang disediakan oleh Availability Zones, Anda dapat menerapkan aplikasi di beberapa Outpost, masing-masing dilampirkan ke Availability Zone yang berbeda. Hal ini memungkinkan Anda untuk membangun ketahanan aplikasi tambahan dan menghindari ketergantungan pada Availability Zone tunggal. Untuk informasi selengkapnya tentang Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Anda dapat menggunakan grup penempatan dengan strategi penyebaran untuk memastikan bahwa instance ditempatkan di rak Outposts yang berbeda. Dengan demikian, ini dapat membantu mengurangi kegagalan yang berkorelasi. Untuk informasi selengkapnya, lihat Grup penempatan di Outposts.

Anda dapat meluncurkan instance di Outposts menggunakan Amazon Auto EC2 Scaling dan membuat Application Load Balancer untuk mendistribusikan lalu lintas antar instans. Untuk informasi selengkapnya, lihat Mengonfigurasi Application Load AWS Outposts Balancer di.

Validasi kepatuhan untuk AWS Outposts

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Kepatuhan dan Tata Kelola Keamanan – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- Referensi Layanan yang Memenuhi Syarat HIPAA — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan,

seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.

- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Akses internet untuk beban AWS Outposts kerja

Bagian ini menjelaskan bagaimana AWS Outposts beban kerja dapat mengakses internet dengan cara berikut:

- Melalui AWS Wilayah induk
- Melalui jaringan pusat data lokal Anda

Akses internet melalui AWS Wilayah induk

Dalam opsi ini, beban kerja di Outposts mengakses internet melalui tautan layanan dan kemudian melalui gateway internet (IGW) di Wilayah induk. AWS Lalu lintas keluar ke internet dapat melalui gateway NAT yang dipakai di VPC Anda. Untuk keamanan tambahan untuk lalu lintas masuk dan keluar, Anda dapat menggunakan layanan AWS keamanan seperti AWS WAF,, AWS Shield dan Amazon CloudFront di Wilayah. AWS

Untuk pengaturan tabel rute pada subnet Outposts, lihat Tabel rute gateway lokal.

Pertimbangan

- Gunakan opsi ini ketika:
  - Anda membutuhkan fleksibilitas dalam mengamankan lalu lintas internet dengan berbagai AWS layanan di AWS Wilayah.
  - Anda tidak memiliki titik kehadiran internet di pusat data atau fasilitas co-location Anda.
- Dalam opsi ini, lalu lintas harus melintasi AWS Wilayah induk, yang memperkenalkan latensi.
- Mirip dengan biaya transfer data di AWS Wilayah, transfer data keluar dari Availability Zone induk ke Outpost menimbulkan biaya. Untuk mempelajari selengkapnya tentang transfer data, lihat Harga EC2 Sesuai Permintaan Amazon.
- Pemanfaatan bandwidth link layanan akan meningkat.

Gambar berikut menunjukkan lalu lintas antara beban kerja di instance Outposts dan internet melalui Wilayah induk. AWS

Akses internet melalui jaringan pusat data lokal Anda

Dalam opsi ini, beban kerja yang berada di Outposts mengakses internet melalui pusat data lokal Anda. Lalu lintas beban kerja yang mengakses internet melintasi titik keberadaan dan jalan keluar internet lokal Anda secara lokal. Lapisan keamanan jaringan pusat data lokal Anda bertanggung jawab untuk mengamankan lalu lintas beban kerja Outposts.

Untuk pengaturan tabel rute pada subnet Outposts, lihat Tabel rute gateway lokal.

Pertimbangan

- Gunakan opsi ini ketika:
  - Beban kerja Anda memerlukan akses latensi rendah ke layanan internet.
  - Anda lebih suka menghindari biaya Transfer Data Out (DTO).
  - Anda ingin mempertahankan bandwidth tautan layanan untuk mengontrol lalu lintas pesawat.
- Lapisan keamanan Anda bertanggung jawab untuk mengamankan lalu lintas beban kerja Outposts.
- Jika Anda memilih Direct VPC Routing (DVR), maka Anda harus memastikan bahwa Outposts CIDRs tidak bertentangan dengan lokal. CIDRs
- Jika rute default (0/0) disebarkan melalui gateway lokal (LGW), maka instance mungkin tidak dapat mencapai titik akhir layanan. Atau, Anda dapat memilih titik akhir VPC untuk mencapai layanan yang diinginkan.

Gambar berikut menunjukkan lalu lintas antara beban kerja di instance Outposts dan internet melalui pusat data lokal Anda.

AWS Outposts terintegrasi dengan layanan berikut yang menawarkan kemampuan pemantauan dan pencatatan:

CloudWatch metrik

Gunakan Amazon CloudWatch untuk mengambil statistik tentang titik data untuk server Outposts Anda sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Anda dapat menggunakan metrik ini untuk memverifikasi bahwa sistem Anda bekerja sesuai harapan. Untuk informasi selengkapnya, lihat CloudWatch .

CloudTrail log

Gunakan AWS CloudTrail untuk menangkap informasi terperinci tentang panggilan yang dilakukan AWS APIs. Anda dapat menyimpan panggilan ini sebagai file log di Amazon S3. Anda dapat menggunakan CloudTrail log ini untuk menentukan informasi seperti panggilan mana yang dibuat, alamat IP sumber dari mana panggilan itu berasal, siapa yang melakukan panggilan, dan kapan panggilan dilakukan.

CloudTrail Log berisi informasi tentang panggilan ke tindakan API untuk AWS Outposts. Mereka juga berisi informasi untuk panggilan ke tindakan API dari layanan di Outpost, seperti Amazon EC2 dan Amazon EBS. Untuk informasi selengkapnya, lihat Log panggilan API menggunakan CloudTrail.

Log Aliran VPC

Gunakan VPC Flow Logs untuk menangkap informasi terperinci tentang lalu lintas yang menuju dan dari Outpost Anda dan di dalam Outpost Anda. Untuk informasi selengkapnya, lihat Log Alur VPC di Panduan Pengguna Amazon VPC.

Pencerminan Lalu lintas

Gunakan Traffic Mirroring untuk menyalin dan meneruskan lalu lintas jaringan dari server Outposts Anda out-of-band ke peralatan keamanan dan pemantauan. Anda dapat menggunakan lalu lintas cermin untuk pemeriksaan konten, pemantauan ancaman, atau pemecahan masalah. Untuk informasi selengkapnya, lihat Panduan Pencerminan Lalu Lintas Amazon VPC.

AWS Health Dashboard

AWS Health Dashboard Menampilkan informasi dan pemberitahuan yang diprakarsai oleh perubahan kesehatan AWS sumber daya. Informasi ini disajikan dalam dua cara: di dasbor yang menampilkan peristiwa terbaru dan mendatang yang diatur berdasarkan kategori, dan dalam catatan peristiwa lengkap yang menampilkan semua peristiwa dari 90 hari terakhir. Misalnya,

masalah konektivitas pada tautan layanan akan memulai peristiwa yang akan muncul di dasbor dan log peristiwa, dan tetap berada di log peristiwa selama 90 hari. Bagian dari AWS Health layanan, tidak AWS Health Dashboard memerlukan pengaturan dan dapat dilihat oleh pengguna mana pun yang diautentikasi di akun Anda. Untuk informasi selengkapnya, lihat Memulai dengan AWS Health Dashboard.

CloudWatch

AWS Outposts menerbitkan titik data ke Amazon CloudWatch untuk Outposts Anda. CloudWatch memungkinkan Anda untuk mengambil statistik tentang titik-titik data tersebut sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Anggap metrik sebagai variabel untuk memantau, dan titik data sebagai nilai variabel tersebut dari waktu ke waktu. Misalnya, Anda dapat memantau kapasitas instans yang tersedia untuk Outpost Anda selama periode waktu tertentu. Setiap titik data memiliki timestamp terkait dan pengukuran unit opsional.

Anda dapat menggunakan metrik untuk memverifikasi bahwa sistem Anda bekerja sesuai harapan. Misalnya, Anda dapat membuat CloudWatch alarm untuk memantau `ConnectedStatus` metrik. Jika metrik rata-rata kurang dari1, CloudWatch dapat memulai tindakan, seperti mengirim pemberitahuan ke alamat email. Anda kemudian dapat menyelidiki potensi masalah jaringan lokal atau uplink yang mungkin memengaruhi operasi Outpost Anda. Masalah umum termasuk perubahan konfigurasi jaringan lokal terbaru ke firewall dan aturan NAT, atau masalah koneksi internet. Untuk `ConnectedStatus` masalah, kami sarankan untuk memverifikasi konektivitas ke AWS Wilayah dari dalam jaringan lokal Anda, dan menghubungi AWS Support jika masalah berlanjut.

Untuk informasi selengkapnya tentang membuat CloudWatch alarm, lihat Menggunakan CloudWatch Alarm Amazon di Panduan CloudWatch Pengguna Amazon. Untuk informasi selengkapnya CloudWatch, lihat Panduan CloudWatch Pengguna Amazon.

Daftar Isi

Metrik

Namespace `AWS/Outposts` mencakup metrik berikut.

`ConnectedStatus`

Status koneksi tautan layanan Outpost. Jika statistik rata-rata kurang dari`1`, koneksi terganggu.

Satuan: Hitung

Resolusi maksimum: 1 menit

Statistics: Statistik yang paling berguna adalah `Average`.

Dimensi: `OutpostId`

`CapacityExceptions`

Jumlah kesalahan kapasitas yang tidak mencukupi misalnya peluncuran.

Satuan: Hitung

Resolusi maksimum: 5 menit

Statistik: Statistik yang paling berguna adalah `Maximum` dan `Minimum`.

Dimensi: `InstanceType` dan `OutpostId`

`IfTrafficIn`

Bitrate data yang diterima Outposts Virtual Interfaces VIFs () dari perangkat jaringan lokal yang terhubung.

Satuan: Bit per detik

Resolusi maksimum: 5 menit

Statistik: Statistik yang paling berguna adalah `Max` dan `Min`.

Dimensi untuk gateway lokal VIFs (lgw-vif):,, dan `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensi untuk tautan layanan VIFs (sl-vif): dan `OutpostsId` `VirtualInterfaceId`

`IfTrafficOut`

Bitrate data yang ditransfer Outposts Virtual Interfaces VIFs () ke perangkat jaringan lokal yang terhubung.

Satuan: Bit per detik

Resolusi maksimum: 5 menit

Statistik: Statistik yang paling berguna adalah `Max` dan `Min`.

Dimensi untuk gateway lokal VIFs (lgw-vif):, , dan `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensi untuk tautan layanan VIFs (sl-vif): dan `OutpostsId` `VirtualInterfaceId`

`InstanceFamilyCapacityAvailability`

Persentase kapasitas instans yang tersedia. Metrik ini tidak termasuk kapasitas untuk Host Khusus yang dikonfigurasi di Outpost.

Satuan: Persen

Resolusi maksimum: 5 menit

Statistics: Statistik yang paling berguna adalah `Average` dan `pNN.NN` (persentil).

Dimensi: `InstanceFamily` dan `OutpostId`

`InstanceFamilyCapacityUtilization`

Persentase kapasitas instance yang digunakan. Metrik ini tidak termasuk kapasitas untuk Host Khusus yang dikonfigurasi di Outpost.

Satuan: Persen

Resolusi maksimum: 5 menit

Statistics: Statistik yang paling berguna adalah `Average` dan `pNN.NN` (persentil).

Dimensi:`Account`,`InstanceFamily`, dan `OutpostId`

`InstanceTypeCapacityAvailability`

Persentase kapasitas instans yang tersedia. Metrik ini tidak termasuk kapasitas untuk Host Khusus yang dikonfigurasi di Outpost.

Satuan: Persen

Resolusi maksimum: 5 menit

Statistics: Statistik yang paling berguna adalah `Average` dan `pNN.NN` (persentil).

Dimensi: `InstanceType` dan `OutpostId`

`InstanceTypeCapacityUtilization`

Persentase kapasitas instance yang digunakan. Metrik ini tidak termasuk kapasitas untuk Host Khusus yang dikonfigurasi di Outpost.

Satuan: Persen

Resolusi maksimum: 5 menit

Statistics: Statistik yang paling berguna adalah `Average` dan `pNN.NN` (persentil).

Dimensi:`Account`,`InstanceType`, dan `OutpostId`

`UsedInstanceType_Count`

Jumlah jenis instans yang saat ini digunakan, termasuk jenis instans apa pun yang digunakan oleh layanan terkelola seperti Amazon Relational Database Service (Amazon RDS) atau Application Load Balancer. Metrik ini tidak termasuk kapasitas untuk Host Khusus yang dikonfigurasi di Outpost.

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi:`Account`,`InstanceType`, dan `OutpostId`

`AvailableInstanceType_Count`

Jumlah jenis instance yang tersedia. Metrik ini termasuk `AvailableReservedInstances` hitungan.

Untuk menentukan jumlah instance yang dapat Anda pesan, kurangi `AvailableReservedInstances` hitungan dari hitungan. `AvailableInstanceType_Count`

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

Metrik ini tidak termasuk kapasitas untuk Host Khusus yang dikonfigurasi di Outpost.

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi: `InstanceType` dan `OutpostId`

`AvailableReservedInstances`

Jumlah instans yang tersedia untuk diluncurkan ke kapasitas komputasi yang dicadangkan menggunakan Reservasi Kapasitas.

Metrik ini tidak termasuk Instans EC2 Cadangan Amazon.

Metrik ini tidak termasuk jumlah instance yang dapat Anda pesan. Untuk menentukan berapa banyak instance yang dapat Anda pesan, kurangi `AvailableReservedInstances` hitungan dari hitungan. `AvailableInstanceType_Count`

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi: `InstanceType` dan `OutpostId`

`UsedReservedInstances`

Jumlah instans yang berjalan dalam kapasitas komputasi yang dicadangkan menggunakan Reservasi Kapasitas. Metrik ini tidak termasuk Instans EC2 Cadangan Amazon.

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi: `InstanceType` dan `OutpostId`

`TotalReservedInstances`

Jumlah total instans, berjalan dan tersedia untuk peluncuran, disediakan oleh kapasitas komputasi yang dicadangkan menggunakan Reservasi Kapasitas. Metrik ini tidak termasuk Instans EC2 Cadangan Amazon.

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi: `InstanceType` dan `OutpostId`

`EBSVolumeTypeCapacityUtilization`

Persentase kapasitas tipe volume EBS yang digunakan.

Satuan: Persen

Resolusi maksimum: 5 menit

Statistics: Statistik yang paling berguna adalah `Average` dan `pNN.NN` (persentil).

Dimensi: `VolumeType` dan `OutpostId`

`EBSVolumeTypeCapacityAvailability`

Persentase kapasitas tipe volume EBS yang tersedia.

Satuan: Persen

Resolusi maksimum: 5 menit

Statistics: Statistik yang paling berguna adalah `Average` dan `pNN.NN` (persentil).

Dimensi: `VolumeType` dan `OutpostId`

`EBSVolumeTypeCapacityUtilizationGB`

Jumlah gigabyte yang digunakan untuk tipe volume EBS.

Satuan: Gigabyte

Resolusi maksimum: 5 menit

Statistics: Statistik yang paling berguna adalah `Average` dan `pNN.NN` (persentil).

Dimensi: `VolumeType` dan `OutpostId`

`EBSVolumeTypeCapacityAvailabilityGB`

Jumlah gigabyte kapasitas yang tersedia untuk tipe volume EBS.

Satuan: Gigabyte

Resolusi maksimum: 5 menit

Statistics: Statistik yang paling berguna adalah `Average` dan `pNN.NN` (persentil).

Dimensi: `VolumeType` dan `OutpostId`

Dimensi metrik

Untuk memfilter metrik untuk Outpost Anda, gunakan dimensi berikut.

Dimensi	Deskripsi
`Account`	Akun atau layanan menggunakan kapasitas.
`InstanceFamily`	Keluarga contoh.
`InstanceType`	Tipe instans.
`OutpostId`	ID Pos Terdepan.
`VolumeType`	Jenis volume EBS.
`VirtualInterfaceId`	ID gateway lokal atau tautan layanan Virtual Interface (VIF).
`VirtualInterfaceGroupId`	ID grup antarmuka virtual untuk gateway lokal Virtual Interface (VIF).

Anda dapat melihat CloudWatch metrik untuk server Outposts Anda menggunakan CloudWatch konsol.

Untuk melihat metrik menggunakan konsol CloudWatch

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Metrik.
3. Pilih namespace Outposts.
4. (Opsional) Untuk melihat metrik di semua dimensi, masukkan namanya di kolom pencarian.

Untuk melihat metrik menggunakan AWS CLI

Gunakan perintah daftar-metrik berikut untuk membuat daftar metrik yang tersedia.

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

Untuk mendapatkan statistik untuk metrik menggunakan AWS CLI

Gunakan get-metric-statisticsperintah berikut untuk mendapatkan statistik untuk metrik dan dimensi yang ditentukan. CloudWatch memperlakukan setiap kombinasi dimensi yang unik sebagai metrik terpisah. Anda tidak dapat mengambil statistik menggunakan kombinasi dimensi yang diterbitkan secara khusus. Anda harus menentukan dimensi yang sama yang digunakan saat metrik dibuat.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/Outposts --metric-name InstanceTypeCapacityUtilization \
--statistics Average --period 3600 \
--dimensions Name=OutpostId,Value=op-01234567890abcdef
 Name=InstanceType,Value=c5.xlarge \
--start-time 2019-12-01T00:00:00Z --end-time 2019-12-08T00:00:00Z
```

Log panggilan AWS Outposts API menggunakan AWS CloudTrail

AWS Outposts terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan. CloudTrail menangkap panggilan API untuk AWS Outposts sebagai acara. Panggilan yang diambil termasuk panggilan dari AWS Outposts konsol dan panggilan kode ke operasi AWS Outposts API. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AWS Outposts, alamat IP dari mana permintaan dibuat, kapan dibuat, dan detail tambahan.

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

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna.
- Apakah permintaan dibuat atas nama pengguna IAM Identity Center.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

CloudTrail aktif di AWS akun Anda saat Anda membuat akun, dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat

dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara CloudTrail Danau.

CloudTrail jalan setapak

Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan AWS Management Console Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak. Wilayah AWS Untuk informasi selengkapnya tentang jejak, lihat Membuat jejak untuk Anda Akun AWS dan Membuat jejak untuk organisasi di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

CloudTrail Penyimpanan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail Lake mengonversi peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat Bekerja dengan AWS CloudTrail Danau di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara danau dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

AWS Outposts acara manajemen di CloudTrail

Acara manajemen memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di Anda Akun AWS. Ini juga dikenal sebagai operasi pesawat kontrol. Secara default, CloudTrail mencatat peristiwa manajemen.

AWS Outposts mencatat semua operasi pesawat kontrol AWS Outposts sebagai peristiwa manajemen. Untuk daftar operasi bidang kontrol AWS Outposts yang dicatat oleh AWS Outposts, CloudTrail lihat Referensi API AWS Outposts.

AWS Outposts contoh acara

Contoh berikut menunjukkan CloudTrail peristiwa yang menunjukkan `SetSiteAddress` operasi.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
```

```
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Di bawah model tanggung jawab bersama model , AWS bertanggung jawab atas perangkat keras dan perangkat lunak yang menjalankan AWS layanan. Ini berlaku untuk AWS Outposts, seperti halnya untuk AWS Wilayah. Misalnya, AWS mengelola patch keamanan, memperbarui firmware, dan memelihara peralatan Outpost. AWS juga memantau kinerja, kesehatan, dan metrik untuk server Outposts Anda dan menentukan apakah pemeliharaan diperlukan.

> **Warning**
>
> Data pada volume penyimpanan instance hilang jika drive disk yang mendasarinya gagal, atau jika instance berhenti, hibernasi, atau berakhir. Untuk mencegah kehilangan data, sebaiknya Anda mencadangkan data jangka panjang pada volume penyimpanan instans ke penyimpanan persisten, seperti bucket Amazon S3, volume Amazon EBS, atau perangkat penyimpanan jaringan di jaringan lokal Anda.

Daftar Isi

Perbarui detail kontak

Jika pemilik Outpost berubah, hubungi AWS Dukungan Pusat dengan nama pemilik baru dan informasi kontak.

Pemeliharaan perangkat keras

Jika AWS mendeteksi masalah perangkat keras yang tidak dapat diperbaiki selama proses penyediaan server atau saat menghosting instans Amazon yang EC2 berjalan di rak Outposts Anda, kami akan memberi tahu pemilik Outpost dan pemilik instans bahwa instans yang terpengaruh dijadwalkan untuk pensiun. Untuk informasi selengkapnya, lihat Pensiun instans di Panduan EC2 Pengguna Amazon.

Pemilik Outpost dan pemilik instans dapat bekerja sama untuk menyelesaikan masalah. Pemilik instans dapat menghentikan dan memulai instance yang terpengaruh untuk memigrasikannya ke kapasitas yang tersedia. Pemilik instans dapat menghentikan dan memulai instance yang terpengaruh pada waktu yang nyaman bagi mereka. Jika tidak, AWS hentikan dan mulai instance yang terpengaruh pada tanggal pensiun instans. Jika tidak ada kapasitas tambahan di Outpost, instance tetap dalam keadaan berhenti. Pemilik Pos Luar dapat mencoba membebaskan kapasitas bekas atau meminta kapasitas tambahan untuk Pos Luar sehingga migrasi dapat selesai.

Jika pemeliharaan perangkat keras diperlukan, AWS akan menghubungi pemilik Outpost untuk mengonfirmasi tanggal dan waktu bagi tim AWS instalasi untuk berkunjung. Kunjungan dapat dijadwalkan segera setelah dua hari kerja sejak pemilik Pos Luar berbicara dengan AWS tim.

Ketika tim AWS instalasi tiba di lokasi, mereka akan mengganti host, switch, atau elemen rak yang tidak sehat dan membawa kapasitas baru secara online. Mereka tidak akan melakukan diagnosa atau perbaikan perangkat keras apa pun di lokasi. Jika mereka mengganti host, mereka akan menghapus dan menghancurkan kunci keamanan fisik yang sesuai dengan NIST, secara efektif merobek-robek data apa pun yang mungkin tertinggal di perangkat keras. Ini memastikan bahwa tidak ada data yang meninggalkan situs Anda. Jika mereka mengganti perangkat jaringan Outpost, informasi konfigurasi jaringan mungkin ada di perangkat saat dihapus dari situs. Informasi ini mungkin termasuk alamat IP dan ASNs digunakan untuk membuat antarmuka virtual untuk mengonfigurasi jalur ke jaringan lokal Anda atau kembali ke Wilayah.

Pembaruan firmware

Memperbarui firmware Outpost biasanya tidak memengaruhi instance di Outpost Anda. Dalam kasus yang jarang terjadi bahwa kita perlu me-reboot peralatan Outpost untuk menginstal pembaruan, Anda akan menerima pemberitahuan pensiun instance untuk setiap instance yang berjalan pada kapasitas itu.

Pemeliharaan peralatan jaringan

Pemeliharaan Outpost Networking Devices (OND) dilakukan tanpa mempengaruhi operasi Outpost reguler dan lalu lintas. Jika pemeliharaan diperlukan lalu lintas bergeser dari OND. Anda mungkin melihat perubahan sementara dalam iklan BGP, seperti prepending AS-path, dan perubahan yang sesuai dalam pola lalu lintas pada uplink Outpost. Dengan pembaruan firmware OND, Anda mungkin melihat BGP mengepak.

Kami menyarankan Anda mengonfigurasi peralatan jaringan pelanggan untuk menerima iklan BGP dari Outposts tanpa mengubah atribut BGP, dan mengaktifkan BGP multipath/load balancing untuk mencapai arus lalu lintas masuk yang optimal. As-path prepending digunakan untuk awalan gateway lokal untuk mengalihkan lalu lintas dari ONDs jika pemeliharaan diperlukan. Jaringan pelanggan harus memilih rute dari Outposts dengan panjang AS-path 1 daripada rute dengan panjang AS-path 4.

Jaringan pelanggan harus mengiklankan awalan BGP yang sama dengan atribut yang sama untuk semua. ONDs Beban jaringan Outpost menyeimbangkan lalu lintas keluar antara semua uplink secara default. Kebijakan routing digunakan di sisi Outpost untuk mengalihkan lalu lintas dari OND jika pemeliharaan diperlukan. Pergeseran lalu lintas ini membutuhkan awalan BGP yang sama dari sisi pelanggan. ONDs Jika pemeliharaan diperlukan pada jaringan pelanggan, kami sarankan Anda menggunakan AS-path prepending untuk sementara mengalihkan array lalu lintas dari uplink tertentu.

Praktik terbaik untuk acara listrik dan jaringan

Sebagaimana dinyatakan dalam Ketentuan AWS Layanan untuk AWS Outposts pelanggan, fasilitas tempat peralatan Outposts berada harus memenuhi persyaratan daya dan jaringan minimum untuk mendukung pemasangan, pemeliharaan, dan penggunaan peralatan Outposts. rak Outposts dapat beroperasi dengan benar hanya ketika daya dan konektivitas jaringan tidak terganggu.

Peristiwa kekuasaan

Dengan pemadaman listrik total, ada risiko yang melekat bahwa AWS Outposts sumber daya mungkin tidak kembali ke layanan secara otomatis. Selain menerapkan daya redundan dan solusi daya cadangan, kami menyarankan Anda melakukan hal berikut terlebih dahulu untuk mengurangi dampak dari beberapa skenario terburuk:

- Pindahkan layanan dan aplikasi Anda dari peralatan Outposts dengan cara yang terkontrol, menggunakan perubahan load-balancing berbasis DNS atau off-rack.
- Hentikan kontainer, instance, database secara bertahap dan gunakan urutan terbalik saat memulihkannya.
- Uji rencana untuk pemindahan atau penghentian layanan yang terkontrol.
- Buat cadangan data dan konfigurasi penting dan simpan di luar Outposts.
- Pertahankan waktu henti daya seminimal mungkin.
- Hindari pengalihan berulang dari umpan daya (off-on-off-on) selama pemeliharaan.

- Berikan waktu ekstra dalam jendela pemeliharaan untuk menangani hal yang tidak terduga.
- Kelola harapan pengguna dan pelanggan Anda dengan mengkomunikasikan kerangka waktu jendela pemeliharaan yang lebih luas daripada yang biasanya Anda butuhkan.
- Setelah daya dipulihkan, buat case di AWS Dukungan Center untuk meminta verifikasi bahwa AWS Outposts dan layanan terkait sedang berjalan.

Acara konektivitas jaringan

Koneksi tautan layanan antara Outpost Anda dan AWS Wilayah atau Outposts home Region biasanya akan secara otomatis pulih dari gangguan jaringan atau masalah yang mungkin terjadi di perangkat jaringan perusahaan hulu Anda atau di jaringan penyedia konektivitas pihak ketiga mana pun setelah pemeliharaan jaringan selesai. Selama koneksi tautan layanan tidak aktif, operasi Outposts Anda terbatas pada aktivitas jaringan lokal.

EC2 Instans Amazon, gateway lokal, dan volume Amazon EBS di Outposts akan terus beroperasi secara normal dan dapat diakses secara lokal melalui jaringan lokal. Demikian pula, sumber daya AWS layanan seperti node pekerja Amazon ECS terus berjalan secara lokal. Namun, ketersediaan API akan terdegradasi. Misalnya, run, start, stop, dan terminate APIs mungkin tidak berfungsi. Metrik dan log instans akan terus di-cache secara lokal hingga 7 hari, dan akan didorong ke AWS Wilayah saat konektivitas kembali. Pemutusan lebih dari 7 hari dapat mengakibatkan hilangnya metrik dan log.

Untuk informasi selengkapnya, lihat pertanyaan Apa yang terjadi ketika koneksi jaringan fasilitas saya mati? di FAQs halaman AWS Outposts rak.

Jika tautan layanan tidak aktif karena masalah daya di tempat atau hilangnya konektivitas jaringan, maka akan AWS Health Dashboard mengirimkan pemberitahuan ke akun yang memiliki Outposts. Baik Anda maupun tidak AWS dapat menekan pemberitahuan gangguan tautan layanan, bahkan jika gangguan diharapkan. Untuk informasi selengkapnya, lihat Memulai dengan Anda AWS Health Dashboard di Panduan AWS Health Pengguna.

Dalam hal pemeliharaan layanan terencana yang akan memengaruhi konektivitas jaringan, ambil langkah-langkah proaktif berikut untuk membatasi dampak skenario bermasalah potensial:

- Jika rak Outposts Anda terhubung ke AWS Wilayah induk melalui Internet atau Direct Connect publik, maka sebelum pemeliharaan yang direncanakan, tangkap rute jejak. Memiliki jalur jaringan (pre-network-maintenance) yang berfungsi dan jalur jaringan (post-network-maintenance) yang

bermasalah untuk mengidentifikasi perbedaan akan membantu dalam pemecahan masalah. Jika Anda meningkatkan masalah pasca-pemeliharaan ke AWS atau ISP Anda, Anda dapat menyertakan informasi ini.

Tangkap rute jejak antara:

- Alamat IP publik di lokasi Outposts dan alamat IP yang dikembalikan oleh. `outposts.region.amazonaws.com` Ganti *`region`* dengan nama AWS Wilayah induk.
- Setiap contoh di Wilayah induk dengan konektivitas Internet publik dan alamat IP publik di lokasi Outposts.

- Jika Anda mengendalikan pemeliharaan jaringan, batasi durasi downtime untuk tautan layanan. Sertakan langkah dalam proses pemeliharaan Anda yang memverifikasi bahwa jaringan telah pulih.
- Jika Anda tidak mengendalikan pemeliharaan jaringan, pantau downtime tautan layanan sehubungan dengan jendela pemeliharaan yang diumumkan dan eskalasi lebih awal kepada pihak yang bertanggung jawab atas pemeliharaan jaringan yang direncanakan jika tautan layanan tidak dicadangkan pada akhir jendela pemeliharaan yang diumumkan.

Sumber daya

Berikut adalah beberapa sumber daya terkait pemantauan yang dapat memberikan jaminan bahwa Outposts beroperasi secara normal setelah peristiwa listrik atau jaringan yang direncanakan atau tidak direncanakan:

- AWS Blog Pemantauan praktik terbaik untuk AWS Outposts mencakup observabilitas dan praktik terbaik manajemen acara khusus untuk Outposts.
- Alat debugging AWS blog untuk konektivitas jaringan dari Amazon VPC menjelaskan AWSSupport-SetupIPMonitoringFromVPCalat ini. Alat ini adalah AWS Systems Manager dokumen (dokumen SSM) yang membuat Instans EC2 Monitor Amazon di subnet yang ditentukan oleh Anda dan memantau alamat IP target. Dokumen menjalankan tes diagnostik ping, MTR, TCP trace-route dan trace-path dan menyimpan hasilnya di Amazon CloudWatch Logs yang dapat divisualisasikan di CloudWatch dasbor (misalnya latensi, kehilangan paket). Untuk pemantauan Outposts, Instans Monitor harus berada di satu subnet dari AWS Wilayah induk dan dikonfigurasi untuk memantau satu atau lebih instance Outpost Anda menggunakan IP pribadinya - ini akan memberikan grafik kehilangan paket dan latensi antara dan Wilayah induk. AWS Outposts AWS
- AWS Blog Menyebarkan CloudWatch dasbor Amazon otomatis untuk AWS Outposts digunakan AWS CDK menjelaskan langkah-langkah yang terlibat dalam menerapkan dasbor otomatis.

- Jika Anda memiliki pertanyaan atau memerlukan informasi selengkapnya, lihat Membuat kasus AWS dukungan di Panduan Pengguna Support.

Opsi rak Outposts end-of-term

Di akhir AWS Outposts masa jabatan Anda, Anda harus memilih di antara opsi-opsi berikut:

- Perbarui langganan Anda dan pertahankan rak Outposts yang ada.
- Akhiri langganan Anda dan siapkan rak Outposts Anda untuk kembali.
- Konversikan ke month-to-month langganan dan simpan rak Outposts yang ada.

Perbarui langganan Anda

Anda harus menyelesaikan langkah-langkah berikut setidaknya 30 hari sebelum langganan saat ini untuk rak Outposts Anda berakhir.

Untuk memperbarui langganan Anda dan menyimpan rak Outposts yang ada

1. Masuk ke Konsol AWS Dukungan Tengah.
2. Pilih Buat kasus.
3. Pilih Akun dan penagihan.
4. Untuk Layanan, pilih Penagihan.
5. Untuk Kategori, pilih Pertanyaan Penagihan Lainnya.
6. Untuk Keparahan, pilih Pertanyaan penting.
7. Pilih Langkah selanjutnya: Informasi tambahan.
8. Pada halaman Informasi tambahan, untuk Subjek, masukkan permintaan Anda untuk memperbarui seperti**`Renew my Outpost subscription`**.
9. Untuk Deskripsi, masukkan salah satu opsi pembayaran berikut:

   - Tidak ada di muka
   - Sebagian di muka
   - Semua dimuka

   Untuk harga, lihat harga AWS Outposts rak. Anda juga dapat meminta penawaran harga.
10. Pilih Langkah selanjutnya: Selesaikan sekarang atau hubungi kami.
11. Pada halaman Hubungi kami, pilih bahasa pilihan Anda.

12. Pilih metode kontak pilihan Anda.
13. Tinjau detail kasus Anda dan kemudian pilih Kirim. Nomor ID kasus dan ringkasan muncul.

AWS Customer Support akan memulai proses perpanjangan langganan. Langganan baru Anda akan dimulai sehari setelah langganan Anda saat ini berakhir.

Jika Anda tidak menunjukkan bahwa Anda ingin memperbarui langganan atau mengembalikan rak Outposts Anda, Anda akan dikonversi ke month-to-month langganan secara otomatis. Rak Outposts Anda akan diperbarui setiap bulan dengan tarif opsi pembayaran No Upfront yang sesuai dengan konfigurasi Anda. AWS Outposts Langganan bulanan baru Anda akan dimulai sehari setelah langganan Anda saat ini berakhir.

Akhiri langganan Anda dan siapkan rak untuk dikembalikan

Anda harus menyelesaikan langkah-langkah berikut setidaknya 30 hari sebelum langganan saat ini untuk rak Outposts Anda berakhir. AWS tidak dapat memulai proses pengembalian sampai Anda melakukannya.

> **Important**
>
> AWS tidak dapat menghentikan proses pengembalian setelah Anda membuka kasus dukungan untuk mengakhiri langganan Anda.

Untuk mengakhiri langganan Anda

1. Masuk ke Konsol AWS Dukungan Tengah.
2. Pilih Buat kasus.
3. Pilih Akun dan penagihan.
4. Untuk Layanan, pilih Penagihan.
5. Untuk Kategori, pilih Pertanyaan Penagihan Lainnya.
6. Untuk Keparahan, pilih Pertanyaan penting.
7. Pilih Langkah selanjutnya: Informasi tambahan.
8. Pada halaman Informasi tambahan, untuk Subjek, masukkan permintaan yang jelas, seperti**`End my Outpost subscription`**.

9. Untuk Deskripsi, masukkan tanggal yang Anda inginkan agar Pos Luar diambil.
10. Pilih Langkah selanjutnya: Selesaikan sekarang atau hubungi kami.
11. Pada halaman Hubungi kami, pilih bahasa pilihan Anda.
12. Pilih metode kontak pilihan Anda.
13. Tinjau detail kasus Anda dan kemudian pilih Kirim. Nomor ID kasus dan ringkasan muncul.

AWS Customer Support akan menghubungi Anda untuk mengoordinasikan pengambilan.

Untuk mempersiapkan AWS Outposts rak Anda untuk kembali:

> **Important**
>
> Jangan matikan rak Outposts sampai AWS berada di tempat untuk pengambilan yang dijadwalkan.

1. Jika sumber daya Outpost dibagikan, Anda harus membatalkan pembagian sumber daya ini.

   Anda dapat membatalkan pembagian sumber daya Outpost bersama dengan salah satu cara berikut:

   - Gunakan AWS RAM konsol. Untuk informasi selengkapnya, lihat Memperbarui pembagian sumber daya di Panduan AWS RAM Pengguna.
   - Gunakan AWS CLI untuk menjalankan disassociate-resource-shareperintah.

   Untuk daftar sumber daya Outpost yang dapat dibagikan, lihat Sumber daya Pos Luar yang Dapat Dibagikan.
2. Hentikan instans aktif yang terkait dengan subnet di Outpost Anda. Untuk menghentikan instans, ikuti petunjuk di Menghentikan instans Anda di Panduan Pengguna Amazon EC2 .

   > **Note**
   >
   > Beberapa layanan AWS terkelola yang berjalan di Outpost Anda, seperti Application Load Balancers atau Amazon Relational Database Service (RDS), menggunakan kapasitas. EC2 Namun, instance terkait mereka tidak terlihat di EC2 dasbor Amazon. Anda harus menghentikan sumber daya yang terkait dengan layanan ini untuk

membebaskan kapasitas. Untuk informasi lebih lanjut, lihat [Mengapa beberapa kapasitas EC2 instance hilang di Pos Luar saya](#)? .

3. instance-capacity-availabilityVerifikasi EC2 instans Amazon Anda di AWS akun Anda.

   a. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.

   b. Pilih Outposts.

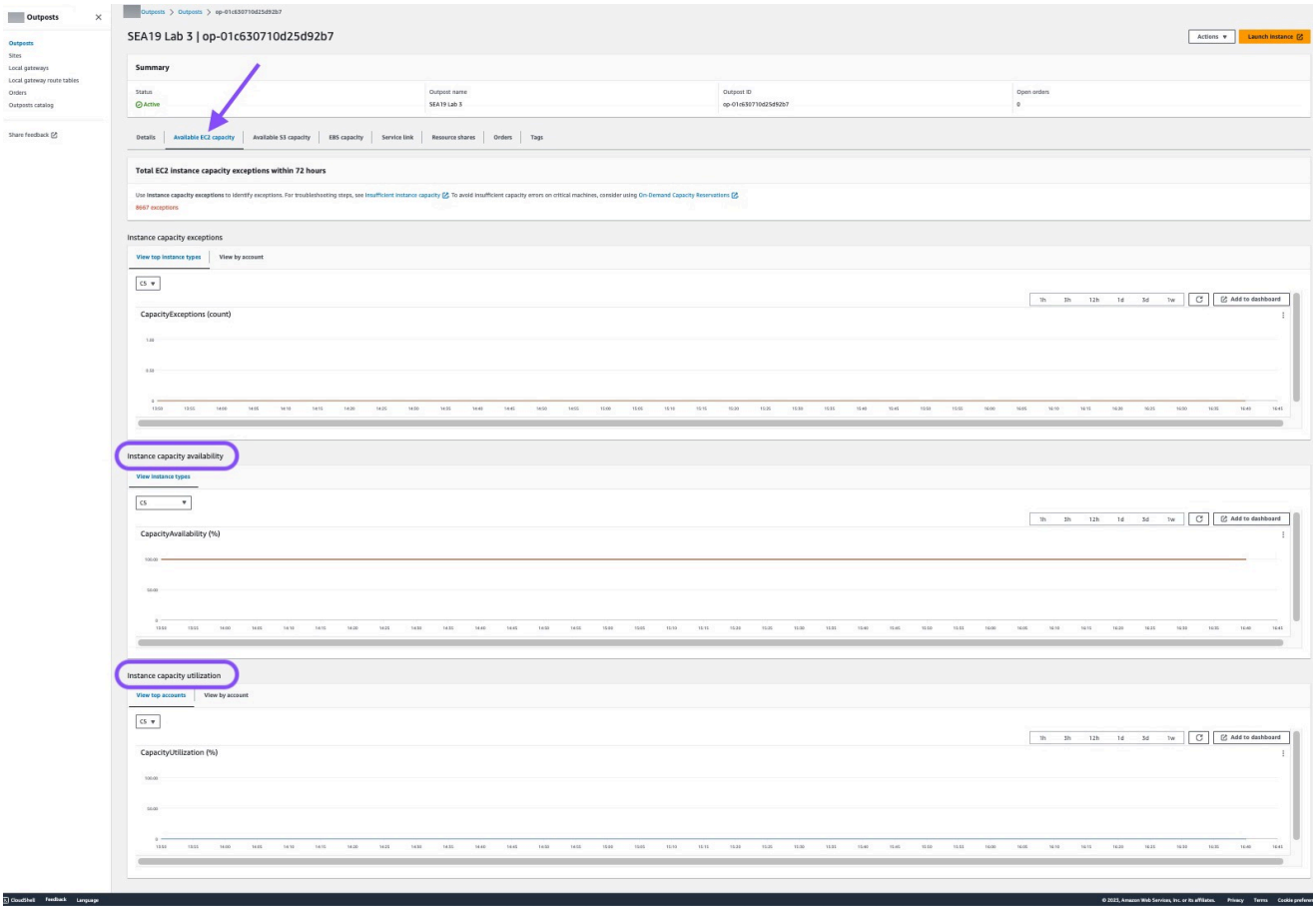
   c. Pilih Outpost spesifik yang akan Anda kembalikan.

   d. Pada halaman untuk Outpost, pilih tab EC2 Kapasitas yang tersedia.

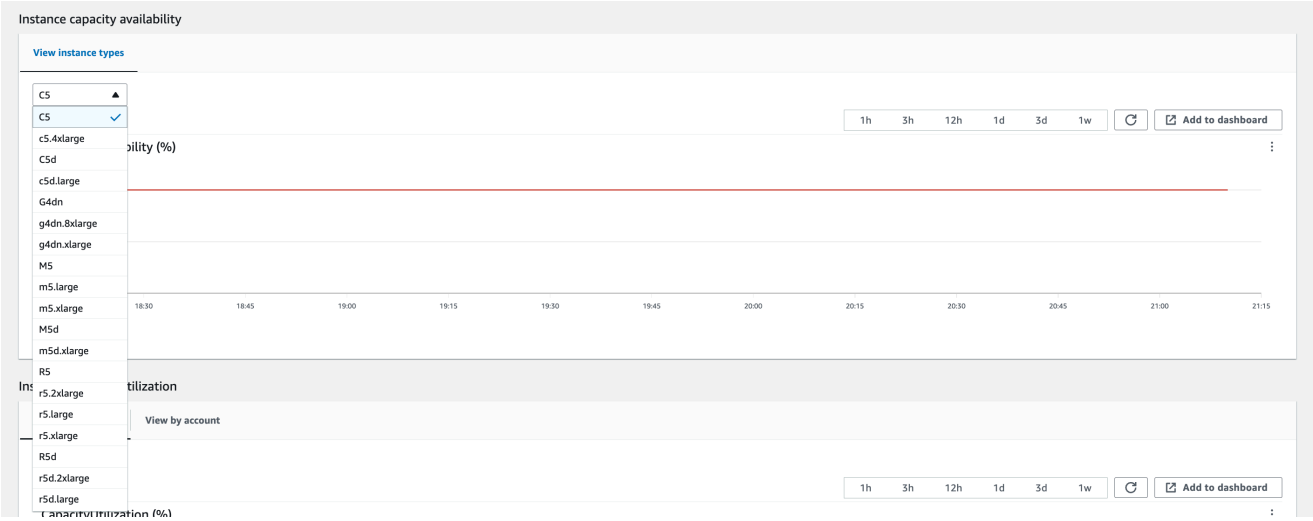
   e. Pastikan ketersediaan kapasitas Instans 100% untuk setiap keluarga instans.

   f. Pastikan bahwa pemanfaatan kapasitas Instans adalah 0% untuk setiap keluarga instance.

   Gambar berikut menunjukkan ketersediaan kapasitas Instans dan grafik pemanfaatan kapasitas Instans pada tab EC2Kapasitas yang tersedia.



Gambar berikut menunjukkan daftar jenis contoh.



4. Buat cadangan EC2 instans Amazon dan volume server Anda. Untuk membuat cadangan, ikuti petunjuk di Backup dan recovery untuk Amazon EC2 dengan volume EBS di panduan panduan AWS preskriptif.
5. Hapus volume Amazon EBS yang terkait dengan Outpost Anda.
   a. Buka konsol EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
   b. Dari panel navigasi, pilih Volume.
   c. Pilih Tindakan dan Hapus volume.
   d. Di kotak dialog konfirmasi, pilih Hapus.
6. Jika Anda memiliki Amazon S3 di Outposts, hapus snapshot lokal apa pun di Outposts.
   a. Buka konsol EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
   b. Dari panel navigasi, pilih Snapshots.
   c. Pilih snapshot dengan Outpost ARN.
   d. Pilih Tindakan dan Hapus snapshot.
   e. Di kotak dialog konfirmasi, pilih Hapus.
7. Hapus bucket Amazon S3 apa pun yang terkait dengan rak Outposts Anda. Untuk menghapus bucket, ikuti petunjuk di Menghapus bucket Amazon S3 on Outposts di Amazon S3 on Outposts User Guide.
8. Hapus asosiasi VPC dan kumpulan alamat IP (CoIP) CIDRs milik pelanggan yang terkait dengan Outpost Anda.

Tim AWS pengambilan akan mematikan rak. Setelah dimatikan, Anda dapat menghancurkan Kunci Keamanan AWS Nitro atau tim AWS pengambilan dapat melakukannya atas nama Anda.

Konversi ke month-to-month langganan

Untuk mengonversi ke month-to-month langganan dan menyimpan rak Outposts yang ada, tidak diperlukan tindakan. Jika Anda memiliki pertanyaan, buka kasus dukungan penagihan.

Rak Outposts Anda akan diperbarui setiap bulan dengan tarif opsi pembayaran No Upfront yang sesuai dengan konfigurasi Outposts Anda. Langganan bulanan baru Anda dimulai sehari setelah langganan Anda saat ini berakhir.

Kuota untuk AWS Outposts

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk masing-masing. Layanan AWS Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta kenaikan untuk beberapa kuota, tetapi tidak untuk semua kuota.

Untuk melihat kuota AWS Outposts, buka konsol Service Quotas. Di panel navigasi, pilih Layanan AWS, dan pilih AWS Outposts.

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

Anda Akun AWS memiliki kuota berikut yang terkait AWS Outposts dengan.

Sumber Daya	Default	Dapat disesuaikan	Komentar
Situs pos terdepan	100	Ya	Situs Outpost adalah bangunan fisik yang dikelola pelanggan di mana Anda memberi daya dan memasang peralatan Outpost Anda ke jaringan. Anda dapat memiliki 100 situs Outposts di setiap Wilayah akun Anda AWS .
Outposts per situs	10	Ya	AWS Outposts termasuk perangkat keras dan sumber daya virtual, yang dikenal sebagai Outposts. Kuota ini membatasi sumber daya virtual Outpost Anda. Anda dapat memiliki 10 Outposts di setiap situs Outpost.

AWS Outposts dan kuota untuk layanan lainnya

AWS Outposts bergantung pada sumber daya layanan lain dan layanan tersebut mungkin memiliki kuota default mereka sendiri. Misalnya, kuota Anda untuk antarmuka jaringan lokal berasal dari kuota VPC Amazon untuk antarmuka jaringan.

Perubahan	Deskripsi	Tanggal
Pembaruan stabilitas statis	Jika jaringan Anda terganggu , metrik dan log instans akan di-cache secara lokal hingga 7 hari. Sebelumnya, Outposts bisa cache log hanya beberapa jam.	1 Mei 2025
Pembaruan untuk peran AWS Identity and Access Management terkait layanan _ AWSService RoleForOutposts *OutpostID*	Izin peran *OutpostID* terkait layanan AWSServic eRoleForOutposts_ diperbaru i untuk menyempurnakan cara AWS Outposts mengelola sumber daya jaringan untuk konektivitas pribadi, dengan kontrol yang lebih tepat atas antarmuka jaringan dan operasi grup keamanan yang diperlukan untuk instance titik akhir tautan layanan.	17 April 2025
Manajemen kapasitas di tingkat aset	Anda dapat memodifikasi konfigurasi kapasitas di tingkat aset.	Maret 31, 2025
Konektivitas pribadi menggunakan AWS Direct Connect transit VIF	Anda sekarang dapat mengonfigurasi tautan layanan untuk menggunakan VIF AWS Direct Connect transit untuk mengaktifkan konektivitas pribadi antara Outposts dan Wilayah asal. AWS	Desember 11, 2024

Volume blok eksternal yang didukung oleh penyimpanan pihak ketiga	Anda sekarang dapat melampirkan volume data blok yang didukung oleh sistem penyimpanan blok pihak ketiga yang kompatibel selama proses peluncuran instans di Outpost.	Desember 1, 2024
Manajemen kapasitas	Anda dapat memodifikasi konfigurasi kapasitas untuk sebuah instance.	November 11, 2024
Manajemen kapasitas	Anda dapat memodifikasi konfigurasi kapasitas default untuk pesanan Outposts baru Anda.	16 April 2024
AWS Outposts rack mendukung metrik throughput antarmuka tautan layanan	Anda sekarang dapat memantau penggunaan throughput antara antarmuka virtual tautan layanan rak Outposts VIFs () dan perangkat jaringan lokal Anda, dengan `IfTrafficIn` memanfaatkan dan metrik. `IfTrafficOut` Amazon CloudWatch	17 November 2023
Komunikasi intra-VPC dengan gateway lokal AWS Outposts	Anda dapat menjalin komunikasi antar subnet dalam VPC yang sama di Outposts yang berbeda dengan gateway lokal.	Agustus 30, 2023

End-of-term pilihan untuk AWS Outposts rak	Di akhir AWS Outposts jangka waktu Anda, Anda dapat memperbarui, mengakhiri, atau mengonversi langganan Anda.	1 Agustus 2023
Amazon Route 53 di Outposts tersedia di AWS Outposts rak.	Amazon Route 53 di Outposts menyertakan Resolver yang menyimpan semua kueri DNS yang berasal dari file. AWS Outposts Anda juga dapat mengatur konektivitas hibrid antara Outpost dan resolver DNS lokal saat menerapkan titik akhir masuk dan keluar.	Juli 20, 2023
Rute masuk gerbang lokal	Anda dapat membuat dan memodifikasi rute masuk gateway lokal ke antarmuka jaringan elastis di Outpost Anda.	15 September 2022
Memperkenalkan perutean VPC langsung untuk AWS Outposts	Menggunakan alamat IP pribadi instance di VPC Anda untuk memfasilitasi komunikasi dengan jaringan lokal Anda.	14 September 2022
Panduan AWS Outposts Pengguna yang Dibuat untuk rak Outposts	AWS Outposts Panduan Pengguna memecah menjadi panduan terpisah untuk rak dan server.	14 September 2022
Membuat dan mengelola tabel rute gateway lokal	Membuat dan memodifikasi tabel rute gateway lokal dan kumpulan CoIP. Kelola asosiasi grup VIF.	14 September 2022

Grup penempatan di AWS Outposts	Grup penempatan yang menggunakan strategi spread dapat mendistribusikan instans di seluruh host.	30 Juni 2022
Tuan Rumah Khusus di AWS Outposts	Anda sekarang dapat menggunakan Host Khusus di Outposts.	31 Mei 2022
Situs pos terdepan bersama	Buat dan kelola situs Outpost dan bagikan dengan AWS akun lain di organisasi Anda.	Oktober 18, 2021
CloudWatch Dimensi baru	CloudWatch Dimensi baru untuk metrik di AWS Outposts namespace.	13 Oktober 2021
Bagikan ember S3	Bagikan dan kelola bucket S3 di Outpost Anda.	5 Agustus 2021
Support untuk beberapa grup penempatan	Anda dapat menggunakan strategi penempatan cluster, partisi, atau spread seperti yang Anda lakukan di Region.	28 Juli 2021
CloudWatch Metrik tambahan	CloudWatch Metrik tambahan tersedia untuk Instans Cadangan.	24 Mei 2021
Daftar periksa pemecahan masalah jaringan	Daftar periksa pemecahan masalah jaringan tersedia.	22 Februari 2021
CloudWatch Metrik tambahan	CloudWatch Metrik tambahan untuk volume EBS tersedia.	2 Februari 2021
Pembaruan pemesanan konsol	Proses pemesanan konsol diperbarui.	Januari 14, 2021

Konektivitas pribadi	Anda dapat mengonfigurasi konektivitas pribadi untuk Outpost Anda saat Anda membuatnya di AWS Outposts konsol.	21 Desember 2020
Daftar periksa kesiapan jaringan	Gunakan daftar periksa kesiapan jaringan saat Anda mengumpulkan informasi untuk konfigurasi Outpost Anda.	28 Oktober 2020
AWS Outposts Sumber daya bersama	Dengan berbagi Outpost, pemilik Outpost dapat membagikan sumber daya Outpost dan Outpost mereka, termasuk tabel rute gateway lokal, dengan AWS akun lain di bawah organisasi yang sama. AWS	15 Oktober 2020
CloudWatch Metrik tambahan	CloudWatch Metrik tambahan untuk jumlah tipe misalnya tersedia.	21 September 2020
CloudWatch Metrik tambahan	CloudWatch Metrik tambahan untuk status terhubung tautan layanan tersedia.	11 September 2020
Support untuk berbagi alamat milik pelanggan IPv4	Gunakan AWS Resource Access Manager untuk berbagi alamat milik pelanggan IPv4 .	20 April 2020
CloudWatch Metrik tambahan	CloudWatch Metrik tambahan untuk volume EBS tersedia.	April 4, 2020

Rilis awal	Ini adalah rilis awal dari AWS Outposts.	3 Desember 2019

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