Panduan Pengguna untuk server

AWS Outposts

AWS Outposts: Panduan Pengguna untuk server

Table of Contents

Apa itu AWS Outposts?

AWS Outposts adalah layanan yang dikelola sepenuhnya yang memperluas AWS infrastruktur, layanan, API, 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 Anda dan menentukannya saat Anda membuat AWS sumber daya seperti instans dan subnet EC2. Instans di subnet Outpost berkomunikasi dengan instans lain di Wilayah AWS menggunakan alamat IP privat, semuanya dalam VPC yang sama.

> **Note**
>
> Anda tidak dapat menghubungkan Pos Luar ke Pos Luar atau Zona Lokal 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.
- 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 pos terdepan termasuk server yang dapat dipasang di rak, sakelar, panel patch jaringan, rak daya, dan panel kosong.
- Anda harus memasang rak ACE jika Anda memiliki lima atau lebih rak komputasi. Jika Anda memiliki kurang dari lima rak komputasi tetapi berencana untuk memperluas ke lima rak atau lebih 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 Outpost menyediakan layanan komputasi dan jaringan lokal ke situs yang memiliki ruang terbatas atau persyaratan kapasitas yang lebih kecil.
- 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 Outpost dan jaringan lokal Anda.
- Antarmuka jaringan lokal — Antarmuka jaringan yang memungkinkan komunikasi dari server Outpost 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:

Hitung

Jenis sumber daya	Rak	Server
Instans Amazon EC2	Y	Ya

Jenis sumber daya	Rak	Server
Cluster Amazon ECS	Y	Ya
Node Amazon EKS	Y	Tidak

Database dan analitik

Jenis sumber daya	Rak	Server
ElastiCache Node Amazon (kluster Redis, kluster Memcached)	Y	Tidak
Cluster EMR Amazon	Y	Tidak
Instans Amazon RDS DB	Y	Tidak

Jaringan

Jenis sumber daya	Rak	Server
Proksi Utusan App Mesh	Y	Ya

Jenis sumber daya	Rak	Server
Penyeimbang Beban Aplikasi	 Y	 Tidak
Amazon VPC subnet	 Y	 Ya
Rute Amazon 53	 Y	 Tidak

Penyimpanan

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

Lainnya Layanan AWS

Layanan	Rak	Server
AWS IoT Greengrass	 Y	 Ya

Layanan	Rak	Server
Manajer Amazon SageMaker Edge	 Y	 Ya

Harga

Anda dapat memilih dari berbagai konfigurasi Outpost, masing-masing menyediakan kombinasi jenis instans EC2 dan opsi penyimpanan. Harga untuk konfigurasi rak termasuk pemasangan, pelepasan, dan pemeliharaan. Untuk server, Anda harus menginstal dan memelihara peralatan.

Anda membeli konfigurasi untuk jangka waktu 3 tahun dan dapat memilih dari tiga opsi pembayaran: All Upfront, Partial Upfront, dan No Upfront. Jika Anda memilih opsi Sebagian atau opsi Tanpa Pembayaran di Muka, biaya bulanan akan berlaku. Setiap biaya di muka berlaku 24 jam setelah Outpost Anda dipasang dan kapasitas komputasi dan penyimpanan tersedia untuk digunakan. Untuk informasi selengkapnya, lihat:

- AWS Outposts harga rak
- AWS Outposts harga server

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 dan ke internet. 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.

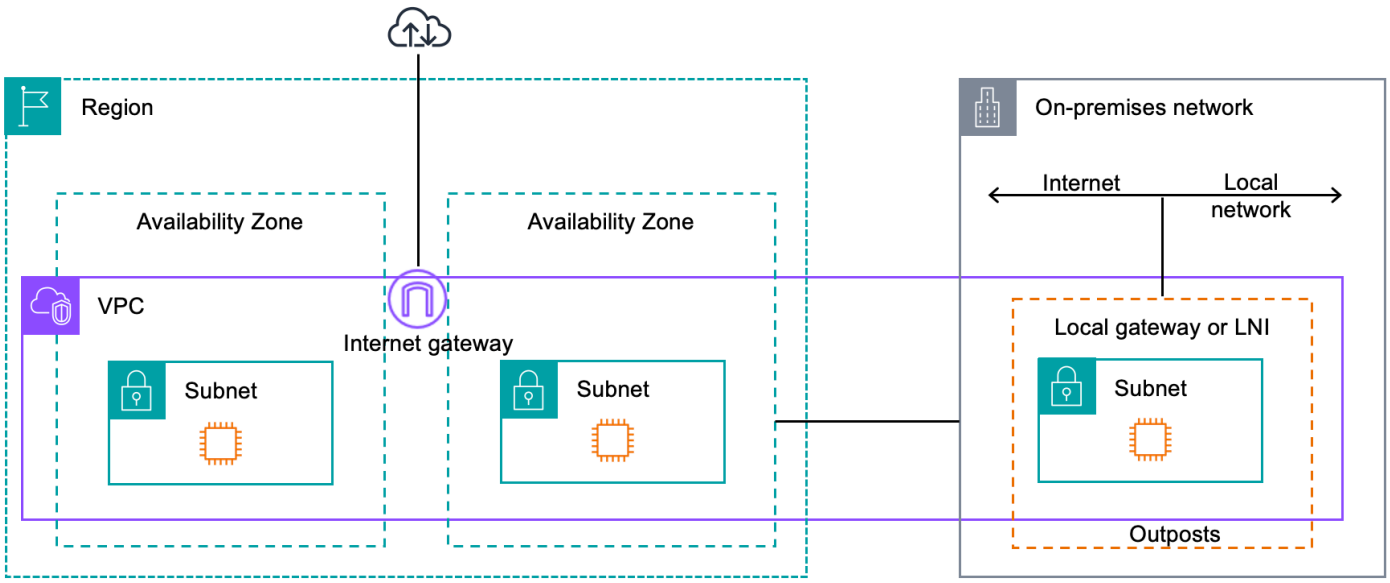
Daftar Isi

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 oleh gateway lokal (rak) atau antarmuka jaringan lokal (server)



VPC 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 instans EC2 saat meluncurkan instans EC2 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 VPC 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 instans EC2 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 VPC di Outpost yang sama, lalu lintas antara VPC tetap berada di Outpost dan tidak menggunakan tautan layanan kembali ke Wilayah.

DNS

Untuk antarmuka jaringan yang terhubung ke VPC, instans EC2 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 Outpost 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:

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

Antarmuka jaringan lokal

Server Outpost 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 instans EC2 di rak Outpost atau di AWS Wilayah. Antarmuka jaringan lokal dimaksudkan hanya untuk lokasi lokal. Untuk informasi selengkapnya, lihat Antarmuka jaringan lokal.

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

Halaman ini mencakup persyaratan untuk server Outposts. Untuk persyaratan rak Outposts, lihat Persyaratan situs untuk rak Outposts di rak AWS Outposts Panduan Pengguna untuk Outposts.

Fasilitas

Ini adalah persyaratan fasilitas untuk server.

> **Note**
>
> Spesifikasi untuk server dalam kondisi operasi normal. Misalnya, akustik mungkin terdengar lebih keras selama instalasi awal dan kemudian beroperasi pada daya suara terukur setelah instalasi selesai.

- Suhu — Suhu lingkungan harus antara 41—95° F (5—35° C).

  Server akan mati ketika suhu berada di luar kisaran ini dan akan restart ketika suhu kembali dalam kisaran.
- Kelembaban — Kelembaban relatif harus antara 8-80 persen tanpa kondensasi.
- Kualitas udara — Udara harus disaring menggunakan filter MERV8 (atau lebih tinggi).
- Aliran udara — Posisi server harus memastikan jarak minimum 6 inci (15 cm) antara server dan dinding di depan dan di belakang server untuk memungkinkan izin aliran udara yang cukup.
- Berat - Server 1U memiliki berat 26 pound dan server 2U memiliki berat 36 pound. Konfirmasikan bahwa lokasi tempat Anda ingin meletakkan server dapat mendukung bobot server.

  Untuk melihat persyaratan bobot untuk sumber daya Outposts yang berbeda, pilih Jelajahi katalog di AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
- Kompatibilitas rail-kit - Kit rel yang disertakan dalam paket pengiriman Anda kompatibel dengan braket pemasangan berbentuk L standar dari rak 19 inci yang sesuai dengan EIA-310-D.

> **Important**
>
> Kit rel tidak kompatibel dengan braket pemasangan berbentuk U seperti yang ditunjukkan pada gambar berikut.

- Penempatan Rak - Kami merekomendasikan penggunaan rak EIA-310D 19 inci standar, dengan kedalaman setidaknya 36 inci (914 mm).
  - Outposts 2U server membutuhkan ruang dengan dimensi sebagai berikut: tinggi 3,5 inci (88,9mm), lebar 17,5 inci (447 mm), kedalaman 30 inci (762 mm)
  - Outposts 1U server membutuhkan ruang dengan dimensi sebagai berikut: tinggi 1,75 inci (44,45 mm), lebar 17,5 inci (447 mm), kedalaman 24 inci (610 mm)

  > **Note**
  >
  > - Pemasangan AWS Outposts server secara vertikal tidak didukung.
  > - Server Outposts 1U memiliki lebar yang sama dengan server Outposts 2U, tetapi setengah tinggi dan kedalaman yang kurang

  AWS menyediakan kit rel untuk memasang rak server. Untuk informasi selengkapnya, lihat Langkah 3: Pemasangan rak.

  Jika Anda tidak menempatkan server di rak, Anda masih harus memenuhi persyaratan lain yang tercantum di bagian ini.
- Kemudahan servis - Server Outposts dapat diservis di lorong depan.
- Akustik - dinilai kurang dari 78 dBA daya suara pada suhu 80° F (27° C) dan memenuhi kepatuhan GR-63 CORE NEBS.
- Seismic bracing — Sejauh yang diperlukan oleh peraturan atau kode, Anda akan menginstal dan memelihara jangkar dan bracing seismik yang sesuai untuk server saat berada di fasilitas Anda.
- Ketinggian - Ketinggian ruangan tempat rak dipasang harus di bawah 10.005 kaki (3.050 meter).
- Pembersihan — Bersihkan permukaan dengan tisu basah yang mengandung bahan kimia pembersih antistatik yang disetujui.

Jaringan

Setiap server Outposts mencakup non-redundan. Port memiliki kecepatan dan persyaratan konektornya sendiri seperti yang dijelaskan di bawah ini.

Label port	Kecepatan	Konektor pada perangkat jaringan hulu	Lalu Lintas
Pelabuhan 3	10Gbe	SFP+	Baik layanan dan lalu lintas tautan LNI — lalu lintas segmen kabel breakout QSFP +(10 kaki/3 m). Untuk informasi selengkap nya, lihat Konfigura sikan jaringan QSFP.

Firewall tautan layanan

UDP dan TCP 443 harus terdaftar secara statis di firewall.

Protokol	Pelabuhan Sumber	Alamat Sumber	Pelabuhan Tujuan	Alamat Tujuan
UDP	1024-65535	Layanan Link IP	53	DHCP menyediakan server DNS
UDP	443, 1024-65535	Layanan Link IP	443	Titik akhir Tautan Layanan Outposts
TCP	1024-65535	Layanan Link IP	443	Titik akhir Pendaftar an Outposts

Anda dapat menggunakan AWS Direct Connect koneksi atau koneksi internet publik untuk menghubungkan Outpost kembali ke AWS Wilayah. Untuk konektivitas tautan layanan Outposts,

Anda dapat menggunakan NAT atau PAT di firewall atau router edge Anda. Pembentukan tautan layanan selalu dimulai dari Pos Terdepan.

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.

Rekomendasi bandwidth tautan layanan

Untuk pengalaman dan ketahanan yang optimal, AWS rekomendasikan agar Anda menggunakan konektivitas redundan minimal 500 Mbps untuk koneksi tautan layanan ke Wilayah. AWS Pemanfaatan maksimum untuk setiap server Outpost adalah 500 Mbps. Untuk meningkatkan kecepatan koneksi, gunakan beberapa server Outpost. Misalnya, jika Anda memiliki tiga AWS Outposts server, kecepatan koneksi maksimum meningkat menjadi 1,5 Gbps (1.500 Mbps). Untuk informasi selengkapnya, lihat Lalu lintas tautan layanan untuk server.

Persyaratan bandwidth tautan AWS Outposts layanan Anda bervariasi tergantung pada karakteristik beban kerja, seperti ukuran AMI, elastisitas aplikasi, kebutuhan kecepatan burst, dan lalu lintas VPC Amazon ke Wilayah. Perhatikan bahwa AWS Outposts server tidak men-cache AMI. AMI diunduh dari Wilayah dengan setiap peluncuran instans.

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

Tautan layanan membutuhkan respons DHCP

Tautan layanan memerlukan respons IPv4 DHCP untuk mengkonfigurasi pengaturan jaringan.

Latensi maksimum tautan layanan

Tautan layanan dapat mendukung latensi jaringan maksimum 250 ms dari server dan Availability Zone-nya.

Daya

Ini adalah persyaratan daya untuk server Outposts.

Persyaratan

Dukungan daya

Server diberi peringkat hingga 1600W 90-264 VAc 47/63 Hz daya AC.

Daya tarik

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

Kabel daya

Server dikirimkan dengan kabel daya IEC C14-C13.

Kabel daya dari server ke rak

Gunakan kabel daya IEC C14-C13 yang disediakan untuk menghubungkan server ke rak.

Kabel daya dari server ke stopkontak

Untuk menghubungkan server ke stopkontak standar, Anda harus menggunakan adaptor untuk saluran masuk C14 atau kabel daya khusus negara.

Pastikan Anda memiliki adaptor atau kabel daya yang benar untuk wilayah Anda untuk menghemat waktu selama instalasi server.

- Di Amerika Serikat, Anda memerlukan kabel listrik IEC C13 ke NEMA 5-15P.
- Di beberapa bagian Eropa, Anda mungkin memerlukan kabel listrik IEC C13 hingga CEE 7/7.
- Di India, Anda memerlukan kabel listrik IEC C13 hingga IS1293.

Redundansi daya

Server mencakup beberapa koneksi daya dan dikirimkan dengan kabel untuk memungkinkan operasi redundan daya. Kami merekomendasikan redundansi daya, tetapi redundansi tidak diperlukan.

Server tidak termasuk Uninterruptible Power Supply (UPS).

Pemenuhan pesanan

Untuk memenuhi pesanan, AWS akan mengirimkan peralatan server Outposts, termasuk dudukan rel dan kabel listrik dan jaringan yang diperlukan, ke alamat yang Anda berikan. Kotak tempat server dikirimkan memiliki dimensi berikut:

- Kotak dengan server 2U:
  - Panjang: 44 inci/111.8 cm
  - Tinggi: 26,5 inci/67,3 cm
  - Lebar: 17 inci/43.2 cm
- Kotak dengan server 1U:
  - Panjang: 34,5 inci/87.6 cm
  - Tinggi: 24 inci/61 cm
  - Lebar: 9 inci/22.9 cm

Tim Anda atau penyedia pihak ketiga harus memasang peralatan. Untuk informasi selengkapnya, lihat Instalasi server pos terdepan.

Instalasi selesai ketika Anda mengonfirmasi bahwa kapasitas Amazon EC2 untuk server Outposts Anda tersedia dari akun Anda. AWS

Memulai dengan AWS Outposts

Pesan pos terdepan untuk memulai. Setelah menginstal peralatan Outpost Anda, luncurkan instans Amazon EC2 dan akses jaringan lokal Anda.

Tugas

- Buat Outpost dan pesan kapasitas Outpost
- Instalasi server pos terdepan
- Luncurkan instance di server Outpost Anda

Buat Outpost dan pesan kapasitas Outpost

Untuk mulai menggunakan AWS Outposts, masuk dengan AWS akun yang akan memiliki Outpost. Buat situs dan pos terdepan. Kemudian, lakukan pemesanan untuk server Outposts yang Anda butuhkan.

Prasyarat

- Tinjau konfigurasi yang tersedia untuk server Outposts Anda.
- Situs Outpost adalah lokasi fisik untuk peralatan Outpost Anda. Sebelum memesan kapasitas, verifikasi bahwa situs Anda memenuhi persyaratan. Untuk informasi selengkapnya, lihat .
- Anda harus memiliki paket AWS Enterprise Support atau paket AWS Enterprise On-Ramp Support.
- Tentukan mana yang Akun AWS akan memiliki pos terdepan. Gunakan akun ini 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 di mana Anda akan menginstal dan menjalankan server Outposts Anda. Setelah Anda membuat situs, AWS Outposts tetapkan ID ke situs Anda. Anda harus menentukan situs ini ketika Anda membuat Outpost.

Prasyarat

- Tentukan alamat operasi.

Untuk membuat situs

1. Masuk untuk AWS menggunakan Akun AWS yang akan memiliki Outpost.
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 Server saja.
7. Masukkan nama, deskripsi, dan alamat operasi untuk situs Anda.
8. (Opsional) Untuk catatan Situs, masukkan informasi lain yang mungkin berguna AWS untuk mengetahui tentang situs.
9. Pilih Buat situs.

Langkah 2: Buat Pos Terdepan

Buat Outpost untuk setiap server. Sebuah Outpost hanya dapat dikaitkan dengan satu server. Anda akan menentukan 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 Server.
4. Masukkan nama dan deskripsi untuk Outpost Anda.
5. Pilih Availability Zone untuk Outpost Anda.
6. Untuk ID Situs, pilih situs Anda.
7. Pilih Buat Pos Terdepan.

Langkah 3: Tempatkan pesanan

Lakukan pemesanan untuk server Outposts yang Anda butuhkan. Setelah Anda mengirimkan pesanan, AWS Outposts perwakilan akan menghubungi Anda.

> **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 memilih opsi pembayaran sebagian di muka atau tanpa di muka, Anda akan membayar biaya bulanan selama jangka waktu tiga tahun.

  Harga termasuk pengiriman, pemeliharaan layanan infrastruktur, dan patch dan peningkatan 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 Server.
4. Untuk menambah kapasitas, pilih konfigurasi.
5. Pilih Selanjutnya.

6. Pilih Gunakan Outpost yang ada dan pilih Outpost Anda.
7. Pilih Selanjutnya.
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 alamat pengiriman pada pesanan yang ada, hubungi Manajer AWS Akun Anda.
10. Pilih Selanjutnya.
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

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 instans, 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 AWS Outposts 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 baru.
2. Pilih Selanjutnya.
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 Selanjutnya.
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.

Upload JSON file

1. Pilih Unggah konfigurasi kapasitas.
2. Pilih Selanjutnya.

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

   Example

   Contoh file JSON:

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

4. Tinjau isi file JSON di bagian Paket konfigurasi Kapasitas.
5. Pilih Selanjutnya.
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.

Langkah selanjutnya

Anda dapat melihat status pesanan Anda menggunakan AWS Outposts konsol. Status awal pesanan Anda adalah Pesanan diterima. AWS Perwakilan akan menghubungi Anda dalam waktu tiga hari kerja. Anda akan menerima konfirmasi email ketika status pesanan Anda berubah menjadi

pemrosesan Pesanan. AWS Perwakilan dapat menghubungi Anda untuk mendapatkan informasi tambahan yang AWS diperlukan.

Jika Anda memiliki pertanyaan tentang pesanan Anda, hubungi AWS Support.

Untuk memenuhi pesanan, AWS akan menjadwalkan tanggal pengiriman.

Anda bertanggung jawab atas semua tugas instalasi, termasuk instalasi fisik dan konfigurasi jaringan. Anda dapat mengontrak pihak ketiga untuk melakukan tugas-tugas ini untuk Anda. Apakah Anda melakukan instalasi atau kontrak dengan pihak ketiga, instalasi memerlukan kredensi IAM di Akun AWS yang berisi Outpost untuk memverifikasi identitas perangkat baru. Anda bertanggung jawab untuk menyediakan dan mengelola akses ini. Untuk informasi selengkapnya, lihat the section called “Instalasi server pos terdepan”.

Instalasi selesai ketika kapasitas Amazon EC2 untuk Outpost Anda tersedia dari Anda. Akun AWS Setelah kapasitas tersedia, Anda dapat meluncurkan instans Amazon EC2 di server Outpost Anda. Untuk informasi selengkapnya, lihat the section called “Luncurkan sebuah instans ”.

Instalasi server pos terdepan

Ketika Anda memesan server Outpost, Anda bertanggung jawab untuk instalasi, apakah Anda melakukannya sendiri atau mengontrak pihak ketiga. Penginstalan pihak memerlukan izin khusus untuk memverifikasi identitas perangkat baru. Untuk informasi selengkapnya, lihat Memberikan izin.

Prasyarat

Anda harus memiliki faktor bentuk server Outpost di situs Anda. Untuk informasi selengkapnya, lihat Buat Outpost dan pesan kapasitas Outpost.

> **Note**
>
> Kami menyarankan Anda melihat video pelatihan Instalasi AWS Outposts Server sebelum dan selama proses instalasi. Untuk mengakses pelatihan, Anda harus masuk atau membuat akun di AWS Skill Builder.

Tugas

- Langkah 1: Berikan izin

Langkah 1: Berikan izin

Untuk memverifikasi identitas perangkat baru, Anda harus memiliki kredenal IAM di Akun AWS yang berisi Outpost. AWSOutpostsAuthorizeServerPolicyKebijakan memberikan izin yang diperlukan untuk menginstal server Outpost. Untuk informasi selengkapnya, lihat the section called “Pengelolaan identitas dan akses”.

Pertimbangan

- Jika Anda menggunakan pihak ketiga yang tidak memiliki akses ke Anda Akun AWS, Anda harus menyediakan akses sementara.
- AWS Outposts mendukung menggunakan kredensial sementara. Anda dapat mengonfigurasi kredensi sementara yang bertahan hingga 36 jam. Pastikan bahwa Anda memberikan installer cukup waktu untuk melakukan semua langkah untuk instalasi server. Untuk informasi selengkapnya, lihat the section called “Kredensial sementara”.

Langkah 2: Periksa

Untuk menyelesaikan pemeriksaan peralatan Outposts, Anda harus memeriksa paket pengiriman untuk kerusakan, membongkar paket pengiriman, dan menemukan Nitro Security Key (NSK). Pertimbangkan informasi berikut tentang memeriksa server:

- Paket pengiriman memiliki sensor kejut yang terletak di dua sisi terbesar kotak.
- Tutup bagian dalam paket pengiriman berisi instruksi tentang cara membongkar server dan menemukan NSK.
- NSK adalah modul enkripsi. Untuk menyelesaikan inspeksi, Anda menemukan NSK. Anda melampirkan NSK ke server di langkah selanjutnya.

Periksa paket pengiriman

Untuk memeriksa paket pengiriman

- Sebelum Anda membuka paket pengiriman, amati kedua sensor kejut dan perhatikan apakah mereka telah diaktifkan. Jika sensor kejut telah diaktifkan, ada kemungkinan unit telah rusak. Lanjutkan dengan instalasi mengambil waktu untuk mencatat kerusakan lebih lanjut pada server atau aksesori. Jika ada bagian dari sistem yang jelas rusak atau instalasi gagal berjalan seperti yang diharapkan, hubungi AWS Support untuk panduan mengganti server Outposts Anda.

  Jika bilah di tengah sensor berwarna merah, sensor telah diaktifkan.

Buka paket pengiriman

Untuk membongkar paket pengiriman

- Buka paket dan pastikan berisi item berikut:
  - Server

- Nitro Security Key (modul enkripsi) — kemasan yang ditandai dengan “NSK” berwarna merah. Lihat prosedur berikut untuk menemukan NSK dari paket pengiriman untuk informasi lebih lanjut.
- Kit pemasangan rak (2 rel dalam, 2 rel luar, dan sekrup)
- Pamflet instalasi
- Kit aksesori
  - Sepasang kabel daya C13/14 - 10 kaki (3m)
  - Kabel breakout QSFP -10 kaki (3m)
  - Kabel USB, Micro-USB ke USB-C - 10 kaki (3m)
  - Pelindung sikat

Temukan NSK

NSK berada di dalam kotak berlabel A yang mencakup aksesori untuk server.

> **Important**
>
> Jangan gunakan NSK untuk menghancurkan data di server selama instalasi.

NSK diperlukan untuk mengaktifkan server. NSK juga digunakan untuk menghancurkan data di server saat Anda mengirim server kembali. Pada langkah instalasi ini, abaikan instruksi pada badan NSK karena instruksi tersebut adalah untuk menghancurkan data.

Langkah 3: Pemasangan rak

Untuk menyelesaikan langkah ini, Anda harus memasang rel dalam ke server, rel luar ke rak, lalu pasang server di rak. Anda memerlukan obeng Phillips-head untuk menyelesaikan langkah-langkah ini.

Alternatif pemasangan rak

Anda tidak diharuskan memasang server di rak. Jika Anda tidak memasang server di rak, pertimbangkan informasi berikut:

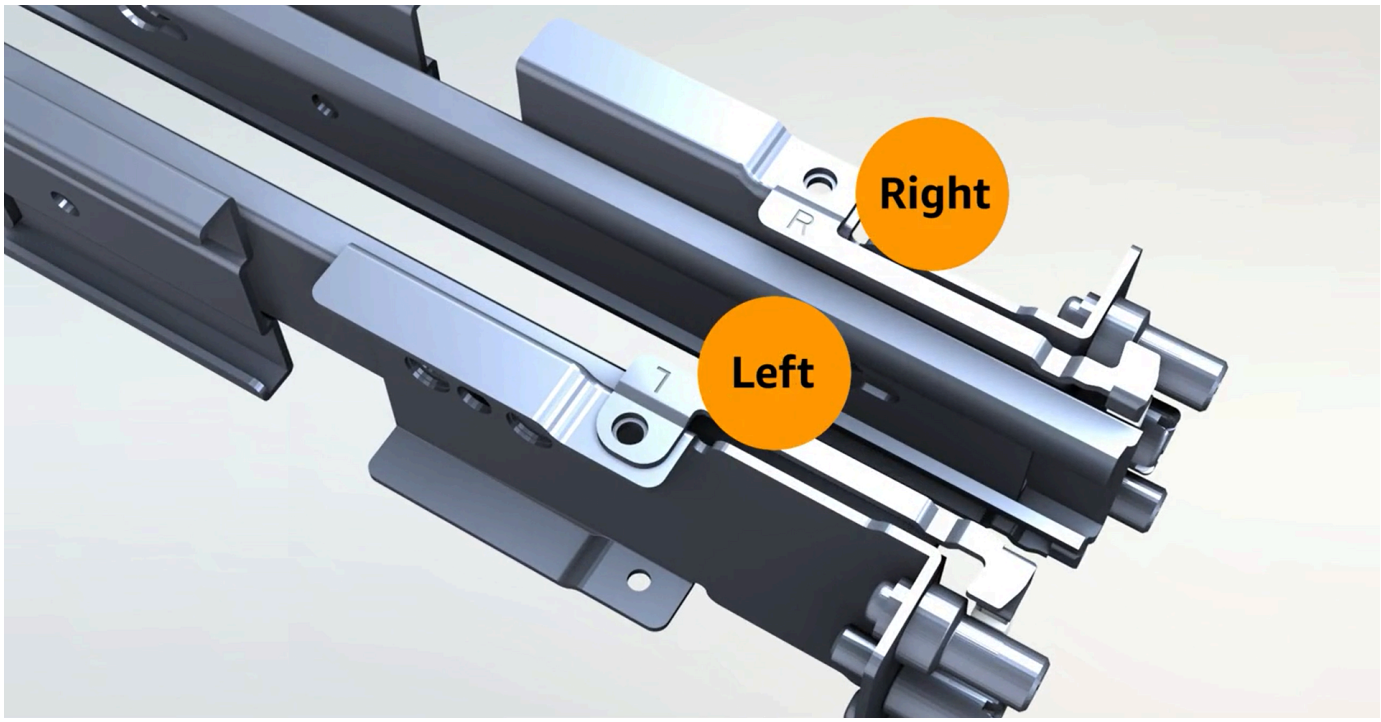
- Pastikan jarak minimum 6 inci (15 cm) antara server dan dinding di depan dan di belakang server untuk memungkinkan udara panas bersirkulasi.

- Tempatkan server pada permukaan yang stabil bebas dari bahaya mekanis seperti kelembaban atau benda jatuh.
- Untuk menggunakan kabel jaringan yang disertakan dengan server, Anda harus menempatkan server dalam jarak 10 kaki (3 m) dari perangkat jaringan hulu Anda.
- Ikuti panduan lokal untuk bracing dan ikatan seismik.

Identifikasi sisi dan ujung

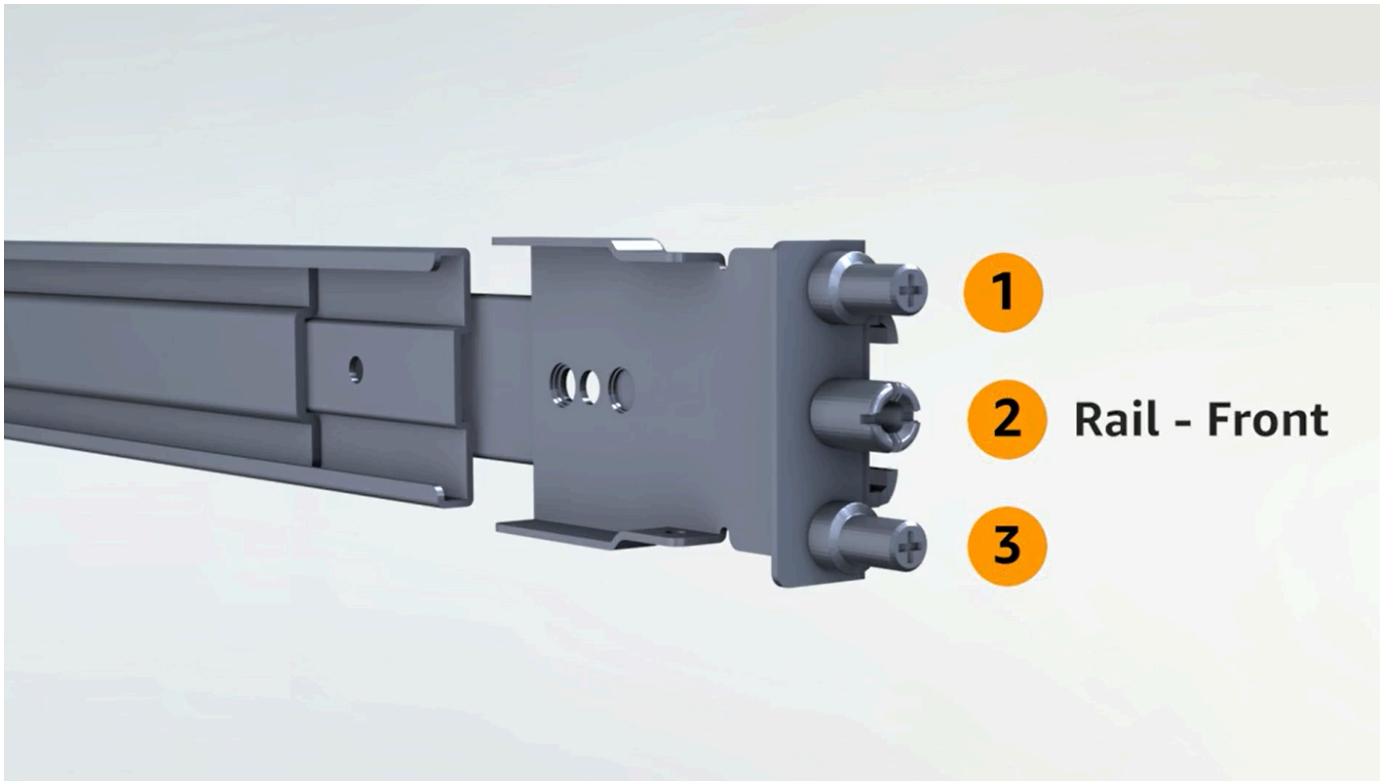
Untuk mengidentifikasi kiri dari kanan, depan dari belakang

1. Temukan dan buka kotak rel rak yang disertakan dengan server.
2. Lihatlah tanda pada rel untuk menentukan mana yang kiri dan kanan. Tanda-tanda ini menentukan ke sisi server mana setiap rel terpasang.

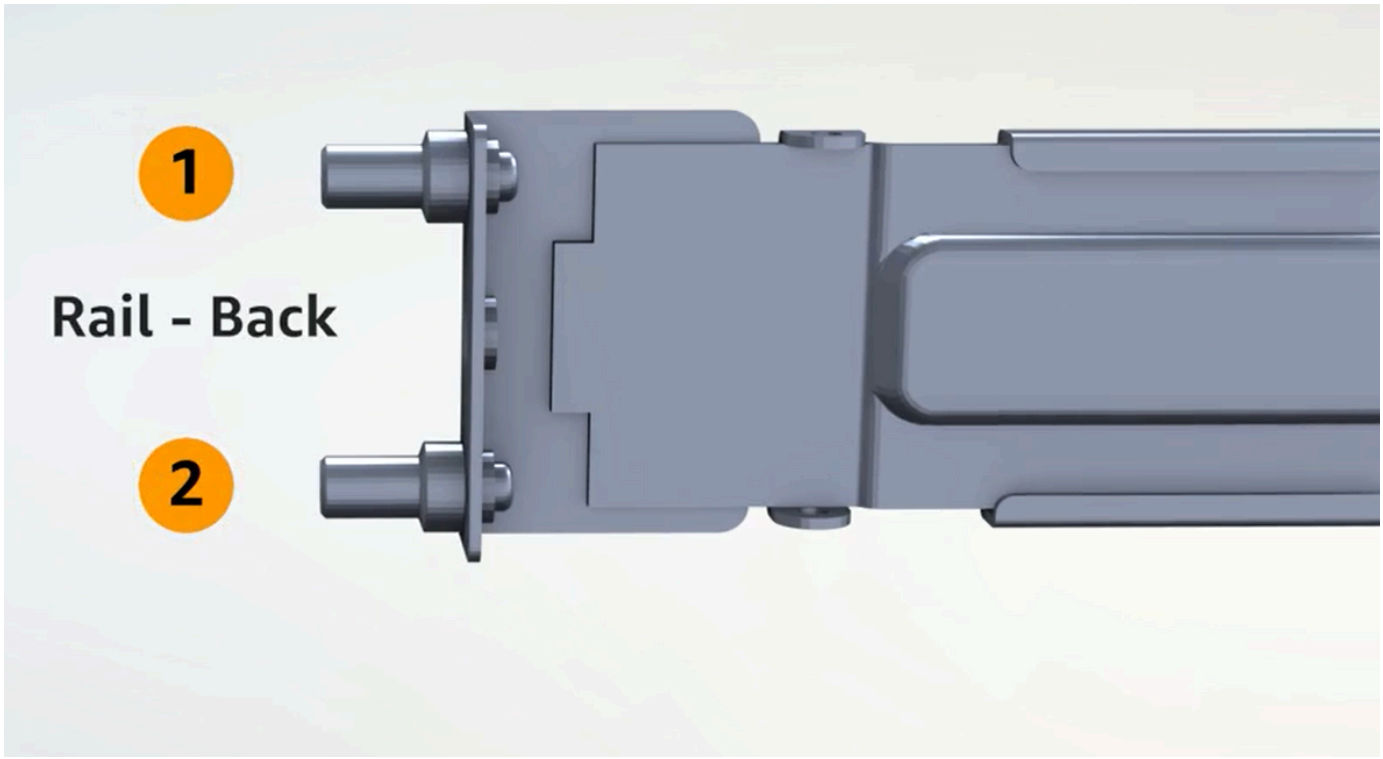


3. Lihatlah posting di setiap ujung rel untuk menentukan mana yang depan, dan mana yang belakang.

   Ujung depan memiliki tiga tiang.



Bagian belakang memiliki dua pos.



Pasang rel bagian dalam

Untuk melampirkan rel dalam ke server

1. Lepaskan rel bagian dalam dari rel luar untuk kedua rel. Anda harus memiliki empat rel.
2. Pasang rel bagian dalam kanan ke sisi kanan server dan kencangkan rel dengan sekrup. Pastikan Anda mengarahkan rel dengan benar dengan server. Arahkan bagian depan rel ke arah depan server.
3. Pasang rel bagian dalam kiri ke sisi kiri server dan kencangkan rel dengan sekrup.

Pasang rel luar

Untuk memasang rel luar ke rak

1. Hadapi rak dan gunakan rel bertanda R di sisi kanan rak. Pasang bagian belakang rel ke rak terlebih dahulu, lalu rentangkan rel untuk menghubungkannya ke bagian depan rak.

   > **Tip**
   >
   > Perhatikan orientasi rel. Gunakan adaptor pin yang disertakan jika perlu.

2. Ulangi dengan rel kiri di sisi kiri.

Pasang server

Untuk memasang server di rak

- Geser server ke rel luar yang Anda pasang di rak pada langkah sebelumnya dan kencangkan server di bagian depan dengan dua sekrup yang disediakan.

  > **Tip**
  >
  > Gunakan dua orang untuk menggeser server ke rak.

Langkah 4: Nyalakan

Untuk menyelesaikan power up, Anda melampirkan NSK, menghubungkan server ke sumber daya, dan memverifikasi bahwa server telah dinyalakan. Pertimbangkan informasi berikut tentang menyalakan server:

- Server berfungsi dengan satu sumber daya, tetapi AWS merekomendasikan Anda menggunakan dua sumber daya untuk redundansi.
- Hubungkan kabel daya sebelum Anda menghubungkan kabel jaringan.
- Gunakan sepasang kabel daya saluran keluar C13/C14 untuk menghubungkan server ke catu daya di rak. Jika Anda tidak menggunakan kabel daya saluran masuk C14 untuk menghubungkan server ke catu daya di rak, Anda harus menyediakan adaptor untuk saluran masuk C14 yang terhubung ke sumber listrik.

Lampirkan NSK

Anda harus melampirkan NSK ke server sehingga dapat mendekripsi data di server selama operasi.

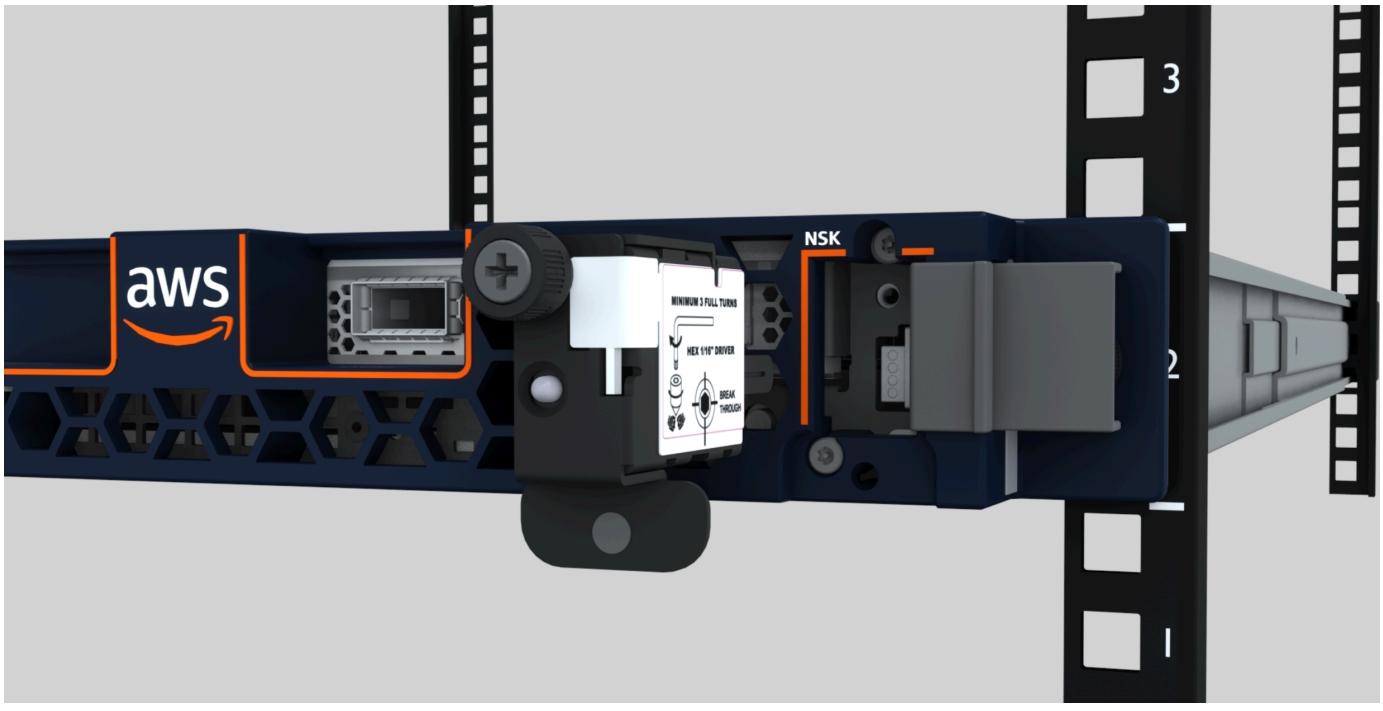
> **Important**
>
> - Sisi NSK memiliki instruksi tentang cara menghancurkan NSK. Jangan ikuti instruksi itu sekarang. Ikuti instruksi tersebut hanya ketika mengembalikan server ke AWS, untuk secara kriptografis menghancurkan data di server.
> - Jika Anda menginstal beberapa server secara bersamaan, pastikan Anda tidak mencampur NSK. Anda harus melampirkan NSK ke server yang dikirimkannya. Jika Anda menggunakan NSK yang berbeda, server tidak akan boot.

Untuk melampirkan NSK

1. Di sisi kanan depan server, buka kompartemen NSK.

   Gambar berikut menunjukkan NSK yang dilampirkan ke server 2U.

Gambar berikut menunjukkan NSK yang dilampirkan ke server 1U.

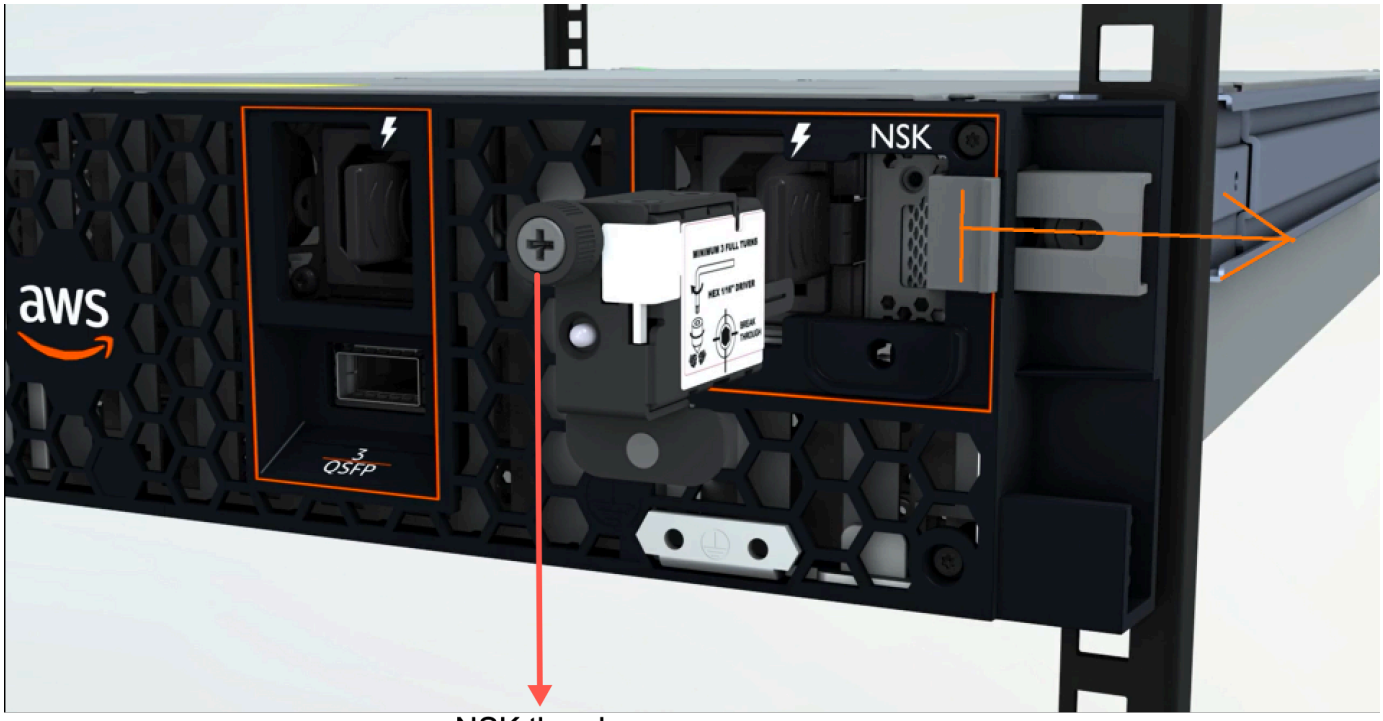


2. Pastikan nomor seri (SN) pada NSK cocok dengan SN pada tab tarik bezel kompartemen NSK di server.

   Gambar berikut menunjukkan nomor SN pada tab tarik keluar NSK dan bezel:

3. Masukkan NSK ke dalam slot.
4. Kencangkan tangan menggunakan sekrup ibu jari atau kencangkan dengan obeng (0,7 Nm/0,52 lb-ft) hingga pas. Jangan gunakan perkakas listrik karena dapat melakukan torsi berlebih dan merusak NSK.

   Gambar berikut menunjukkan lokasi thumbscrew.



NSK thumbscrew

Gambar berikut menunjukkan jenis obeng yang dapat Anda gunakan untuk melampirkan NSK ke server.

Naik daya

Untuk menghubungkan server ke daya

1. Temukan pasangan kabel daya C13/C14 yang disertakan dengan server.
2. Connect ujung C14 dari kedua kabel ke sumber listrik Anda.
3. Connect ujung C13 dari kedua kabel ke port di bagian depan server.

Verifikasi daya server

Untuk memverifikasi bahwa server memiliki daya

1. Verifikasi bahwa Anda dapat mendengar server berjalan.

   > **Tip**
   >
   > Tingkat kebisingan turun setelah server menyediakan itu sendiri.

2. Verifikasi bahwa lampu daya LED di atas port daya menyala.

   Gambar berikut menunjukkan lampu daya LED pada server 2U

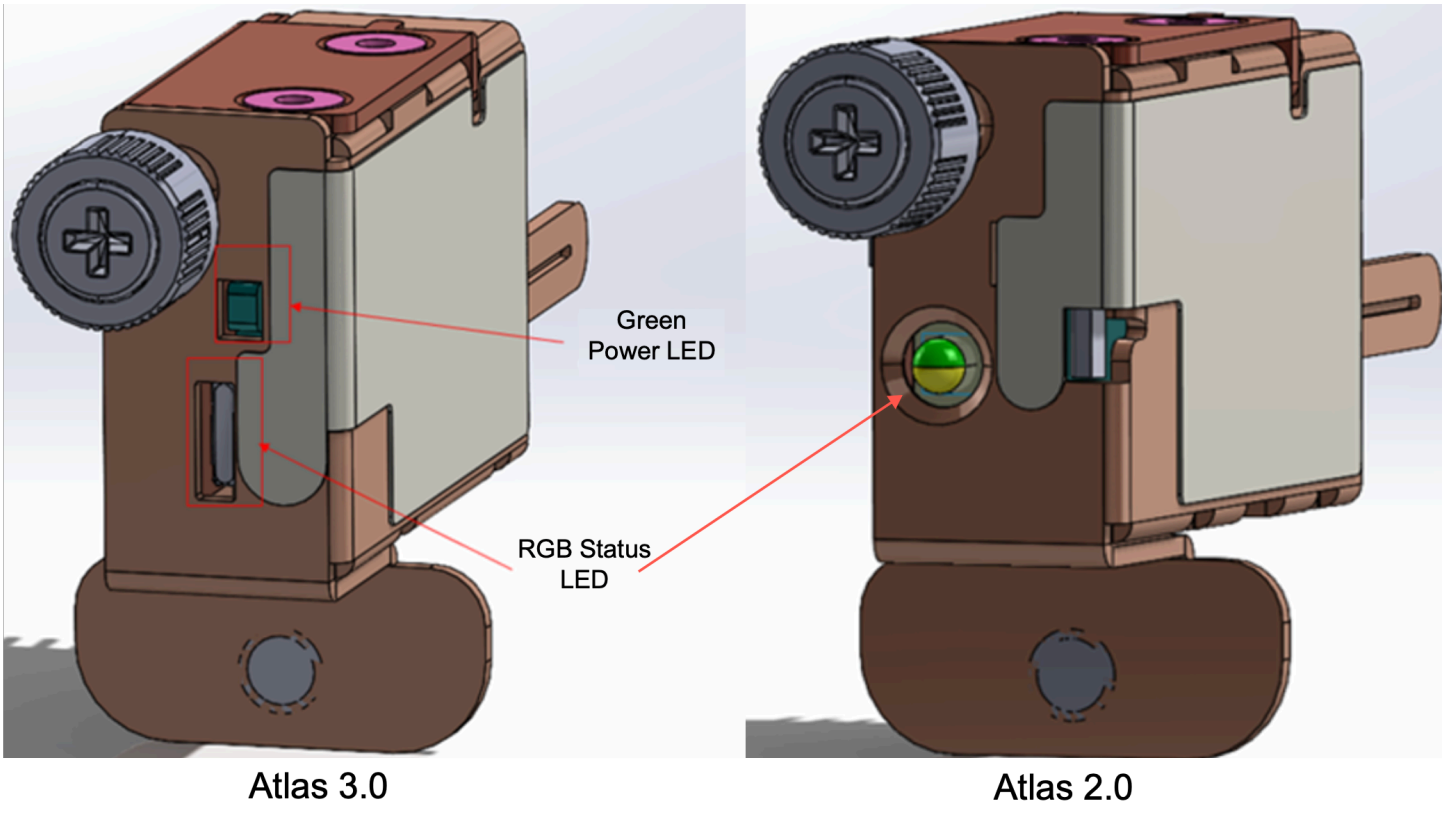
   

   Gambar berikut menunjukkan lampu daya LED pada server 1U

Periksa LED Daya pada Atlas 3.0. NSK

AWS Outposts mendukung dua versi NSK: Atlas 2.0 dan Atlas 3.0. Kedua versi NSK memiliki LED Status RGB. Selain itu, Atlas 3.0 memiliki Power LED hijau. Langkah ini hanya untuk Atlas 3.0 NSK.

Gambar berikut menunjukkan lokasi LED pada Atlas 2.0 dan Atlas 3.0 NSK:



Jika Anda memiliki Atlas 2.0 NSK, lewati ke langkah berikutnya, Langkah 5: Connect jaringan karena versi NSK ini hanya memiliki LED Status RGB yang harus Anda periksa setelah server Outpost disediakan dan diaktifkan.

Jika Anda memiliki Atlas 3.0 NSK, periksa LED Daya hijau:

- Jika lampu hijau menyala, NSK terhubung dengan benar ke host dan memiliki daya. Anda dapat melanjutkan ke langkah berikutnya.
- Jika lampu hijau mati, NSK tidak terhubung dengan benar ke host atau/dan tidak memiliki daya. Kontak AWS Support.

Langkah 5: Connect jaringan

Untuk menyelesaikan pengaturan jaringan, Anda menghubungkan server ke perangkat jaringan hulu Anda dengan kabel jaringan.

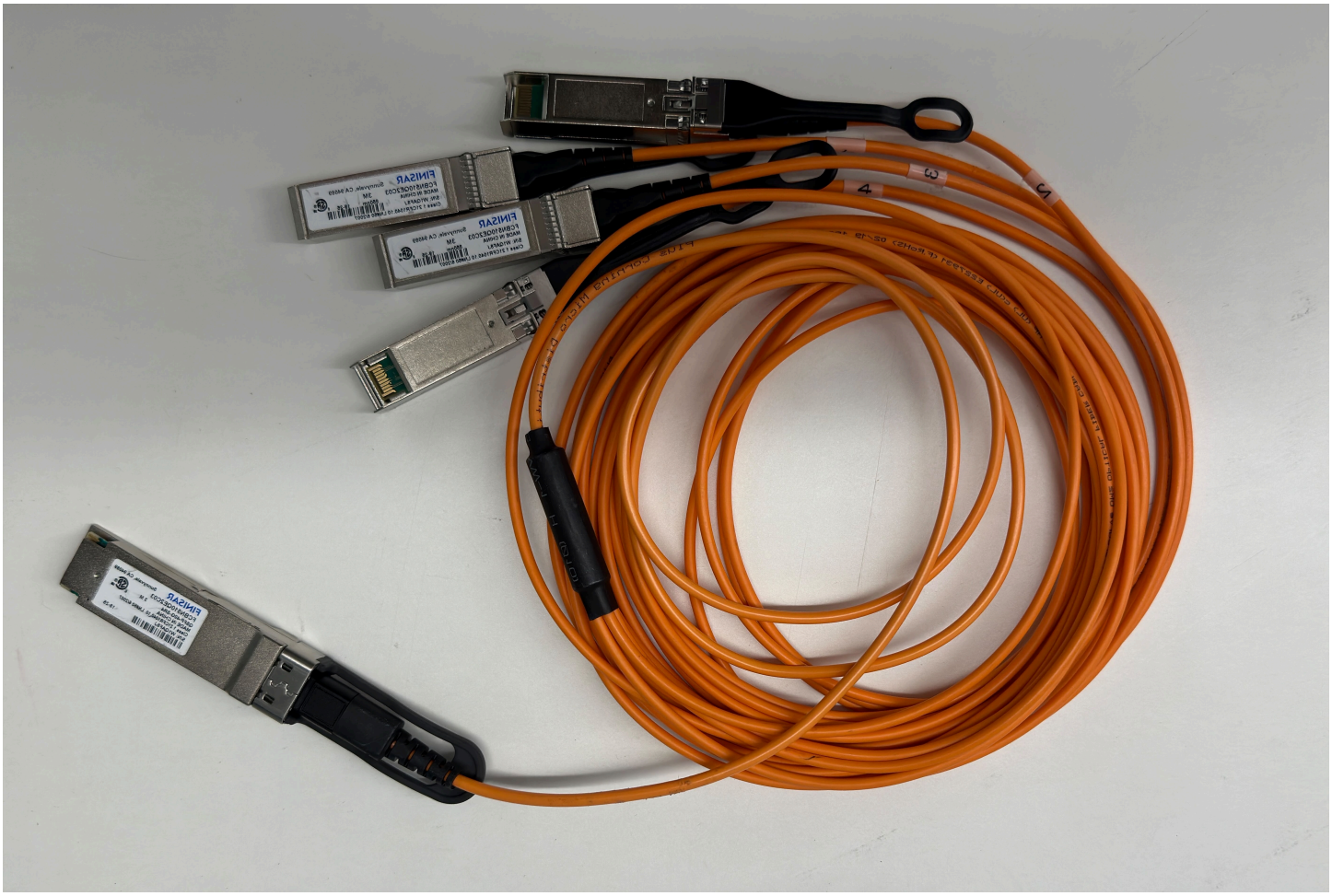
Pertimbangkan informasi berikut tentang menghubungkan ke jaringan:

- Server memerlukan koneksi untuk dua jenis lalu lintas: lalu lintas tautan layanan dan lalu lintas tautan antarmuka jaringan lokal (LNI). Petunjuk di bagian berikut menjelaskan port mana yang akan digunakan di server untuk menyegmentasikan lalu lintas. Konsultasikan dengan grup TI Anda untuk menentukan port mana pada perangkat jaringan hulu Anda yang harus membawa setiap jenis lalu lintas.
- Pastikan server telah terhubung ke perangkat jaringan hulu Anda dan telah diberi alamat IP. Untuk informasi selengkapnya, lihat Penetapan alamat IP server.
- Koneksi optik pada AWS Outposts server hanya mendukung 10 Gbits dan tidak mendukung negosiasi otomatis kecepatan port. Jika port host mencoba menegosiasikan kecepatan port, misalnya, antara 10 hingga 25 Gbits, Anda dapat mengalami masalah. Dalam kasus seperti itu, kami sarankan Anda melakukan hal berikut:
  - Atur kecepatan port pada port sakelar ke 10 Gbits.
  - Bekerja dengan vendor sakelar Anda untuk mendukung konfigurasi statis.

Konfigurasikan jaringan QSFP

Dengan kabel breakout QSFP, Anda menggunakan breakout untuk mengelompokkan lalu lintas.

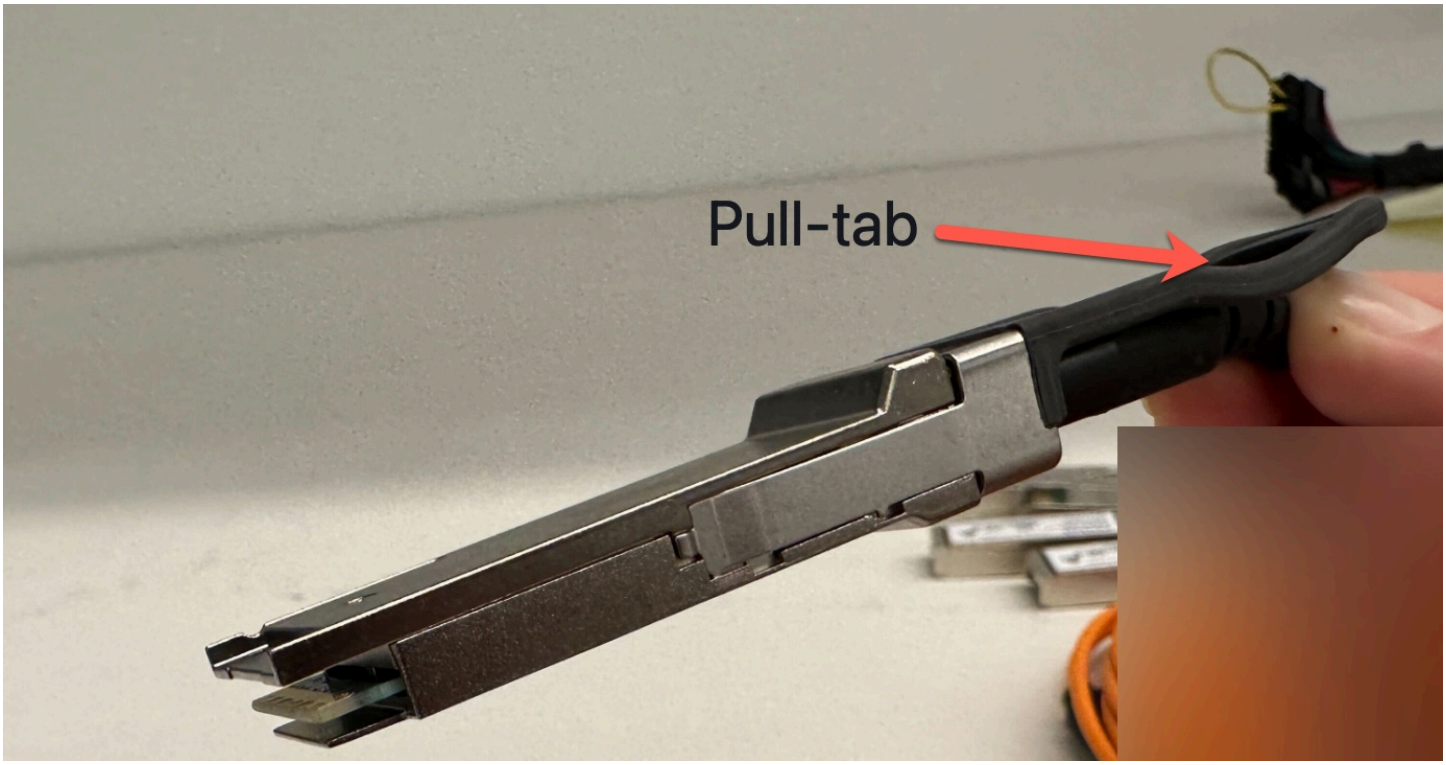
Gambar berikut menunjukkan kabel breakout QSFP:



> **Note**
>
> AWS Outposts server memiliki port RJ45 fisik di samping port QSFP. Namun, port RJ45 ini tidak diaktifkan untuk penggunaan pelanggan apa pun. Jika Anda memerlukan konektivitas RJ45 1GbE, gunakan kabel QSFP yang disertakan untuk menghubungkan 10GBASE-X SFP +ke konverter media 1GbE RJ45.

Salah satu ujung kabel QSFP memiliki konektor tunggal. Connect ujung ini ke server.

Gambar berikut menunjukkan ujung kabel dengan konektor tunggal:



Ujung lain dari kabel QSFP memiliki 4 kabel breakout berlabel 1 hingga 4. Gunakan kabel berlabel 1 untuk lalu lintas tautan LNI dan kabel berlabel 2 untuk lalu lintas tautan layanan.

Gambar berikut menunjukkan ujung kabel dengan 4 kabel breakout:

Untuk menghubungkan server ke jaringan dengan kabel breakout QSFP

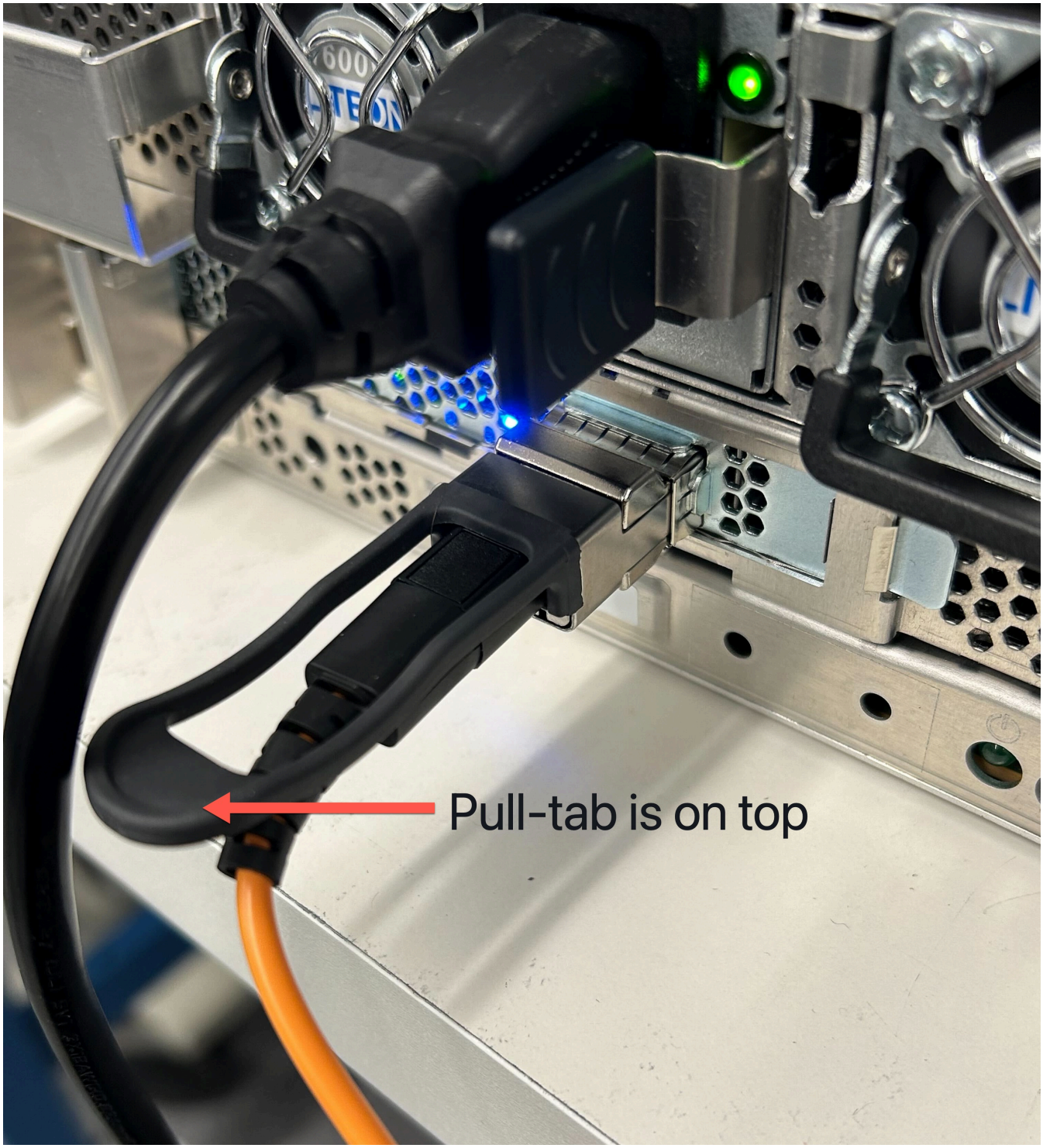
1. Temukan kabel breakout QSFP yang disertakan dengan server.
2. Hubungkan ujung tunggal kabel breakout QSFP ke port QSFP di server.
    1. Temukan port QSFP.

        Gambar berikut menunjukkan lokasi port QSFP di server 2U.

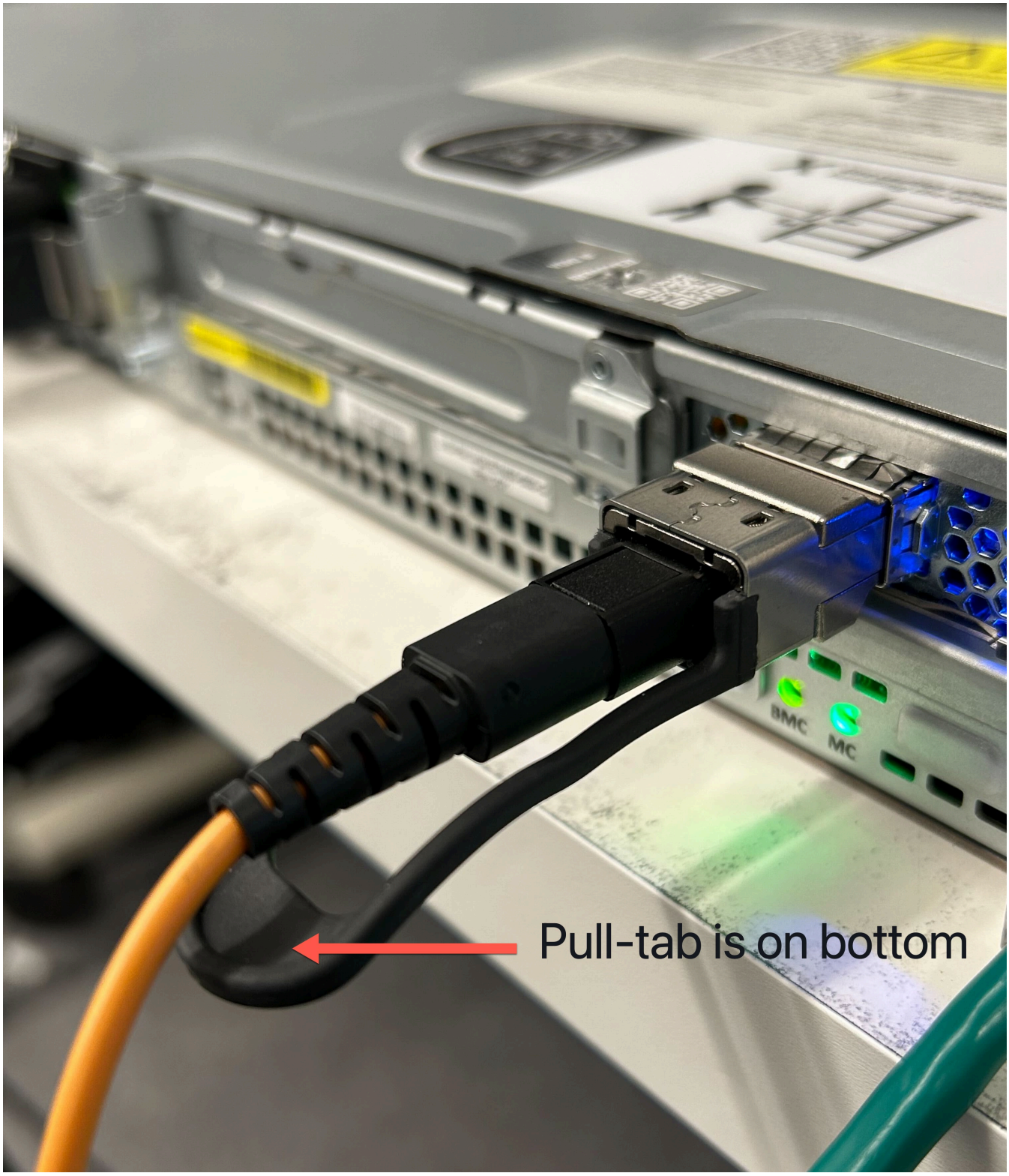
Gambar berikut menunjukkan lokasi port QSFP di server 1U.

2. Colokkan QSFP dengan tab tarik dalam orientasi yang benar.

   Untuk server 2U, colokkan QSFP dengan tab tarik di atas seperti yang ditunjukkan gambar berikut.



Untuk server 1U, colokkan QSFP dengan tab tarik di bagian bawah seperti yang ditunjukkan gambar berikut.



3. Pastikan Anda merasakan atau mendengar bunyi klik saat memasang kabel. Ini menunjukkan bahwa Anda mencolokkan kabel dengan benar.

3. Connect breakouts 1 dan 2 dari kabel QSFP ke perangkat jaringan hulu.

> **Important**
>
> Kedua kabel berikut diperlukan agar server Outpost berfungsi.
>
> - Gunakan kabel berlabel 1 untuk lalu lintas tautan LNI.
> - Gunakan kabel berlabel 2 untuk lalu lintas tautan layanan.

Langkah 6: Otorisasi server

Untuk mengotorisasi server, Anda harus menghubungkan laptop Anda ke server dengan kabel USB, kemudian menggunakan protokol serial berbasis perintah untuk menguji koneksi dan mengotorisasi server. Selain kredensil IAM, Anda memerlukan kabel USB, laptop, dan perangkat lunak terminal serial, seperti PuTTY atauscreen, untuk menyelesaikan langkah-langkah ini.

Atau, jika Anda memiliki ponsel atau tablet Android dengan konektor USB-C atau Micro-USB dengan dukungan USB On The Go (OTG), Anda dapat menggunakan aplikasi Outposts Server Activator untuk memandu Anda melalui proses otorisasi server. Anda dapat mengunduh aplikasi dari Google Play

Pertimbangkan informasi berikut tentang otorisasi server:

- Untuk mengotorisasi server, Anda atau pihak yang menginstal server memerlukan kredensi IAM di Akun AWS yang berisi Outpost. Untuk informasi selengkapnya, lihat the section called “Langkah 1: Berikan izin”.
- Anda tidak perlu mengautentikasi dengan kredensi IAM untuk menguji koneksi Anda.
- Pertimbangkan untuk menguji koneksi sebelum Anda menggunakan perintah export untuk menyetel kredenal IAM sebagai variabel lingkungan.
- Untuk melindungi akun Anda, Outpost Configuration Tool tidak pernah menyimpan kredensi IAM Anda.
- Untuk menghubungkan laptop Anda ke server, selalu colokkan kabel USB ke laptop Anda terlebih dahulu dan kemudian ke server.

Tugas

- Connect laptop Anda ke server
- Buat koneksi serial ke server

- Uji koneksi
- Otorisasi server
- Verifikasi LED NSK

Connect laptop Anda ke server

Hubungkan kabel USB ke laptop Anda terlebih dahulu dan kemudian ke server. Server menyertakan chip USB yang membuat port serial virtual yang tersedia untuk Anda di laptop. Anda dapat menggunakan port serial virtual ini untuk terhubung ke server dengan perangkat lunak emulasi terminal serial. Anda hanya dapat menggunakan port serial virtual ini untuk menjalankan perintah Outpost Configuration Tool.

Untuk menghubungkan laptop ke server

Colokkan kabel USB ke laptop Anda terlebih dahulu, lalu ke server.

> **Note**
>
> Chip USB membutuhkan driver untuk membuat port serial virtual. Sistem operasi Anda harus secara otomatis menginstal driver yang diperlukan jika belum ada. Untuk mengunduh dan menginstal driver, lihat Panduan Instalasi dari FTDI.

Buat koneksi serial ke server

Bagian ini berisi instruksi untuk menggunakan program terminal serial populer, tetapi Anda tidak diharuskan menggunakan program ini. Gunakan program terminal serial yang Anda sukai dengan kecepatan koneksi `115200` baud.

Contoh

- Koneksi serial Windows
- Koneksi serial Mac

Koneksi serial Windows

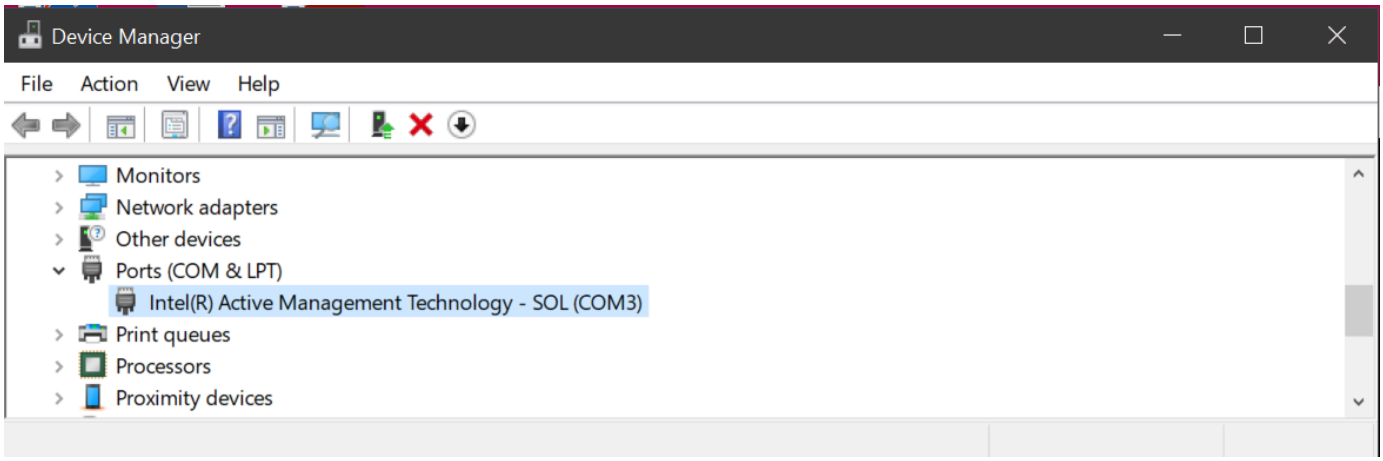
Instruksi berikut adalah untuk Putty di Windows. PuTTY gratis, tetapi Anda mungkin harus mengunduhnya.

Unduh PuTTY

Unduh dan pasang PuTTY dari halaman unduhan PuTTY.

Untuk membuat terminal serial pada Windows menggunakan PuTTY

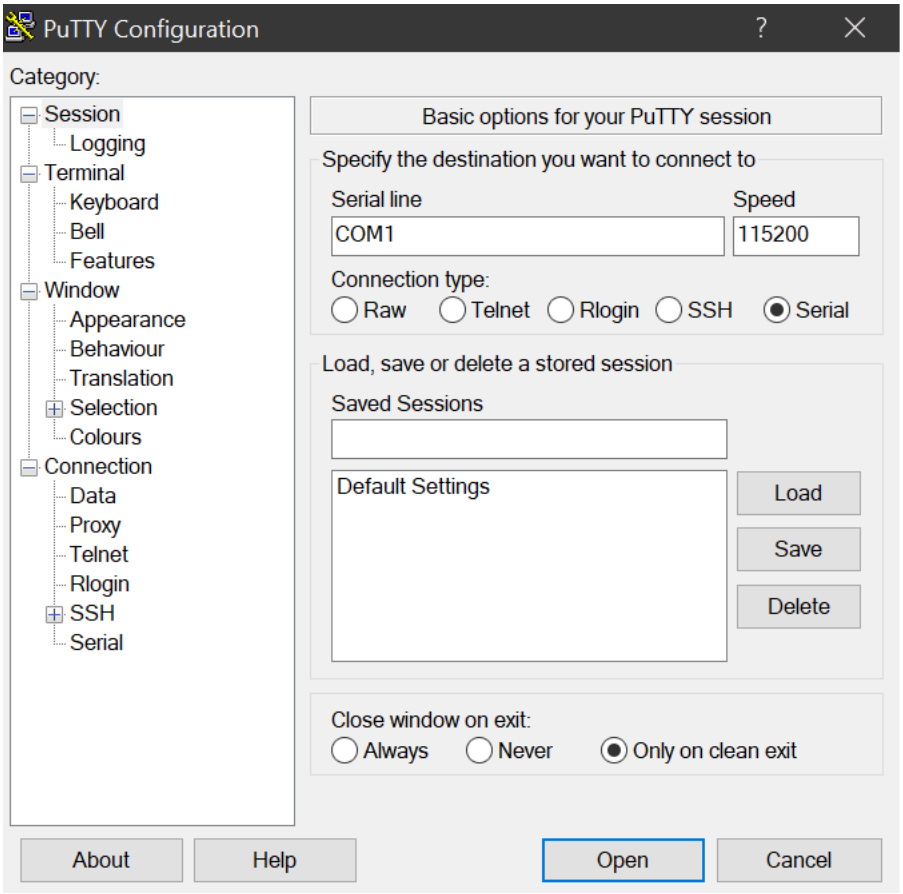
1. Colokkan kabel USB ke laptop Windows Anda terlebih dahulu, lalu ke server.
2. Dari Desktop, klik kanan Mulai, dan pilih Device Manager.
3. Di Device Manager, perluas Port (COM & LPT) untuk menentukan port COM untuk koneksi serial USB. Anda akan melihat sebuah node bernama USB Serial Port (COM **#**). Nilai untuk port COM tergantung pada perangkat keras Anda.



4. Di PuTTY, dari Session, pilih Serial for Connection type, lalu masukkan informasi berikut:

   - Di bawah baris Serial, masukkan port COM # dari Device Manager.
   - Di bawah Kecepatan, masukkan: `115200`

   Gambar berikut menunjukkan contoh pada halaman Konfigurasi PuTTY:



5. Pilih Buka.

   Jendela konsol kosong muncul. Diperlukan waktu antara 1 hingga 2 menit agar salah satu dari berikut ini muncul:

   - `Please wait for the system to stabilize. This can take up to 900 seconds, so far` *`x seconds`* `have elapsed on this boot.`
   - `Outpost>`Prompt.

Koneksi serial Mac

Petunjuk berikut adalah untuk screen di macOS. Anda dapat menemukan screen disertakan dengan sistem operasi.

Untuk membuat terminal serial di macOS menggunakan screen

1. Colokkan kabel USB ke laptop Mac Anda terlebih dahulu, lalu ke server.
2. Di Terminal, daftar `/dev` dengan `*usb*` filter untuk output untuk menemukan port serial virtual.

```
ls -ltr /dev/*usb*
```

Perangkat serial muncul sebagai`tty`. Misalnya, pertimbangkan contoh output berikut dari perintah daftar sebelumnya:

```
ls -ltr /dev/*usb*
crw-rw-rw-  1 root  wheel   21,   3 Feb  8 15:48 /dev/cu.usbserial-EXAMPLE1
crw-rw-rw-  1 root  wheel   21,   2 Feb  9 08:56 /dev/tty.usbserial-EXAMPLE1
```

3. Di Terminal, gunakan screen dengan perangkat serial dan baud rate dari koneksi serial untuk mengatur koneksi serial. Dalam perintah berikut, ganti *EXAMPLE1* dengan nilai dari laptop Anda.

```
screen /dev/tty.usbserial-EXAMPLE1 115200
```

Jendela konsol kosong muncul. Diperlukan waktu antara 1 hingga 2 menit agar salah satu dari berikut ini muncul:

- `Please wait for the system to stabilize. This can take up to 900 seconds, so far x seconds have elapsed on this boot.`
- `Outpost>`Prompt.

Uji koneksi

Bagian ini menjelaskan cara menggunakan Outpost Configuration Tool untuk menguji koneksi. Anda tidak memerlukan kredensi IAM untuk menguji koneksi. Koneksi Anda harus dapat menyelesaikan DNS untuk mengakses file. Wilayah AWS

1. Uji tautan dan kumpulkan informasi tentang koneksi
2. Uji untuk DNS resolver
3. Uji akses ke Wilayah AWS

Untuk menguji tautan

1. Colokkan kabel USB ke laptop Anda terlebih dahulu dan kemudian ke server.
2. Gunakan program terminal serial, seperti PuTTY atauscreen, untuk terhubung ke server. Untuk informasi selengkapnya, lihat the section called “Buat koneksi serial ke server”.

3. Tekan Enter untuk mengakses prompt perintah Outpost Configuration Tool.

```
Outpost>
```

> **Note**
>
> Jika Anda melihat lampu merah persisten di dalam sasis server di sisi kiri setelah Anda menyalakan dan Anda tidak dapat terhubung ke Outpost Configuration Tool, Anda mungkin perlu mematikan dan menguras server untuk melanjutkan. Untuk menguras server, lepaskan semua jaringan dan kabel daya, tunggu lima menit, lalu nyalakan dan sambungkan jaringan lagi.

4. Gunakan describe-links untuk mengembalikan informasi tentang tautan jaringan di server. Server pos terdepan harus memiliki satu tautan layanan dan satu tautan antarmuka jaringan lokal (LNI).

```
Outpost>describe-links
---
service_link_connected: True
local_link_connected: False
links:
-
  name: local_link
  connected: False
  mac: 00:00:00:00:00:00
-
  name: service_link
  connected: True
  mac: 0A:DC:FE:D7:8E:1F
checksum: 0x46FDC542
```

Jika Anda mendapatkan `connected: False` salah satu tautan, pecahkan masalah koneksi jaringan pada perangkat keras.

5. Gunakan describe-ip untuk mengembalikan status penetapan IP dan konfigurasi tautan layanan.

```
Outpost>describe-ip
---
links:
-
  name: service_link
  configured: True
```

```
  ip: 192.168.0.0
  netmask: 255.255.0.0
  gateway: 192.168.1.1
  dns: [ "192.168.1.1" ]
  ntp: [ ]
checksum: 0x8411B47C
```

Nilai NTP mungkin hilang karena NTP adalah opsional dalam set opsi DHCP. Anda seharusnya tidak memiliki nilai lain yang hilang.

Untuk menguji DNS

1. Colokkan kabel USB ke laptop Anda terlebih dahulu dan kemudian ke server.
2. Gunakan program terminal serial, seperti PuTTY atauscreen, untuk terhubung ke server. Untuk informasi selengkapnya, lihat the section called “Buat koneksi serial ke server”.
3. Tekan Enter untuk mengakses prompt perintah Outpost Configuration Tool.

```
Outpost>
```

> **Note**
>
> Jika Anda melihat lampu merah persisten di dalam sasis server di sisi kiri setelah Anda menyalakan dan Anda tidak dapat terhubung ke Outpost Configuration Tool, Anda mungkin perlu mematikan dan menguras server untuk melanjutkan. Untuk menguras server, lepaskan semua jaringan dan kabel daya, tunggu lima menit, lalu nyalakan dan sambungkan jaringan lagi.

4. Gunakan export untuk memasukkan Wilayah induk dari server Outpost sebagai nilai untuk`AWS_DEFAULT_REGION`.

   `AWS_DEFAULT_REGION=`*`Wilayah`*

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: 0xB2A945RE
```

   - Jangan menyertakan spasi sebelum atau sesudah tanda sama (=).

- Tidak ada nilai lingkungan yang disimpan. Anda harus mengekspor Wilayah AWS setiap kali Anda menjalankan Outpost Configuration Tool.
- Jika Anda menggunakan pihak ketiga untuk menginstal server, Anda harus memberikan pihak ketiga dengan Wilayah induk.

5. Gunakan describe-resolve untuk menentukan apakah server Outpost dapat mencapai resolver DNS dan menyelesaikan alamat IP dari titik akhir konfigurasi Outpost di Wilayah. Membutuhkan setidaknya satu tautan dengan konfigurasi IP.

```
Outpost>describe-resolve
---
dns_responding: True
dns_resolving: True
dns: [ "198.xx.xxx.xx", "198.xx.xxx.xx" ]
query: outposts.us-west-2.amazonaws.com
records: [ "18.xxx.xx.xxx", "44.xxx.xxx.xxx", "44.xxx.xxx.xxx" ]
checksum: 0xB6A961CE
```

Untuk menguji akses ke Wilayah AWS

1. Colokkan kabel USB ke laptop Anda terlebih dahulu dan kemudian ke server.
2. Gunakan program terminal serial, seperti PuTTY atauscreen, untuk terhubung ke server. Untuk informasi selengkapnya, lihat the section called “Buat koneksi serial ke server”.
3. Tekan Enter untuk mengakses prompt perintah Outpost Configuration Tool.

```
Outpost>
```

> **Note**
>
> Jika Anda melihat lampu merah persisten di dalam sasis server di sisi kiri setelah Anda menyalakan dan Anda tidak dapat terhubung ke Outpost Configuration Tool, Anda mungkin perlu mematikan dan menguras server untuk melanjutkan. Untuk menguras server, lepaskan semua jaringan dan kabel daya, tunggu lima menit, lalu nyalakan dan sambungkan jaringan lagi.

4. Gunakan export untuk memasukkan Wilayah induk dari server Outpost sebagai nilai untuk`AWS_DEFAULT_REGION`.

`AWS_DEFAULT_REGION=Wilayah`

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: 0xB2A945RE
```

- Jangan menyertakan spasi sebelum atau sesudah tanda sama (=).
- Tidak ada nilai lingkungan yang disimpan. Anda harus mengekspor Wilayah AWS setiap kali Anda menjalankan Outpost Configuration Tool.
- Jika Anda menggunakan pihak ketiga untuk menginstal server, Anda harus memberikan pihak ketiga dengan Wilayah induk.

5. Gunakan describe-reachability untuk menentukan apakah server Outpost dapat mencapai titik akhir konfigurasi Outpost di Wilayah. Membutuhkan konfigurasi DNS yang berfungsi, yang dapat Anda tentukan dengan menggunakandescribe-resolve.

```
Outpost>describe-reachability
---
is_reachable: True
src_ip: 10.0.0.0
dst_ip: 54.xx.x.xx
dst_port: xxx
checksum: 0xCB506615
```

- `is_reachable`menunjukkan hasil tes
- `src_ip`adalah alamat IP server
- `dst_ip`adalah alamat IP dari titik akhir konfigurasi Outpost di Wilayah
- `dst_port`adalah port yang digunakan server untuk terhubung `dst_ip`

Otorisasi server

Bagian ini menjelaskan cara menggunakan Outpost Configuration Tool dan kredenal IAM dari AWS akun yang berisi Outpost untuk mengotorisasi server.

Untuk mengotorisasi server

1. Colokkan kabel USB ke laptop Anda terlebih dahulu dan kemudian ke server.

2. Gunakan program terminal serial, seperti PuTTY atauscreen, untuk terhubung ke server. Untuk informasi selengkapnya, lihat the section called “Buat koneksi serial ke server”.
3. Tekan Enter untuk mengakses prompt perintah Outpost Configuration Tool.

```
Outpost>
```

> **Note**
>
> Jika Anda melihat lampu merah persisten di dalam sasis server di sisi kiri setelah Anda menyalakan dan Anda tidak dapat terhubung ke Outpost Configuration Tool, Anda mungkin perlu mematikan dan menguras server untuk melanjutkan. Untuk menguras server, lepaskan semua jaringan dan kabel daya, tunggu lima menit, lalu nyalakan dan sambungkan jaringan lagi.

4. Gunakan export untuk memasukkan kredensil IAM Anda ke Outpost Configuration Tool. Jika Anda menggunakan pihak ketiga untuk menginstal server, Anda harus memberikan kredensi IAM kepada pihak ketiga.

   Untuk mengautentikasi, Anda harus mengekspor empat variabel berikut. Ekspor satu variabel pada satu waktu. Jangan menyertakan spasi sebelum atau sesudah tanda sama (=).

   - `AWS_ACCESS_KEY_ID=`*`akses-kunci-id`*
   - `AWS_SECRET_ACCESS_KEY=`*`kunci akses-rahasia`*
   - `AWS_SESSION_TOKEN=`*`token sesi`*
     - Gunakan AWS CLI `GetSessionToken` perintah untuk mendapatkan`AWS_SESSION_TOKEN`. Untuk informasi selengkapnya, lihat get-session-token di Command Reference.AWS CLI

       > **Note**
       >
       > Anda harus memiliki AWSOutpostsAuthorizeServerPolicyketerikatan pada peran IAM Anda untuk mendapatkan. `AWS_SESSION_TOKEN`

     - Untuk menginstal AWS CLI, lihat Menginstal atau memperbarui AWS CLI versi terbaru di Panduan AWS CLI Pengguna untuk Versi 2.
   - `AWS_DEFAULT_REGION=`*`Wilayah`*

Gunakan Wilayah induk dari server Outpost sebagai nilai untuk`AWS_DEFAULT_REGION`. Jika Anda menggunakan pihak ketiga untuk menginstal server, Anda harus memberikan pihak ketiga dengan Wilayah induk.

Output dalam contoh berikut menunjukkan ekspor yang berhasil.

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

5. Gunakan start-connection untuk membuat koneksi aman ke Wilayah.

   Output dalam contoh berikut menunjukkan koneksi berhasil dimulai.

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connection-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

6. Tunggu sekitar 5 menit.
7. Gunakan get-connection untuk memeriksa apakah koneksi ke Wilayah telah dibuat.

   Output dalam contoh berikut menunjukkan koneksi yang berhasil.

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

Setelah `keys_exchanged` dan `connection_established` berubah`True`, server Outpost secara otomatis disediakan dan diperbarui ke perangkat lunak dan konfigurasi terbaru.

> **Note**
>
> Perhatikan hal berikut tentang proses penyediaan:
>
> - Setelah aktivasi selesai, dapat memakan waktu hingga 10 jam hingga server Outpost Anda dapat digunakan.
> - Anda harus menjaga daya dan jaringan server Outpost tetap terhubung dan stabil selama proses ini.
> - Adalah normal jika tautan layanan berfluktuasi selama proses ini.
> - Jika `exchange_active` ya`True`, koneksi masih terjalin. Coba lagi dalam 5 menit.
> - Jika `keys_exchanged` atau `connection_established` sedang`False`, dan jika `exchange_active` ada`True`, koneksi masih terjalin. Coba lagi dalam 5 menit.
> - Jika `keys_exchanged` atau `connection_established` `False` bahkan setelah 1 jam, hubungi AWS Support Pusat.
> - Jika pesan `primary_status: No such asset id found.` muncul, konfirmasikan hal berikut:
>   - Anda menentukan Wilayah yang benar.
>   - Anda menggunakan akun yang sama dengan yang digunakan untuk memesan server Outpost.
>
>   Jika Region benar dan Anda menggunakan akun yang sama dengan yang digunakan untuk memesan server Outpost, hubungi AWS Support Pusat.
> - `LifeCycleStatus`Atribut Outpost akan bertransisi dari `Provisioning` ke`Active`. Anda kemudian akan menerima email yang memberi tahu Anda bahwa server Outpost Anda disediakan dan diaktifkan.
> - Anda tidak perlu mengotorisasi ulang server Outposts setelah server Outposts diaktifkan.

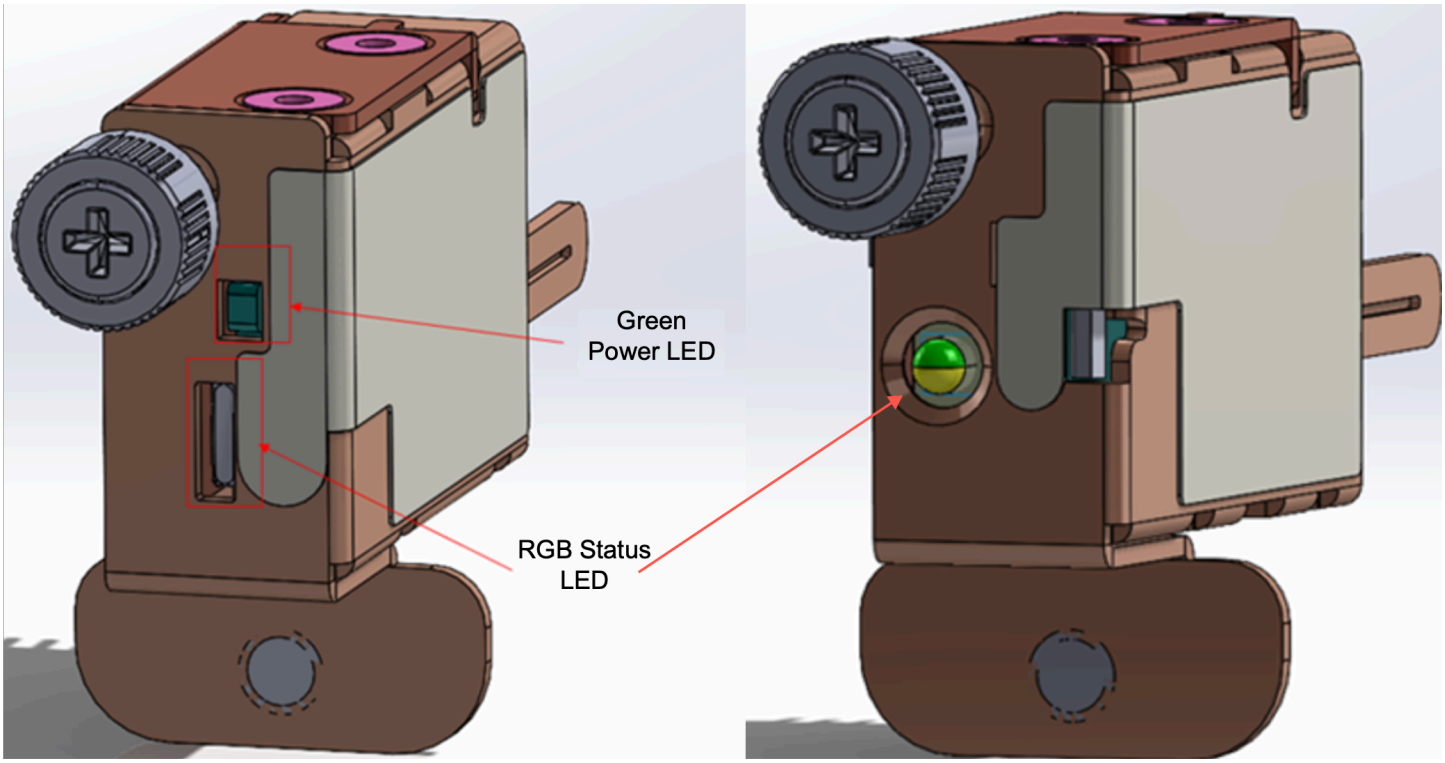
8. Setelah Anda membuat koneksi yang sukses, Anda dapat memutuskan sambungan laptop Anda dari server.

Verifikasi LED NSK

Setelah proses penyediaan selesai, periksa LED NSK.

AWS Outposts mendukung dua versi NSK: Atlas 2.0 dan Atlas 3.0. Kedua versi NSK memiliki LED Status RGB. Selain itu, Atlas 3.0 memiliki Power LED hijau.

Gambar berikut menunjukkan lokasi LED pada Atlas 2.0 dan Atlas 3.0:



Atlas 3.0 Atlas 2.0

Untuk memverifikasi Status dan LED Daya pada NSK

1. Periksa warna LED Status RGB. Jika warnanya hijau, NSK sehat. Jika warnanya tidak hijau, hubungi AWS Support.
2. Jika Anda memiliki Atlas 3.0 NSK, periksa LED Daya hijau. Jika lampu hijau menyala, NSK terhubung dengan benar ke host dan memiliki daya. Jika lampu hijau tidak menyala, hubungi AWS Support.

Referensi perintah Alat Konfigurasi Outpost

Outpost Configuration Tool menyediakan perintah berikut.

Commands

Ekspor

ekspor

Gunakan export untuk mengatur kredenal IAM sebagai variabel lingkungan.

Sintaks

```
Outpost>export variable=value
```

exportmengambil pernyataan penugasan variabel.

Harus menggunakan format berikut: *variable*=*value*

Untuk mengautentikasi, Anda harus mengekspor empat variabel berikut. Ekspor satu variabel pada satu waktu. Jangan menyertakan spasi sebelum atau sesudah tanda sama (=).

- AWS_ACCESS_KEY_ID=*akses-kunci-id*
- AWS_SECRET_ACCESS_KEY=*kunci akses-rahasia*
- AWS_SESSION_TOKEN=*token sesi*
- AWS_DEFAULT_REGION=*Wilayah*

  Gunakan Wilayah induk dari server Outpost sebagai nilai untukAWS_DEFAULT_REGION.

Example : impor kredensitas yang berhasil

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
```

```
result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

Gema

gema

Gunakan echo untuk menampilkan nilai yang Anda tetapkan untuk variabel menggunakan export perintah.

Sintaks

```
Outpost>echo $variable-name
```

Nama variabel dapat berupa salah satu dari yang berikut:

- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_SESSION_TOKEN
- AWS_DEFAULT_REGION

Example : Sukses

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum

---

Outpost>echo $AWS_DEFAULT_REGION

variable name: AWS_DEFAULT_REGION
variable value: us-west-2
checksum: example-checksum
```

Example : Kegagalan karena nilai variabel tidak disetel dengan export perintah

```
Outpost> echo $AWS_ACCESS_KEY_ID

error_type: execution_error
error_attributes:
  AWS_ACCESS_KEY_ID: no value set
error_message: No value set for AWS_ACCESS_KEY_ID using export.
checksum: example-checksum
```

Example : Kegagalan karena nama variabel tidak valid

```
Oupost>echo $foo

error_type: invalid_argument
error_attributes:
  foo: invalid variable name
error_message: Variables can only be AWS credentials.
```

```
checksum: example-checksum
```

Example : Kegagalan karena masalah sintaks

```
Outpost>echo AWS_SECRET_ACCESS_KEY

error_type: invalid_argument
error_attributes:
  AWS_SECRET_ACCESS_KEY: not a variable
error_message: Expecting $ before variable name.
checksum: example-checksum
```

Jelaskan tautan

jelaskan-link

Gunakan describe-links untuk mengembalikan informasi tentang tautan jaringan di server. Server pos terdepan harus memiliki satu tautan layanan dan satu tautan antarmuka jaringan lokal (LNI).

Sintaks

```
Outpost>describe-links
```

describe-linkstidak membutuhkan argumen.

Jelaskan IP

jelaskan-ip

Gunakan describe-ip untuk mengembalikan status penetapan IP dan konfigurasi setiap tautan yang terhubung.

Sintaks

```
Outpost>describe-ip
```

describe-iptidak membutuhkan argumen.

Jelaskan penyelesaian

jelaskan-selesaikan

Gunakan describe-resolve untuk menentukan apakah server Outpost dapat mencapai resolver DNS dan menyelesaikan alamat IP dari titik akhir konfigurasi Outpost di Wilayah. Membutuhkan setidaknya satu tautan dengan konfigurasi IP.

Sintaks

```
Outpost>describe-resolve
```

describe-resolvetidak membutuhkan argumen.

Jelaskan jangkauan

deskripsi-jangkauan

Gunakan describe-reachability untuk menentukan apakah server Outpost dapat mencapai titik akhir konfigurasi Outpost di Wilayah. Membutuhkan konfigurasi DNS yang berfungsi, yang dapat Anda tentukan dengan menggunakandescribe-resolve.

Sintaks

```
Outpost>describe-reachability
```

describe-reachabilitytidak membutuhkan argumen.

Mulai koneksi

start-koneksi

Gunakan start-connection untuk memulai koneksi dengan layanan Outpost di Wilayah. Perintah ini mendapatkan kredensi Signature Version 4 (SigV4) dari variabel lingkungan yang Anda muat. export Koneksi berjalan secara asinkron dan segera kembali. Untuk memeriksa status koneksi, gunakanget-connection.

Sintaks

```
Outpost>start-connection [0|1]
```

start-connectionmengambil indeks koneksi opsional untuk memulai koneksi lain. Hanya nilai `0` dan 1 valid.

Example : koneksi dimulai

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connecdtion-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

Dapatkan koneksi

dapatkan-koneksi

Gunakan get-connection untuk mengembalikan status koneksi.

Sintaks

```
Outpost>get-connection [0|1]
```

get-connectionmengambil indeks koneksi opsional untuk mengembalikan status koneksi lain. Hanya nilai `0` dan 1 valid.

Example : koneksi yang sukses

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
```

```
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

Catatan:

- Jika `exchange_active` ya`True`, koneksi masih terjalin. Coba lagi dalam 5 menit.
- Jika `keys_exchanged` atau `connection_established` sedang`False`, dan jika `exchange_active` ada`True`, koneksi masih terjalin. Coba lagi dalam 5 menit.

Jika masalah berlanjut setelah 1 jam, hubungi AWS Support Pusat.

Luncurkan instance di server Outpost Anda

Setelah Outpost Anda diinstal dan kapasitas komputasi dan penyimpanan tersedia untuk digunakan, Anda dapat memulai dengan membuat sumber daya. Misalnya, Anda dapat meluncurkan instans Amazon EC2.

Prasyarat

Anda harus menginstal Outpost di situs Anda. Untuk informasi selengkapnya, lihat Buat Outpost dan pesan kapasitas Outpost.

Tugas

- Langkah 1: Buat subnet
- Langkah 2: Luncurkan instance di Outpost
- Langkah 3: Konfigurasikan konektivitas
- Langkah 4: Uji konektivitas

Langkah 1: Buat subnet

Anda dapat menambahkan subnet Outpost ke VPC apa pun di AWS Region for the Outpost. Ketika Anda melakukannya, VPC juga mencakup 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 2: Luncurkan instance di Outpost

Untuk membuat subnet pos terdepan

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 dan tentukan rentang alamat IP untuk subnet.
5. Pilih Buat.
6. Setelah subnet dibuat, aktifkan subnet untuk antarmuka jaringan lokal.

Langkah 2: Luncurkan instance di Outpost

Anda dapat meluncurkan instans EC2 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 instans EC2 di subnet Outpost, Anda dapat menentukan key pair saat meluncurkan instance, seperti yang Anda lakukan untuk instance di subnet Availability Zone.

Pertimbangan

- Instans di server Outposts menyertakan volume penyimpanan instans tetapi bukan volume EBS. Pilih ukuran instans dengan penyimpanan instans yang cukup untuk memenuhi kebutuhan aplikasi Anda. Untuk informasi selengkapnya, lihat Volume penyimpanan instans di Panduan Pengguna Amazon EC2.

- Anda harus menentukan AMI hanya dengan satu snapshot. AMI dengan lebih dari satu snapshot tidak didukung.
- Data pada volume penyimpanan instance tetap ada setelah instance reboot tetapi tidak bertahan setelah penghentian instance. Untuk menyimpan data jangka panjang pada volume penyimpanan instans Anda di luar masa pakai instans, pastikan untuk mencadangkan data ke penyimpanan persisten, seperti bucket Amazon S3 atau perangkat penyimpanan jaringan di jaringan lokal Anda.
- Untuk menghubungkan instans di subnet Outpost ke jaringan lokal, Anda harus menambahkan antarmuka jaringan lokal, seperti yang dijelaskan dalam prosedur berikut.

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 konsol Amazon EC2. Kami memilih subnet Outpost untuk Anda, dan hanya menampilkan jenis instans yang didukung oleh server Outposts Anda.
5. Pilih jenis instans yang didukung oleh server Outposts Anda.
6. (Opsional) Anda dapat menambahkan antarmuka jaringan lokal sekarang atau setelah Anda membuat instance. Untuk menambahkannya sekarang, perluas Konfigurasi jaringan lanjutan dan pilih Tambahkan antarmuka jaringan. Pilih subnet Outpost. Ini menciptakan antarmuka jaringan untuk instance menggunakan indeks perangkat 1. Jika Anda menentukan 1 sebagai indeks perangkat LNI untuk subnet Outpost, maka antarmuka jaringan ini akan menjadi antarmuka jaringan lokal untuk instance tersebut.
7. Selesaikan wizard untuk meluncurkan instance di subnet Outpost Anda. Untuk informasi selengkapnya, lihat berikut ini di Panduan Pengguna Amazon EC2:
   - Linux - Luncurkan instance menggunakan wizard instance peluncuran baru
   - Windows - Luncurkan instance menggunakan wizard instance peluncuran baru

Langkah 3: Konfigurasikan konektivitas

Jika Anda tidak menambahkan antarmuka jaringan lokal ke instans Anda selama peluncuran instance, Anda harus melakukannya sekarang. Untuk informasi selengkapnya, lihat Menambahkan LNI setelah peluncuran.

Anda harus mengkonfigurasi antarmuka jaringan lokal untuk contoh dengan alamat IP dari jaringan lokal Anda. Biasanya, Anda melakukan ini dengan menggunakan DHCP. Untuk informasi, lihat dokumentasi untuk sistem operasi yang berjalan pada instance. Cari informasi tentang mengkonfigurasi antarmuka jaringan tambahan dan alamat IP sekunder.

Langkah 4: 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 antarmuka jaringan lokal 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 instance 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 instans Linux, lihat Connect ke instans Linux Anda di Panduan Pengguna Amazon EC2. Untuk informasi tentang menghubungkan ke instans Windows, lihat Connect ke instans Windows Anda di Panduan Pengguna Amazon EC2.

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 konsol Amazon EC2 di halaman detail instans.
2. Bergantung pada sistem operasi Anda, gunakan ssh atau sambungkan rdp ke alamat IP pribadi dari instans Outpost Anda.
3. Jalankan ping perintah dari instance Outpost Anda, dengan menentukan 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
```

AWS Outposts konektivitas ke AWS Wilayah

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

> **Note**
>
> Anda tidak dapat menggunakan konektivitas pribadi untuk koneksi tautan layanan Anda yang menghubungkan server Outpost Anda ke AWS Wilayah atau Wilayah AWS Outposts asal Anda.

Daftar Isi

Konektivitas melalui tautan layanan

Selama AWS Outposts penyediaan, Anda atau AWS membuat koneksi tautan layanan yang menghubungkan Pos Luar Anda kembali ke AWS Wilayah atau AWS Outposts Wilayah asal yang Anda pilih. 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

Outpost mampu membuat tautan layanan VPN kembali ke AWS Wilayah melalui konektivitas Wilayah publik. Untuk melakukannya, Outpost membutuhkan konektivitas ke rentang IP publik AWS Wilayah, baik melalui internet publik atau antarmuka virtual AWS Direct Connect publik. Konektivitas ini dapat melalui rute tertentu di tautan layanan VLAN, atau melalui rute default 0.0.0.0/0. Untuk informasi selengkapnya tentang rentang publik AWS, lihat Rentang Alamat AWS IP.

Setelah tautan layanan dibuat, Pos Luar dalam layanan dan dikelola oleh AWS. Tautan layanan digunakan untuk lalu lintas berikut:

- Manajemen lalu lintas ke Outpost melalui tautan layanan, termasuk lalu lintas pesawat kontrol internal, pemantauan sumber daya internal, dan pembaruan firmware dan perangkat lunak.

- Lalu lintas antara Outpost dan VPC terkait, termasuk lalu lintas pesawat data pelanggan.

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 Untuk informasi tentang MTU yang diperlukan antara instans di Pos Luar dan instans di AWS Wilayah melalui tautan layanan, lihat Unit transmisi maksimum jaringan (MTU) untuk instans Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

Rekomendasi bandwidth tautan layanan

Untuk pengalaman dan ketahanan yang optimal, AWS rekomendasikan agar Anda menggunakan konektivitas redundan minimal 500 Mbps untuk koneksi tautan layanan ke Wilayah. AWS Penggunaan maksimum untuk setiap server Outpost adalah 500 Mbps. Untuk meningkatkan kecepatan koneksi, gunakan beberapa server Outpost. Misalnya, jika Anda memiliki tiga AWS Outposts server, kecepatan koneksi maksimum meningkat menjadi 1,5 Gbps (1.500 Mbps). Untuk informasi selengkapnya, lihat Lalu lintas tautan layanan untuk server.

Persyaratan bandwidth tautan AWS Outposts layanan Anda bervariasi tergantung pada karakteristik beban kerja, seperti ukuran AMI, elastisitas aplikasi, kebutuhan kecepatan burst, dan lalu lintas VPC Amazon ke Wilayah. Perhatikan bahwa AWS Outposts server tidak men-cache AMI. AMI diunduh dari Wilayah dengan setiap peluncuran instans.

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

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 VPC terkait

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	1024-65535	Layanan Link IP	53	DHCP menyediakan server DNS
UDP	443, 1024-65535	Layanan Link IP	443	AWS Outposts Titik akhir Tautan Layanan
TCP	1024-65535	Layanan Link IP	443	AWS Outposts Titik akhir pendaftaran

> **Note**
>
> Instance di Outpost tidak dapat menggunakan tautan layanan untuk berkomunikasi dengan instans di Outposts lain. Manfaatkan routing melalui gateway lokal atau antarmuka jaringan lokal untuk berkomunikasi antara Outposts.

Pembaruan dan tautan layanan

AWS memelihara koneksi jaringan yang aman antara server Outpost Anda dan AWS Wilayah induknya. Koneksi jaringan ini, yang disebut link layanan, sangat penting dalam mengelola Outpost dengan menyediakan lalu lintas intra-VPC antara Outpost dan Region. AWS AWS Praktik terbaik

yang Dirancang dengan Baik merekomendasikan penerapan aplikasi di dua Outposts yang diasuh ke Availability Zone yang berbeda dengan desain aktif-aktif. Untuk informasi selengkapnya, lihat Pertimbangan Desain dan Arsitektur Ketersediaan AWS Outposts Tinggi.

Tautan layanan diperbarui secara berkala untuk menjaga kualitas dan kinerja operasional. Selama pemeliharaan, Anda mungkin mengamati periode singkat latensi dan kehilangan paket pada jaringan ini yang mengakibatkan dampak pada beban kerja yang bergantung pada konektivitas VPC ke sumber daya yang dihosting di wilayah. Namun, lalu lintas yang melintasi Antarmuka Jaringan Lokal (LNI) tidak akan terpengaruh. Anda dapat menghindari dampak pada aplikasi Anda dengan mengikuti praktik terbaik AWS Well-Architected dan dengan memastikan aplikasi Anda tahan terhadap kegagalan atau aktivitas pemeliharaan yang memengaruhi satu server Outpost.

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.

Outposts dan situs

Kelola Outposts dan situs untuk. AWS Outposts

Anda dapat menandai Outposts dan situs untuk membantu Anda mengidentifikasi mereka atau mengkategorikannya sesuai dengan kebutuhan organisasi Anda. Untuk informasi selengkapnya tentang penandaan, lihat Menandai AWS Sumber Daya di Panduan.Referensi Umum AWS

Topik

- Kelola Outposts
- Mengelola situs Outpost

Kelola Outposts

AWS Outposts termasuk perangkat keras dan sumber daya virtual yang dikenal sebagai Outposts. Gunakan bagian ini untuk membuat dan mengelola Outposts, termasuk mengubah nama, dan menambahkan atau melihat detail atau tag.

Untuk membuat Outpost

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 Outposts.
4. Pilih Buat Pos Terdepan.
5. Pilih jenis perangkat keras untuk Outpost ini.
6. Masukkan nama dan deskripsi untuk Outpost Anda.
7. Pilih Availability Zone untuk Outpost Anda.
8. (Opsional) Pilih opsi Konektivitas pribadi. Untuk VPC dan Subnet, pilih VPC dan subnet di AWS akun dan Availability Zone yang sama dengan Outpost Anda.

> **Note**
>
> Jika Anda perlu membatalkan konektivitas pribadi untuk Outpost Anda, Anda harus menghubungi Enterprise AWS Support.

9. Dari ID Situs, lakukan salah satu hal berikut:

   - Untuk memilih situs yang ada, pilih situs.
   - Untuk membuat situs baru, pilih Buat situs, klik Berikutnya, dan masukkan informasi tentang situs Anda di jendela baru.

     Setelah Anda membuat situs, kembali ke jendela ini untuk memilih situs. Anda mungkin perlu me-refresh daftar situs untuk melihat situs baru. Untuk me-refresh data Anda, pilih ikon refresh ( ).

     Untuk informasi selengkapnya, lihat the section called “Situs”.

10. Pilih Buat Pos Terdepan.

> **Tip**
>
> Untuk menambah kapasitas ke Outpost baru Anda, Anda harus melakukan pemesanan.

Gunakan langkah-langkah berikut untuk mengedit nama dan deskripsi Outpost.

Untuk mengedit nama dan deskripsi Outpost

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 Outposts.
4. Pilih Outpost, lalu pilih Actions, Edit Outpost.
5. Ubah nama dan deskripsi.

   Untuk Nama, masukkan nama.

   Untuk Deskripsi, masukkan deskripsi.
6. Pilih Simpan perubahan.

Gunakan langkah-langkah berikut untuk melihat detail Pos Luar.

Untuk melihat rincian Outpost

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 Outposts.
4. Pilih Outpost, lalu pilih Actions, View details.

Anda juga dapat menggunakan AWS CLI untuk melihat rincian Outpost.

Untuk melihat detail Outpost dengan AWS CLI

- Gunakan perintah get-outpost AWS CLI .

Gunakan langkah-langkah berikut untuk mengelola tag di Outpost.

Untuk mengelola tag Outpost

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 Outposts.
4. Pilih Outpost, lalu pilih Actions, Manage tags.
5. Menambah atau menghapus tanda.

   Untuk menambahkan tag, pilih Tambahkan tag baru dan lakukan hal berikut:

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

   Untuk menghapus tag, pilih Hapus di sebelah kanan kunci dan nilai tag.
6. Pilih Simpan perubahan.

Mengelola situs Outpost

Bangunan fisik yang dikelola pelanggan tempat AWS akan memasang Pos Luar Anda. Sebuah situs harus memenuhi fasilitas, jaringan, dan persyaratan daya untuk Outpost Anda. Untuk informasi selengkapnya, lihat Persyaratan.

Untuk membuat situs Outpost

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 Situs.
4. Pilih Buat situs.
5. Pilih jenis perangkat keras yang didukung untuk situs.
6. Masukkan nama, deskripsi, dan alamat operasi untuk situs Anda. Jika Anda memilih untuk mendukung rak di situs, masukkan informasi berikut:
   - Berat maksimum - Tentukan berat rak maksimum yang dapat didukung situs ini.
   - Power draw — Tentukan dalam kVA daya tarik yang tersedia pada posisi penempatan perangkat keras untuk rak.
   - Opsi daya - Tentukan opsi daya yang dapat Anda sediakan untuk perangkat keras.
   - Konektor daya — Tentukan konektor daya yang AWS harus direncanakan untuk menyediakan koneksi ke perangkat keras.
   - Penurunan umpan daya - Tentukan apakah umpan daya berada di atas atau di bawah rak.
   - Kecepatan uplink - Tentukan kecepatan uplink yang harus didukung rak untuk koneksi ke Wilayah.
   - Jumlah uplink — Tentukan jumlah uplink untuk setiap perangkat jaringan Outpost yang ingin Anda gunakan untuk menghubungkan rak ke jaringan Anda.
   - Jenis serat - Tentukan jenis serat yang akan Anda gunakan untuk memasang Outpost ke jaringan Anda.
   - Standar optik - Tentukan jenis standar optik yang akan Anda gunakan untuk memasang Outpost ke jaringan Anda.
   - Catatan — Tentukan catatan tentang situs.
7. Baca persyaratan fasilitas dan pilih Saya telah membaca persyaratan fasilitas.
8. Pilih Buat situs.

Gunakan langkah-langkah berikut untuk mengedit situs Outpost.

Untuk mengedit situs

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 Situs.
4. Pilih situs, lalu pilih Tindakan, Edit situs.
5. Anda dapat mengubah nama, deskripsi, alamat operasi, dan detail situs.

   Jika Anda mengubah alamat operasi, ketahuilah bahwa perubahan tidak akan menyebar ke pesanan yang ada.
6. Pilih Simpan perubahan.

Gunakan langkah-langkah berikut untuk melihat detail situs Outpost.

Untuk melihat detail situs

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 Situs.
4. Pilih situs, lalu pilih Tindakan, Lihat detail.

Gunakan langkah-langkah berikut untuk mengelola tag di situs Outpost.

Untuk mengelola tag situs

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 Situs.
4. Pilih situs, lalu pilih Tindakan, Kelola tag.
5. Menambah atau menghapus tanda.

   Untuk menambahkan tag, pilih Tambahkan tag baru dan lakukan hal berikut:

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

   Untuk menghapus tag, pilih Hapus di sebelah kanan kunci dan nilai tag.
6. Pilih Simpan perubahan.

Kembalikan AWS Outposts server

Jika AWS Outposts mendeteksi cacat di server, kami akan memberi tahu Anda, memulai proses penggantian untuk mengirimi Anda server baru, dan memberi Anda label pengiriman melalui AWS Outposts konsol.

Jika Anda ingin mengembalikan server karena server mencapai akhir masa kontrak atau karena alasan lain, hubungi AWS Support Pusat.

Topik

Langkah-langkah berikut menjelaskan cara mengembalikan server ke AWS.

1. Siapkan server untuk kembali

Untuk mempersiapkan server untuk pengembalian, batalkan pembagian sumber daya, data cadangan, hapus antarmuka jaringan lokal, dan hentikan instance aktif.

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 perintah disassociate-resource-share.

   Untuk daftar sumber daya Outpost yang dapat dibagikan, lihat Sumber daya Pos Luar yang Dapat Dibagikan.
2. Buat cadangan data yang disimpan dalam penyimpanan instans instans Amazon EC2 yang berjalan di server. AWS Outposts
3. Hapus antarmuka jaringan lokal yang terkait dengan instance yang berjalan di server.

4. Hentikan instans aktif yang terkait dengan subnet di Outpost Anda. Untuk menghentikan instans, ikuti petunjuk di Menghentikan instans Anda di Panduan Pengguna Amazon EC2.

2. Dapatkan label pengiriman kembali

> **Important**
>
> Anda hanya boleh menggunakan label pengiriman yang AWS menyediakan. Jangan membuat label pengiriman Anda sendiri.

Dapatkan label pengiriman Anda berdasarkan alasan pengembalian Anda.

Shipping label for a server that is being replaced

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Pada panel navigasi, pilih Pesanan.
3. Di bawah Ringkasan pesanan pengganti, pilih Cetak label pengembalian dan pilih ID konfigurasi server yang akan Anda kembalikan.

Shipping label for a server that is not being replaced

1. AWS Support Pusat Kontak.
2. Minta label pengiriman untuk server yang ingin Anda kembalikan.

3. Kemas server

Untuk mengemas server Anda, gunakan kotak dan bahan kemasan tempat server awalnya masuk. Anda juga dapat menggunakan kotak tempat server pengganti masuk. Atau, hubungi AWS Support Pusat untuk meminta kotak. Setelah mengemas server, tempelkan label pengiriman yang AWS disediakan.

4. Kembalikan server melalui kurir

Anda harus mengembalikan server melalui kurir yang ditunjuk untuk negara Anda. Anda dapat mengirimkan server ke kurir atau menjadwalkan hari dan waktu yang Anda inginkan agar kurir

mengambil server. Label pengiriman yang AWS menyediakan berisi alamat yang benar untuk mengembalikan server.

Tabel berikut menunjukkan siapa yang harus dihubungi untuk negara tempat Anda mengirim:

Negara	Kontak
Argentina	AWS Support Pusat Kontak. Dalam permintaan Anda, sertakan informasi berikut: • Nomor pelacakan yang ada di label pengiriman AWS yang disediakan • Tanggal dan waktu yang Anda inginkan kurir untuk mengambil server • Nama kontak • Nomor telepon • Alamat email
Bahrain	
Brazil	
Brunei	
Kanada	
Chili	
Kolombia	
Hong Kong	
India	
Indonesia	
Jepang	
Malaysia	
Nigeria	
Oman	
Panama	
Peru	
Filipina	
Serbia	

Negara	Kontak
Singapura	
Afrika Selatan	
Korea Selatan	
Taiwan	
Thailand	
Uni Emirat Arab	
Vietnam	
Amerika Serikat	Hubungi UPS. Anda dapat mengembalikan server dengan cara berikut: • Kembalikan server selama pengambilan UPS rutin di situs Anda. • Drop-off server di lokasi UPS. • Jadwalkan penjemputan untuk tanggal dan waktu yang Anda inginkan. Masukkan nomor pelacakan dari label pengiriman AWS yang disediakan untuk pengiriman gratis.

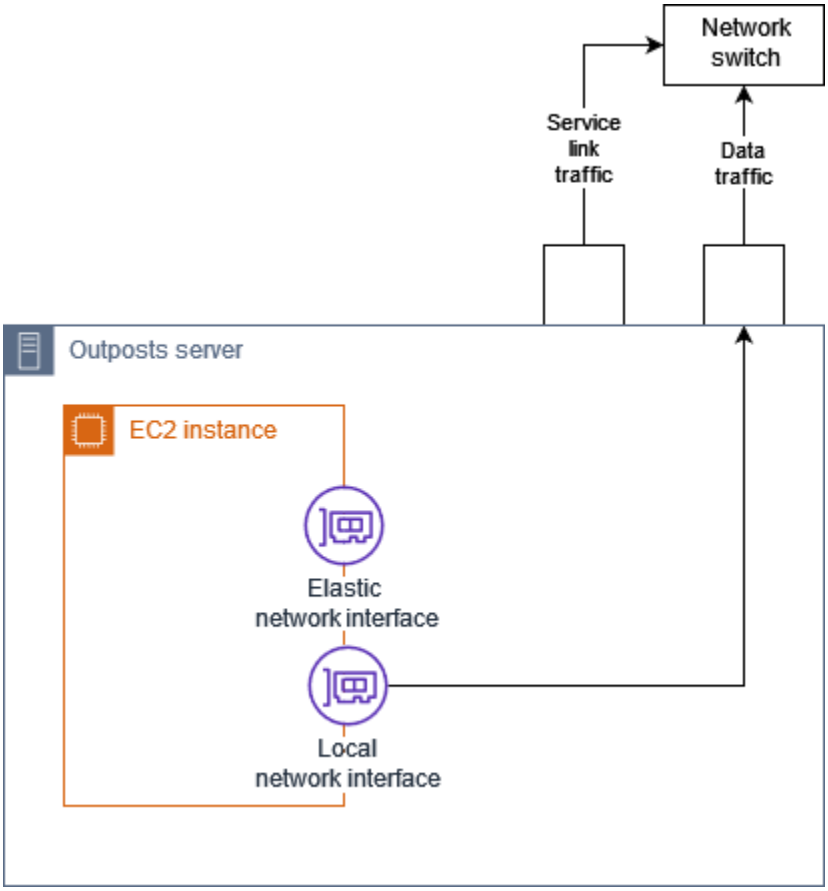
Negara	Kontak
Semua negara lain	Hubungi DHL. Anda dapat mengembalikan server dengan cara berikut: • Drop-off server di lokasi DHL. • Jadwalkan penjemputan untuk tanggal dan waktu yang Anda inginkan. Masukkan nomor DHL Waybill dari label pengiriman AWS yang disediakan untuk pengiriman gratis. Jika Anda mendapatkan kesalahan berikut`Courier pickup cannot be scheduled for an import shipment`, biasanya berarti bahwa negara penjemputan yang Anda pilih tidak cocok dengan negara penjemputan pada label pengiriman kembali. Pilih negara asal kiriman dan coba lagi.

Antarmuka jaringan lokal

Dengan AWS Outposts server, antarmuka jaringan lokal (LNI) adalah komponen jaringan logis yang menghubungkan instans Amazon EC2 di subnet Outposts Anda ke jaringan lokal Anda.

Antarmuka jaringan lokal berjalan langsung di jaringan area lokal Anda. Dengan jenis konektivitas lokal ini, Anda tidak memerlukan router atau gateway untuk berkomunikasi dengan peralatan lokal Anda. Antarmuka jaringan lokal diberi nama mirip dengan antarmuka jaringan atau antarmuka jaringan elastis. Kami membedakan antara dua antarmuka dengan selalu menggunakan lokal ketika kami merujuk ke antarmuka jaringan lokal.

Setelah Anda mengaktifkan antarmuka jaringan lokal pada subnet Outpost, Anda dapat mengonfigurasi instans EC2 di subnet Outpost untuk menyertakan antarmuka jaringan lokal selain antarmuka jaringan elastis. Antarmuka jaringan lokal terhubung ke jaringan lokal sementara antarmuka jaringan terhubung ke VPC. Diagram berikut menunjukkan instans EC2 pada server Outposts dengan antarmuka jaringan elastis dan antarmuka jaringan lokal.



Anda harus mengkonfigurasi sistem operasi untuk mengaktifkan antarmuka jaringan lokal untuk berkomunikasi di jaringan area lokal Anda, seperti yang Anda lakukan untuk peralatan lokal lainnya. Anda tidak dapat menggunakan set opsi DHCP di VPC untuk mengonfigurasi antarmuka jaringan lokal karena antarmuka jaringan lokal berjalan di jaringan area lokal Anda.

Elastic network interface bekerja persis seperti halnya untuk instance di subnet Availability Zone. Misalnya, Anda dapat menggunakan koneksi jaringan VPC untuk mengakses titik akhir Regional publik Layanan AWS, atau Anda dapat menggunakan titik akhir VPC antarmuka untuk mengakses menggunakan. Layanan AWS AWS PrivateLink Untuk informasi selengkapnya, lihat AWS Outposts konektivitas ke AWS Wilayah.

Daftar Isi

Dasar-dasar antarmuka jaringan lokal

Antarmuka jaringan lokal menyediakan akses ke jaringan lapisan-dua fisik. VPC adalah jaringan layer-tiga tervirtualisasi. Antarmuka jaringan lokal tidak mendukung komponen jaringan VPC. Komponen-komponen ini termasuk grup keamanan, daftar kontrol akses jaringan, router virtual atau tabel rute, dan log aliran. Antarmuka jaringan lokal tidak menyediakan server Outpost dengan visibilitas ke dalam aliran lapisan tiga VPC. Sistem operasi host dari instance ini memang memiliki visibilitas penuh ke dalam frame dari jaringan fisik. Anda dapat menerapkan logika firewall standar ke informasi dalam bingkai ini. Namun, komunikasi ini terjadi di dalam instance tetapi di luar lingkup konstruksi tervirtualisasi.

Pertimbangan

- Antarmuka jaringan lokal mendukung protokol ARP dan DHCP. Mereka tidak mendukung pesan siaran L2 umum.
- Kuota untuk antarmuka jaringan lokal keluar dari kuota Anda untuk antarmuka jaringan. Untuk informasi selengkapnya, lihat Antarmuka jaringan di Panduan Pengguna Amazon VPC.
- Setiap instans EC2 dapat memiliki satu antarmuka jaringan lokal.
- Antarmuka jaringan lokal tidak dapat menggunakan antarmuka jaringan utama (eth0) dari instance.

- Server Outposts dapat meng-host beberapa instans EC2, masing-masing dengan antarmuka jaringan lokal.

> **Note**
>
> Instans EC2 dalam server yang sama dapat berkomunikasi secara langsung tanpa mengirim data di luar server Outposts. Komunikasi ini mencakup lalu lintas melalui antarmuka jaringan lokal atau antarmuka jaringan elastis.

- Antarmuka jaringan lokal hanya tersedia untuk instance yang berjalan di subnet Outposts di server Outpost.
- Antarmuka jaringan lokal tidak mendukung mode promiscuous atau spoofing alamat MAC.

Kinerja

LNI dari setiap ukuran instans menyediakan sebagian dari bandwidth fisik 10 GbE LNI yang tersedia. Tabel berikut mencantumkan kinerja jaringan LNI untuk setiap jenis instance:

Jenis instans	Bandwidth acuan (Gbps)	Bandwidth lonjakan (Gbps)
c6id.large	0,1625	2.5
c6id.large	0,1625	2.5
c6id.xlarge	0.3125	2.5
c6id.2xlarge	0.625	2.5
c6id.4xlarge	1,25	2.5
c6id.8xlarge	2.5	2.5
c6id.12xlarge	3,75	3,75
c6id.16xlarge	5	5
c6id.24xlarge	7.5	7.5
c6id.32xlarge	10	10

Jenis instans	Bandwidth acuan (Gbps)	Bandwidth lonjakan (Gbps)
c6gd.medium	0,1625	4
c6gd.large	0.3125	4
c6gd.xlarge	0.625	4
c6gd.2xlarge	1,25	4
c6gd.4xlarge	2.5	4
c6gd.8xlarge	4.8	4.8
c6gd.12xlarge	7.5	7.5
c6gd.16xlarge	10	10

Grup keamanan

Secara desain, antarmuka jaringan lokal tidak menggunakan grup keamanan di VPC Anda. Grup keamanan mengontrol lalu lintas VPC masuk dan keluar. Antarmuka jaringan lokal tidak terpasang ke VPC. Antarmuka jaringan lokal dilampirkan ke jaringan lokal Anda. Untuk mengontrol lalu lintas masuk dan keluar pada antarmuka jaringan lokal, gunakan firewall atau strategi serupa, seperti yang Anda lakukan dengan peralatan lokal lainnya.

Pemantauan

CloudWatch metrik diproduksi untuk setiap antarmuka jaringan lokal, sama seperti untuk antarmuka jaringan elastis. Untuk informasi selengkapnya tentang instans Linux, lihat Memantau performa jaringan untuk instans EC2 Anda di Panduan Pengguna Amazon EC2. Untuk instans Windows, lihat Memantau kinerja jaringan untuk instans EC2 Anda di Panduan Pengguna Amazon EC2.

Alamat MAC

AWS menyediakan alamat MAC untuk antarmuka jaringan lokal. Antarmuka jaringan lokal menggunakan alamat yang dikelola secara lokal (LAA) untuk alamat MAC mereka. Antarmuka jaringan lokal menggunakan alamat MAC yang sama sampai Anda menghapus antarmuka. Setelah

Anda menghapus antarmuka jaringan lokal, hapus alamat MAC dari konfigurasi lokal Anda. AWS dapat menggunakan kembali alamat MAC yang tidak lagi digunakan.

Aktifkan subnet di server Outposts untuk antarmuka jaringan lokal

Gunakan perintah modify-subnet-attribute dari AWS CLI untuk mengaktifkan subnet Outpost untuk antarmuka jaringan lokal. Anda harus menentukan posisi antarmuka jaringan pada indeks perangkat. Semua instance yang diluncurkan di subnet Outpost yang diaktifkan menggunakan posisi perangkat ini untuk antarmuka jaringan lokal. Misalnya, nilai 1 menunjukkan bahwa antarmuka jaringan sekunder (eth1) untuk sebuah instance di subnet Outpost adalah antarmuka jaringan lokal.

Untuk mengaktifkan subnet Outpost untuk antarmuka jaringan lokal

Pada prompt perintah, gunakan perintah berikut untuk menentukan posisi perangkat untuk antarmuka jaringan lokal.

```
aws ec2 modify-subnet-attribute \
    --subnet-id subnet-1a2b3c4d \
    --enable-lni-at-device-index 1
```

Bekerja dengan antarmuka jaringan lokal

Gunakan bagian ini untuk memahami cara bekerja dengan antarmuka jaringan lokal.

Tugas

- Tambahkan antarmuka jaringan lokal
- Lihat antarmuka jaringan lokal
- Konfigurasikan sistem operasi

Tambahkan antarmuka jaringan lokal

Anda dapat menambahkan antarmuka jaringan lokal (LNI) ke instans Amazon EC2 di subnet Outposts selama atau setelah peluncuran. Anda melakukannya dengan menambahkan antarmuka jaringan sekunder ke instance, menggunakan indeks perangkat yang Anda tentukan saat mengaktifkan subnet Outpost untuk antarmuka jaringan lokal.

Pertimbangan

Saat Anda menentukan antarmuka jaringan sekunder menggunakan konsol, antarmuka jaringan dibuat menggunakan indeks perangkat 1. Jika ini bukan indeks perangkat yang Anda tentukan saat mengaktifkan subnet Outpost untuk antarmuka jaringan lokal, Anda dapat menentukan indeks perangkat yang benar dengan menggunakan AWS CLI atau SDK sebagai AWS gantinya. Misalnya, gunakan perintah berikut dari AWS CLI: create-network-interface dan attach-network-interface.

Untuk menambahkan LNI selama peluncuran instans

1. Di wizard peluncuran instance, pilih Edit di samping Pengaturan jaringan.
2. Perluas Konfigurasi jaringan lanjutan.
3. Pilih Tambahkan antarmuka jaringan. Ini menciptakan antarmuka jaringan menggunakan indeks perangkat 1. Jika Anda menentukan 1 sebagai indeks perangkat LNI untuk subnet Outpost, maka antarmuka jaringan ini akan menjadi antarmuka jaringan lokal untuk instance tersebut.
4. Pilih subnet Outpost, dan perbarui konfigurasi untuk antarmuka jaringan sesuai kebutuhan.
5. Selesaikan wizard untuk meluncurkan instance.

Untuk menambahkan LNI setelah peluncuran instance

1. Di panel navigasi, pilih Jaringan dan Keamanan, Antarmuka Jaringan.
2. Buat antarmuka jaringan
    a. Pilih Buat antarmuka jaringan.
    b. Pilih subnet Outpost yang sama dengan instance.
    c. Verifikasi bahwa alamat IPv4 Pribadi disetel ke Tetapkan otomatis.
    d. Pilih grup keamanan apa pun. Grup keamanan tidak berlaku untuk LNI, sehingga grup keamanan yang Anda pilih tidak relevan.
    e. Pilih Buat antarmuka jaringan.
3. Lampirkan antarmuka jaringan ke instance
    a. Pilih kotak centang untuk antarmuka jaringan yang baru dibuat.
    b. Pilih Tindakan, Lampirkan.
    c. Pilih instance.
    d. Pilih Lampirkan. Antarmuka jaringan terpasang pada indeks perangkat 1. Jika Anda menetapkan 1 sebagai indeks perangkat LNI untuk subnet Outpost, maka antarmuka jaringan ini adalah antarmuka jaringan lokal untuk instance tersebut.

Lihat antarmuka jaringan lokal

Saat instans dalam status berjalan, Anda dapat menggunakan konsol Amazon EC2 untuk melihat elastis network interface dan antarmuka jaringan lokal untuk instance di subnet Outpost Anda. Pilih instance dan pilih tab Networking.

Konsol menampilkan alamat IPv4 pribadi untuk LNI dari subnet CIDR. Alamat ini bukan alamat IP LNI, dan tidak dapat digunakan. Namun, alamat ini dialokasikan dari subnet CIDR, jadi Anda harus memperhitungkannya dalam ukuran subnet Anda. Anda harus mengatur alamat IP untuk LNI dalam sistem operasi tamu, baik secara statis atau melalui server DHCP Anda.

Konfigurasikan sistem operasi

Setelah Anda mengaktifkan antarmuka jaringan lokal, instans Amazon EC2 akan memiliki dua antarmuka jaringan, salah satunya adalah antarmuka jaringan lokal. Pastikan Anda mengonfigurasi sistem operasi instans Amazon EC2 yang Anda luncurkan untuk mendukung konfigurasi jaringan multi-homed.

Konektivitas jaringan lokal untuk server

Gunakan topik ini untuk memahami kabel jaringan dan persyaratan topologi untuk hosting server Outpost. Untuk informasi selengkapnya, lihat Antarmuka jaringan lokal.

Daftar Isi

Topologi server di jaringan Anda

Server Outpost membutuhkan dua koneksi berbeda ke peralatan jaringan Anda. Setiap koneksi menggunakan kabel yang berbeda dan membawa jenis lalu lintas yang berbeda. Beberapa kabel hanya untuk isolasi kelas lalu lintas, dan bukan untuk redundansi. Kedua kabel tidak perlu terhubung ke jaringan umum.

Tabel berikut menjelaskan jenis lalu lintas server Outpost dan label.

Label lalu lintas	Deskripsi
2	Lalu lintas tautan layanan — Lalu lintas ini memungkinkan komunikasi antara Pos Terdepan dan AWS Wilayah untuk pengelola an lalu lintas Outpost dan intra-VPC antara Wilayah dan Pos Luar. AWS Lalu lintas tautan layanan mencakup koneksi tautan layanan dari Pos Terdepan ke Wilayah. Tautan layanan adalah VPN atau VPN khusus dari Pos Luar ke Wilayah. Pos Terdepan terhubung ke Availabil ity Zone di Wilayah yang Anda pilih pada saat pembelian.
1	Lalu lintas tautan antarmuka jaringan lokal (LNI) - Lalu lintas ini memungkinkan komunikas i dari VPC Anda ke LAN lokal Anda melalui antarmuka jaringan lokal. Lalu lintas tautan lokal mencakup instance yang berjalan di Pos Luar yang berkomunikasi dengan jaringan lokal Anda. Lalu lintas tautan lokal juga dapat mencakup contoh yang berkomunikasi dengan internet melalui jaringan lokal Anda.

Konektivitas fisik server

Setiap server Outpost mencakup fisik non-redundan. Port memiliki kecepatan dan persyaratan konektornya sendiri sebagai berikut:

- 10Gbe - jenis konektor QSFP +

QSFP+Kabel

Kabel QSFP+memiliki konektor yang Anda pasang ke port 3 di server Outpost. Ujung lain dari kabel QSFP+memiliki empat antarmuka SFP+yang Anda sambungkan ke sakelar Anda. Dua antarmuka

sisi sakelar diberi label dan. 1 2 Kedua antarmuka diperlukan agar server Outpost berfungsi. Gunakan 2 antarmuka untuk lalu lintas tautan layanan dan 1 antarmuka untuk lalu lintas tautan LNI. Antarmuka yang tersisa tidak digunakan.

Lalu lintas tautan layanan untuk server

Konfigurasikan port tautan layanan pada sakelar Anda sebagai port akses yang tidak ditandai ke VLAN dengan gateway dan rute ke titik akhir Wilayah berikut:

- Titik akhir tautan layanan
- Titik akhir pendaftaran Outposts

Koneksi tautan layanan harus memiliki DNS publik yang tersedia bagi Pos Luar untuk menemukan titik akhir pendaftarannya di Wilayah. AWS Koneksi dapat memiliki perangkat NAT antara server Outpost dan titik akhir pendaftaran. Untuk informasi selengkapnya tentang rentang alamat publik AWS, lihat rentang alamat AWS IP di Panduan Pengguna Amazon VPC serta AWS Outposts titik akhir serta kuota di. Referensi Umum AWS

Untuk mendaftarkan server, buka port jaringan berikut:

- TCP 443
- UDP 443
- UDP 53

Kecepatan uplink

Setiap server Outposts membutuhkan kecepatan uplink minimal 20 Mbps ke Wilayah. AWS

Anda mungkin memerlukan uplink yang lebih cepat tergantung pada tautan LNI dan pemanfaatan tautan layanan Anda. Untuk informasi selengkapnya, lihat Rekomendasi bandwidth untuk tautan layanan.

Lalu lintas tautan antarmuka jaringan lokal (LNI)

Konfigurasikan port tautan LNI di perangkat jaringan hulu Anda sebagai port akses standar ke VLAN di jaringan lokal Anda. Jika Anda memiliki lebih dari satu VLAN, konfigurasikan semua port pada perangkat jaringan hulu sebagai port trunk. Konfigurasikan port pada perangkat jaringan hulu Anda untuk mengharapkan beberapa alamat MAC. Setiap instance yang diluncurkan di server akan

menggunakan alamat MAC. Beberapa perangkat jaringan menawarkan fitur keamanan port yang akan mematikan port yang melaporkan beberapa alamat MAC.

> **Note**
>
> AWS Outposts server tidak menandai lalu lintas VLAN. Jika Anda mengkonfigurasi LNI Anda sebagai trunk, Anda harus memastikan bahwa OS Anda menandai lalu lintas VLAN.

Contoh berikut menunjukkan cara mengonfigurasi penandaan VLAN untuk LNI Anda di Amazon Linux 2023. Jika Anda menggunakan distribusi Linux lain, lihat dokumentasi untuk distribusi Linux Anda tentang mengonfigurasi penandaan VLAN.

Contoh: Untuk mengonfigurasi penandaan VLAN untuk LNI Anda di Amazon Linux 2023 dan Amazon Linux 2

1. Pastikan modul 8021q dimuat ke dalam kernel. Jika tidak, muat menggunakan `modprobe` perintah.

   ```
   modinfo 8021q
   modprobe --first-time 8021q
   ```

2. Buat perangkat VLAN. Dalam contoh ini:

   - Nama antarmuka LNI adalah `ens6`
   - Id VLAN adalah `59`
   - Nama yang ditetapkan untuk perangkat VLAN adalah `ens6.59`

   ```
   ip link add link ens6 name ens6.59 type vlan id 59
   ```

3. Tidak wajib. Selesaikan langkah ini jika Anda ingin menetapkan IP secara manual. Dalam contoh ini kami menetapkan IP 192.168.59.205, di mana subnet CIDR adalah 192.168.59.0/24.

   ```
   ip addr add 192.168.59.205/24 brd 192.168.59.255 dev ens6.59
   ```

4. Aktifkan tautannya.

   ```
   ip link set dev ens6.59 up
   ```

Untuk mengonfigurasi antarmuka jaringan Anda di tingkat OS dan membuat penandaan VLAN berubah terus-menerus, lihat sumber daya berikut:

- Jika Anda menggunakan Amazon Linux 2, lihat Mengkonfigurasi antarmuka jaringan menggunakan ec2-net-utils untuk Amazon Linux di Panduan Pengguna Amazon EC2.
- Jika Anda menggunakan Amazon Linux 2023, lihat Layanan jaringan di Panduan Pengguna Amazon Linux 2023.

Penetapan alamat IP server

Anda tidak memerlukan penugasan alamat IP publik untuk server Outpost.

Dynamic host control protocol (DHCP) adalah protokol manajemen jaringan yang digunakan untuk mengotomatiskan proses konfigurasi perangkat pada jaringan IP. Dalam konteks server Outpost, Anda dapat menggunakan DHCP dua cara:

- Kartu jaringan di server
- Antarmuka jaringan lokal pada instance

Untuk tautan layanan, server Outpost menggunakan DHCP untuk melampirkan ke jaringan lokal. DHCP harus mengembalikan server nama DNS dan gateway default. Server pos terdepan tidak mendukung penetapan IP statis dari tautan layanan.

Untuk tautan LNI, gunakan DHCP untuk mengonfigurasi instance yang akan dilampirkan ke jaringan lokal Anda. Untuk informasi lebih lanjut lihat,the section called “Konfigurasikan sistem operasi”.

> **Note**
>
> Pastikan Anda menggunakan alamat IP yang stabil untuk server Outpost. Perubahan alamat IP dapat menyebabkan gangguan layanan sementara pada subnet Outpost.

Registrasi server

Ketika server Outpost membuat koneksi di jaringan lokal, mereka menggunakan koneksi tautan layanan untuk terhubung ke titik akhir pendaftaran Outpost dan mendaftarkan diri. Pendaftaran membutuhkan DNS publik. Ketika server mendaftar, mereka membuat terowongan aman ke titik

akhir tautan layanan mereka di Wilayah. Server pos terdepan menggunakan port TCP 443 untuk memfasilitasi komunikasi dengan Wilayah melalui internet publik. Saat ini, AWS Outposts server tidak mendukung konektivitas pribadi melalui VPC. Untuk informasi selengkapnya, lihat the section called “Langkah 6: Otorisasi server”.

Bekerja dengan AWS Outposts sumber daya bersama

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 VPC, 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 contoh yang diluncurkan konsumen ke Cadangan 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:

- AWSAkun spesifik di dalam organisasinya diAWS Organizations.
- Unit organisasi di dalam organisasinya diAWS Organizations.
- Seluruh organisasinya di AWS Organizations

Daftar Isi

- Berbagi sumber daya Outpost
- Membatalkan berbagi sumber daya Outpost bersama
- Mengidentifikasi sumber daya Outpost bersama
- Izin sumber daya Pos Luar Bersama
- Penagihan dan pengukuran
- Keterbatasan:

Sumber daya Outpost yang dapat dibagikan

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

Ini adalah sumber daya yang tersedia untuk server Outpost. Untuk sumber daya rak, lihat Bekerja dengan AWS Outposts sumber daya bersama di rak Panduan AWS Outposts Pengguna untuk Outposts.

- Host Khusus yang Dialokasikan — Konsumen yang memiliki akses ke sumber daya ini dapat:
  - Luncurkan dan jalankan instans EC2 pada Host Khusus.
- Outposts — Konsumen dengan akses ke sumber daya ini dapat:
  - Buat dan kelola subnet di Outpost.
  - Gunakan AWS Outposts API untuk melihat informasi tentang 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 instans EC2 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 diAWS Organizations, Anda harus mengaktifkan berbagi denganAWS 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 dengan 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 RAMadalah layanan yang memungkinkan Anda untuk berbagi AWS sumber daya Anda dengan AWS akun apa pun atau melaluiAWS Organizations. Dengan, AWS RAMAnda 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 dalamnyaAWS Organizations.

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

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 Availability Zone di seluruh akun. Misalnya, Availability Zone `us-east-1a` untuk akun AWS Anda mungkin tidak memiliki lokasi yang sama karena `us-east-1a` untuk akun AWS lainnya.

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

Untuk melihat ID AZ untuk Availability Zone di akun Anda

1. Buka konsol AWS RAM di https://console.aws.amazon.com/ram.
2. ID AZ 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 sumber daya AWS RAM yang memungkinkan Anda berbagi sumber daya di seluruh akun AWS. Pembagian sumber daya menentukan sumber daya untuk dibagikan, dan konsumen dengan siapa mereka berbagi. 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 RAMkonsol.

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 konsol AWS Outposts 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 Berbagi Sumber Daya 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 Outpost bersama tidak dibagikan, konsumen tidak dapat lagi melihat Outpost di konsol. AWS Outposts Mereka tidak dapat membuat subnet baru di Outpost, membuat volume EBS baru di Outpost, atau melihat detail Outpost dan jenis instans menggunakan konsol atau. AWS Outposts AWS CLI Subnet, volume, atau instance yang ada yang dibuat oleh konsumen tidak dihapus. Setiap subnet yang ada yang dibuat konsumen di Outpost masih dapat digunakan untuk meluncurkan instance baru.

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 dalam VPC ini dapat terus merutekan lalu lintas ke gateway lokal.

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 atauAWS CLI.

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

Lihat Memperbarui Berbagi Sumber Daya 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 menggunakanAWS CLI.

Untuk mengidentifikasi Outpost bersama menggunakan konsol AWS Outposts

1. Buka konsol AWS Outposts 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.

Penagihan 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

Keterbatasan:

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 .

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 kredensil 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).

Enkripsi bergerak

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

Penghapusan data

Ketika Anda instans EC2, memori yang dialokasikan untuk itu 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. Untuk informasi selengkapnya, lihat Data server rusak secara kriptografis.

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 yang dapat Anda gunakan 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
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin prinsipal	Ya
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 Membuat kebijakan IAM dalam Panduan Pengguna IAM.

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

Contoh kebijakan berbasis identitas untuk Outposts AWS

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

Kebijakan berbasis sumber daya dalam Outposts AWS

Mendukung kebijakan berbasis sumber daya	Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan

prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

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.

Menyertakan 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 ARN dengan koma.

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

Untuk melihat daftar jenis sumber daya AWS Outposts dan ARNnya, 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 AWS Outposts.

Kunci kondisi kebijakan untuk AWS Outposts

Mendukung kunci kondisi kebijakan khusus layanan	Ya

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

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

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

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

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

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

ACL di Outposts AWS

Mendukung ACL	Tidak

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

ABAC dengan 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 tag milik prinsipal cocok dengan tag yang ada di sumber daya yang ingin diakses.

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

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

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

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

Menggunakan kredensyal sementara dengan Outposts AWS

Mendukung penggunaan 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 kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

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

Izin utama lintas layanan untuk 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 layanan untuk AWS Outposts

Mendukung peran layanan	Tidak

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

Peran terkait layanan untuk 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. Menggunakan 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 akan dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

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

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS Outposts, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, sumber daya, dan kunci kondisi untuk AWS Outposts dalam 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 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 Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan dalam 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"
    }
  ]
}
```

Menggunakan peran terkait layanan untuk AWS Outposts

AWS Outposts menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS Outposts Peran terkait layanan telah ditentukan sebelumnya oleh AWS Outposts dan mencakup semua izin yang diperlukan layanan 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, serta bahwa kebijakan izin 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.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya dengan tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk AWS Outposts

AWS Outposts menggunakan peran terkait layanan bernama AWSServiceRoleForOutposts_ ***Outpostid - Memungkinkan Outposts*** AWS mengakses sumber daya untuk konektivitas pribadi atas nama Anda. Peran terkait layanan ini memungkinkan konfigurasi konektivitas pribadi, membuat antarmuka jaringan, dan melampirkannya ke instance titik akhir tautan layanan.

Peran terkait layanan AWSServiceRoleForOutposts _ *Outpostid* mempercayai layanan berikut untuk mengambil peran:

- `outposts.amazonaws.com`

Peran terkait layanan AWSServiceRoleForOutposts_ ***Outpostid*** mencakup kebijakan berikut:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_ ***Outpostid***

AWSOutpostsServiceRolePolicyKebijakan ini adalah kebijakan peran terkait layanan untuk mengaktifkan 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 `all AWS resources`

- Tindakan: `ec2:DescribeSecurityGroups` pada `all AWS resources`
- Tindakan: `ec2:CreateSecurityGroup` pada `all AWS resources`
- Tindakan: `ec2:CreateNetworkInterface` pada `all AWS resources`

Kebijakan AWSOutpostsPrivateConnectivityPolicy_ ***Outpostid*** memungkinkan AWS Outposts untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `ec2:AuthorizeSecurityGroupIngress` pada `all AWS resources that match the following Condition:`

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

- Tindakan: `ec2:AuthorizeSecurityGroupEgress` pada `all AWS resources that match the following Condition:`

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

- Tindakan: `ec2:CreateNetworkInterfacePermission` pada `all AWS resources that match the following Condition:`

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

- Tindakan: `ec2:CreateTags` pada `all AWS resources that match the following Condition:`

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}}
```

Anda harus mengonfigurasikan izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, menyunting, atau menghapus peran terhubung dengan layanan. Untuk informasi selengkapnya, silakan lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat peran yang terhubung dengan layanan untuk AWS Outposts

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

Mengedit peran terkait layanan untuk AWS Outposts

AWS Outposts tidak mengizinkan Anda mengedit peran terkait layanan AWSServiceRoleForOutposts _ *outpostid*. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit Peran Tertaut Layanan dalam 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.

> **Note**
>
> 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.

> **Warning**
>
> Anda harus menghapus Outpost Anda sebelum dapat menghapus peran terkait layanan AWSServiceRoleForOutposts _ *Outpostid*. Prosedur berikut menghapus Outpost Anda.

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 AWSServiceRoleForOutposts _ ***outPostID***

- Hubungi AWS Enterprise Support untuk menghapus Outpost Anda.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran terkait layanan AWSServiceRoleForOutposts _ *Outpostid*. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang didukung untuk peran yang terhubung dengan layanan AWS Outposts

AWS Outposts mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat AWS Outposts kuota dan titik akhir.

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 AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSOutpostsServiceRolePolicy

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

AWS kebijakan terkelola: AWSOutpostsPrivateConnectivityPolicy

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

AWS kebijakan terkelola: AWSOutpostsAuthorizeServerPolicy

Gunakan kebijakan ini untuk memberikan izin yang diperlukan untuk mengotorisasi perangkat keras server Outpost di jaringan lokal Anda. Untuk informasi selengkapnya, lihat Memberi izin.

Kebijakan ini mencakup izin berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Outposts pembaruan kebijakan AWS terkelola

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

Perubahan	Deskripsi	Tanggal
AWSOutpostsAuthorizeServerPolicy – Kebijakan baru	AWS Outposts menambahkan kebijakan yang memberikan izin untuk mengotorisasi perangkat keras server Outpost di jaringan lokal Anda.	4 Januari 2023

Perubahan	Deskripsi	Tanggal
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 instans EC2 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.

Ketahanan di AWS Outposts

Untuk ketersediaan tinggi, Anda dapat order server Outposts 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 control plane 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. Ini memungkinkan Anda membangun ketahanan aplikasi tambahan dan menghindari ketergantungan pada satu Availability Zone. Untuk informasi selengkapnya tentang Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Server Outposts menyertakan volume penyimpanan instans tetapi tidak mendukung volume Amazon EBS. Data pada volume penyimpanan instance tetap ada setelah instance reboot tetapi tidak bertahan setelah penghentian instance. Untuk menyimpan data jangka panjang pada volume penyimpanan instans Anda di luar masa pakai instans, pastikan untuk mencadangkan data ke penyimpanan persisten, seperti bucket Amazon S3 atau perangkat penyimpanan jaringan di jaringan lokal Anda.

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:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

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

Pantau pos terdepan Anda

AWS Outpostsberintegrasi dengan layanan berikut yang menawarkan kemampuan pemantauan dan pencatatan:

CloudWatch metrik

Gunakan Amazon CloudWatch untuk mengambil statistik tentang titik data untuk 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 metrik untuk AWS Outposts.

CloudTrail log

Gunakan AWS CloudTrail untuk menangkap informasi terperinci tentang panggilan yang dilakukan ke AWS API. 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 untukAWS Outposts. Mereka juga berisi informasi untuk panggilan ke tindakan API dari layanan di Outpost, seperti Amazon EC2 dan Amazon EBS. Untuk informasi selengkapnya, lihat AWS Outpostsinformasi di 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 Outpost ke peralatan out-of-band keamanan dan pemantauan di Outpost. Anda dapat menggunakan lalu lintas cermin untuk pemeriksaan konten, pemantauan ancaman, atau pemecahan masalah. Untuk informasi selengkapnya, lihat Panduan Pencerminan Lalu Lintas untuk Amazon Virtual Private Cloud.

AWS Health Dashboard

AWS Health DashboardMenampilkan 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 metrik untuk AWS Outposts

AWS Outpostsmenerbitkan 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, sebaiknya verifikasi konektivitas ke AWS Wilayah dari dalam jaringan lokal Anda, dan hubungi 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 pos terdepan

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`

`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 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 di Outpost for On-Demand Capacity Reservations (ODCR). Metrik ini tidak mengukur Instans Cadangan Amazon EC2.

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi: `InstanceType` dan `OutpostId`

`UsedReservedInstances`

Jumlah instans yang tersedia di Outpost for On-Demand Capacity Reservations (ODCR). Metrik ini tidak mengukur Instans Cadangan Amazon EC2.

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi: `InstanceType` dan `OutpostId`

`TotalReservedInstances`

Jumlah instans yang tersedia di Outpost for On-Demand Capacity Reservations (ODCR). Metrik ini tidak mengukur Instans Cadangan Amazon EC2.

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi: `InstanceType` dan `OutpostId`

Dimensi metrik pos terdepan

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).

Lihat CloudWatch metrik untuk pos terdepan Anda

Anda dapat melihat CloudWatch metrik untuk penyeimbang beban menggunakan konsol. CloudWatch

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 kotak 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 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 Outpoststerintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan diAWS Outposts. CloudTrail menangkap semua panggilan API untuk AWS Outposts sebagai peristiwa. Panggilan yang direkam mencakup panggilan dari AWS Outposts konsol dan panggilan kode ke operasi API AWS Outposts ini. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket S3, termasuk acara untukAWS Outposts. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuatAWS Outposts, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk informasi selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

AWS Outpostsinformasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi diAWS Outposts, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail acara.

Untuk catatan berkelanjutan tentang peristiwa di akun AWS Anda, termasuk peristiwa untuk AWS Outposts, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket S3 di indukWilayah AWS. Secara bawaan, ketika Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail Layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa Wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua AWS Outposts tindakan dicatat oleh CloudTrail. Mereka didokumentasikan dalam Referensi AWS Outposts API. Misalnya, panggilan ke`CreateOutpost`,`GetOutpostInstanceTypes`, dan `ListSites` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Dengan kredensi root atau pengguna.
- Dengan kredensi keamanan sementara untuk peran atau pengguna federasi.
- Oleh yang lainLayanan AWS.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file log AWS Outposts

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa menunjukkan satu permintaan dari sumber mana pun. Ini mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `CreateOutpost` tindakan.

```
{
    "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"
}
```

Pemeliharaan pos terdepan

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 Outpost Anda dan menentukan apakah pemeliharaan diperlukan.

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

Daftar Isi

Pemeliharaan perangkat keras

Jika AWS mendeteksi masalah yang tidak dapat diperbaiki dengan hosting perangkat keras instans Amazon EC2 yang berjalan di Outpost Anda, kami akan memberi tahu pemilik Outpost dan pemilik instans bahwa instans yang terkena dampak dijadwalkan untuk pensiun. Untuk informasi selengkapnya, lihat Pensiun instans di Panduan Pengguna Amazon EC2.

AWS mengakhiri instance yang terpengaruh pada tanggal pensiun instans. Data pada volume penyimpanan instance tidak bertahan setelah penghentian instance. Karena itu, penting bagi Anda untuk mengambil tindakan sebelum tanggal pensiun contoh. Pertama, transfer data jangka panjang Anda dari volume penyimpanan instans untuk setiap instans yang terpengaruh ke penyimpanan persisten, seperti bucket Amazon S3 atau perangkat penyimpanan jaringan di jaringan Anda.

Server pengganti akan dikirim ke situs Outpost. Kemudian, lakukan hal berikut:

- Lepaskan jaringan dan kabel daya dari server yang tidak dapat diperbaiki dan jika perlu lepaskan dari rak Anda.
- Instal server pengganti di lokasi yang sama. Ikuti petunjuk penginstalan di instalasi server Outpost.
- Kemas server yang tidak dapat diperbaiki ke AWS dalam kemasan yang sama dengan server pengganti.
- Gunakan label pengiriman pengembalian prabayar yang tersedia di konsol yang dilampirkan pada detail konfigurasi pesanan atau pesanan server pengganti.
- Kembalikan server ke AWS. Untuk informasi selengkapnya, lihat Mengembalikan AWS Outposts server.

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.

Praktik terbaik untuk acara AWS Outposts 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. Server 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) selama perawatan.
- 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.

Acara konektivitas jaringan

Koneksi tautan layanan antara Outpost Anda dan AWS Region 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.

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 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:

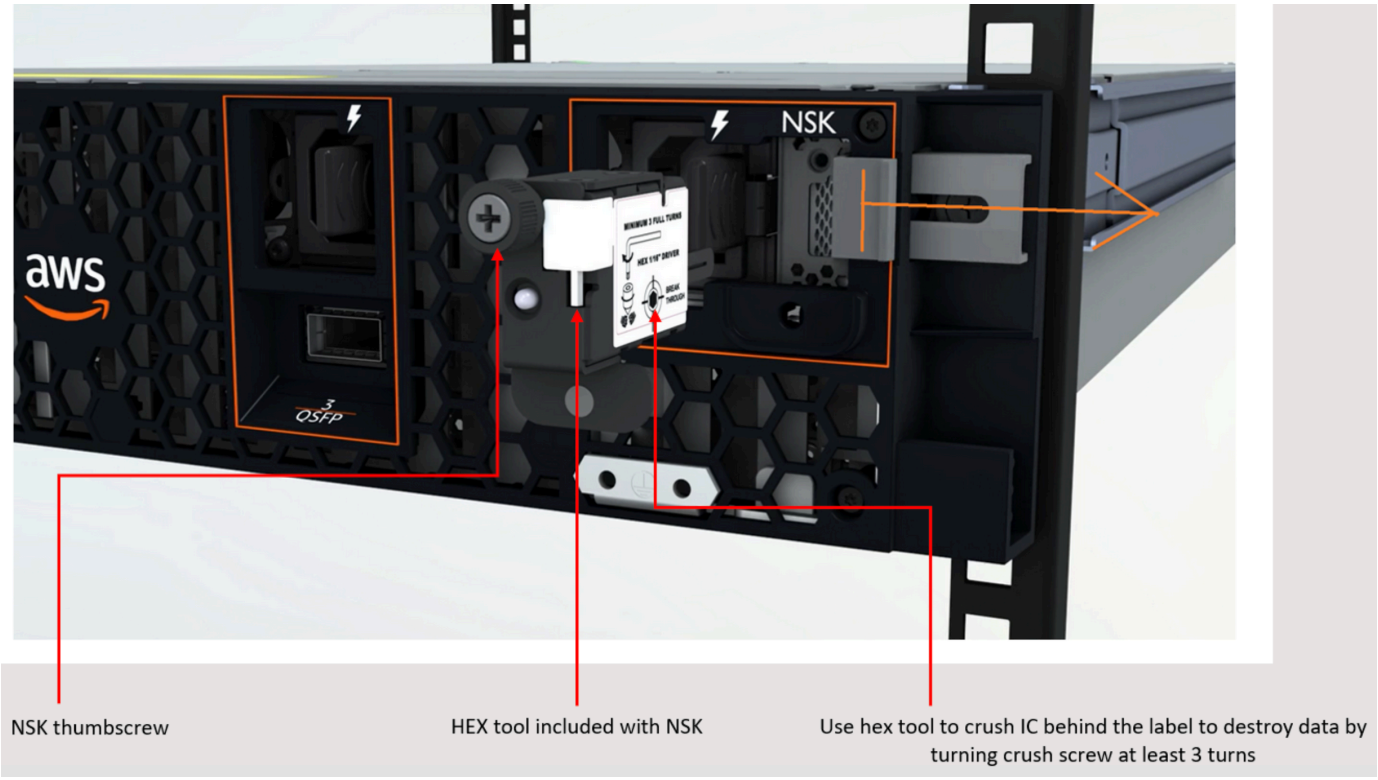
- AWS Blog Pemantauan praktik terbaik untuk AWS Outposts mencakup observabilitas dan praktik terbaik manajemen acara khusus untuk Outposts.
- Alat Debugging AWS blog untuk konektivitas jaringan dari Amazon VPC menjelaskan alat VPC AWSSupport MonitoringFrom-SetuPip. Alat ini adalah AWS Systems Manager dokumen (dokumen SSM) yang membuat Instans Monitor Amazon EC2 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.

Data server rusak secara kriptografis

Kunci Keamanan Nitro (NSK) diperlukan untuk mendekripsi data di server. Ketika Anda mengembalikan server ke AWS, baik karena Anda mengganti server atau menghentikan layanan, Anda dapat menghancurkan NSK untuk secara kriptografis menghancurkan data di server.

Untuk menghancurkan data secara kriptografis di server

1. Hapus NSK dari server sebelum mengirim server kembali ke AWS.
2. Pastikan Anda memiliki NSK yang benar yang dikirimkan bersama server.
3. Lepaskan alat hex kecil/kunci pas Allen dari bawah stiker.
4. Gunakan alat hex untuk memutar sekrup kecil di bawah stiker tiga putaran penuh. Tindakan ini menghancurkan NSK dan secara kriptografis menghancurkan semua data di server.


NSK
aws
QSFP
NSK thumbscrew
HEX tool included with NSK
Use hex tool to crush IC behind the label to destroy data by turning crush screw at least 3 turns

AWS Outposts end-of-term pilihan

Di akhir AWS Outposts masa jabatan Anda, Anda memiliki tiga opsi:

- Perbarui langganan Anda dan pertahankan Pos Luar yang ada.
- Akhiri langganan Anda dan kembalikan server Outpost Anda.
- Konversikan ke month-to-month langganan dan pertahankan server Outpost Anda yang ada.

Topik

Perbarui langganan Anda

Untuk memperbarui langganan Anda dan mempertahankan server Outpost yang ada:

Selesaikan langkah-langkah berikut setidaknya 30 hari sebelum masa jabatan Outpost Anda berakhir:

1. Masuk ke Konsol AWS Support 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 server. 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 server Outpost Anda, Anda akan dikonversi ke month-to-month langganan secara otomatis. Pos Luar Anda akan diperpanjang 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 kembalikan server

> **Important**
>
> AWS tidak dapat memulai proses pengembalian sampai Anda menyelesaikan prosedur berikut. Kami tidak dapat menghentikan proses pengembalian setelah Anda membuka kasus dukungan untuk mengakhiri langganan Anda.

Untuk mengakhiri langganan Anda:

Selesaikan langkah-langkah berikut setidaknya 30 hari sebelum masa jabatan Outpost Anda berakhir:

1. Masuk ke Konsol AWS Support 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 Anda ingin mengakhiri langganan Anda.
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. Jika perlu, buat cadangan instans dan data instans apa pun yang ada di server Anda.
14. Menghentikan instans yang diluncurkan di server Anda.
15. Tinjau detail kasus Anda dan kemudian pilih Kirim. Nomor ID kasus dan ringkasan muncul.
16. JANGAN matikan atau putuskan sambungan server dari jaringan sampai diinstruksikan untuk melakukannya dalam kasus dukungan.

Untuk mengembalikan AWS Outposts server Anda, ikuti prosedur di Kembalikan AWS Outposts server.

Konversi ke month-to-month langganan

Untuk mengonversi ke month-to-month langganan dan mempertahankan server Outpost yang ada, tidak diperlukan tindakan. Jika Anda memiliki pertanyaan, buka kasus dukungan penagihan.

Pos Luar Anda akan diperpanjang 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.

Kuota untuk AWS Outposts

AndaAkun AWS memiliki kuota default, yang sebelumnya disebut sebagai batas, untuk masing-masingLayanan AWS. Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota, tetapi tidak untuk semua kuota.

Untuk melihat kuotaAWS 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.

AndaAkun AWS memiliki kuota berikut yang terkait denganAWS Outposts.

Sumber daya	Default	Dapat Disesuaikan	Comments
Outpost	100	Ya	Sebuah situs Outpost adalah pelanggan dikelola bangunan fisik di mana Anda kekuasaan dan melampirkan peralatan Outpost Anda ke jaringan. Anda dapat memiliki 100 situs Outposts di setiap WilayahAWS akun Anda.
Outposts per situs	10	Ya	AWS Outpoststermasuk 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 Outpostsdan kuota untuk layanan lainnya

AWS Outpostsbergantung pada sumber daya layanan lain dan layanan tersebut mungkin memiliki kuota default mereka sendiri. Misalnya, kuota Anda untuk antarmuka jaringan lokal berasal dari kuota Amazon VPC untuk antarmuka jaringan.

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada Panduan AWS Outposts Pengguna.

Perubahan	Deskripsi	Tanggal
Manajemen kapasitas	Anda dapat memodifikasi konfigurasi kapasitas default untuk pesanan Outposts baru Anda.	April 16, 2024
nd-of-term Opsi E untuk AWS Outposts server	Di akhir AWS Outposts jangka waktu Anda, Anda dapat memperbarui, mengakhiri, atau mengonversi langganan Anda.	1 Agustus 2023
Panduan AWS Outposts Pengguna yang Dibuat untuk server Outposts	AWS Outposts Panduan Pengguna memecah menjadi panduan terpisah untuk rak dan server.	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
Memperkenalkan server Outpost	Ditambahkan Outposts server, faktor AWS Outposts bentuk baru.	30 November 2021

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