Panduan Pengguna untuk server Outposts

AWS Outposts

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Outposts: Panduan Pengguna untuk server Outposts

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AWS Outposts? ... 1
Konsep utama ... 1
AWS sumber daya di Outposts ... 2
Harga ... 5
Bagaimana cara AWS Outposts kerja ... 6
Komponen jaringan ... 6
VPCs dan subnet ... 7
Perutean ... 7
DNS ... 8
Tautan layanan ... 9
Antarmuka jaringan lokal ... 9
Persyaratan situs ... 10
Fasilitas ... 10
Jaringan ... 11
Firewall tautan layanan ... 12
Unit transmisi maksimum tautan layanan (MTU) ... 12
Rekomendasi bandwidth tautan layanan ... 13
Tautan layanan membutuhkan respons DHCP ... 13
Daya ... 13
Dukungan daya ... 13
Daya tarik ... 14
Kabel daya ... 14
Redundansi daya ... 14
Pemenuhan pesanan ... 14
Memulai ... 16
Buat Pos Terdepan dan kapasitas pesanan ... 16
Langkah 1: Buat situs ... 17
Langkah 2: Buat Pos Terdepan ... 17
Langkah 3: Tempatkan pesanan ... 18
Langkah 4: Ubah kapasitas instance ... 19
Langkah selanjutnya ... 21
Luncurkan sebuah instans ... 22
Langkah 1: Buat subnet ... 22
Langkah 2: Luncurkan instance di Outpost ... 23

Langkah 3: Konfigurasikan konektivitas ... 25
Langkah 4: Uji konektivitas ... 25
Tautan layanan ... 28
Konektivitas ... 28
Persyaratan unit transmisi maksimum (MTU) ... 29
Rekomendasi bandwidth ... 13
Koneksi internet redundan ... 29
Pembaruan dan tautan layanan ... 30
Firewall dan tautan layanan ... 30
Pemecahan masalah jaringan ... 31
Penilaian awal ... 31
Langkah 1. Periksa konektivitas fisik ... 32
Langkah 2. Uji koneksi server Outposts ke AWS ... 32
Langkah 3. Membangun kembali konektivitas ... 33
Kembalikan server ... 34
Langkah 1: Siapkan server untuk kembali ... 34
Langkah 2: Dapatkan label pengiriman kembali ... 35
Langkah 3: Kemas server ... 35
Langkah 4: Kembalikan server melalui kurir ... 36
Antarmuka jaringan lokal ... 39
Dasar-dasar antarmuka jaringan lokal ... 40
Kinerja ... 41
Grup keamanan ... 42
Pemantauan ... 42
Alamat MAC ... 42
Tambahkan antarmuka jaringan lokal ... 43
Lihat antarmuka jaringan lokal ... 44
Konfigurasikan sistem operasi ... 44
Konektivitas lokal ... 44
Topologi server di jaringan Anda ... 45
Konektivitas fisik server ... 45
Lalu lintas tautan layanan untuk server ... 46
Antarmuka jaringan lokal menghubungkan lalu lintas ... 46
Penetapan alamat IP server ... 48
Pendaftaran server ... 49
Manajemen kapasitas ... 50

Lihat kapasitas ... 50
Memodifikasi kapasitas instans ... 19
Pertimbangan ... 51
Memecahkan masalah tugas kapasitas ... 55
Pesanan *oo-xxxxxx* tidak terkait dengan Outpost ID *op-xxxxx* ... 55
Paket kapasitas mencakup jenis instans yang tidak didukung ... 55
Tidak ada pos terdepan dengan Outpost ID *op-xxxxx* ... 56
CapacityTaskTutup aktif- *XXXX* sudah ditemukan untuk Outpost op- *XXXX* ... 57
CapacityTaskCap aktif- *XXXX* sudah ditemukan untuk Aset *XXXX* di Outpost OP-XXXX ... 57
AssetId= tidak *XXXX* valid untuk outPost=op- *XXXX* ... 58
Sumber Daya Bersama ... 60
Sumber daya Outpost yang dapat dibagikan ... 61
Prasyarat untuk berbagi sumber daya Outposts ... 62
Layanan terkait ... 62
Berbagi di seluruh Availability Zone ... 62
Berbagi sumber daya Outpost ... 63
Membatalkan berbagi sumber daya Outpost bersama ... 64
Mengidentifikasi sumber daya Outpost bersama ... 65
Izin sumber daya Pos Luar Bersama ... 66
Izin untuk pemilik ... 66
Izin untuk konsumen ... 66
Tagihan dan pengukuran ... 66
Batasan ... 66
Keamanan ... 68
Perlindungan data ... 69
Enkripsi diam ... 69
Enkripsi bergerak ... 69
Penghapusan data ... 69
Manajemen identitas dan akses ... 69
Bagaimana AWS Outposts bekerja dengan IAM ... 70
Contoh kebijakan ... 75
Peran terkait layanan ... 78
AWS kebijakan terkelola ... 81
Keamanan infrastruktur ... 83
Ketahanan ... 84
Validasi kepatuhan ... 84

Pemantauan 86
CloudWatch metrik 87
Metrik 87
Dimensi metrik 91
Lihat CloudWatch metrik untuk server rak 91
Log panggilan API menggunakan CloudTrail 92
AWS Outposts acara manajemen di CloudTrail 94
AWS Outposts contoh acara 94
Maintenance 96
Perbarui detail kontak 96
Pemeliharaan perangkat keras 96
Pembaruan firmware 97
Acara daya dan jaringan 97
Peristiwa kekuasaan 98
Acara konektivitas jaringan 98
Sumber daya 99
Data server rusak secara kriptografis 100
End-of-term pilihan 101
Perpanjang langganan 101
Akhiri langganan 102
Konversi langganan 103
Kuota 104
AWS Outposts dan kuota untuk layanan lainnya 105
Riwayat dokumen 106
..... cviii

Apa itu AWS Outposts?

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

Outpost adalah kumpulan kapasitas AWS komputasi dan penyimpanan yang digunakan di situs pelanggan. AWS mengoperasikan, memantau, dan mengelola kapasitas ini sebagai bagian dari suatu AWS Wilayah. Anda dapat membuat subnet di Outpost Anda dan menentukannya saat Anda membuat AWS sumber daya seperti EC2 instance dan subnet. 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 Outpost ke Outpost atau Local Zone lain yang berada dalam VPC yang sama.

Untuk informasi lebih lanjut, lihat halaman AWS Outposts produk.

Konsep utama

Ini adalah konsep kunci untuk AWS Outposts.

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

- Peralatan pos terdepan — Perangkat keras fisik yang menyediakan akses ke AWS Outposts layanan. Perangkat keras termasuk rak, server, sakelar, dan kabel yang dimiliki dan dikelola oleh. AWS
- Rak Outposts — Faktor bentuk Outpost yang merupakan rak 42U standar industri. Rak Outposts termasuk server yang dapat dipasang di rak, sakelar, panel patch jaringan, rak daya, dan panel kosong.
- Server Outposts - Faktor bentuk Outpost yang merupakan server 1U atau 2U standar industri, yang dapat dipasang di rak 4 pos standar yang sesuai dengan EIA-310D 19. Server Outposts menyediakan layanan komputasi dan jaringan lokal ke situs yang memiliki ruang terbatas atau persyaratan kapasitas yang lebih kecil.
- Pemilik pos terdepan — Pemilik akun untuk akun yang AWS Outposts melakukan pemesanan. Setelah AWS terlibat dengan pelanggan, pemilik dapat menyertakan titik kontak tambahan. AWS akan berkomunikasi dengan kontak untuk mengklarifikasi pesanan, janji pemasangan, dan pemeliharaan dan penggantian perangkat keras. Contact AWS Dukungan Center jika informasi kontak berubah.
- Tautan layanan — Rute jaringan yang memungkinkan komunikasi antara Outpost Anda dan AWS Wilayah terkaitnya. Setiap Pos Luar adalah perpanjangan dari Availability Zone dan Wilayah terkaitnya.
- Local Gateway (LGW) — Router virtual interkoneksi logis yang memungkinkan komunikasi antara rak Outposts dan jaringan lokal Anda.
- Antarmuka jaringan lokal — Antarmuka jaringan yang memungkinkan komunikasi dari server Outposts dan jaringan lokal Anda.

AWS sumber daya di Outposts

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

Komputasi

Jenis sumber daya	Rak	Peladen
EC2 Contoh Amazon	Y	Ya

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

Database dan analitik

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

Jaringan

Jenis sumber daya	Rak	Peladen
Proksi Utusan App Mesh	Y	Ya

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

Penyimpanan

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

Lainnya Layanan AWS

Layanan	Rak	Peladen
AWS IoT Greengrass	Y	Ya

Harga

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

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

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

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

- Harga rak Outposts
- Harga server Outposts

Bagaimana cara AWS Outposts kerja

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

Diagram berikut menggambarkan kedua faktor bentuk Outpost.

Daftar Isi

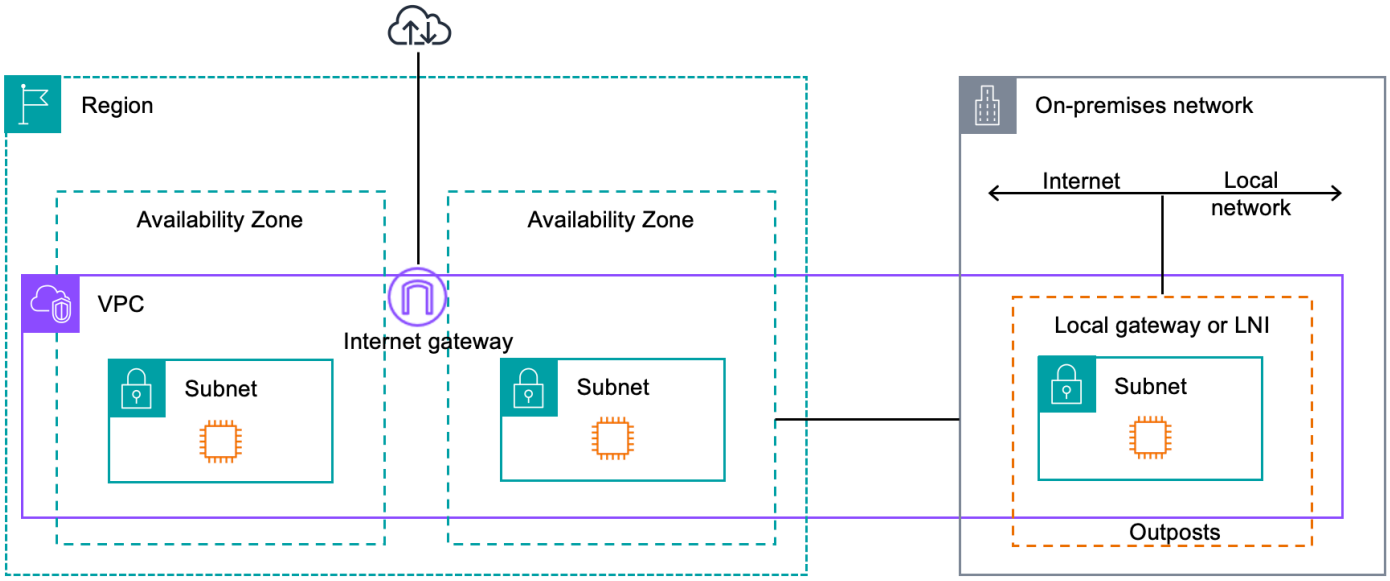
- Komponen jaringan
- VPCs dan subnet
- Perutean
- DNS
- Tautan layanan
- Antarmuka jaringan lokal

Komponen jaringan

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

Diagram berikut menunjukkan komponen jaringan untuk Outpost Anda.

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



VPCs dan subnet

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

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

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

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

Perutean

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

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

Tabel rute subnet pos terdepan dapat mencakup tujuan berikut:

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

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

DNS

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

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

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

Tautan layanan

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

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

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

Antarmuka jaringan lokal

Server Outposts menyertakan antarmuka jaringan lokal untuk menyediakan konektivitas ke jaringan lokal Anda. Antarmuka jaringan lokal hanya tersedia untuk server Outposts yang berjalan di subnet Outpost. Anda tidak dapat menggunakan antarmuka jaringan lokal dari EC2 instance di rak Outposts atau di Region. AWS Antarmuka jaringan lokal dimaksudkan hanya untuk lokasi lokal. Lihat informasi yang lebih lengkap di Antarmuka jaringan lokal untuk server Outposts Anda.

Persyaratan situs untuk server Outposts

Situs Outpost adalah lokasi fisik tempat Outpost Anda beroperasi. Situs hanya tersedia di negara dan wilayah tertentu. Untuk informasi selengkapnya, lihat AWS Outposts server FAQs. 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 Panduan Pengguna AWS Outposts untuk rak Outposts.

Daftar Isi

- Fasilitas
- Jaringan
- Daya
- Pemenuhan pesanan

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 berat 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. 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 minimal 36 inci (914 mm). AWS menyediakan kit rel untuk memasang rak server.
  - 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)
  - Pemasangan AWS Outposts server secara vertikal tidak didukung.
  - Server Outposts 1U memiliki lebar yang sama dengan server Outposts 2U, tetapi setengah tinggi dan kedalaman kurang

  Jika Anda tidak menempatkan server di rak, Anda masih harus memenuhi persyaratan situs lainnya.
- 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).

Firewall tautan layanan

UDP dan TCP 443 harus terdaftar secara statis di firewall.

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	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 Outpost.

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, lihat AWS Outposts konektivitas ke AWS Wilayah di panduan AWS Outposts pengguna untuk server.

Rekomendasi bandwidth tautan layanan

Untuk pengalaman dan ketahanan yang optimal, Anda AWS mengharuskan Anda menggunakan konektivitas redundan minimal 500 Mbps dan latensi pulang-pergi maksimum 175 ms untuk koneksi tautan layanan ke Wilayah. AWS Pemanfaatan maksimum untuk setiap server Outposts adalah 500 Mbps. Untuk meningkatkan kecepatan koneksi, gunakan beberapa server Outposts. 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 di panduan AWS Outposts pengguna 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 cache AMIs. AMIs diunduh dari Wilayah dengan setiap peluncuran instance.

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.

Daya

Ini adalah persyaratan daya untuk server Outposts.

Persyaratan

- Dukungan daya
- Daya tarik
- Kabel daya
- Redundansi daya

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 IEC C13 untuk kabel IS1293 listrik.

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 dikirim 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 Lalu lintas tautan layanan untuk server di panduan AWS Outposts pengguna untuk server.

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

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

Tugas

- Buat Outpost dan pesan kapasitas Outpost
- Luncurkan instance di server Outposts Anda

Buat Outpost dan pesan kapasitas Outpost

Untuk mulai menggunakan AWS Outposts, masuk dengan AWS akun Anda. 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 Persyaratan situs untuk server Outposts.
- Anda harus memiliki paket AWS Enterprise Support atau paket AWS Enterprise On-Ramp Support.
- Tentukan mana yang akan Akun AWS Anda gunakan untuk membuat situs Outposts, membuat Outpost, dan melakukan pemesanan. Pantau email yang terkait dengan akun ini untuk informasi dari AWS.

Tugas

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

Langkah 1: Buat situs

Buat situs untuk menentukan alamat operasi. Alamat operasi adalah lokasi di mana Anda akan menginstal dan menjalankan server Outposts Anda. Setelah Anda membuat situs, AWS Outposts berikan ID ke situs Anda. Anda harus menentukan situs ini ketika Anda membuat Outpost.

Prasyarat

- Tentukan alamat operasi.

Untuk membuat situs

1. Masuk ke AWS.
2. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
3. Untuk memilih induk Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
4. Di panel navigasi, pilih Situs.
5. Pilih Buat situs.
6. Untuk jenis perangkat keras yang didukung, pilih 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.

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

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 tersebut.

  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 Berikutnya.

6. Pilih Gunakan Outpost yang ada dan pilih Outpost Anda.
7. Pilih Berikutnya.
8. Pilih jangka waktu kontrak dan opsi pembayaran.
9. Tentukan alamat pengiriman. Anda dapat menentukan alamat baru atau memilih alamat operasi situs. Jika Anda memilih alamat operasi, ketahuilah bahwa perubahan masa depan pada alamat operasi situs tidak akan menyebar ke pesanan yang ada. Jika Anda perlu mengubah alamat pengiriman pada pesanan yang ada, hubungi Manajer AWS Akun Anda.
10. Pilih Berikutnya.
11. Pada halaman Tinjauan dan pemesanan, verifikasi bahwa informasi Anda benar dan edit sesuai kebutuhan. Anda tidak akan dapat mengedit pesanan setelah Anda mengirimkannya.
12. Pilih Tempatkan pesanan.

Langkah 4: Ubah kapasitas instance

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 Berikutnya.
3. Pada halaman Configure instance capacity, setiap tipe instance menampilkan satu ukuran instans dengan jumlah maksimum yang telah dipilih sebelumnya. Untuk menambahkan lebih banyak ukuran instance, pilih Tambahkan ukuran instans.
4. Tentukan kuantitas instance dan catat kapasitas yang ditampilkan untuk ukuran instance tersebut.
5. Lihat pesan di akhir setiap bagian tipe instans yang memberi tahu Anda jika Anda berada di atas atau di bawah kapasitas. Lakukan penyesuaian pada ukuran instans atau tingkat kuantitas untuk mengoptimalkan total kapasitas yang tersedia.
6. Anda juga dapat meminta AWS Outposts untuk mengoptimalkan kuantitas instans untuk ukuran instans tertentu. Untuk melakukannya:
   a. Pilih ukuran instans.
   b. Pilih Saldo otomatis di akhir bagian tipe instans terkait.
7. Untuk setiap jenis instance, pastikan bahwa kuantitas instance ditentukan untuk setidaknya satu ukuran instance.
8. Pilih Berikutnya.
9. Pada halaman Tinjau dan buat, verifikasi pembaruan yang Anda minta.
10. Pilih Buat. AWS Outposts menciptakan tugas kapasitas.
11. Pada halaman tugas kapasitas, pantau status tugas.

> **Note**
>
> AWS Outposts mungkin meminta Anda untuk menghentikan satu atau beberapa instance yang berjalan untuk mengaktifkan menjalankan tugas kapasitas. Setelah Anda menghentikan instance ini, AWS Outposts akan menjalankan tugas.

Upload JSON file

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

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

   Example

   Contoh file JSON:

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

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

> **Note**
>
> AWS Outposts mungkin meminta Anda untuk menghentikan satu atau beberapa instance yang berjalan untuk mengaktifkan menjalankan tugas kapasitas. Setelah Anda menghentikan instance ini, AWS Outposts akan menjalankan tugas.

Langkah selanjutnya

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

Untuk memenuhi pesanan, AWS akan menjadwalkan tanggal 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 panduan instalasi Server.

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

Luncurkan instance di server Outposts Anda

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

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, Anda harus mengaktifkan subnet untuk antarmuka jaringan lokal. Gunakan modify-subnet-attributeperintah dari AWS CLI. 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. Contoh berikut menggunakan nilai 1 untuk menentukan antarmuka jaringan sekunder.

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

Langkah 2: Luncurkan instance di Outpost

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

Pertimbangan

- Jika Anda melampirkan volume data blok yang didukung oleh sistem penyimpanan blok pihak ketiga yang kompatibel selama proses peluncuran instans di Outpost, lihat posting blog ini Menyederhanakan penggunaan penyimpanan blok pihak ketiga dengan. AWS Outposts

Integrasi penyimpanan pihak ketiga hanya tersedia saat menggunakan EC2 instans Amazon dengan server AWS Outposts 2U yang didukung oleh prosesor Intel Xeon Scalable x86. Ini tidak tersedia dengan server AWS Outposts 1U yang didukung oleh prosesor Graviton2 ARM.

- 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 dan Membuat instance store-backed AMI di Panduan Pengguna Amazon. EC2
- Anda harus menggunakan AMI yang didukung Amazon EBS-backed hanya dengan satu snapshot EBS. AMIs dengan lebih dari satu snapshot EBS 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 EC2 konsol Amazon. 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 menetapkan 1 sebagai indeks perangkat antarmuka jaringan lokal untuk subnet Outpost, antarmuka jaringan ini adalah antarmuka jaringan lokal untuk instance. Atau, untuk menambahkannya nanti, lihatTambahkan antarmuka jaringan lokal.
7. Selesaikan wizard untuk meluncurkan instance di subnet Outpost Anda. Untuk informasi selengkapnya, lihat Meluncurkan EC2 instance di Panduan EC2 Pengguna Amazon:

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 Tambahkan antarmuka jaringan lokal.

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 instans Outpost.

```
ping 10.0.3.128
```

Berikut ini adalah output contoh.

```
Pinging 10.0.3.128

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

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

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

Uji konektivitas dari instans Outpost ke jaringan lokal Anda

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

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

```
ping 172.16.0.130
```

Berikut ini adalah output contoh.

```
Pinging 172.16.0.130

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

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

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

Uji konektivitas antara AWS Wilayah dan Pos Terdepan

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

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

Setelah instance berjalan, lakukan operasi berikut:

1. Dapatkan alamat IP pribadi dari instance di AWS Wilayah. Informasi ini tersedia di EC2 konsol Amazon di halaman detail instance.
2. Bergantung pada sistem operasi Anda, gunakan ssh atau sambungkan rdp ke alamat IP pribadi 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 yang menghubungkan server Outposts Anda ke AWS Wilayah atau Wilayah AWS Outposts asal Anda.

Daftar Isi

- Konektivitas melalui tautan layanan
- Pembaruan dan tautan layanan
- Firewall dan tautan layanan
- Pemecahan masalah jaringan server Outposts

Konektivitas melalui tautan layanan

Selama AWS Outposts penyediaan, Anda atau AWS membuat koneksi tautan layanan yang menghubungkan server Outposts Anda ke Wilayah atau AWS Wilayah asal 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

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 di Panduan Pengguna Amazon VPC.

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 yang terkait VPCs, 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

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

Rekomendasi bandwidth tautan layanan

Untuk pengalaman dan ketahanan yang optimal, Anda AWS mengharuskan Anda menggunakan konektivitas redundan minimal 500 Mbps dan latensi pulang-pergi maksimum 175 ms untuk koneksi tautan layanan ke Wilayah. AWS Pemanfaatan maksimum untuk setiap server Outposts adalah 500 Mbps. Untuk meningkatkan kecepatan koneksi, gunakan beberapa server Outposts. 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 cache AMIs. AMIs diunduh dari Wilayah dengan setiap peluncuran instance.

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

Koneksi internet redundan

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

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

Pembaruan dan tautan layanan

AWS memelihara koneksi jaringan yang aman antara server Outposts Anda dan Wilayah AWS 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 Outpost yang diawetkan 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 Outposts.

Firewall dan tautan layanan

Bagian ini membahas konfigurasi firewall dan koneksi link layanan.

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

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

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

Jika Anda menggunakan firewall untuk membatasi konektivitas dari tautan layanan VLAN, Anda dapat memblokir semua koneksi masuk. Anda harus mengizinkan koneksi keluar kembali ke Pos

Luar dari AWS Wilayah sesuai tabel berikut. Jika firewall stateful, koneksi keluar dari Outpost yang diizinkan, yang berarti bahwa mereka dimulai dari Outpost, harus diizinkan kembali masuk.

Protokol	Port Sumber	Alamat Sumber	Pelabuhan Tujuan	Alamat Tujuan
UDP	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 link layanan untuk berkomunikasi dengan instance di Outposts lain. Manfaatkan routing melalui gateway lokal atau antarmuka jaringan lokal untuk berkomunikasi antara Outposts.

Pemecahan masalah jaringan server Outposts

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

Penilaian awal

Verifikasi status tautan layanan melalui CloudWatch metrik Amazon:

1. Pantau ConnectedStatusmetrik di AWS Outposts namespace.
2. Jika nilai rata-rata kurang dari 1, ini menegaskan bahwa tautan layanan terganggu.
3. Jika tautan layanan terganggu, selesaikan langkah-langkah di bagian berikut untuk menyelesaikan dan membangun kembali koneksi.

Langkah 1. Periksa konektivitas fisik

1. Verifikasi Anda menggunakan kabel breakout QSFP yang disediakan. Jika masalah terus berlanjut, uji dengan kabel breakout QSFP yang berbeda jika tersedia.
2. Verifikasi bahwa kabel breakout QSFP di server Outposts terpasang dengan kuat.
3. Pastikan kabel 1 (LNI) terpasang dengan kuat di sakelar.
4. Verifikasi bahwa kabel 2 (tautan layanan) terpasang dengan kuat di sakelar.
5. Selesaikan pemeriksaan kewarasan sakelar umum seperti, memeriksa lampu tautan.

Langkah 2. Uji koneksi server Outposts ke AWS

Buat koneksi serial ke server Outposts dan lakukan tes berikut:

1. Uji tautannya.
   a. Jika berhasil, lanjutkan dengan tes berikutnya.
   b. Jika gagal,Verifikasi konfigurasi jaringan.
2. Uji resolusi DNS.
   a. Jika berhasil, lanjutkan dengan tes berikutnya.
   b. Jika gagal,Periksa aturan firewall.
3. Uji akses ke AWS Wilayah.
   a. Jika berhasil, lanjutkan untuk membangun kembali koneksi.
   b. Jika gagal,Verifikasi MTU.

Verifikasi konfigurasi jaringan

Pastikan sakelar Anda memenuhi spesifikasi berikut:

- Konfigurasi dasar — Port tautan layanan harus berupa port akses yang tidak ditandai ke VLAN dengan gateway dan rute ke titik akhir AWS.
- DHCP — DHCP harus digunakan dan harus mengembalikan server nama DNS dan gateway default.
- Kecepatan tautan - Port sakelar harus memiliki kecepatan tautan yang disetel ke 10 Gb dan negosiasi otomatis harus dimatikan.

Verifikasi MTU

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

Periksa aturan firewall

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

Langkah 3. Membangun kembali konektivitas

Jika pemeriksaan sebelumnya lulus tetapi tautan layanan tetap `DOWN` (ConnectedStatuskurang dari 1 in CloudWatch), maka ikuti langkah-langkah di Otorisasi server Outposts menggunakan Outpost Configuration Tool untuk membangun kembali koneksi.

> **Note**
>
> Jika tautan layanan tetap turun, buat kasing di AWS Dukungan Pusat.

Kembalikan server Outposts

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. Untuk memulai, selesaikan langkah-langkah berikut.

Tugas

- Langkah 1: Siapkan server untuk kembali
- Langkah 2: Dapatkan label pengiriman kembali
- Langkah 3: Kemas server
- Langkah 4: Kembalikan server melalui kurir

Untuk mengembalikan server karena server mencapai akhir masa kontrak, atau karena alasan lain, hubungi AWS Dukungan Pusat.

Langkah 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 bagian sumber daya di Panduan AWS RAM Pengguna.
   - Gunakan AWS CLI untuk menjalankan disassociate-resource-shareperintah.

   Untuk daftar sumber daya Outpost yang dapat dibagikan, lihat Sumber daya Pos Luar yang Dapat Dibagikan.
2. Buat cadangan data yang disimpan dalam penyimpanan instans EC2 instans Amazon 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 .

Langkah 2: Dapatkan label pengiriman kembali

> **Important**
>
> Anda hanya boleh menggunakan label pengiriman yang AWS menyediakan karena berisi informasi spesifik, seperti ID Aset, tentang server yang Anda kembalikan. 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 Dukungan Pusat Kontak.
2. Minta label pengiriman untuk server yang ingin Anda kembalikan.

Langkah 3: Kemas server

Untuk mengemas server Anda, gunakan kotak dan bahan kemasan yang disediakan oleh AWS.

1. Kemas server di salah satu kotak berikut:

   - Kotak dan bahan kemasan tempat server awalnya masuk.
   - Kotak dan bahan kemasan tempat server pengganti masuk.

   Atau, hubungi AWS Dukungan Pusat untuk meminta kotak.

2. Tempelkan label pengiriman yang AWS disediakan, ke bagian luar kotak.

> **Important**
>
> Verifikasi bahwa ID Aset pada label pengiriman cocok dengan ID Aset di server yang Anda kembalikan.
> ID Aset terletak di tab tarik keluar di bagian depan server. Contoh: `1203779889` atau `9305589922`

3. Tutup kotak dengan aman.

Langkah 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 Dukungan 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	

Negara	Kontak
Indonesia	
Jepang	
Malaysia	
Nigeria	
Oman	
Panama	
Peru	
Filipina	
Serbia	
Singapura	
Afrika Selatan	
Korea Selatan	
Taiwan	
Thailand	
Uni Emirat Arab	
Vietnam	

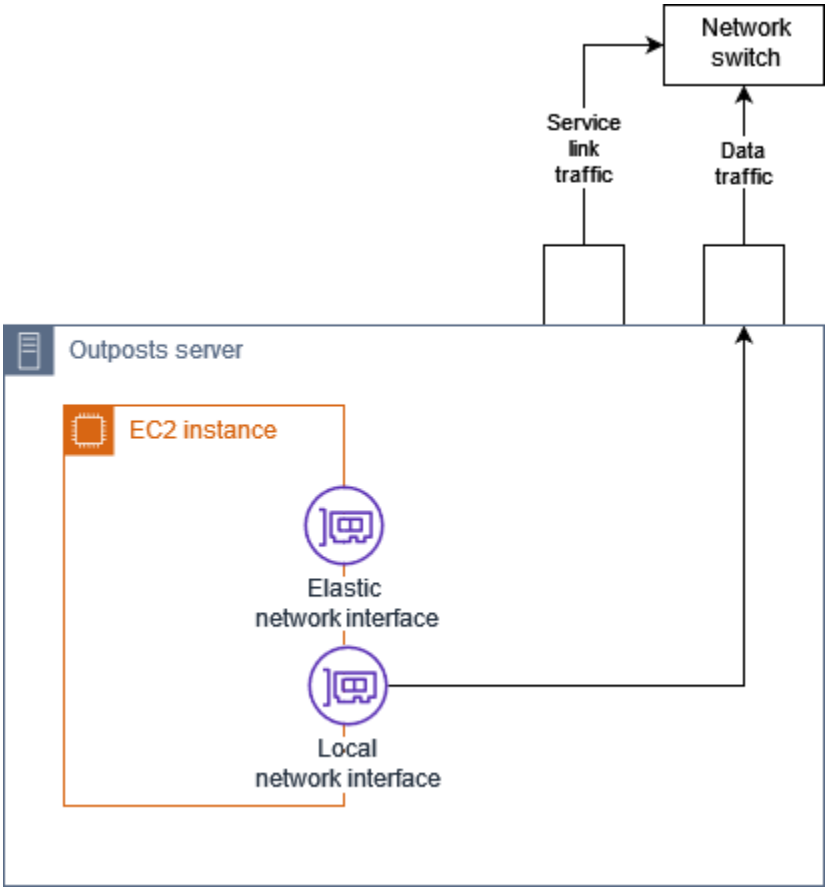
Negara	Kontak
Amerika Serikat	Hubungi UPS. Anda dapat mengembalikan server dengan cara berikut: • Kembalikan server selama pengambilan UPS rutin di situs Anda. • Drop-off server di lokasi UPS. • Jadwalkan penjemputan untuk tanggal dan waktu yang Anda inginkan. Masukkan nomor pelacakan dari label pengiriman AWS yang disediakan untuk pengiriman gratis.
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 can't be scheduled for an import shipment`, biasanya berarti bahwa negara penjemputan yang Anda pilih tidak cocok dengan negara pengambilan pada label pengiriman kembali. Pilih negara asal kiriman dan coba lagi.

Antarmuka jaringan lokal untuk server Outposts Anda

Dengan server Outposts, antarmuka jaringan lokal adalah komponen jaringan logis yang menghubungkan EC2 instans Amazon 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 EC2 instance 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 EC2 contoh pada server Outposts dengan kedua elastic network interface 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
- Tambahkan antarmuka jaringan lokal ke EC2 instance di subnet Outposts
- Konektivitas jaringan lokal untuk server Outposts

Dasar-dasar antarmuka jaringan lokal

Antarmuka jaringan lokal menyediakan akses ke jaringan lapisan-dua fisik. VPC adalah jaringan layer-tiga virtual. 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 Outposts 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 frame 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 Kuota antarmuka jaringan di Panduan Pengguna Amazon VPC.
- Setiap EC2 instance dapat memiliki satu antarmuka jaringan lokal.
- Antarmuka jaringan lokal tidak dapat menggunakan antarmuka jaringan utama instance.

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

> **Note**
>
> EC2 instance 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 Outposts.
- Antarmuka jaringan lokal tidak mendukung mode promiscuous atau spoofing alamat MAC.

Kinerja

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

Jenis instans	Bandwidth acuan (Gbps)	Bandwidth lonjakan (Gbps)
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
c6gd.medium	0,1625	4

Jenis instans	Bandwidth acuan (Gbps)	Bandwidth lonjakan (Gbps)
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, lihat Memantau performa jaringan untuk setelan ENA pada EC2 instans Anda di Panduan EC2 Pengguna Amazon.

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.

Tambahkan antarmuka jaringan lokal ke EC2 instance di subnet Outposts

Anda dapat menambahkan antarmuka jaringan lokal ke EC2 instans Amazon 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-interfacedan attach-network-interface.

Gunakan prosedur berikut untuk menambahkan antarmuka jaringan lokal setelah Anda meluncurkan instance. Untuk informasi tentang menambahkannya selama peluncuran instance, lihat Meluncurkan instance di Outpost.

Untuk menambahkan antarmuka jaringan lokal ke sebuah EC2 instance

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Jaringan dan Keamanan, Antarmuka Jaringan.
3. Buat antarmuka jaringan
   a. Pilih Buat antarmuka jaringan.
   b. Pilih subnet Outpost yang sama dengan instance.
   c. Verifikasi bahwa IPv4 alamat Pribadi disetel ke Tetapkan otomatis.
   d. Pilih grup keamanan apa pun. Grup keamanan tidak berlaku untuk antarmuka jaringan lokal, sehingga grup keamanan yang Anda pilih tidak relevan.
   e. Pilih Buat antarmuka jaringan.
4. 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 untuk antarmuka jaringan lokal untuk subnet Outpost, antarmuka jaringan ini adalah antarmuka jaringan lokal untuk instance.

Lihat antarmuka jaringan lokal

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

Konsol menampilkan IPv4 alamat pribadi untuk antarmuka jaringan lokal dari subnet CIDR. Alamat ini bukan alamat IP dari antarmuka jaringan lokal, 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 antarmuka jaringan lokal dalam sistem operasi tamu, baik secara statis atau melalui server DHCP Anda.

Konfigurasikan sistem operasi

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

Konektivitas jaringan lokal untuk server Outposts

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

Daftar Isi

- Topologi server di jaringan Anda
- Konektivitas fisik server
- Lalu lintas tautan layanan untuk server
- Antarmuka jaringan lokal menghubungkan lalu lintas
- Penetapan alamat IP server
- Pendaftaran server

Topologi server di jaringan Anda

Server Outposts 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 Outposts 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 khusus atau VPNs dari Pos Luar ke Wilayah. Pos Terdepan terhubung ke Availability Zone di Wilayah yang Anda pilih pada saat pembelian.
1	Lalu lintas tautan antarmuka jaringan lokal — 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 Outposts mencakup 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 Outposts. 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 Outposts berfungsi. Gunakan 2 antarmuka untuk lalu lintas tautan layanan dan 1 antarmuka untuk lalu lintas tautan antarmuka jaringan lokal. 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 Outposts 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

Antarmuka jaringan lokal menghubungkan lalu lintas

Konfigurasikan port tautan antarmuka jaringan lokal pada 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 antarmuka jaringan lokal Anda sebagai trunk, Anda harus memastikan bahwa OS Anda menandai lalu lintas VLAN.

Contoh berikut menunjukkan cara mengonfigurasi penandaan VLAN untuk antarmuka jaringan lokal 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 antarmuka jaringan lokal 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 antarmuka jaringan lokal 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 Mengonfigurasi antarmuka jaringan menggunakan ec2-net-utils untuk di Panduan Pengguna AL2 Amazon Linux 2.
- 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 Outposts.

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

- Kartu jaringan di server
- Antarmuka jaringan lokal pada instance

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

Untuk tautan antarmuka jaringan lokal, 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 Outposts. Perubahan alamat IP dapat menyebabkan gangguan layanan sementara pada subnet Outpost.

Pendaftaran server

Ketika server Outposts 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 Outposts menggunakan port TCP 443 untuk memfasilitasi komunikasi dengan Wilayah melalui internet publik. Server Outposts tidak mendukung konektivitas pribadi melalui VPC.

Manajemen kapasitas untuk AWS Outposts

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

Topik

- Lihat AWS Outposts kapasitas
- Memodifikasi kapasitas AWS Outposts instans
- Memecahkan masalah tugas kapasitas

Lihat AWS Outposts kapasitas

Anda dapat melihat konfigurasi kapasitas pada tingkat instans atau Outpost.

Untuk melihat konfigurasi kapasitas untuk Outpost Anda menggunakan konsol

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
2. Dari panel navigasi kiri, pilih Outposts.
3. Pilih pos terdepan.
4. Pada halaman Detail Outpost pilih tampilan Instance atau tampilan Rack.
    - Tampilan instance - Menyediakan informasi tentang instance yang dikonfigurasi di Outposts dan distribusi instance berdasarkan ukuran dan keluarga.
    - Tampilan rak - Menyediakan visualisasi instans pada setiap aset dalam setiap Pos Luar dan memungkinkan Anda memilih Ubah kapasitas instans untuk membuat perubahan pada kapasitas instans.

Memodifikasi kapasitas AWS Outposts instans

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

Pertimbangan

Pertimbangkan hal berikut sebelum memodifikasi kapasitas instance:

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

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

Untuk mengubah konfigurasi kapasitas untuk Outpost Anda menggunakan konsol

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

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

Console steps

1. Pilih Tampilan Instance atau Tampilan rak.
2. Pilih Ubah konfigurasi kapasitas Outpost atau Ubah pada satu aset.
3. Pilih Outpost atau aset jika berbeda dari pilihan saat ini.
4. Pilih untuk menjalankan tugas kapasitas ini segera atau secara berkala selama 48 jam.
5. Pilih Berikutnya.
6. Pada halaman Configure instance capacity, setiap tipe instance menampilkan satu ukuran instans dengan jumlah maksimum yang telah dipilih sebelumnya. Untuk menambahkan lebih banyak ukuran instance, pilih Tambahkan ukuran instans.
7. Tentukan kuantitas instance dan catat kapasitas yang ditampilkan untuk ukuran instance tersebut.
8. Lihat pesan di akhir setiap bagian tipe instans yang memberi tahu Anda jika Anda berada di atas atau di bawah kapasitas. Lakukan penyesuaian pada ukuran instans atau tingkat kuantitas untuk mengoptimalkan total kapasitas yang tersedia.
9. Anda juga dapat meminta AWS Outposts untuk mengoptimalkan kuantitas instans untuk ukuran instans tertentu. Untuk melakukannya:
   a. Pilih ukuran instans.
   b. Pilih Saldo otomatis di akhir bagian tipe instans terkait.
10. Untuk setiap jenis instance, pastikan bahwa kuantitas instance ditentukan untuk setidaknya satu ukuran instance.
11. Secara opsional, pilih instance untuk tetap apa adanya.
12. Pilih Berikutnya.
13. Pada halaman Tinjau dan buat, verifikasi pembaruan yang Anda minta.
14. Pilih Buat. AWS Outposts menciptakan tugas kapasitas.

15. Pada halaman tugas kapasitas, pantau status tugas.

Upload a JSON file

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

   Example

   Contoh file JSON:

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

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

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

Memecahkan masalah tugas kapasitas

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

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

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

Untuk menyelesaikan masalah ini:

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

Paket kapasitas mencakup jenis instans yang tidak didukung

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

Untuk mengatasi masalah ini, gunakan konsol atau CLI.

Gunakan konsol

1. Masuk ke AWS.

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

Gunakan CLI

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

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

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

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

Untuk menyelesaikan masalah ini:

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

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

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

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

Gunakan konsol

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

Gunakan CLI

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

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

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

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

Gunakan konsol

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

Gunakan CLI

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

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

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

- Aset tidak terkait dengan Outpost.
- Aset terisolasi.

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

Gunakan konsol

1. Masuk ke AWS.

2. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
3. Pilih Tampilan rak untuk Pos Terdepan.
4. Verifikasi AssetId bahwa permintaan terkait dengan Outpost, dan tidak ditandai sebagai Host Terisolasi.
   a. Jika Aset diisolasi, ini mungkin karena tugas kapasitas berjalan di atasnya. Anda dapat menavigasi ke panel tugas kapasitas dan memeriksa apakah ada tugas Outpost atau tingkat aset yang sedang berjalan untuk dan. OutpostId AssetId Jika ada, maka tunggu tugas berakhir dan aset tersedia lagi.
   b. Jika tidak ada tugas kapasitas berjalan untuk aset yang terisolasi, maka aset tersebut dapat terdegradasi.
5. Setelah Anda memverifikasi bahwa aset tersebut ada dan dalam status valid, coba lagi permintaan Anda untuk membuat tugas kapasitas.

Gunakan CLI

1. Gunakan ListAssetsperintah untuk menemukan aset yang terkait dengan Outpostid.
2. Verifikasi bahwa AssetId yang diminta terkait dengan Pos Terdepan, dan bahwa Negaranya adalah`ACTIVE`.
   a. Jika Negara aset tidak AKTIF, ini mungkin karena tugas kapasitas berjalan di atasnya. Gunakan ListCapacityTasksperintah untuk menentukan apakah ada tugas Outpost atau tingkat aset yang sedang berjalan untuk dan. OutpostId AssetId Jika ada, maka tunggu tugas berakhir dan aset menjadi AKTIF lagi.
   b. Jika tidak ada tugas kapasitas berjalan untuk aset yang terisolasi, maka aset tersebut dapat terdegradasi.
3. Setelah Anda memverifikasi bahwa aset tersebut ada dan dalam status valid, coba lagi permintaan Anda untuk membuat tugas kapasitas.

Bagikan AWS Outposts sumber daya Anda

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

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

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

Pemilik Outpost dapat berbagi sumber daya Outpost dengan:

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

Daftar Isi

- Sumber daya Outpost yang dapat dibagikan
- Prasyarat untuk berbagi sumber daya Outposts
- Layanan terkait

- Berbagi di seluruh Availability Zone
- Berbagi sumber daya Outpost
- Membatalkan berbagi sumber daya Outpost bersama
- Mengidentifikasi sumber daya Outpost bersama
- Izin sumber daya Pos Luar Bersama
- Tagihan dan pengukuran
- Batasan

Sumber daya Outpost yang dapat dibagikan

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

Untuk sumber daya server Outposts, lihat Bekerja dengan sumber daya bersama AWS Outposts.

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

- Host Khusus yang Dialokasikan — Konsumen yang memiliki akses ke sumber daya ini dapat:
  - Luncurkan dan jalankan EC2 instance di 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 EC2 instance di subnet.

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

Prasyarat untuk berbagi sumber daya Outposts

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

Layanan terkait

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

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

Berbagi di seluruh Availability Zone

Untuk memastikan bahwa sumber daya didistribusikan di seluruh Availability Zone untuk suatu Wilayah, kami secara independen memetakan Availability Zone ke nama untuk setiap akun. Hal ini dapat menyebabkan perbedaan penamaan Zona Ketersediaan di seluruh akun. Misalnya, Availability Zone `us-east-1a` untuk AWS akun Anda mungkin tidak memiliki lokasi yang sama dengan AWS akun lain. `us-east-1a`

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

Untuk melihat Availability Zone di akun Anda IDs

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

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

Berbagi sumber daya Outpost

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

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

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

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

Untuk berbagi Outpost yang Anda miliki menggunakan konsol AWS Outposts

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

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

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

Lihat Membuat Sumber Daya Bersama di Panduan Pengguna AWS RAM .

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

Gunakan perintah create-resource-share.

Membatalkan berbagi sumber daya Outpost bersama

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

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

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

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

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

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

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

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

Lihat Memperbarui Sumber Daya Bersama di Panduan Pengguna AWS RAM .

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

Gunakan perintah disassociate-resource-share.

Mengidentifikasi sumber daya Outpost bersama

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

Untuk mengidentifikasi Outpost bersama menggunakan konsol AWS Outposts

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

Untuk mengidentifikasi sumber daya Outpost bersama menggunakan AWS CLI

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

Izin sumber daya Pos Luar Bersama

Izin untuk pemilik

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

Izin untuk konsumen

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

Tagihan dan pengukuran

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

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

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

Batasan

Batasan berikut berlaku untuk bekerja dengan AWS Outposts berbagi:

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

Keamanan di AWS Outposts

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

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

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

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

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
- Manajemen identitas dan akses (IAM) untuk AWS Outposts
- Keamanan infrastruktur di AWS Outposts
- Ketahanan di AWS Outposts
- Validasi kepatuhan untuk AWS Outposts

Perlindungan data di AWS Outposts

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

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

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

Enkripsi diam

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

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

Menghancurkan Kunci Keamanan Nitro secara kriptografis menghancurkan data di Pos Luar Anda. 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
- AWS Contoh kebijakan Outposts
- Peran terkait layanan untuk AWS Outposts
- AWS kebijakan terkelola untuk AWS Outposts

Bagaimana AWS Outposts bekerja dengan IAM

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

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

Kebijakan berbasis identitas untuk Outposts AWS

Mendukung kebijakan berbasis identitas: Ya

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

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

Contoh kebijakan berbasis identitas untuk Outposts AWS

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

Tindakan kebijakan untuk AWS Outposts

Mendukung tindakan kebijakan: Ya

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

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

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

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

Tindakan kebijakan di AWS Outposts menggunakan awalan berikut sebelum tindakan:

```
outposts
```

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

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

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

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

Sumber daya kebijakan untuk AWS Outposts

Mendukung sumber daya kebijakan: Ya

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

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

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

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

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

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

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

Kunci kondisi kebijakan untuk AWS Outposts

Mendukung kunci kondisi kebijakan khusus layanan: Yes

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

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

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

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

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

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

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

ABAC dengan Outposts AWS

Mendukung ABAC (tanda dalam kebijakan): Ya

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

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

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

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

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

Menggunakan kredensil sementara dengan Outposts AWS

Mendukung kredensial sementara: Ya

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

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

selengkapnya tentang peralihan peran, lihat Beralih dari pengguna ke peran IAM (konsol) dalam Panduan Pengguna IAM.

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

Izin utama lintas layanan untuk Outposts AWS

Mendukung sesi akses maju (FAS): Ya

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

Peran terkait layanan untuk Outposts AWS

Mendukung peran terkait layanan: Ya

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

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

AWS Contoh kebijakan Outposts

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

administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

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

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

Daftar Isi

- Praktik terbaik kebijakan
- Contoh: Menggunakan izin tingkat sumber daya

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua

permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.

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

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

Contoh: Menggunakan izin tingkat sumber daya

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetOutpost",
      "Resource": "arn:aws:outposts:region:12345678012:outpost/op-1234567890abcdef0"
    }
  ]
}
```

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

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

Peran terkait layanan untuk AWS Outposts

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

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

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

Izin peran terkait layanan untuk AWS Outposts

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

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

- `outposts.amazonaws.com`

Kebijakan peran terkait layanan

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

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_*`OutpostID`*

AWSOutpostsServiceRolePolicy

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

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

- Tindakan: `ec2:DescribeNetworkInterfaces` pada semua AWS sumber daya
- Tindakan: `ec2:DescribeSecurityGroups` pada semua AWS sumber daya
- Tindakan: `ec2:CreateSecurityGroup` pada semua AWS sumber daya
- Tindakan: `ec2:CreateNetworkInterface` pada semua AWS sumber daya

AWSOutpostsPrivateConnectivityPolicy_OutpostID

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

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

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

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

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

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

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

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

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

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

Buat peran terkait layanan untuk AWS Outposts

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

Mengedit peran terkait layanan untuk AWS Outposts

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

Menghapus peran terkait layanan untuk AWS Outposts

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

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

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

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

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

Hubungi AWS Enterprise Support untuk menghapus Outpost Anda.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

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

Wilayah yang Didukung untuk AWS Outposts peran terkait layanan

AWS Outposts mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat FAQs untuk Outposts server.

AWS kebijakan terkelola untuk AWS Outposts

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

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

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

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

AWS kebijakan terkelola: AWSOutposts ServiceRolePolicy

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

AWS kebijakan terkelola: AWSOutposts AuthorizeServerPolicy

Gunakan kebijakan ini untuk memberikan izin yang diperlukan untuk mengotorisasi perangkat keras server Outposts di jaringan lokal Anda.

Kebijakan ini mencakup izin berikut.

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

AWS Update Outposts ke AWS kebijakan terkelola

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

Perubahan	Deskripsi	Tanggal
AWSOutpostsAuthorizeServerPolicy – Kebijakan baru	AWS Outposts menambahkan kebijakan yang memberikan izin untuk mengotorisasi perangkat keras server Outposts 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 EC2 instans dan volume EBS yang berjalan di Pos Luar Anda, lihat Keamanan Infrastruktur di Amazon. EC2

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

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

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:

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

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

CloudWatch metrik

Gunakan Amazon CloudWatch untuk mengambil statistik tentang titik data untuk server rak 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 server racks.

CloudTrail log

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

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

Log Aliran VPC

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

Pencerminan Lalu lintas

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

AWS Health Dashboard

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

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

CloudWatch metrik untuk server racks

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

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

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

Daftar Isi

- Metrik
- Dimensi metrik
- Lihat CloudWatch metrik untuk server rak

Metrik

Namespace `AWS/Outposts` mencakup metrik berikut.

`ConnectedStatus`

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

Satuan: Hitung

Resolusi maksimum: 1 menit

Statistics: Statistik yang paling berguna adalah `Average`.

Dimensi: `OutpostId`

`CapacityExceptions`

Jumlah kesalahan kapasitas yang tidak mencukupi misalnya peluncuran.

Satuan: Hitung

Resolusi maksimum: 5 menit

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

Dimensi: `InstanceType` dan `OutpostId`

`InstanceFamilyCapacityAvailability`

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

Satuan: Persen

Resolusi maksimum: 5 menit

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

Dimensi: `InstanceFamily` dan `OutpostId`

`InstanceFamilyCapacityUtilization`

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

Satuan: Persen

Resolusi maksimum: 5 menit

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

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

`InstanceTypeCapacityAvailability`

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

Satuan: Persen

Resolusi maksimum: 5 menit

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

Dimensi: `InstanceType` dan `OutpostId`

`InstanceTypeCapacityUtilization`

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

Satuan: Persen

Resolusi maksimum: 5 menit

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

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

`UsedInstanceType_Count`

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

Satuan: Hitung

Resolusi maksimum: 5 menit

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

`AvailableInstanceType_Count`

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

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

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

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

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi: `InstanceType` dan `OutpostId`

`AvailableReservedInstances`

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

Metrik ini tidak termasuk Instans EC2 Cadangan Amazon.

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

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

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi: `InstanceType` dan `OutpostId`

`UsedReservedInstances`

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

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi: `InstanceType` dan `OutpostId`

`TotalReservedInstances`

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

Satuan: Hitung

Resolusi maksimum: 5 menit

Dimensi: `InstanceType` dan `OutpostId`

Dimensi metrik

Untuk memfilter metrik untuk Outpost Anda, gunakan dimensi berikut.

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

Lihat CloudWatch metrik untuk server rak

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

Untuk melihat metrik menggunakan konsol CloudWatch

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

Untuk melihat metrik menggunakan AWS CLI

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

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

Untuk mendapatkan statistik untuk metrik menggunakan AWS CLI

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

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

Log panggilan AWS Outposts API menggunakan AWS CloudTrail

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

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

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

CloudTrail aktif di AWS akun Anda saat Anda membuat akun, dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

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

CloudTrail jalan setapak

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

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

CloudTrail Penyimpanan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail Lake mengonversi peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda

pilih dengan menerapkan pemilih acara tingkat lanjut. Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat Bekerja dengan AWS CloudTrail Danau di Panduan AWS CloudTrail Pengguna.

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

AWS Outposts acara manajemen di CloudTrail

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

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

AWS Outposts contoh acara

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

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
```

```
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Pemeliharaan server Outposts

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

> **Warning**
>
> Data pada volume penyimpanan instance hilang jika drive disk yang mendasarinya gagal, atau jika instance berakhir. 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.

Daftar Isi

- Perbarui detail kontak
- Pemeliharaan perangkat keras
- Pembaruan firmware
- Praktik terbaik untuk acara listrik dan jaringan
- Data server rusak secara kriptografis

Perbarui detail kontak

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

Pemeliharaan perangkat keras

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

AWS mengakhiri instance yang terpengaruh pada tanggal pensiun instans. Data pada volume penyimpanan instance tidak bertahan setelah penghentian instance. Oleh 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 Outposts.
- 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 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-on) selama pemeliharaan.
- Berikan waktu ekstra dalam jendela pemeliharaan untuk menangani hal yang tidak terduga.
- Kelola harapan pengguna dan pelanggan Anda dengan mengkomunikasikan kerangka waktu jendela pemeliharaan yang lebih luas daripada yang biasanya Anda butuhkan.
- Setelah daya dipulihkan, buat case di AWS Dukungan Center untuk meminta verifikasi bahwa AWS Outposts dan layanan terkait sedang berjalan.

Acara konektivitas jaringan

Koneksi tautan layanan antara Outpost Anda dan AWS Wilayah atau Outposts home Region biasanya akan secara otomatis pulih dari gangguan jaringan atau masalah yang mungkin terjadi di perangkat jaringan perusahaan hulu Anda atau di jaringan penyedia konektivitas pihak ketiga mana pun setelah pemeliharaan jaringan selesai. Selama koneksi tautan layanan tidak aktif, operasi Outposts Anda terbatas pada aktivitas jaringan lokal.

EC2 Instans Amazon, jaringan LNI, dan volume penyimpanan instans di server Outposts akan terus beroperasi secara normal dan dapat diakses secara lokal melalui jaringan lokal dan LNI. Demikian pula, sumber daya AWS layanan seperti node pekerja Amazon ECS terus berjalan secara lokal. Namun, ketersediaan API akan terdegradasi. Misalnya, run, start, stop, dan terminate APIs mungkin tidak berfungsi. Metrik dan log instans akan terus di-cache secara lokal hingga 7 hari, dan akan didorong ke AWS Wilayah saat konektivitas kembali. Pemutusan lebih dari 7 hari dapat mengakibatkan hilangnya metrik dan log.

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 AWSSupport-SetupIPMonitoringFromVPCalat ini. Alat ini adalah AWS Systems Manager dokumen (dokumen SSM) yang membuat Instans EC2 Monitor Amazon di subnet yang ditentukan oleh Anda dan memantau alamat IP target. Dokumen menjalankan tes diagnostik ping, MTR, TCP trace-route dan trace-path dan menyimpan hasilnya di Amazon CloudWatch Logs yang dapat divisualisasikan di CloudWatch dasbor (misalnya latensi, kehilangan paket). Untuk pemantauan Outposts, Instans Monitor harus berada di satu subnet dari AWS Wilayah induk dan dikonfigurasi untuk memantau satu atau lebih instance Outpost Anda menggunakan IP pribadinya - ini akan memberikan grafik kehilangan paket dan latensi antara dan Wilayah induk. AWS Outposts AWS
- AWS Blog Menyebarkan CloudWatch dasbor Amazon otomatis untuk AWS Outposts digunakan AWS CDK menjelaskan langkah-langkah yang terlibat dalam menerapkan dasbor otomatis.

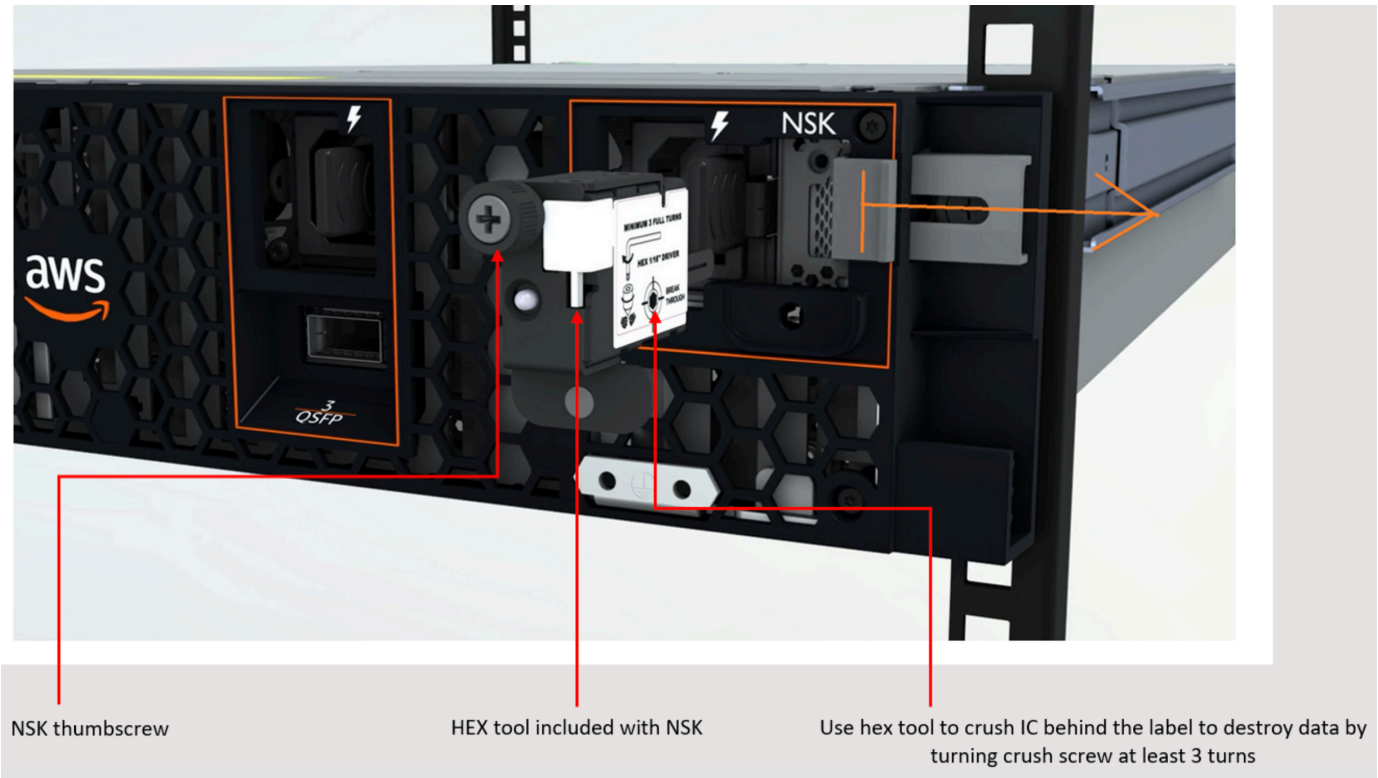
- Jika Anda memiliki pertanyaan atau memerlukan informasi selengkapnya, lihat Membuat kasus AWS dukungan di Panduan Pengguna Support.

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.



Opsi server Outposts end-of-term

Di akhir AWS Outposts masa jabatan Anda, Anda harus memilih di antara opsi-opsi berikut:

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

Perbarui langganan Anda

Anda harus menyelesaikan langkah-langkah berikut setidaknya 30 hari sebelum langganan saat ini untuk server Outposts Anda berakhir.

Untuk memperbarui langganan Anda dan mempertahankan server Outposts yang ada

1. Masuk ke Konsol AWS Dukungan Tengah.
2. Pilih Buat kasus.
3. Pilih Akun dan penagihan.
4. Untuk Layanan, pilih Penagihan.
5. Untuk Kategori, pilih Pertanyaan Penagihan Lainnya.
6. Untuk Keparahan, pilih Pertanyaan penting.
7. Pilih Langkah selanjutnya: Informasi tambahan.
8. Pada halaman Informasi tambahan, untuk Subjek, masukkan permintaan Anda untuk memperbarui seperti**`Renew my Outpost subscription`**.
9. Untuk Deskripsi, masukkan salah satu opsi pembayaran berikut:

   - Tidak ada di muka
   - Sebagian di muka
   - Semua dimuka

   Untuk harga, lihat harga AWS Outposts 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 Outposts 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

Anda harus menyelesaikan langkah-langkah berikut setidaknya 30 hari sebelum langganan saat ini untuk server Outposts Anda berakhir. AWS tidak dapat memulai proses pengembalian sampai Anda melakukannya.

> **Important**
>
> AWS tidak dapat menghentikan proses pengembalian setelah Anda membuka kasus dukungan untuk mengakhiri langganan Anda.

Untuk mengakhiri langganan Anda

1. Masuk ke Konsol AWS Dukungan Tengah.
2. Pilih Buat kasus.
3. Pilih Akun dan penagihan.
4. Untuk Layanan, pilih Penagihan.
5. Untuk Kategori, pilih Pertanyaan Penagihan Lainnya.
6. Untuk Keparahan, pilih Pertanyaan penting.
7. Pilih Langkah selanjutnya: Informasi tambahan.
8. Pada halaman Informasi tambahan, untuk Subjek, masukkan permintaan yang jelas, seperti**`End my Outpost subscription`**.

9. Untuk Deskripsi, masukkan tanggal 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 Outposts 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 dimulai sehari setelah langganan Anda saat ini berakhir.

Kuota untuk AWS Outposts

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

Untuk melihat kuota AWS Outposts, buka konsol Service Quotas. Di panel navigasi, pilih Layanan AWS, dan pilih AWS Outposts.

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

Anda Akun AWS memiliki kuota berikut yang terkait AWS Outposts dengan.

Sumber Daya	Default	Dapat disesuaikan	Komentar
Situs pos terdepan	100	Ya	Situs Outpost adalah bangunan fisik yang dikelola pelanggan di mana Anda memberi daya dan memasang peralatan Outpost Anda ke jaringan. Anda dapat memiliki 100 situs Outposts di setiap Wilayah akun Anda AWS .
Outposts per situs	10	Ya	AWS Outposts termasuk perangkat keras dan sumber daya virtual, yang dikenal sebagai Outposts. Kuota ini membatasi sumber daya virtual Outpost Anda. Anda dapat memiliki 10 Outposts di setiap situs Outpost.

AWS Outposts dan kuota untuk layanan lainnya

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

Tabel berikut menjelaskan pembaruan dokumentasi untuk server Outposts.

Perubahan	Deskripsi	Tanggal
Memecahkan masalah koneksi tautan layanan	Jika koneksi antara server Outposts dan AWS Region Anda tidak aktif, ikuti langkah-langkah berikut untuk memecahkan masalah dan menyelesaikannya.	5 Mei 2025
Pembaruan stabilitas statis	Jika jaringan Anda terganggu , metrik dan log instans akan di-cache secara lokal hingga 7 hari. Sebelumnya, Outposts bisa cache log hanya beberapa jam.	1 Mei 2025
Manajemen kapasitas di tingkat aset	Anda dapat memodifikasi konfigurasi kapasitas di tingkat aset.	Maret 31, 2025
Volume blok eksternal yang didukung oleh penyimpanan pihak ketiga	Anda sekarang dapat melampirkan volume data blok yang didukung oleh sistem penyimpanan blok pihak ketiga yang kompatibel selama proses peluncuran instans di Outpost.	Desember 1, 2024
Manajemen kapasitas	Anda dapat memodifikasi konfigurasi kapasitas default untuk pesanan Outposts baru Anda.	16 April 2024
End-of-term pilihan untuk AWS Outposts server	Di akhir AWS Outposts jangka waktu Anda, Anda dapat	1 Agustus 2023

	memperbarui, mengakhiri, atau mengonversi langganan Anda.	
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
Memperkenalkan server Outposts	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.