



Panduan Pengguna untuk server Outposts

# AWS Outposts



# AWS Outposts: Panduan Pengguna untuk server Outposts

Copyright © 2024 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
VPC 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) .....	13
Rekomendasi bandwidth tautan layanan .....	13
Tautan layanan membutuhkan DHCP respons .....	13
Latensi maksimum tautan layanan .....	13
Daya .....	13
Dukungan daya .....	14
Daya tarik .....	14
Kabel daya .....	14
Redundansi daya .....	14
Pemenuhan pesanan .....	15
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: Konfigurasi konektivitas .....	25
Langkah 4: Uji konektivitas .....	25
Tautan layanan .....	28
Konektivitas melalui tautan layanan .....	28
Persyaratan unit transmisi maksimum tautan layanan (MTU) .....	29
Rekomendasi bandwidth tautan layanan .....	13
Firewall dan tautan layanan .....	29
Pembaruan dan tautan layanan .....	30
Koneksi internet redundan .....	31
Kembalikan server .....	32
Langkah 1: Siapkan server untuk kembali .....	32
Langkah 2: Dapatkan label pengiriman kembali .....	33
Langkah 3: Kemas server .....	33
Langkah 4: Kembalikan server melalui kurir .....	34
Antarmuka jaringan lokal .....	37
Dasar-dasar antarmuka jaringan lokal .....	38
Kinerja .....	39
Grup keamanan .....	40
Pemantauan .....	40
MACalamat .....	40
Tambahkan antarmuka jaringan lokal .....	41
Lihat antarmuka jaringan lokal .....	42
Konfigurasi sistem operasi .....	42
Konektivitas lokal .....	42
Topologi server di jaringan Anda .....	43
Konektivitas fisik server .....	43
Lalu lintas tautan layanan untuk server .....	44
Antarmuka jaringan lokal menghubungkan lalu lintas .....	45
Penetapan alamat IP server .....	46
Pendaftaran server .....	47
Sumber Daya Bersama .....	48
Sumber daya Outpost yang dapat dibagikan .....	49
Prasyarat untuk berbagi sumber daya Outposts .....	49
Layanan terkait .....	50
Berbagi di seluruh Availability Zone .....	50

Berbagi sumber daya Outpost .....	51
Membatalkan berbagi sumber daya Outpost bersama .....	52
Mengidentifikasi sumber daya Outpost bersama .....	53
Izin sumber daya Pos Luar Bersama .....	53
Izin untuk pemilik .....	53
Izin untuk konsumen .....	53
Tagihan dan pengukuran .....	54
Batasan .....	54
Keamanan .....	55
Perlindungan data .....	56
Enkripsi diam .....	56
Enkripsi bergerak .....	56
Penghapusan data .....	56
Pengelolaan identitas dan akses .....	56
Bagaimana AWS Outposts bekerja dengan IAM .....	57
Contoh kebijakan .....	63
Peran terkait layanan .....	66
AWS kebijakan terkelola .....	69
Keamanan infrastruktur .....	71
Ketangguhan .....	72
Validasi kepatuhan .....	72
Pemantauan .....	75
CloudWatch metrik .....	76
Metrik .....	76
Dimensi metrik .....	80
Lihat CloudWatch metrik untuk server rak Anda .....	80
Log API panggilan menggunakan CloudTrail .....	81
AWS Outposts acara manajemen di CloudTrail .....	83
AWS Outposts contoh acara .....	83
Maintenance .....	85
Perbarui detail kontak .....	85
Pemeliharaan perangkat keras .....	85
Pembaruan firmware .....	86
Acara daya dan jaringan .....	86
Peristiwa kekuasaan .....	86
Acara konektivitas jaringan .....	87

---

Sumber daya .....	88
Data server rusak secara kriptografis .....	89
End-of-term Opsi E .....	90
Perpanjang langganan .....	90
Akhiri langganan .....	91
Konversi langganan .....	92
Quotas .....	93
AWS Outposts dan kuota untuk layanan lainnya .....	94
Riwayat dokumen .....	95
.....	xcvi

# 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. Instance dalam subnet Outpost berkomunikasi dengan instans lain di AWS Wilayah menggunakan alamat IP pribadi, semuanya dalam hal yang sama. VPC

## Note

Anda tidak dapat menghubungkan Pos Luar ke Pos Luar atau Zona Lokal lain yang berada dalam posisi yang sama. VPC

Untuk informasi lebih lanjut, lihat [halaman AWS Outposts produk](#).

## Konsep utama

Ini adalah konsep kunci untuk AWS Outposts.

- Situs pos terdepan — Bangunan fisik yang dikelola pelanggan tempat AWS akan memasang Pos Luar Anda. Sebuah situs harus memenuhi fasilitas, jaringan, dan persyaratan daya untuk Outpost Anda.
- Kapasitas pos terdepan — Sumber daya komputasi dan penyimpanan yang tersedia di Outpost. Anda dapat melihat dan mengelola kapasitas untuk Outpost Anda dari AWS Outposts konsol.
- Peralatan pos terdepan — Perangkat keras fisik yang menyediakan akses ke AWS Outposts layanan. Perangkat keras termasuk rak, server, sakelar, dan kabel yang dimiliki dan dikelola oleh AWS

- **Rak Outposts** — Faktor bentuk Outpost yang merupakan rak 42U standar industri. Rak 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 -310D 19 yang sesuai EIA. 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 Support Center](#) jika informasi kontak berubah.
- **Tautan layanan** — Rute jaringan yang memungkinkan komunikasi antara Outpost Anda dan AWS Wilayah terkait. Setiap Pos Luar adalah perpanjangan dari Availability Zone dan Wilayah terkait.
- **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:

Hitung

Jenis sumber daya	Rak	Server
<a href="#">EC2 Contoh Amazon</a>		 Ya
<a href="#">ECSCluster Amazon</a>		 Ya

Jenis sumber daya	Rak	Server	
<a href="#">EKSNode Amazon</a>		Y 	Tidak

## Database dan analitik

Jenis sumber daya	Rak	Server	
ElastiCache Node Amazon (kluster <a href="#">Redis</a> , kluster <a href="#">Memcached</a> )		Y 	Tidak
<a href="#">EMRCluster Amazon</a>		Y 	Tidak
<a href="#">Instans Amazon RDS DB</a>		Y 	Tidak

## Jaringan

Jenis sumber daya	Rak	Server	
<a href="#">Proksi Utusan App Mesh</a>		Y 	Ya
<a href="#">Penyeimbang Beban Aplikasi</a>		Y 	Tidak

Jenis sumber daya	Rak	Server
<a href="#">Amazon VPC subnet</a>		 Ya
<a href="#">Rute Amazon 53</a>		 Tidak

Penyimpanan

Jenis sumber daya	Rak	Server
<a href="#">EBSVolume Amazon</a>		 Tidak
<a href="#">Ember Amazon S3</a>		 Tidak

Lainnya Layanan AWS

Layanan	Rak	Server
AWS IoT Greengrass		 Ya
Manajer Amazon SageMaker Edge		 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 Pos Luar ke jaringan lokal. Jaringan lokal Anda harus menyediakan akses jaringan area luas (WAN) kembali ke Wilayah dan ke internet. Ini juga harus menyediakan LAN atau WAN mengakses ke jaringan lokal tempat beban kerja atau aplikasi lokal Anda berada.

Diagram berikut menggambarkan kedua faktor bentuk Outpost.

## Daftar Isi

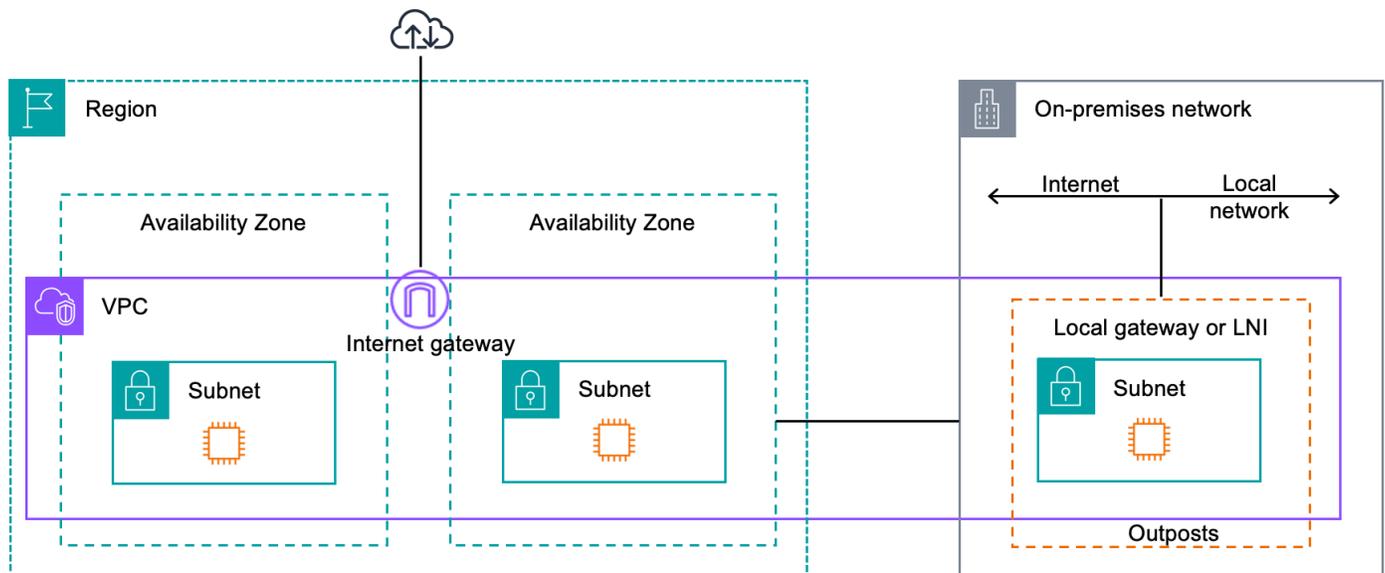
- [Komponen jaringan](#)
- [VPC dan subnet](#)
- [Perutean](#)
- [DNS](#)
- [Tautan layanan](#)
- [Antarmuka jaringan lokal](#)

## Komponen jaringan

AWS Outposts memperluas Amazon VPC dari AWS Wilayah ke Pos Luar dengan VPC komponen yang dapat diakses di Wilayah, termasuk gateway internet, gateway pribadi virtual, Gateway Transit Amazon VPC, 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
- A VPC dengan beberapa subnet di Wilayah
- Pos terdepan di jaringan lokal
- Konektivitas antara Outpost dan jaringan lokal yang disediakan oleh gateway lokal (rak) atau antarmuka jaringan lokal (server)



## VPCs dan subnet

Virtual private cloud (VPC) mencakup semua Availability Zone di AWS Wilayahnya. Anda dapat memperluas apa pun VPC di Wilayah ke Pos Luar Anda dengan menambahkan subnet Outpost. Untuk menambahkan subnet Outpost ke aVPC, tentukan Amazon Resource Name (ARN) dari 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 VPC kuota, lihat [VPC Kuota Amazon](#) di VPC Panduan Pengguna Amazon.

Anda membuat subnet Outpost dari VPC CIDR kisaran 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 nya. VPC 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 VPC CIDR sisa-sisa dirutekan di VPC

Tabel rute subnet pos terdepan dapat mencakup tujuan berikut:

- VPC CIDR rentang - AWS mendefinisikan ini pada instalasi. Ini adalah rute lokal dan berlaku untuk semua VPC perutean, termasuk lalu lintas antara instance Outpost dalam hal yang sama. VPC
- 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 aVPC, EC2 instance di subnet Outposts dapat menggunakan Amazon Route 53 DNS Service untuk menyelesaikan nama domain ke alamat IP. Route 53 mendukung DNS fitur, seperti pendaftaran domain, DNS perutean, 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 DNS fitur-fitur ini berfungsi.

Anda mungkin menemukan waktu DNS resolusi yang lebih lama dengan Route 53, tergantung pada latensi jalur antara Pos Luar dan Wilayah. AWS Dalam kasus seperti itu, Anda dapat menggunakan DNS server yang diinstal secara lokal di lingkungan lokal Anda. Untuk menggunakan DNS server Anda sendiri, Anda harus membuat set DHCP opsi untuk DNS server lokal Anda dan mengaitkannya dengan server. VPC Anda juga harus memastikan bahwa ada konektivitas IP ke DNS server 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 DHCP opsi memiliki VPC cakupan, instance di subnet Outpost dan subnet Availability Zone untuk VPC akan mencoba menggunakan DNS server yang ditentukan untuk resolusi nama. DNS

Pencatatan kueri tidak didukung untuk DNS kueri 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 VPN koneksi terenkripsi yang digunakan setiap kali Outpost berkomunikasi dengan Wilayah rumah pilihan Anda. Anda menggunakan virtual LAN (VLAN) untuk mengelompokkan lalu lintas pada tautan layanan. Tautan layanan VLAN memungkinkan komunikasi antara Pos Terdepan dan AWS Wilayah untuk pengelolaan Pos Luar dan intra VPC lalu lintas antara AWS Wilayah dan Pos Terdepan.

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

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

## Antarmuka jaringan lokal

Server Outposts menyertakan antarmuka jaringan lokal untuk menyediakan konektivitas ke jaringan lokal Anda. Antarmuka jaringan lokal hanya tersedia untuk server Outposts yang berjalan di subnet Outpost. Anda tidak dapat menggunakan antarmuka jaringan lokal dari EC2 instance di rak Outposts atau di Region. AWS Antarmuka jaringan lokal dimaksudkan hanya untuk lokasi lokal. Untuk informasi selengkapnya, lihat [Antarmuka jaringan lokal 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 EIA -310-D. Kit rel tidak kompatibel dengan braket pemasangan berbentuk U, seperti yang ditunjukkan pada gambar berikut.
- Penempatan Rak - Kami merekomendasikan penggunaan rak standar 19-inci EIA -310D, dengan kedalaman setidaknya 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 yang 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 CORE NEBS GR-63.
- 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 lalu lintas layanan dan LNI tautan — QSFP + kabel breakout (10 kaki/3 m) segmen lalu lintas.

## Firewall tautan layanan

UDP dan TCP 443 harus terdaftar secara statis di firewall.

Protokol	Pelabuhan Sumber	Alamat Sumber	Pelabuhan Tujuan	Alamat Tujuan
UDP	1024-65535	Layanan Link IP	53	DHCPDNSserver yang disediakan
UDP	443, 1024-65535	Layanan Link IP	443	Titik akhir Tautan Layanan Outposts
TCP	1024-65535	Layanan Link IP	443	Titik akhir Pendaftaran Outposts

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

## Unit transmisi maksimum tautan layanan (MTU)

Jaringan harus mendukung 1500-byte MTU antara Outpost dan titik akhir tautan layanan di Wilayah induk. AWS Untuk informasi selengkapnya tentang tautan layanan, 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 AMI ukuran, elastisitas aplikasi, kebutuhan kecepatan burst, dan VPC lalu lintas 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 APN mitra Anda.

## Tautan layanan membutuhkan DHCP respons

Tautan layanan memerlukan IPv4 DHCP respons untuk mengkonfigurasi pengaturan jaringan.

## Latensi maksimum tautan layanan

Tautan layanan dapat mendukung latensi jaringan maksimum 175 ms dari server dan Availability Zone-nya.

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

## 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 menyertakan Uninterruptible Power Supply (). UPS

## Pemenuhan pesanan

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

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

Tim Anda atau penyedia pihak ketiga harus memasang peralatan. Untuk informasi selengkapnya, lihat [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 konfigurasi 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 tetapkan 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 Support 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 JSON file.

## 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 JSON file yang menentukan jenis, ukuran, dan kuantitas instans.

#### Example

Contoh JSON file:

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

4. Tinjau isi JSON file 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 Support 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 IAM kredensi 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: Konfigurasi konektivitas](#)
- [Langkah 4: Uji konektivitas](#)

## Langkah 1: Buat subnet

Anda dapat menambahkan subnet Outpost ke mana pun VPC di AWS Wilayah untuk Pos Luar. 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 AmazonVPC. 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-attribute](#) perintah 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 VPC lalu lintas 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

- Instance di server Outposts menyertakan volume penyimpanan instance tetapi bukan EBS volume. Pilih ukuran instans dengan penyimpanan instans yang cukup untuk memenuhi kebutuhan aplikasi

Anda. Untuk informasi selengkapnya, lihat [Volume penyimpanan instans](#) dan [Membuat instans yang didukung toko AMI](#) di EC2Panduan Pengguna Amazon.

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

Untuk meluncurkan instans di subnet Outpost Anda

1. Buka AWS Outposts konsol di <https://console.aws.amazon.com/outposts/>.
2. Pada panel navigasi, pilih Outposts.
3. Pilih Outpost, lalu pilih Actions, View details.
4. Pada halaman ringkasan Outpost, pilih Launch instance. Anda dialihkan ke wizard peluncuran instans di 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, lihat [Tambahkan 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: Konfigurasi 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 Outpost.

```
ping 10.0.3.128
```

Berikut ini adalah output contoh.

```
Pinging 10.0.3.128

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

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

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

Uji konektivitas dari instance Outpost ke jaringan lokal Anda

Tergantung pada sistem operasi Anda, gunakan ssh atau rdp untuk terhubung ke alamat IP pribadi dari instance Outpost Anda. Untuk informasi tentang menghubungkan ke 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 pada halaman detail instance.
2. Bergantung pada sistem operasi Anda, gunakan ssh atau sambungkan rdp ke alamat IP pribadi instans Outpost Anda.
3. Jalankan ping perintah dari instance Outpost Anda, 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](#)
- [Koneksi internet redundan](#)

## 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 VPN koneksi terenkripsi yang digunakan setiap kali Outpost berkomunikasi dengan Wilayah rumah pilihan Anda. Anda menggunakan virtual LAN (VLAN) untuk mengelompokkan lalu lintas pada tautan layanan. Tautan layanan VLAN memungkinkan komunikasi antara Pos Terdepan dan AWS Wilayah untuk pengelolaan Pos Luar dan intra VPC lalu lintas antara AWS Wilayah dan Pos Terdepan.

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

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

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

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

## Persyaratan unit transmisi maksimum tautan layanan (MTU)

Unit transmisi maksimum (MTU) dari koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang diizinkan yang dapat dilewatkan melalui koneksi. Jaringan harus mendukung 1500-byte MTU antara Outpost dan titik akhir tautan layanan di Wilayah induk. AWS Untuk informasi tentang persyaratan MTU antara instans di Pos Luar dan instans di AWS Wilayah melalui tautan layanan, lihat [Unit transmisi maksimum jaringan \(MTU\) untuk EC2 instans Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

## 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 AMI ukuran, elastisitas aplikasi, kebutuhan kecepatan burst, dan VPC lalu lintas 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 APN mitra Anda.

## Firewall dan tautan layanan

Bagian ini membahas konfigurasi firewall dan koneksi link layanan.

Dalam diagram berikut, konfigurasi memperluas Amazon VPC dari AWS Wilayah ke 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 Pos Terdepan 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. Hal ini karena link layanan VPN dimulai hanya dari Outpost ke Region, bukan dari Region ke Outpost.

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	DHCPDNSserver yang disediakan
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.

## 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 intra- VPC lalu lintas antara Outpost dan Region. AWS AWS Praktik [terbaik](#)

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

Tautan layanan diperbarui secara berkala untuk menjaga kualitas dan kinerja operasional. Selama pemeliharaan, Anda mungkin mengamati periode singkat latensi dan kehilangan paket pada jaringan ini yang mengakibatkan dampak pada beban kerja yang bergantung pada VPC konektivitas 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.

## 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.

# 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 Support 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 pembagian sumber daya](#) di Panduan AWS RAM Pengguna.
- Gunakan AWS CLI untuk menjalankan [disassociate-resource-share](#) perintah.

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 Support 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 Support 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	<a href="#">AWS Support Pusat</a> Kontak. Dalam permintaan Anda, sertakan informasi berikut: <ul style="list-style-type: none"><li>• Nomor pelacakan yang ada di label pengiriman AWS yang disediakan</li><li>• Tanggal dan waktu yang Anda inginkan kurir untuk mengambil server</li><li>• Nama kontak</li><li>• Nomor telepon</li><li>• Alamat email</li></ul>
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	

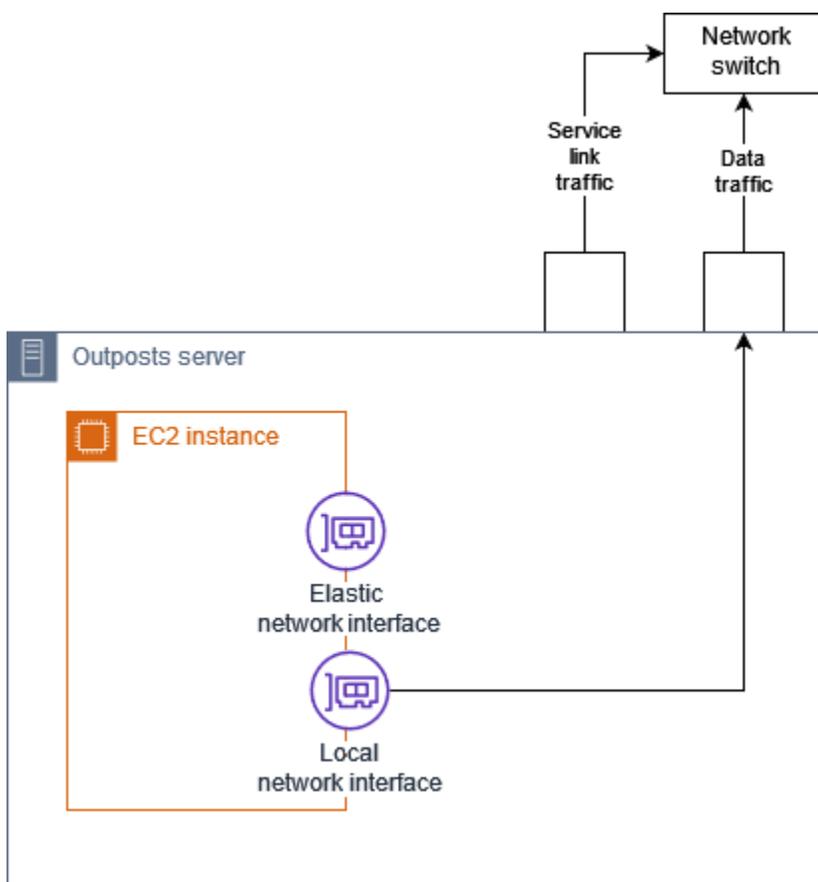
Negara	Kontak
Amerika Serikat	<p>Kontak <a href="#">UPS</a>.</p> <p>Anda dapat mengembalikan server dengan cara berikut:</p> <ul style="list-style-type: none"><li>• Kembalikan server selama UPS pengambilan rutin di situs Anda.</li><li>• Drop-off server di suatu <a href="#">UPSlokasi</a>.</li><li>• Jadwalkan <a href="#">penjemputan</a> untuk tanggal dan waktu yang Anda inginkan. Masukkan nomor pelacakan dari label pengiriman AWS yang disediakan untuk pengiriman gratis.</li></ul>
Semua negara lain	<p>Kontak <a href="#">DHL</a>.</p> <p>Anda dapat mengembalikan server dengan cara berikut:</p> <ul style="list-style-type: none"><li>• Drop-off server di suatu <a href="#">DHLlokasi</a>.</li><li>• Jadwalkan <a href="#">penjemputan</a> untuk tanggal dan waktu yang Anda inginkan. Masukkan nomor DHL Waybill dari label pengiriman AWS yang disediakan untuk pengiriman gratis.</li></ul> <p>Jika Anda mendapatkan kesalahan berikut <code>Courier pickup can't be scheduled for an import shipment</code>, biasanya berarti bahwa negara penjemputan yang Anda pilih tidak cocok dengan negara penjemputan pada label pengiriman kembali. Pilih negara asal kiriman dan coba lagi.</p>

# 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 jaringan. 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 DHCP opsi dalam a VPC untuk mengkonfigurasi 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 VPC jaringan untuk mengakses titik akhir Regional publik Layanan AWS, atau Anda dapat menggunakan VPC titik akhir antarmuka untuk mengakses Layanan AWS menggunakan 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. A VPC adalah jaringan layer-tiga tervirtualisasi. Antarmuka jaringan lokal tidak mendukung komponen VPC jaringan. 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 VPC alur lapisan-tiga. Sistem operasi host dari instance ini memang memiliki visibilitas penuh ke dalam frame dari jaringan fisik. Anda dapat menerapkan logika firewall standar ke informasi dalam bingkai ini. Namun, komunikasi ini terjadi di dalam instance tetapi di luar lingkup konstruksi virtual.

## Pertimbangan

- Dukungan ARP dan DHCP protokol antarmuka jaringan lokal. 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 VPC Pengguna Amazon.
- 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 MAC spoofing alamat.

## 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 AndaVPC. Grup keamanan mengontrol lalu lintas masuk dan keluarVPC. Antarmuka jaringan lokal tidak dilampirkan ke fileVPC. 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 ENA setelan EC2 instans Anda di](#) Panduan EC2 Pengguna Amazon.

## MACalamat

AWS menyediakan MAC alamat untuk antarmuka jaringan lokal. Antarmuka jaringan lokal menggunakan alamat (LAA) yang dikelola secara lokal untuk alamatnyaMAC. Antarmuka jaringan lokal menggunakan MAC alamat yang sama sampai Anda menghapus antarmuka. Setelah Anda menghapus antarmuka jaringan lokal, hapus MAC alamat dari konfigurasi lokal Anda. AWS dapat menggunakan kembali MAC alamat 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 sebagai gantinya. AWS SDK Misalnya, gunakan perintah berikut dari AWS CLI: [create-network-interface](#) dan [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 IPv4alamat 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 subnetCIDR. Alamat ini bukan alamat IP dari antarmuka jaringan lokal, dan tidak dapat digunakan. Namun, alamat ini dialokasikan dari subnetCIDR, 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 DHCP server Anda.

## Konfigurasi 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 pengelolaan Pos Luar dan intra VPC lalu lintas antara AWS Wilayah dan Pos Terdepan. Lalu lintas tautan layanan mencakup koneksi tautan layanan dari Pos Luar ke Wilayah. Tautan layanan adalah kustom VPN atau VPNs dari Pos Terdepan 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 komunikasi dari Anda VPC ke lokal Anda LAN 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 - tipe 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

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

- Titik akhir tautan layanan
- Titik akhir pendaftaran Outposts

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

Untuk mendaftarkan server, buka port jaringan berikut:

- TCP443
- UDP443
- UDP53

### Kecepatan uplink

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

Anda mungkin memerlukan uplink yang lebih cepat tergantung pada tautan antarmuka jaringan lokal Anda dan pemanfaatan tautan layanan. Untuk informasi selengkapnya, lihat [Rekomendasi bandwidth untuk tautan layanan](#).

## Antarmuka jaringan lokal menghubungkan lalu lintas

Konfigurasi port tautan antarmuka jaringan lokal pada perangkat jaringan hulu Anda sebagai port akses standar ke jaringan lokal Anda. VLAN Jika Anda memiliki lebih dari satu VLAN, konfigurasi semua port pada perangkat jaringan hulu sebagai port trunk. Konfigurasi port pada perangkat jaringan hulu Anda untuk mengharapkan beberapa MAC alamat. Setiap instance yang diluncurkan di server akan menggunakan MAC alamat. Beberapa perangkat jaringan menawarkan fitur keamanan port yang akan mematikan port yang melaporkan beberapa MAC alamat.

### Note

AWS Outposts server tidak menandai VLAN lalu lintas. Jika Anda mengonfigurasi antarmuka jaringan lokal Anda sebagai trunk, Anda harus memastikan bahwa VLAN lalu lintas tag OS Anda.

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

Contoh: Untuk mengonfigurasi VLAN penandaan 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 VLAN perangkat. Dalam contoh ini:

- Nama antarmuka antarmuka jaringan lokal adalah ens6
- VLANId adalah 59
- Nama yang ditetapkan untuk VLAN perangkat 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 subnetnya adalah 192.168.59.0/24. CIDR

```
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 perubahan VLAN penandaan tetap ada, lihat sumber daya berikut:

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

## Penetapan alamat IP server

Anda tidak memerlukan penugasan alamat IP publik untuk server 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 digunakan DHCP untuk melampirkan ke jaringan lokal. DHCP harus mengembalikan server DNS nama 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 "Konfigurasi 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 publikDNS. Ketika server mendaftar, mereka membuat terowongan aman ke titik akhir tautan layanan mereka di Wilayah. Server Outposts menggunakan TCP port 443 untuk memfasilitasi komunikasi dengan Wilayah melalui internet publik. Server Outposts tidak mendukung konektivitas pribadi melalui VPC.

# 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.

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 VPC konsol Amazon untuk berbagi subnet Outpost. Untuk informasi selengkapnya, lihat [Berbagi subnet](#) di Panduan VPC Pengguna Amazon.

## 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 AZ IDs untuk Availability Zones di akun Anda

1. Buka AWS RAM konsol di <https://console.aws.amazon.com/ram>.
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 dengan akses ke tabel rute gateway lokal bersama dapat membuat dan mengelola VPC asosiasi. 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 Outpost bersama tidak dibagikan, konsumen tidak dapat lagi melihat Outpost di konsol. AWS Outposts Mereka tidak dapat membuat subnet baru di Outpost, membuat EBS volume baru di Outpost, atau melihat detail Outpost dan jenis instance menggunakan konsol atau. AWS Outposts AWS CLI Subnet, volume, atau instance yang ada yang dibuat oleh konsumen tidak dihapus. Setiap subnet yang ada yang dibuat konsumen di Outpost masih dapat digunakan untuk meluncurkan instance baru.

Ketika tabel rute gateway lokal bersama tidak dibagikan, konsumen tidak dapat lagi membuat VPC asosiasi baru untuk itu. Setiap VPC asosiasi yang ada yang dibuat konsumen tetap terkait dengan tabel rute. Sumber daya di dalamnya VPCs dapat terus mengarahkan lalu lintas ke gateway lokal.

Untuk membatalkan pembagian sumber daya Outpost bersama yang Anda miliki, Anda harus menghapusnya dari pembagian sumber daya. Anda dapat melakukan ini menggunakan AWS RAM konsol 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 yang terkait dengan VPN lalu lintas tautan layanan Outpost mereka dari Wilayah. AWS

Tidak ada biaya tambahan untuk berbagi tabel rute gateway lokal. Untuk subnet bersama, VPC pemilik ditagih untuk sumber daya VPC -level seperti AWS Direct Connect dan VPN koneksi, NAT gateway, 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 VPC berbagi, lihat [Batasan](#) di Panduan Pengguna Amazon Virtual Private Cloud.
- Service quotas berlaku per akun individu.

# Keamanan di AWS Outposts

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

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

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

Untuk informasi selengkapnya tentang keamanan dan kepatuhan AWS Outposts, lihat FAQ [AWS Outposts server AWS Outposts](#) FAQ.

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 kredensial 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.

Untuk informasi selengkapnya tentang privasi data, lihat [Privasi Data FAQ](#). Untuk informasi tentang perlindungan data di Eropa, lihat [Model Tanggung Jawab AWS Bersama dan](#) posting GDPR blog di Blog AWS Keamanan.

### 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). 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. IAM administrator 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 IAM fitur apa saja yang tersedia untuk digunakan dengan AWS Outposts.

IAM fitur yang dapat Anda gunakan dengan AWS Outposts

IAM fitur	AWS Dukungan Outposts
<a href="#">Kebijakan berbasis identitas</a>	Ya
<a href="#">Kebijakan berbasis sumber daya</a>	Tidak
<a href="#">Tindakan kebijakan</a>	Ya
<a href="#">Sumber daya kebijakan</a>	Ya
<a href="#">kunci-kunci persyaratan kebijakan (spesifik layanan)</a>	Ya
<a href="#">ACLs</a>	Tidak
<a href="#">ABAC(tag dalam kebijakan)</a>	Ya
<a href="#">Kredensial sementara</a>	Ya
<a href="#">Izin prinsipal</a>	Ya
<a href="#">Peran layanan</a>	Tidak
<a href="#">Peran terkait layanan</a>	Ya

## Kebijakan berbasis identitas untuk Outposts AWS

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Membuat IAM kebijakan di Panduan Pengguna](#). IAM

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. 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 JSON kebijakan, lihat [referensi elemen IAM JSON kebijakan](#) di Panduan IAM Pengguna.

Contoh kebijakan berbasis identitas untuk Outposts AWS

Untuk melihat contoh kebijakan berbasis identitas AWS Outposts, lihat. [AWS Contoh kebijakan Outposts](#)

## Kebijakan berbasis sumber daya dalam Outposts AWS

Mendukung kebijakan berbasis sumber daya: Tidak

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

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

memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun IAM di](#) Panduan IAM Pengguna.

## Tindakan kebijakan untuk AWS Outposts

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

ActionElemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

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

Untuk melihat daftar tindakan AWS Outposts, lihat [Tindakan yang ditentukan oleh AWS Outposts](#) dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di AWS Outposts menggunakan awalan berikut sebelum tindakan:

```
outposts
```

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

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

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

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

## Sumber daya kebijakan untuk AWS Outposts

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, 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 API tindakan AWS Outposts mendukung banyak 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 mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang ditentukan oleh AWS Outposts](#).

## Kunci kondisi kebijakan untuk AWS Outposts

Mendukung kunci kondisi kebijakan khusus layanan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

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

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

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat [elemen IAM kebijakan: variabel dan tag](#) di Panduan IAM Pengguna.

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 IAM Pengguna.

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](#)

## ACLs di AWS Outposts

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

## ABAC dengan AWS Outposts

Mendukung ABAC (tag dalam kebijakan): Ya

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna

atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABAC membantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

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

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

Untuk informasi lebih lanjut tentang ABAC, lihat [Apa itu ABAC?](#) dalam IAM User Guide. Untuk melihat tutorial dengan langkah-langkah persiapan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) di IAM Panduan Pengguna.

## Menggunakan kredensial sementara dengan Outposts AWS

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensial sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensial sementara, lihat [Layanan AWS yang berfungsi IAM](#) di IAM Panduan Pengguna.

Anda menggunakan kredensial sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensial sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat [Beralih ke peran \(konsol\)](#) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensial sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensial sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensial 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 IAM pengguna atau peran 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. FAS permintaan 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 saat membuat FAS permintaan, lihat [Meneruskan sesi akses](#).

## Peran layanan untuk AWS Outposts

Mendukung peran layanan: Tidak

Peran layanan adalah [IAM peran](#) yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAM Administrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke Layanan AWS](#) dalam IAM Panduan Pengguna.

## 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. IAM Administrator dapat melihat, tetapi tidak 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 pada sumber daya yang mereka butuhkan, IAM

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

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat [Membuat JSON IAM kebijakan 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 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 AWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan](#) di Panduan IAM Pengguna.
- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya 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 penggunaan IAM untuk menerapkan izin, lihat [Kebijakan dan izin IAM di IAM Panduan Pengguna](#).
- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, 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 IAM JSON kebijakan: Kondisi](#) dalam Panduan IAM Pengguna.

- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa IAM kebijakan ( ) JSON dan praktik terbaik. IAM IAMAccess Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan IAM Access Analyzer](#) di IAMPanduan Pengguna.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di Anda Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat [Mengonfigurasi API akses MFA yang dilindungi](#) di IAMPanduan Pengguna.

Untuk informasi selengkapnya tentang praktik terbaik di IAM, lihat [Praktik terbaik keamanan IAM di](#) Panduan IAM Pengguna.

### 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 (IAM) peran terkait layanan. 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 ditetapkan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas lain. IAM

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 `_AWSServiceRoleForOutposts`***OutpostID***— Memungkinkan Outposts mengakses AWS sumber daya untuk konektivitas pribadi atas nama Anda. Peran terkait layanan ini memungkinkan konfigurasi konektivitas pribadi, membuat antarmuka jaringan, dan melampirkannya ke instance titik akhir tautan layanan.

`AWSServiceRoleForOutposts_`***OutpostID*** peran terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `outposts.amazonaws.com`

AWSServiceRoleForOutposts\_ **OutpostID** peran terkait layanan mencakup kebijakan berikut:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy\_ **OutpostID**

AWSOutpostsServiceRolePolicyKebijakan ini adalah kebijakan peran terkait layanan untuk mengaktifkan akses ke AWS sumber daya yang dikelola oleh AWS Outposts

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

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

AWSOutpostsPrivateConnectivityPolicy\_ **OutpostID** kebijakan memungkinkan AWS Outposts untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

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

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

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

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

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

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

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

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

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

## Membuat peran terkait layanan untuk AWS Outposts

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

## Mengedit peran terkait layanan untuk AWS Outposts

AWS Outposts tidak memungkinkan Anda untuk mengedit `AWSServiceRoleForOutposts_`*OutpostID* peran terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit deskripsi 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 Anda dapat menghapus `AWSServiceRoleForOutposts`*OutpostID* peran terkait layanan.

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

Untuk menghapus AWS Outposts sumber daya yang digunakan oleh `AWSServiceRoleForOutposts_`***OutpostID***

Hubungi AWS Enterprise Support untuk menghapus Outpost Anda.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) di IAMPanduan Pengguna.

### Wilayah yang Didukung untuk AWS Outposts peran terkait layanan

AWS Outposts mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. [Untuk informasi lebih lanjut, lihat FAQs untuk Outposts rack dan 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 API operasi baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat [kebijakan AWS terkelola](#) di Panduan IAM Pengguna.

### AWS kebijakan terkelola: `AWSOutpostsServiceRolePolicy`

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: AWSOutpostsPrivateConnectivityPolicy

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: AWSOutpostsAuthorizeServerPolicy

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
<a href="#">AWSOutpostsAuthorizeServerPolicy</a> – 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 API panggilan yang AWS dipublikasikan untuk mengakses AWS Outposts melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju yang sempurna (PFS) seperti (Ephemeral Diffie-Hellman) atau DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan IAM prinsipal. 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 EBS volume yang berjalan di Pos Luar Anda, lihat [Keamanan Infrastruktur di Amazon](#). EC2

VPCFlow Logs berfungsi dengan cara yang sama seperti di AWS Region. 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 pesawat kontrol seperti menanggapi API panggilan, memantau Outpost, dan memperbarui Outpost. Untuk mendapatkan manfaat dari ketahanan yang disediakan oleh Availability Zones, Anda dapat menerapkan aplikasi di beberapa Outpost, masing-masing dilampirkan ke Availability Zone yang berbeda. Ini memungkinkan Anda membangun ketahanan aplikasi tambahan dan menghindari ketergantungan pada satu Availability Zone. Untuk informasi selengkapnya tentang Wilayah dan Availability Zone, lihat [Infrastruktur AWS Global](#).

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

## Validasi kepatuhan untuk AWS Outposts

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

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#) .

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

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

 Note

Tidak semua Layanan AWS HIPAA memenuhi syarat. Untuk informasi selengkapnya, lihat [Referensi Layanan yang HIPAA Memenuhi Syarat](#).

- [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 yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCIDSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.

- [AWS Audit Manager](#) Ini 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 API tindakan untuk AWS Outposts. Mereka juga berisi informasi untuk panggilan ke API tindakan dari layanan di Outpost, seperti Amazon EC2 dan AmazonEBS. Untuk informasi selengkapnya, lihat [Log API panggilan menggunakan CloudTrail](#).

### VPCLog Aliran

Gunakan VPC Flow Logs untuk menangkap informasi rinci tentang lalu lintas yang menuju dan dari Outpost Anda dan di dalam Outpost Anda. Untuk informasi selengkapnya, lihat [Log VPC Aliran](#) di Panduan VPC Pengguna Amazon.

### 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 VPC Lalu Lintas Amazon](#).

### 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 dari 1, 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 NAT aturan, atau masalah koneksi internet. Untuk `ConnectedStatus` masalah, sebaiknya verifikasi konektivitas ke AWS Wilayah dari dalam jaringan lokal Anda, dan hubungi AWS Support jika masalah berlanjut.

Untuk informasi selengkapnya tentang membuat CloudWatch alarm, lihat [Menggunakan CloudWatch Alarm Amazon](#) di Panduan CloudWatch Pengguna Amazon. Untuk informasi selengkapnya CloudWatch, lihat [Panduan CloudWatch Pengguna Amazon](#).

### Daftar Isi

- [Metrik](#)
- [Dimensi metrik](#)
- [Lihat CloudWatch metrik untuk server rak Anda](#)

## 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 instans 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 instans 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 (RDSAmazon) 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 EBS volume.
VirtualInterfaceId	ID gateway lokal atau tautan layanan Antarmuka Virtual (VIF).
VirtualInterfaceGroupId	ID grup antarmuka virtual untuk gateway lokal Virtual Interface (VIF).

## Lihat CloudWatch metrik untuk server rak Anda

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. Di panel navigasi, 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-statistics](#) perintah 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 AWS Outposts API panggilan menggunakan AWS CloudTrail

AWS Outposts terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan. CloudTrail menangkap API panggilan untuk AWS Outposts sebagai acara. Panggilan yang diambil termasuk panggilan dari AWS Outposts konsol dan panggilan kode ke AWS Outposts API operasi. 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 siapa 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 Pusat IAM Identitas.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- 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 [CloudTrailDanau](#).

#### 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 Menyimpan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri SQL berbasis pada acara Anda. CloudTrail [Lake mengonversi peristiwa yang ada dalam JSON format 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 pesawat kontrol AWS Outposts yang dicatat oleh Outposts, CloudTrail lihat Referensi AWS Outposts.AWS API](#)

## AWS Outposts contoh acara

Contoh berikut menunjukkan CloudTrail peristiwa yang menunjukkan SetSiteAddress operasi.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAIOSFODNN7EXAMPLE:jdoh",
    "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoh",
    "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 . 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 Support 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. 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 DNS berbasis 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 Support 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.

EC2Instans Amazon, LNI jaringan, 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 ECS pekerja Amazon terus berjalan secara lokal. Namun, API ketersediaan akan terdegradasi. Misalnya, run, start, stop, dan terminate APIs mungkin tidak berfungsi. Metrik dan log instans akan terus di-cache secara lokal selama beberapa jam, dan akan didorong ke AWS Wilayah saat konektivitas kembali. Namun, pemutusan lebih dari beberapa jam 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 alat AWSSupport-S etupIPMonitoring From VPC. Alat ini adalah AWS Systems Manager dokumen (SSMdokumen) yang membuat Instans EC2 Monitor Amazon di subnet yang ditentukan oleh Anda dan memantau alamat IP target. Dokumen menjalankan tes diagnostik ping, MTR, TCP trace-route dan trace-path dan menyimpan hasilnya di Amazon CloudWatch Logs yang dapat divisualisasikan di CloudWatch dasbor (misalnya latensi, kehilangan paket). Untuk pemantauan Outposts, Instans Monitor harus berada di satu subnet dari AWS Wilayah induk dan dikonfigurasi untuk memantau satu atau lebih instance Outpost Anda menggunakan IP pribadinya - ini akan memberikan grafik kehilangan paket dan latensi antara dan Wilayah induk. AWS Outposts AWS
- AWS Blog [Menyebarkan CloudWatch dasbor Amazon otomatis untuk AWS Outposts digunakan AWS CDK](#) menjelaskan langkah-langkah yang terlibat dalam menerapkan dasbor otomatis.
- Jika Anda memiliki pertanyaan atau memerlukan informasi selengkapnya, lihat [Membuat kasus AWS dukungan](#) di Panduan Pengguna Support.



## Opsi 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 Support Tengah](#).
2. Pilih Buat kasus.
3. Pilih Akun dan penagihan.
4. Untuk Layanan, pilih Penagihan.
5. Untuk Kategori, pilih Pertanyaan Penagihan Lainnya.
6. Untuk Keparahan, pilih Pertanyaan penting.
7. Pilih Langkah selanjutnya: Informasi tambahan.
8. Pada halaman Informasi tambahan, untuk Subjek, masukkan permintaan Anda untuk memperbarui seperti **Renew my Outpost subscription**.
9. Untuk Deskripsi, masukkan salah satu opsi pembayaran berikut:
  - Tidak ada di muka
  - Sebagian di muka
  - Semua dimuka

Untuk harga, lihat [harga AWS Outposts server](#). Anda juga dapat meminta penawaran harga.

10. Pilih Langkah selanjutnya: Selesaikan sekarang atau hubungi kami.
11. Pada halaman Hubungi kami, pilih bahasa pilihan Anda.

12. Pilih metode kontak pilihan Anda.
13. Tinjau detail kasus Anda dan kemudian pilih Kirim. Nomor ID kasus dan ringkasan muncul.

AWS Customer Support akan memulai proses perpanjangan langganan. Langganan baru Anda akan dimulai sehari setelah langganan Anda saat ini berakhir.

Jika Anda tidak menunjukkan bahwa Anda ingin memperbarui langganan atau mengembalikan server 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 Support Tengah](#).
2. Pilih Buat kasus.
3. Pilih Akun dan penagihan.
4. Untuk Layanan, pilih Penagihan.
5. Untuk Kategori, pilih Pertanyaan Penagihan Lainnya.
6. Untuk Keperahan, 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. NOTMatikan 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, yang sebelumnya disebut sebagai batas, untuk masing-masing Layanan AWS. Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan 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 dengan AWS Outposts.

Sumber daya	Default	Dapat Disesuaikan	Comments
Outpost	100	<a href="#">Ya</a>	<p>Sebuah situs Outpost adalah pelanggan dikelola bangunan fisik di mana Anda kekuasaan dan melampirkan peralatan Outpost Anda ke jaringan.</p> <p>Anda dapat memiliki 100 situs Outposts di setiap Wilayah AWS akun Anda.</p>
Outposts per situs	10	<a href="#">Ya</a>	<p>AWS Outposts termasuk perangkat keras dan sumber daya virtual, yang dikenal sebagai Outposts. Kuota ini membatasi sumber daya virtual Outpost Anda.</p> <p>Anda dapat memiliki 10 Outposts di setiap situs Outpost.</p>

## 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 Amazon VPC untuk antarmuka jaringan.

Tabel berikut menjelaskan pembaruan dokumentasi untuk server Outposts.

Perubahan	Deskripsi	Tanggal
<a href="#">Manajemen kapasitas</a>	Anda dapat mengubah konfigurasi kapasitas default untuk pesanan Outposts baru Anda.	April 16, 2024
<a href="#">End-of-term Opsi E untuk AWS Outposts server</a>	Di akhir AWS Outposts jangka waktu Anda, Anda dapat memperbarui, mengakhiri, atau mengonversi langganan Anda.	1 Agustus 2023
<a href="#">Panduan AWS Outposts Pengguna yang Dibuat untuk server Outposts</a>	AWS Outposts Panduan Pengguna masuk ke panduan terpisah untuk rak dan server.	14 September 2022
<a href="#">Grup penempatan di AWS Outposts</a>	Grup penempatan yang menggunakan strategi spread dapat mendistribusikan instans di seluruh host.	30 Juni 2022
<a href="#">Tuan Rumah Khusus di AWS Outposts</a>	Anda sekarang dapat menggunakan Host Khusus di Outposts.	31 Mei 2022
<a href="#">Memperkenalkan server Outposts</a>	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.