Praktik terbaik untuk membangun arsitektur cloud hybrid dengan Layanan AWS

AWS Panduan Preskriptif

AWS Panduan Preskriptif: Praktik terbaik untuk membangun arsitektur cloud hybrid dengan Layanan AWS

Table of Contents

Pengantar 1
Gambaran umum 3
  Lokakarya cloud hybrid 3
  PoCs 3
  Pilar 4
Prasyarat dan batasan 5
  Prasyarat 5
    AWS Outposts 5
    AWS Local Zones 5
  Batasan 6
    AWS Outposts 6
    AWS Local Zones 6
Proses adopsi cloud hybrid 8
  Jaringan di tepi 8
    Arsitektur VPC 8
    Lalu lintas Edge ke Region 9
    Edge ke lalu lintas lokal 12
  Keamanan di tepi 16
    Perlindungan data 16
    Manajemen identitas dan akses 20
    Keamanan infrastruktur 21
    Akses internet 23
    Tata kelola infrastruktur 25
  Ketahanan di tepi 27
    Pertimbangan infrastruktur 27
    Pertimbangan jaringan 29
    Mendistribusikan Instance di Outposts dan Local Zones 33
    Amazon RDS di Multi-AZ AWS Outposts 34
    Mekanisme failover 35
  Perencanaan kapasitas di tepi 39
    Perencanaan kapasitas di Outposts 40
    Perencanaan Kapasitas untuk Local Zones 40
  Manajemen infrastruktur tepi 41
    Menyebarkan layanan di tepi 41

CLI dan SDK khusus Outpost 43
Sumber daya 45
AWS referensi 45
AWS posting blog 45
Kontributor 46
Mengotorisasi 46
Meninjau 46
Penulisan teknis 46
Riwayat dokumen 47
..... xlviii

Praktik terbaik untuk membangun arsitektur cloud hybrid dengan Layanan AWS

Amazon Web Services (kontributor)

Juni 2025 (sejarah dokumen)

Banyak bisnis dan organisasi telah mengadopsi komputasi awan sebagai aspek kunci dari strategi teknologi mereka. Mereka biasanya memigrasikan beban kerja mereka ke AWS Cloud untuk meningkatkan kelincahan, penghematan biaya, kinerja, ketersediaan, ketahanan, dan skalabilitas. Sebagian besar aplikasi dapat dengan mudah dimigrasi, tetapi beberapa aplikasi harus tetap berada di lokasi untuk memanfaatkan latensi rendah dan pemrosesan data lokal dari lingkungan lokal, untuk menghindari biaya transfer data yang tinggi, atau untuk kepatuhan terhadap peraturan. Selain itu, sebagian aplikasi mungkin perlu dirancang ulang atau dimodernisasi sebelum dapat dipindahkan ke cloud. Hal ini menyebabkan banyak organisasi mencari arsitektur cloud hybrid untuk mengintegrasikan operasi lokal dan cloud mereka untuk mendukung spektrum kasus penggunaan yang luas. Pendekatan hybrid ini dapat memberikan manfaat dari komputasi lokal dan berbasis cloud, dan dapat sangat berguna untuk skenario komputasi tepi.

Saat Anda membangun cloud hybrid AWS, kami sarankan Anda menentukan strategi cloud hybrid dan strategi teknis Anda:

- Strategi cloud hybrid menyediakan panduan yang mengatur konsumsi cloud dan sumber daya lokal untuk mendukung tujuan bisnis Anda. Panduan ini menjelaskan kasus penggunaan umum untuk membangun cloud hybrid, seperti mendukung migrasi berkelanjutan ke cloud, memastikan kelangsungan bisnis selama bencana, memperluas infrastruktur cloud ke lingkungan lokal untuk mendukung aplikasi latensi rendah, atau memperluas kehadiran internasional Anda. AWS Mendefinisikan strategi ini membantu Anda mengidentifikasi dan menentukan tujuan bisnis Anda untuk membangun cloud hybrid, dan memberikan panduan untuk penempatan beban kerja di cloud hybrid.
- Strategi teknis untuk cloud hybrid mengidentifikasi prinsip panduan arsitektur cloud hybrid dan mendefinisikan kerangka implementasi. Panduan ini menguraikan persyaratan umum untuk arsitektur cloud hybrid yang diterapkan dan dikelola secara konsisten untuk membantu Anda menentukan prinsip implementasi cloud hybrid yang direncanakan. Persyaratan ini mencakup antarmuka standar untuk penyediaan dan pengelolaan sumber daya di seluruh infrastruktur cloud Anda.

Panduan ini menjelaskan kerangka kerja operasi dan manajemen untuk membantu arsitek dan operator solusi mengidentifikasi blok bangunan, praktik terbaik, dan cloud AWS hybrid dan layanan In-region untuk mengimplementasikan cloud hybrid. AWS

Banyak organisasi telah menggunakan solusi yang dijelaskan dalam panduan ini untuk berhasil menerapkan lingkungan cloud hybrid yang memanfaatkan skala, kelincahan, inovasi, dan jejak global yang disediakan oleh perusahaan. AWS Cloud(Lihat studi kasus.) AWS Layanan cloud hybrid memberikan AWS pengalaman yang konsisten dari cloud ke tempat, dan di tepi. Layanan seperti AWS Outposts dan AWS Local Zones tempat komputasi, penyimpanan, database, dan lainnya memilih Layanan AWS dekat dengan populasi besar dan pusat industri ketika Anda memerlukan latensi rendah antara perangkat pengguna akhir atau pusat data lokal dan server beban kerja yang ada.

Dalam panduan ini:

- Ikhtisar
- Prasyarat dan batasan
- Proses adopsi cloud hybrid:
  - Jaringan di tepi
  - Keamanan di tepi
  - Ketahanan di tepi
  - Perencanaan kapasitas di tepi
  - Manajemen infrastruktur tepi
- Sumber Daya
- Kontributor
- Sejarah dokumen

Gambaran umum

Panduan ini mengklasifikasikan AWS rekomendasi untuk cloud hybrid menjadi lima pilar: jaringan, keamanan, ketahanan, perencanaan kapasitas, dan manajemen infrastruktur. Ini memberikan panduan untuk membantu Anda meningkatkan kesiapan Anda dan mengembangkan strategi migrasi dengan menggunakan layanan edge AWS hybrid seperti AWS Outposts atau AWS Local Zones. Kami sangat menyarankan agar Anda bekerja dengan Akun AWS tim Anda atau AWS Partner untuk memastikan bahwa spesialis cloud AWS hybrid tersedia untuk membantu Anda saat Anda mengikuti panduan ini dan mengembangkan proses Anda.

> **Note**
>
> Meskipun AWS Outposts dan Local Zones mengatasi masalah serupa, kami menyarankan Anda meninjau kasus penggunaan serta layanan dan fitur yang tersedia untuk memutuskan penawaran mana yang paling sesuai dengan kebutuhan Anda. Untuk informasi lebih lanjut, lihat posting AWS blog AWS Local Zones dan AWS Outposts, memilih teknologi yang tepat untuk beban kerja tepi Anda.

Lokakarya cloud hybrid

Dengan bantuan ahli subjek cloud AWS hybrid (SME), Anda dapat menjalankan lokakarya cloud hybrid untuk menilai tingkat kematangan perusahaan Anda sehubungan dengan lima pilar yang dibahas dalam panduan ini.

Lokakarya ini berfokus pada area internal dalam organisasi Anda, seperti jaringan, keamanan, kepatuhan DevOps, virtualisasi, dan unit bisnis. Ini membantu Anda merancang arsitektur cloud hybrid yang memenuhi persyaratan organisasi Anda dan menentukan detail implementasi, mengikuti langkah-langkah di bagian proses adopsi cloud Hybrid dari panduan ini.

PoCs

Jika Anda memiliki persyaratan khusus, Anda dapat menggunakan proofs of concept (PoCs) untuk memvalidasi fungsionalitas di Local Zones dan AWS Outposts terhadap persyaratan tersebut.

AWS digunakan PoCs untuk membantu Anda menguji beban kerja yang ingin Anda pindahkan ke Outpost atau Local Zone, untuk menentukan apakah beban kerja akan berfungsi di bawah arsitektur

pengujian. Untuk mengakses Zona Lokal untuk pengujian, ikuti petunjuk dalam dokumentasi Local Zones. Untuk menguji beban kerja Anda AWS Outposts, bekerja dengan Akun AWS tim Anda atau AWS Partner untuk mengakses laboratorium AWS Outposts uji dan menerima bimbingan dari arsitek AWS solusi. Dalam semua skenario, pengembangan PoC mengharuskan Anda untuk menghasilkan dokumen uji yang berisi:

- Layanan AWS untuk digunakan, seperti Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), Amazon Virtual Private Cloud (Amazon VPC), dan Amazon Elastic Kubernetes Service (Amazon EKS)
- Ukuran dan jumlah instans untuk dikonsumsi (misalnya, `m5.xlarge` atau`c5.2xlarge`)
- Diagram arsitektur uji
- Uji kriteria keberhasilan
- Detail dan tujuan dari setiap tes yang akan dijalankan

Pilar

Bagian selanjutnya mencakup prasyarat dan batasan untuk menggunakan arsitektur yang dibahas dalam panduan ini. Bagian setelah itu mencakup detail setiap pilar sehingga dokumen rekomendasi yang Anda buat selama lokakarya cloud hybrid dapat mencerminkan detail desain yang diperlukan untuk implementasi.

- Jaringan di tepi
- Keamanan di tepi
- Ketahanan di tepi
- Perencanaan kapasitas di tepi
- Manajemen infrastruktur tepi

Prasyarat dan batasan

Sebelum Anda mengikuti panduan ini, bekerjalah dengan Akun AWS tim Anda atau AWS Partner tinjau prasyarat dan batasan untuk menerapkan arsitektur tepi dengan dan Local Zones. AWS Outposts

Prasyarat

AWS Outposts

- Pusat data Anda yang ada harus memenuhi AWS Outposts persyaratan untuk fasilitas, jaringan, dan daya. AWS Outposts dirancang untuk beroperasi di lingkungan pusat data yang memiliki input daya redundan 5-15 kVA, 145,8 kali kVA aliran udara kaki kubik per menit (CFM), dan suhu sekitar antara 41° F (5° C) dan 95° F (35° C), di antara persyaratan lainnya.
- Konfirmasikan bahwa AWS Outposts layanan tersedia di negara Anda dengan berkonsultasi dengan AWS Outposts rak FAQs. Lihat pertanyaannya: Di negara dan wilayah mana rak Outposts tersedia?
- Jika organisasi Anda memerlukan empat AWS Outposts rak atau lebih, pusat data Anda harus memenuhi persyaratan rak Agregasi, Inti, Edge (ACE).
- Internet atau AWS Direct Connect tautan minimal 500 Mbps (1 Gbps lebih baik) harus disediakan dan dipertahankan untuk terhubung AWS Outposts ke Wilayah AWS, dengan konektivitas cadangan yang sesuai jika kasus penggunaan Anda memerlukannya. Latensi waktu pulang-pergi dari AWS Outposts ke Wilayah harus maksimal 175 milidetik.
- Anda harus memiliki kontrak aktif untuk AWS Enterprise Support atau rencana Operasi AWS Terpadu.

AWS Local Zones

- Zona AWS Lokal harus tersedia dekat dengan pusat data atau pengguna Anda. Lihat AWS Local Zones lokasi.
- Konfirmasikan bahwa Anda memiliki konektivitas jaringan dari infrastruktur lokal ke Zona Lokal:
  - Opsi 1: Direct Connect Tautan dari pusat data Anda ke Direct Connect titik kehadiran (PoP) yang paling dekat dengan Zona Lokal. Untuk informasi selengkapnya, lihat Direct Connect di dokumentasi Local Zones.

- Opsi 2: Tautan internet selain alat jaringan pribadi virtual (VPN) lokal dan lisensi yang diperlukan untuk meluncurkan alat VPN berbasis perangkat lunak di Amazon EC2 di Zona Lokal. Untuk informasi selengkapnya, lihat Koneksi VPN di dokumentasi Local Zones.

Untuk opsi konektivitas tambahan, lihat dokumentasi Local Zones.

Batasan

AWS Outposts

- Amazon Relational Database Service (Amazon RDS) AWS Outposts pada penerapan multi-AZ memerlukan kumpulan alamat IP (CoIP) milik pelanggan. Untuk informasi selengkapnya, lihat Alamat IP milik pelanggan untuk Amazon RDS. AWS Outposts
- Multi-AZ aktif AWS Outposts tersedia untuk semua versi MySQL dan PostgreSQL yang didukung di Amazon RDS aktif. AWS Outposts Untuk informasi selengkapnya, lihat Dukungan Amazon RDS on AWS Outposts untuk fitur Amazon RDS. Amazon RDS AWS Outposts mendukung SQL Server, Amazon RDS for MySQL, dan Amazon RDS for PostgreSQL database.
- AWS Outposts tidak dirancang untuk beroperasi ketika terputus dari file Wilayah AWS. Untuk informasi lebih lanjut, lihat bagian Berpikir dalam hal mode kegagalan di AWS whitepaper Desain Ketersediaan AWS Outposts Tinggi dan Pertimbangan Arsitektur.
- Amazon Simple Storage Service (Amazon S3) AWS Outposts on memiliki beberapa keterbatasan. Ini dibahas dalam Bagaimana Amazon S3 di Outposts berbeda dari Amazon S3? bagian dari Amazon S3 pada Panduan Pengguna Outposts.
- Application Load Balancer aktif AWS Outposts tidak mendukung sesi TLS (mTL) atau sticky.
- Rak ACE tidak sepenuhnya tertutup dan tidak termasuk pintu depan atau belakang.
- Alat kapasitas instans hanya berlaku untuk pesanan baru.

AWS Local Zones

- Local Zones tidak memiliki AWS Site-to-Site VPN titik akhir. Sebagai gantinya, gunakan VPN berbasis perangkat lunak di Amazon EC2.
- Local Zones tidak mendukung AWS Transit Gateway. Sebagai gantinya, sambungkan ke Local Zone dengan menggunakan Direct Connect Private Virtual Interface (VIF).

- Tidak semua Local Zones mendukung layanan seperti Amazon RDS, Amazon FSx, Amazon EMR, atau ElastiCache Amazon, atau gateway NAT. Untuk informasi selengkapnya, lihat AWS Local Zones fitur.
- Application Load Balancers di Local Zones tidak mendukung MTL atau sticky session.

Proses adopsi cloud hybrid

Bagian berikut membahas arsitektur dan detail desain untuk setiap pilar cloud AWS hybrid:

- Jaringan di tepi
- Keamanan di tepi
- Ketahanan di tepi
- Perencanaan kapasitas di tepi
- Manajemen infrastruktur tepi

Jaringan di tepi

Saat Anda merancang solusi yang menggunakan infrastruktur AWS tepi, seperti AWS Outposts atau Local Zones, Anda harus mempertimbangkan desain jaringan dengan cermat. Jaringan membentuk fondasi konektivitas untuk mencapai beban kerja yang digunakan di lokasi tepi ini, dan sangat penting untuk memastikan latensi rendah. Bagian ini menguraikan berbagai aspek konektivitas edge hybrid.

Arsitektur VPC

Virtual Private Cloud (VPC) mencakup semua Availability Zone di dalamnya. Wilayah AWS Anda dapat memperluas VPC apa pun di Region ke Outposts atau Local Zones dengan mulus AWS menggunakan konsol AWS Command Line Interface atau () untuk menambahkan subnet Outpost atau AWS CLI Local Zone. Contoh berikut menunjukkan cara membuat subnet di AWS Outposts dan Local Zones dengan menggunakan: AWS CLI

- AWS Outposts: Untuk menambahkan subnet Outpost ke VPC, tentukan Amazon Resource Name (ARN) dari Outpost.

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.0.0/24 \
--outpost-arn arn:aws:outposts:us-west-2:11111111111:outpost/op-0e32example1 \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

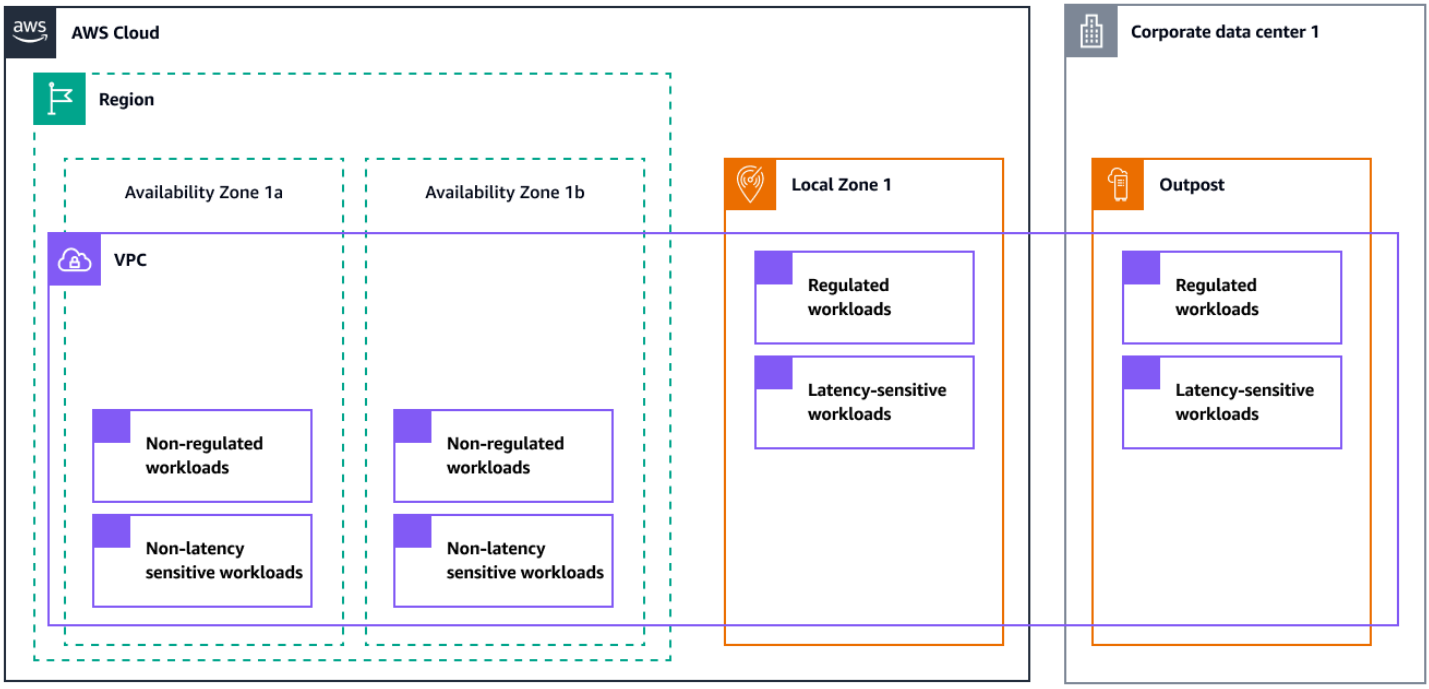
  Lihat informasi yang lebih lengkap dalam dokumentasi AWS Outposts.

- Local Zones: Untuk menambahkan subnet Zona Lokal ke VPC, ikuti prosedur yang sama yang Anda gunakan dengan Availability Zones, tetapi tentukan ID Zona Lokal `<local-zone-name>` (dalam contoh berikut).

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.1.0/24 \
--availability-zone <local-zone-name> \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  Untuk informasi selengkapnya, lihat dokumentasi Local Zones.

Diagram berikut menunjukkan AWS arsitektur yang mencakup subnet Outpost dan Local Zone.

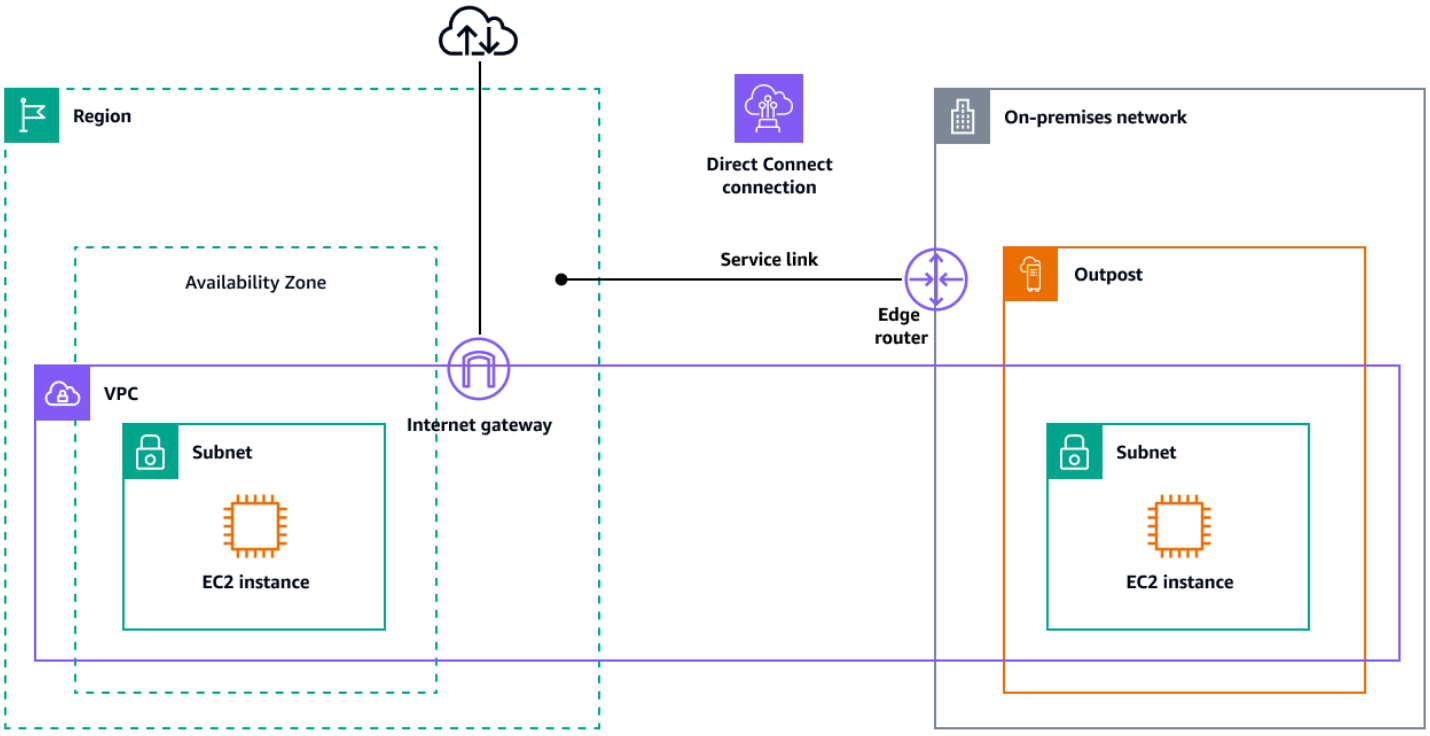


Lalu lintas Edge ke Region

Saat Anda mendesain arsitektur hybrid dengan menggunakan layanan seperti Local Zones dan AWS Outposts, pertimbangkan arus kontrol dan arus lalu lintas data antara infrastruktur edge dan Wilayah AWS. Bergantung pada jenis infrastruktur edge, tanggung jawab Anda mungkin berbeda: Beberapa infrastruktur mengharuskan Anda untuk mengelola koneksi ke Wilayah induk, sedangkan yang lain menangani ini melalui infrastruktur AWS global. Bagian ini mengeksplorasi implikasi konektivitas bidang kontrol dan bidang data untuk Local Zones dan. AWS Outposts

AWS Outposts pesawat kontrol

AWS Outposts menyediakan konstruksi jaringan yang disebut link layanan. Tautan layanan adalah koneksi yang diperlukan antara AWS Outposts dan Wilayah yang dipilih Wilayah AWS atau induk (juga disebut sebagai Wilayah asal). Hal ini memungkinkan pengelolaan Outpost dan pertukaran lalu lintas antara Outpost dan. Wilayah AWS Tautan layanan menggunakan seperangkat koneksi VPN terenkripsi untuk berkomunikasi dengan Wilayah asal. Anda harus menyediakan konektivitas antara AWS Outposts dan Wilayah AWS baik melalui tautan internet atau antarmuka virtual Direct Connect publik (VIF publik), atau melalui antarmuka virtual Direct Connect pribadi (VIF pribadi). Untuk pengalaman dan ketahanan yang optimal, AWS merekomendasikan agar Anda menggunakan konektivitas redundan minimal 500 Mbps (1 Gbps lebih baik) untuk koneksi tautan layanan ke. Wilayah AWS Koneksi tautan layanan minimum 500 Mbps memungkinkan Anda meluncurkan instans Amazon EC2, melampirkan volume Amazon EBS, dan akses Layanan AWS seperti metrik Amazon EKS, Amazon EMR, dan Amazon. CloudWatch Jaringan harus mendukung unit transmisi maksimum (MTU) 1.500 byte antara Outpost dan titik akhir tautan layanan di induk. Wilayah AWSUntuk informasi selengkapnya, lihat AWS Outposts konektivitas ke Wilayah AWS dalam dokumentasi Outposts.



Untuk informasi tentang membuat arsitektur tangguh untuk tautan layanan yang menggunakan Direct Connect dan internet publik, lihat bagian Konektivitas jangkar di AWS whitepaper Pertimbangan Desain dan Arsitektur Ketersediaan AWS Outposts Tinggi.

AWS Outposts pesawat data

Bidang data antara AWS Outposts dan Wilayah AWS didukung oleh arsitektur tautan layanan yang sama yang digunakan oleh bidang kontrol. Bandwidth dari tautan layanan bidang data antara AWS Outposts dan Wilayah AWS harus berkorelasi dengan jumlah data yang harus dipertukarkan: Semakin besar ketergantungan data, semakin besar bandwidth tautan yang seharusnya.

Persyaratan bandwidth bervariasi tergantung pada karakteristik berikut:

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

Lalu lintas antara instans EC2 AWS Outposts dan instans EC2 di Wilayah AWS memiliki MTU 1.300 byte. Kami menyarankan Anda mendiskusikan persyaratan ini dengan spesialis cloud AWS hybrid sebelum Anda mengusulkan arsitektur yang memiliki ketergantungan bersama antara Wilayah dan. AWS Outposts

Pesawat data Local Zones

Bidang data antara Local Zones dan Local Zones didukung melalui infrastruktur AWS global. Wilayah AWS Pesawat data diperpanjang melalui VPC dari Wilayah AWS ke Zona Lokal. Local Zones juga menyediakan bandwidth tinggi, koneksi aman ke Wilayah AWS, dan memungkinkan Anda terhubung dengan mulus ke berbagai layanan Regional melalui API dan set alat yang sama.

Tabel berikut menunjukkan opsi koneksi dan MTU terkait.

Dari	Untuk	MTU
Amazon EC2 di Wilayah	Amazon EC2 di Local Zones	1.300 byte
Direct Connect	Zona Lokal	1.468 byte
gateway internet	Zona Lokal	1.500 byte
Amazon EC2 di Local Zones	Amazon EC2 di Local Zones	9.001 byte

Local Zones menggunakan infrastruktur AWS global untuk terhubung Wilayah AWS. Infrastruktur dikelola sepenuhnya oleh AWS, jadi Anda tidak perlu mengatur konektivitas ini. Kami menyarankan Anda mendiskusikan persyaratan dan pertimbangan Local Zones Anda dengan spesialis cloud AWS hybrid sebelum Anda merancang arsitektur apa pun yang memiliki ketergantungan bersama antara Region dan Local Zones.

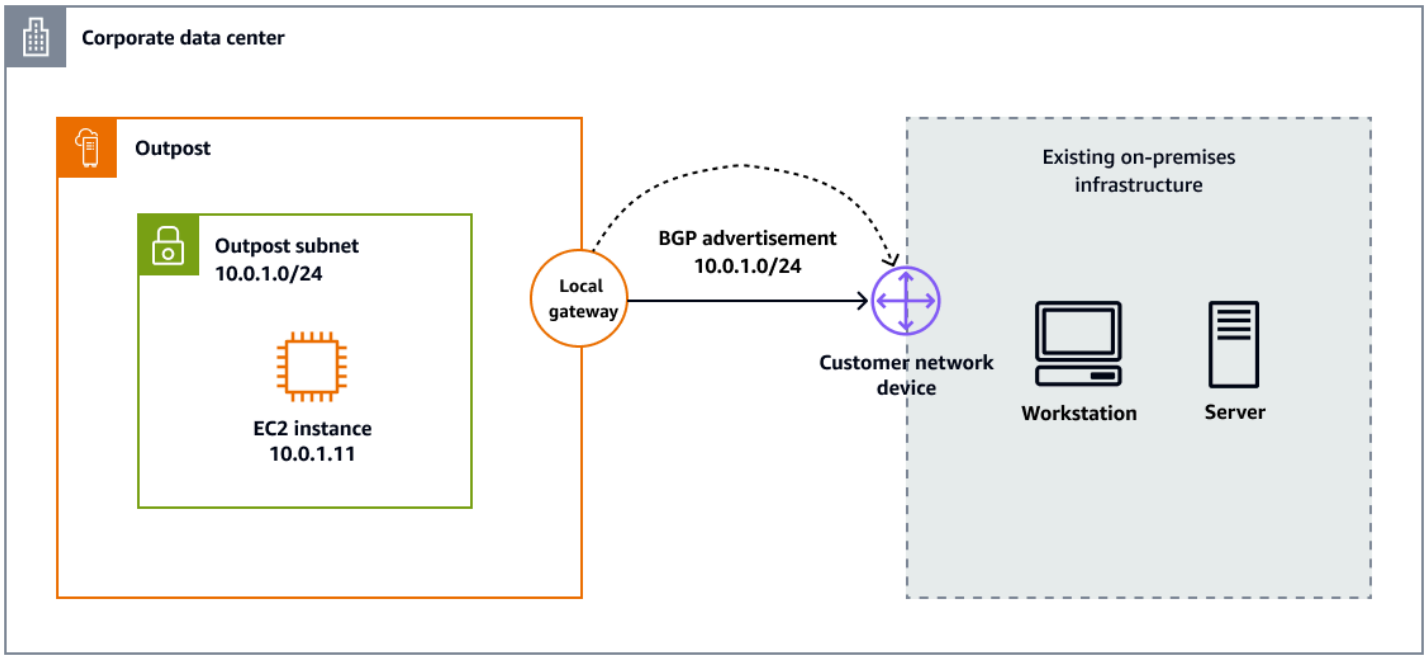
Edge ke lalu lintas lokal

AWS Layanan cloud hybrid dirancang untuk mengatasi kasus penggunaan yang memerlukan latensi rendah, pemrosesan data lokal, atau kepatuhan residensi data. Arsitektur jaringan untuk mengakses data ini penting, dan itu tergantung pada apakah beban kerja Anda berjalan di AWS Outposts atau Local Zones. Konektivitas lokal juga membutuhkan ruang lingkup yang terdefinisi dengan baik, seperti yang dibahas di bagian berikut.

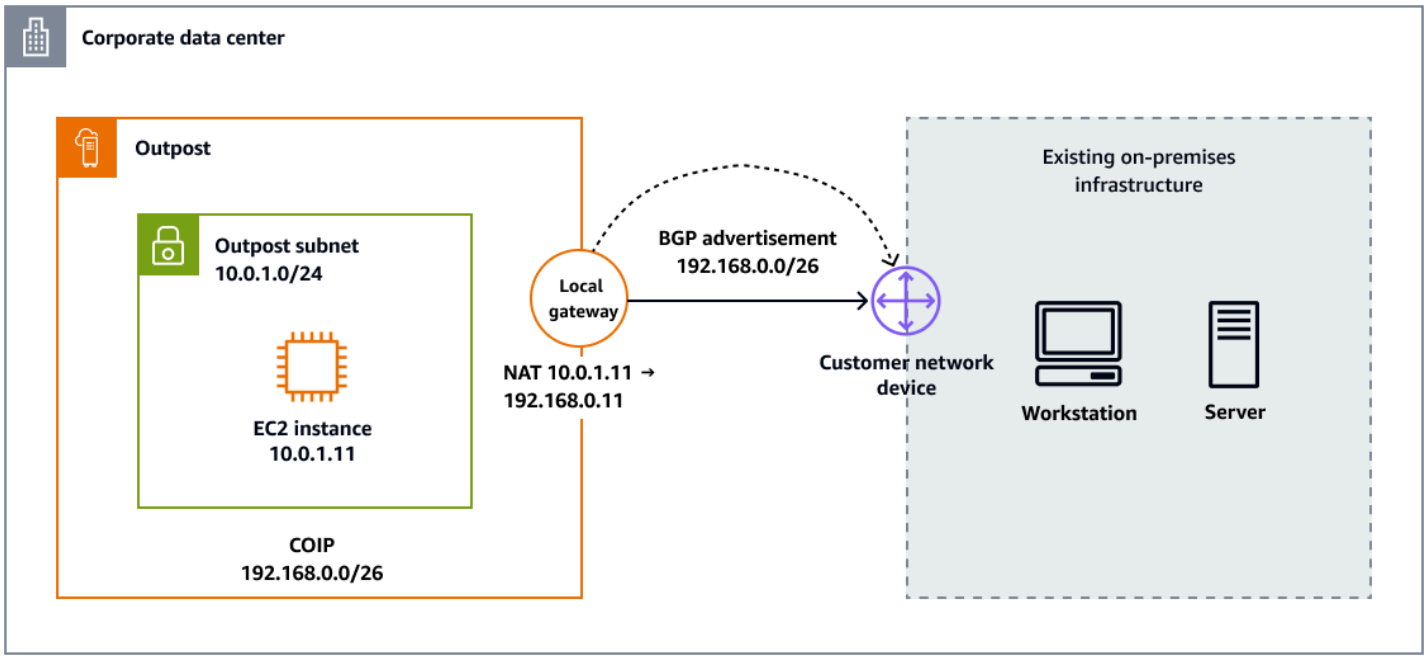
AWS Outposts gerbang lokal

Lokal gateway (LGW) adalah komponen inti dari arsitektur. AWS Outposts Gateway lokal memungkinkan konektivitas antara subnet Outpost Anda dan jaringan lokal Anda. Peran utama LGW adalah menyediakan konektivitas dari Outpost ke jaringan lokal lokal Anda. Ini juga menyediakan konektivitas ke internet melalui jaringan lokal Anda melalui perutean VPC langsung atau alamat IP milik pelanggan.

- Perutean VPC langsung menggunakan alamat IP pribadi instans di VPC Anda untuk memfasilitasi komunikasi dengan jaringan lokal Anda. Alamat ini diiklankan ke jaringan lokal Anda dengan Border Gateway Protocol (BGP). Iklan ke BGP hanya untuk alamat IP pribadi yang termasuk dalam subnet di rak Outpost Anda. Jenis routing ini adalah mode default untuk AWS Outposts. Dalam mode ini, gateway lokal tidak menjalankan NAT untuk instance, dan Anda tidak perlu menetapkan alamat IP Elastis ke instans EC2 Anda. Diagram berikut menunjukkan gateway AWS Outposts lokal yang menggunakan routing VPC langsung.



- Dengan alamat IP milik pelanggan, Anda dapat memberikan rentang alamat, yang dikenal sebagai kumpulan alamat IP (CoIP) milik pelanggan, yang mendukung rentang CIDR yang tumpang tindih dan topologi jaringan lainnya. Ketika Anda memilih CoIP, Anda harus membuat kumpulan alamat, menetapkannya ke tabel rute gateway lokal, dan mengiklankan alamat ini kembali ke jaringan Anda melalui BGP. Alamat CoIP menyediakan konektivitas lokal atau eksternal ke sumber daya di jaringan lokal Anda. Anda dapat menetapkan alamat IP ini ke sumber daya di Outpost Anda, seperti instans EC2, dengan mengalokasikan alamat IP Elastis baru dari CoIP, dan kemudian menetapkannya ke sumber daya Anda. Diagram berikut menunjukkan gateway AWS Outposts lokal yang menggunakan mode CoIP.



Konektivitas lokal dari AWS Outposts ke jaringan lokal memerlukan beberapa konfigurasi parameter, seperti mengaktifkan protokol routing BGP dan awalan iklan antara rekan-rekan BGP. MTU yang dapat didukung antara Outpost Anda dan gateway lokal adalah 1.500 byte. Untuk informasi lebih lanjut, hubungi spesialis cloud AWS hybrid atau tinjau AWS Outposts dokumentasinya.

Local Zones dan Internet

Industri yang membutuhkan latensi rendah atau residensi data lokal (contohnya termasuk game, streaming langsung, layanan keuangan, dan pemerintah) dapat menggunakan Local Zones untuk menyebarkan dan menyediakan aplikasi mereka kepada pengguna akhir melalui internet. Selama penyebaran Zona Lokal, Anda harus mengalokasikan alamat IP publik untuk digunakan di Zona Lokal. Ketika Anda mengalokasikan alamat IP elastis, Anda dapat menentukan lokasi dari mana alamat IP diiklankan. Lokasi ini disebut grup perbatasan jaringan. Grup perbatasan jaringan adalah kumpulan Availability Zones, Local Zones, atau AWS Wavelength Zones dari mana AWS mengiklankan alamat IP publik. Ini membantu memastikan latensi minimum atau jarak fisik antara AWS jaringan dan pengguna yang mengakses sumber daya di Zona ini. Untuk melihat semua grup perbatasan jaringan untuk Local Zones, lihat Available Local Zones dalam dokumentasi Local Zones.

Untuk mengekspos EC2-hosted beban kerja Amazon di Zona Lokal ke internet, Anda dapat mengaktifkan opsi IP Auto-assign Publik saat meluncurkan instans EC2. Jika Anda menggunakan Application Load Balancer, Anda dapat mendefinisikannya sebagai menghadap ke internet sehingga alamat IP publik yang ditetapkan ke Zona Lokal dapat disebarkan oleh jaringan perbatasan yang

terkait dengan Zona Lokal. Selain itu, saat Anda menggunakan alamat IP Elastic, Anda dapat mengaitkan salah satu sumber daya ini dengan instans EC2 setelah diluncurkan. Saat Anda mengirim lalu lintas melalui gateway internet di Local Zones, spesifikasi bandwidth instance yang sama yang digunakan oleh Wilayah diterapkan. Lalu lintas jaringan Zona Lokal langsung menuju internet atau ke titik kehadiran (PoPs) tanpa melintasi Wilayah induk Zona Lokal, untuk memungkinkan akses ke komputasi latensi rendah.

Local Zones menyediakan opsi konektivitas berikut melalui internet:

- Akses publik: Menghubungkan beban kerja atau peralatan virtual ke internet dengan menggunakan alamat IP Elastis melalui gateway internet.
- Akses internet keluar: Memungkinkan sumber daya untuk mencapai titik akhir publik melalui instance terjemahan alamat jaringan (NAT) atau peralatan virtual dengan alamat IP Elastis terkait, tanpa paparan internet langsung.
- Konektivitas VPN: Menetapkan koneksi pribadi dengan menggunakan Internet Protocol Security (IPsec) VPN melalui peralatan virtual dengan alamat IP Elastis terkait.

Untuk informasi selengkapnya, lihat Opsi konektivitas untuk Local Zones di dokumentasi Local Zones.

Local Zones dan Direct Connect

Local Zones juga mendukung Direct Connect, yang memungkinkan Anda merutekan lalu lintas melalui koneksi jaringan pribadi. Untuk informasi selengkapnya, lihat Direct Connect di Local Zones dalam dokumentasi Local Zones.

Local Zones dan gateway transit

AWS Transit Gateway tidak mendukung lampiran VPC langsung ke subnet Zona Lokal. Namun, Anda dapat terhubung ke beban kerja Zona Lokal dengan membuat lampiran Transit Gateway di subnet Availability Zone induk dari VPC yang sama. Konfigurasi ini memungkinkan interkonektivitas antara beberapa VPC dan beban kerja Zona Lokal Anda. Untuk informasi selengkapnya, lihat Koneksi gateway transit antara Local Zones dalam dokumentasi Local Zones.

Local Zones dan VPC mengintip

Anda dapat memperluas VPC apa pun dari Wilayah induk ke Zona Lokal dengan membuat subnet baru dan menetapkannya ke Zona Lokal. Peering VPC dapat dibuat antara VPC yang diperluas ke

Local Zones. Ketika VPC yang diintip berada di Zona Lokal yang sama, lalu lintas tetap berada di dalam Zona Lokal dan tidak menjepit rambut melalui Wilayah induk.

Keamanan di tepi

Dalam AWS Cloud, keamanan adalah prioritas utama. Ketika organisasi mengadopsi skalabilitas dan fleksibilitas cloud, AWS membantu mereka mengadopsi keamanan, identitas, dan kepatuhan sebagai faktor bisnis utama. AWS mengintegrasikan keamanan ke dalam infrastruktur intinya dan menawarkan layanan untuk membantu Anda memenuhi persyaratan keamanan cloud unik Anda. Ketika Anda memperluas cakupan arsitektur Anda ke dalam AWS Cloud, Anda mendapat manfaat dari integrasi infrastruktur seperti Local Zones dan Wilayah AWS Outposts ke dalamnya. Integrasi ini memungkinkan AWS untuk memperluas grup layanan keamanan inti tertentu ke tepi.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab AWS bersama membedakan antara keamanan cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang berjalan Layanan AWS di dalamnya AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-party Auditor secara teratur menguji dan memverifikasi efektivitas AWS keamanan sebagai bagian dari program AWS kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh Layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Perlindungan data

Model tanggung jawab AWS bersama berlaku untuk perlindungan data di AWS Outposts dan AWS Local Zones. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan AWS Cloud (keamanan cloud). Anda bertanggung jawab untuk menjaga kontrol atas konten Anda yang di-host di infrastruktur ini (keamanan di cloud). Konten ini mencakup konfigurasi keamanan dan tugas manajemen untuk Layanan AWS yang Anda gunakan.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS Identity and Access Management (IAM) atau. AWS IAM Identity Center Ini memberi setiap pengguna hanya izin yang diperlukan untuk memenuhi tugas pekerjaan mereka.

Enkripsi saat diam

Enkripsi dalam volume EBS

Dengan AWS Outposts, semua data dienkripsi saat istirahat. Bahan utama dibungkus dengan kunci eksternal, Nitro Security Key (NSK), yang disimpan dalam perangkat yang dapat dilepas. NSK diperlukan untuk mendekripsi data di rak Outpost Anda. Anda dapat menggunakan enkripsi Amazon EBS untuk volume dan snapshot EBS Anda. Enkripsi Amazon EBS menggunakan AWS Key Management Service (AWS KMS) dan kunci KMS.

Dalam kasus Local Zones, semua volume EBS dienkripsi secara default di semua Local Zones, kecuali untuk daftar yang didokumentasikan dalam AWS Local Zones FAQ (lihat pertanyaan: Apa perilaku enkripsi default volume EBS di Local Zones?), kecuali enkripsi diaktifkan untuk akun.

Enkripsi di Amazon S3 di Outposts

Secara default, semua data yang disimpan di Amazon S3 di Outposts dienkripsi dengan menggunakan enkripsi sisi server dengan kunci enkripsi terkelola Amazon S3 (). SSE-S3 Anda dapat secara opsional menggunakan enkripsi sisi server dengan kunci enkripsi yang disediakan pelanggan (). SSE-C Untuk menggunakan SSE-C, tentukan kunci enkripsi sebagai bagian dari permintaan API objek Anda. Server-side enkripsi mengenkripsi hanya data objek, bukan metadata objek.

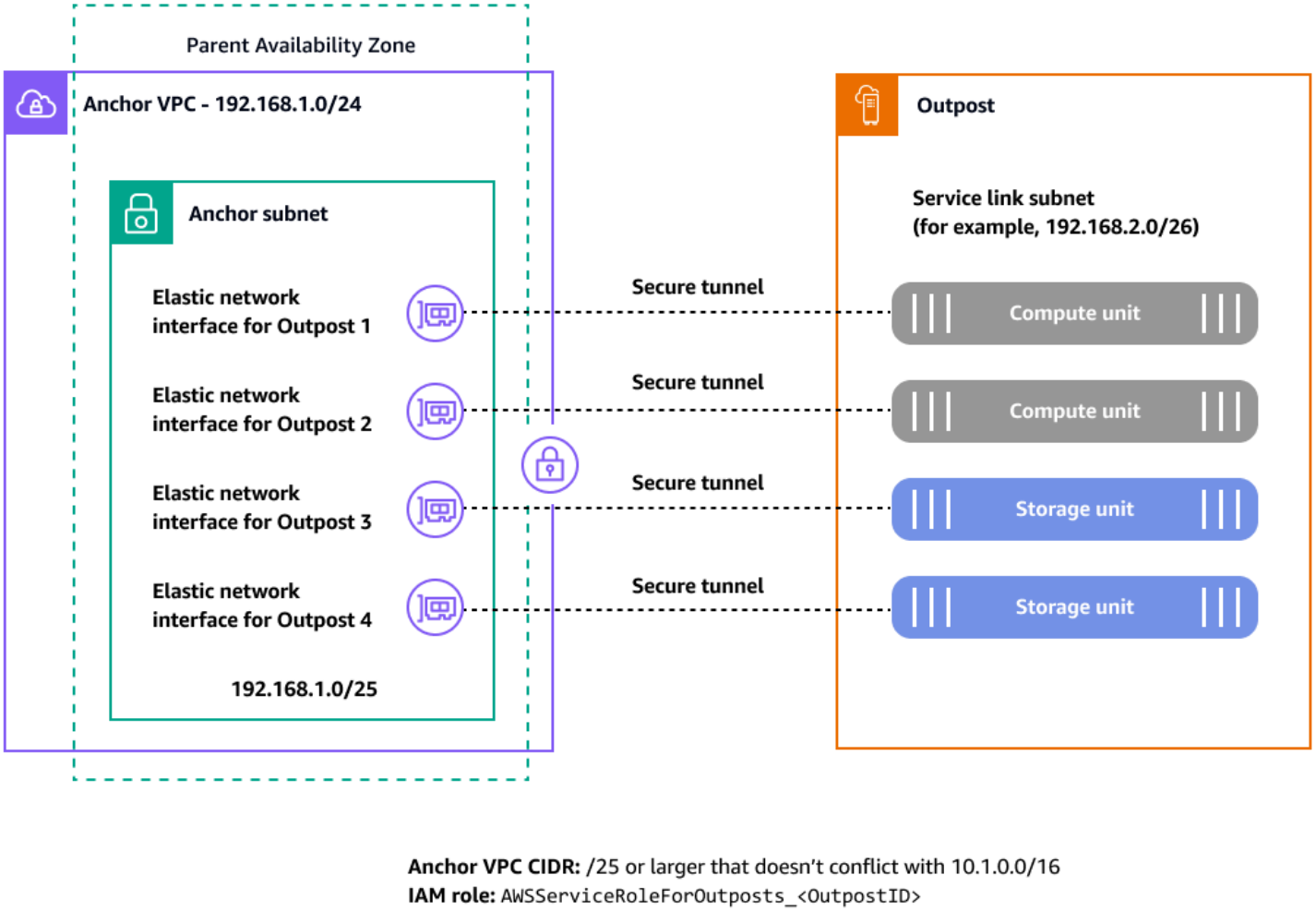
> **Note**
>
> Amazon S3 di Outposts tidak mendukung enkripsi sisi server dengan kunci KMS (). SSE-KMS

Enkripsi saat bergerak

Untuk AWS Outposts, tautan layanan adalah koneksi yang diperlukan antara server Outposts Anda dan yang Anda pilih Wilayah AWS (atau Wilayah rumah) dan memungkinkan pengelolaan Pos Luar dan pertukaran lalu lintas ke dan dari. Wilayah AWS Tautan layanan menggunakan VPN AWS terkelola untuk berkomunikasi dengan Wilayah asal. Setiap host di dalamnya AWS Outposts membuat satu set terowongan VPN untuk membagi lalu lintas pesawat kontrol dan lalu lintas VPC. Bergantung pada konektivitas tautan layanan (internet atau Direct Connect) untuk AWS Outposts, terowongan tersebut memerlukan port firewall untuk dibuka untuk tautan layanan untuk membuat overlay di atasnya. Untuk informasi teknis terperinci tentang keamanan AWS Outposts dan tautan

layanan, lihat Konektivitas melalui tautan layanan dan keamanan Infrastruktur AWS Outposts dalam AWS Outposts dokumentasi.

Tautan AWS Outposts layanan membuat terowongan terenkripsi yang membangun bidang kontrol dan konektivitas bidang data ke induk Wilayah AWS, seperti yang diilustrasikan dalam diagram berikut.



Setiap AWS Outposts host (komputasi dan penyimpanan) memerlukan terowongan terenkripsi ini melalui port TCP dan UDP yang terkenal untuk berkomunikasi dengan Wilayah induknya. Tabel berikut menunjukkan port sumber dan tujuan dan alamat untuk protokol UDP dan TCP.

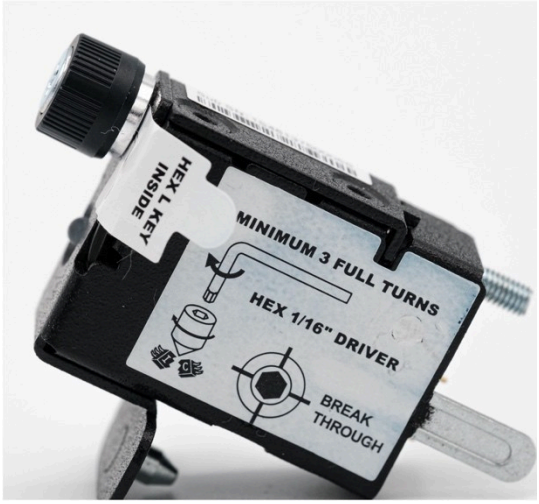
Protokol	Port sumber	Alamat sumber	Pelabuhan tujuan	Alamat tujuan
UDP	443	AWS Outposts tautan layanan /26	443	AWS Outposts Rute umum wilayah atau jangkar VPC CIDR
TCP	1025-65535	AWS Outposts tautan layanan /26	443	AWS Outposts Rute umum wilayah atau jangkar VPC CIDR

Local Zones juga terhubung ke Wilayah induk melalui tulang punggung pribadi global Amazon yang redundan dan sangat tinggi bandwidth. Koneksi ini memberikan aplikasi yang berjalan di Local Zones akses cepat, aman, dan mulus ke lainnya Layanan AWS. Selama Local Zones adalah bagian dari infrastruktur AWS global, semua data yang mengalir melalui jaringan AWS global secara otomatis dienkripsi pada lapisan fisik sebelum meninggalkan fasilitas yang AWS aman. Jika Anda memiliki persyaratan khusus untuk mengenkripsi data dalam perjalanan antara lokasi lokal dan Direct Connect PoPs untuk mengakses Zona Lokal, Anda dapat mengaktifkan MAC Security (MACSec) antara router atau switch lokal dan titik akhir. Direct Connect Untuk informasi selengkapnya, lihat posting AWS blog Menambahkan keamanan MacSec ke Direct Connect koneksi.

Penghapusan data

Saat Anda menghentikan atau menghentikan instans EC2 AWS Outposts, memori yang dialokasikan padanya akan digosok (disetel ke nol) oleh hypervisor sebelum dialokasikan ke instance baru, dan setiap blok penyimpanan diatur ulang. Menghapus data dari perangkat keras Outpost melibatkan penggunaan perangkat keras khusus. NSK adalah perangkat kecil, diilustrasikan dalam foto berikut, yang menempel di bagian depan setiap unit komputasi atau penyimpanan di Pos Luar. Ini dirancang untuk menyediakan mekanisme untuk mencegah data Anda terpapar dari pusat data atau situs colocation Anda. Data pada perangkat Outpost dilindungi dengan membungkus bahan kunci yang digunakan untuk mengenkripsi perangkat dan menyimpan bahan yang dibungkus di NSK. Ketika Anda mengembalikan host Outpost, Anda menghancurkan NSK dengan memutar sekrup kecil

pada chip yang menghancurkan NSK dan secara fisik menghancurkan chip. Menghancurkan NSK menghancurkan data secara kriptografis di Outpost Anda.



Manajemen identitas dan akses

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

Tabel berikut mencantumkan fitur IAM yang dapat Anda gunakan. AWS Outposts

Fitur IAM	AWS Outposts dukungan
Identity-based kebijakan	Ya
Resource-based kebijakan	Ya*
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
Daftar kontrol akses (ACL)	Tidak

Fitur IAM	AWS Outposts dukungan
Attribute-based kontrol akses (ABAC) (tag dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Service-linked peran	Ya

* Selain kebijakan berbasis identitas IAM, Amazon S3 di Outposts mendukung kebijakan bucket dan access point. Ini adalah kebijakan berbasis sumber daya yang dilampirkan ke sumber daya Amazon S3 di Outposts.

Untuk informasi selengkapnya tentang cara fitur ini didukung AWS Outposts, lihat panduan AWS Outposts pengguna.

Keamanan infrastruktur

Perlindungan infrastruktur adalah bagian penting dari sebuah program keamanan informasi. Ini memastikan bahwa sistem dan layanan beban kerja dilindungi dari akses yang tidak diinginkan dan tidak sah, dan potensi kerentanan. Misalnya, Anda menentukan batas kepercayaan (misalnya, batas jaringan dan akun), konfigurasi dan pemeliharaan keamanan sistem (misalnya, pengerasan, minimalisasi, dan penambalan), otentikasi dan otorisasi sistem operasi (misalnya, pengguna, kunci, dan tingkat akses), dan poin penegakan kebijakan lain yang sesuai (misalnya, firewall aplikasi web atau gateway API).

AWS menyediakan sejumlah pendekatan untuk perlindungan infrastruktur, seperti yang dibahas dalam bagian berikut.

Melindungi jaringan

Pengguna Anda mungkin menjadi bagian dari tenaga kerja atau pelanggan Anda, dan dapat ditemukan di mana saja. Untuk alasan ini, Anda tidak dapat mempercayai semua orang yang memiliki akses ke jaringan Anda. Ketika Anda mengikuti prinsip menerapkan keamanan di semua lapisan,

Anda menggunakan pendekatan nol kepercayaan. Dalam model keamanan zero trust, komponen aplikasi atau layanan mikro dianggap terpisah, dan tidak ada komponen atau layanan mikro yang mempercayai komponen atau layanan mikro lainnya. Untuk mencapai keamanan tanpa kepercayaan, ikuti rekomendasi ini:

- Buat lapisan jaringan. Jaringan berlapis membantu secara logis mengelompokkan komponen jaringan serupa. Mereka juga mengecilkan ruang lingkup potensi dampak akses jaringan yang tidak sah.
- Kontrol lapisan lalu lintas. Terapkan beberapa kontrol dengan pendekatan defense-in-depth untuk lalu lintas masuk dan keluar. Ini termasuk penggunaan grup keamanan (firewall inspeksi stateful), ACL jaringan, subnet, dan tabel rute.
- Menerapkan inspeksi dan perlindungan. Periksa dan filter lalu lintas Anda di setiap lapisan. Anda dapat memeriksa konfigurasi VPC Anda untuk potensi akses yang tidak diinginkan dengan menggunakan Network Access Analyzer. Anda dapat menentukan persyaratan akses jaringan Anda dan mengidentifikasi jalur jaringan potensial yang tidak memenuhi mereka.

Melindungi sumber daya komputasi

Sumber daya komputasi mencakup instans EC2, wadah, AWS Lambda fungsi, layanan basis data, perangkat IoT, dan banyak lagi. Setiap jenis sumber daya komputasi memerlukan pendekatan keamanan yang berbeda. Namun, sumber daya ini berbagi strategi umum yang perlu Anda pertimbangkan: pertahanan secara mendalam, manajemen kerentanan, pengurangan permukaan serangan, otomatisasi konfigurasi dan operasi, dan melakukan tindakan di kejauhan.

Berikut panduan umum untuk melindungi sumber daya komputasi Anda untuk layanan utama:

- Membuat dan memelihara program manajemen kerentanan. Memindai dan menambal resource secara teratur seperti instans EC2, container Amazon Elastic Container Service (Amazon ECS), dan beban kerja Amazon Elastic Kubernetes Service (Amazon EKS).
- Otomatiskan perlindungan komputasi. Otomatiskan mekanisme komputasi protektif Anda, termasuk manajemen kerentanan, pengurangan permukaan serangan, dan pengelolaan sumber daya. Otomatisasi ini membebaskan waktu yang dapat Anda gunakan untuk mengamankan aspek lain dari beban kerja Anda, dan membantu mengurangi risiko kesalahan manusia.
- Kurangi permukaan serangan. Kurangi eksposur Anda terhadap akses yang tidak diinginkan dengan memperkuat sistem operasi Anda dan meminimalkan komponen, pustaka, dan layanan yang dapat dikonsumsi secara eksternal yang Anda gunakan.

Selain itu, untuk setiap Layanan AWS yang Anda gunakan, periksa rekomendasi keamanan spesifik dalam dokumentasi layanan.

Akses internet

Keduanya AWS Outposts dan Local Zones menyediakan pola arsitektur yang memberikan beban kerja Anda akses ke dan dari internet. Saat Anda menggunakan pola-pola ini, pertimbangkan konsumsi internet dari Wilayah sebagai opsi yang layak hanya jika Anda menggunakannya untuk menambal, memperbarui, mengakses repositori Git yang berada di luar, dan skenario AWS serupa. Untuk pola arsitektur ini, konsep inspeksi masuk terpusat dan jalan keluar internet terpusat berlaku. Pola akses ini menggunakan AWS Transit Gateway, gateway NAT, firewall jaringan, dan komponen lain yang berada di Wilayah AWS, tetapi terhubung ke atau Local AWS Outposts Zones melalui jalur data antara Region dan edge.

Local Zones mengadopsi konstruksi jaringan yang disebut grup perbatasan jaringan, yang digunakan dalam. Wilayah AWS AWS mengiklankan alamat IP publik dari grup unik ini. Grup perbatasan jaringan terdiri dari Availability Zones, Local Zones, atau Wavelength Zones. Anda dapat secara eksplisit mengalokasikan kumpulan alamat IP publik untuk digunakan dalam grup perbatasan jaringan. Anda dapat menggunakan grup perbatasan jaringan untuk memperluas gateway internet ke Local Zones dengan mengizinkan alamat IP Elastic dilayani dari grup. Opsi ini mengharuskan Anda menerapkan komponen lain untuk melengkapi layanan inti yang tersedia di Local Zones. Komponen tersebut mungkin berasal dari ISV dan membantu Anda membangun lapisan inspeksi di Zona Lokal Anda, seperti yang dijelaskan dalam posting AWS blog Arsitektur inspeksi hibrida dengan. AWS Local Zones

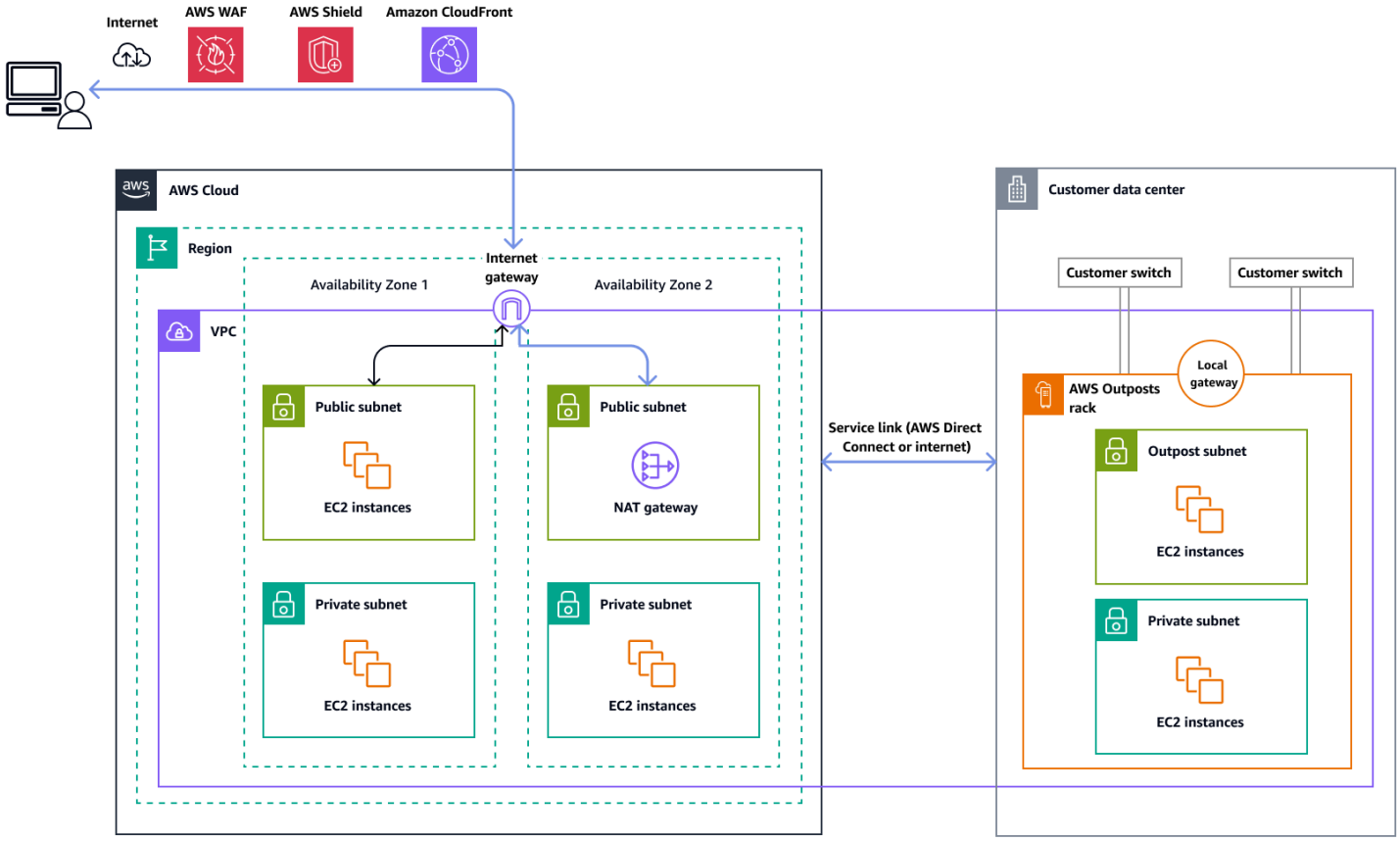
Dalam AWS Outposts, jika Anda ingin menggunakan gateway lokal (LGW) untuk menjangkau internet dari jaringan Anda, Anda harus memodifikasi tabel rute khusus yang terkait dengan subnet. AWS Outposts Tabel rute harus memiliki entri rute default (0.0.0. 0/0) yang menggunakan LGW sebagai lompatan berikutnya. Anda bertanggung jawab untuk menerapkan kontrol keamanan yang tersisa di jaringan lokal Anda, termasuk pertahanan perimeter seperti firewall dan sistem pencegahan intrusi atau sistem deteksi intrusi (). IPS/IDS Ini sejalan dengan model tanggung jawab bersama, yang membagi tugas keamanan antara Anda dan penyedia cloud.

Akses internet melalui orang tua Wilayah AWS

Dalam opsi ini, beban kerja di Outpost mengakses internet melalui tautan layanan dan gateway internet di induk. Wilayah AWS Lalu lintas keluar ke internet dapat dialihkan melalui gateway NAT yang dipakai di VPC Anda. Untuk keamanan tambahan untuk lalu lintas masuk dan keluar,

Anda dapat menggunakan layanan AWS keamanan seperti AWS WAF,, AWS Shield dan Amazon CloudFront di. Wilayah AWS

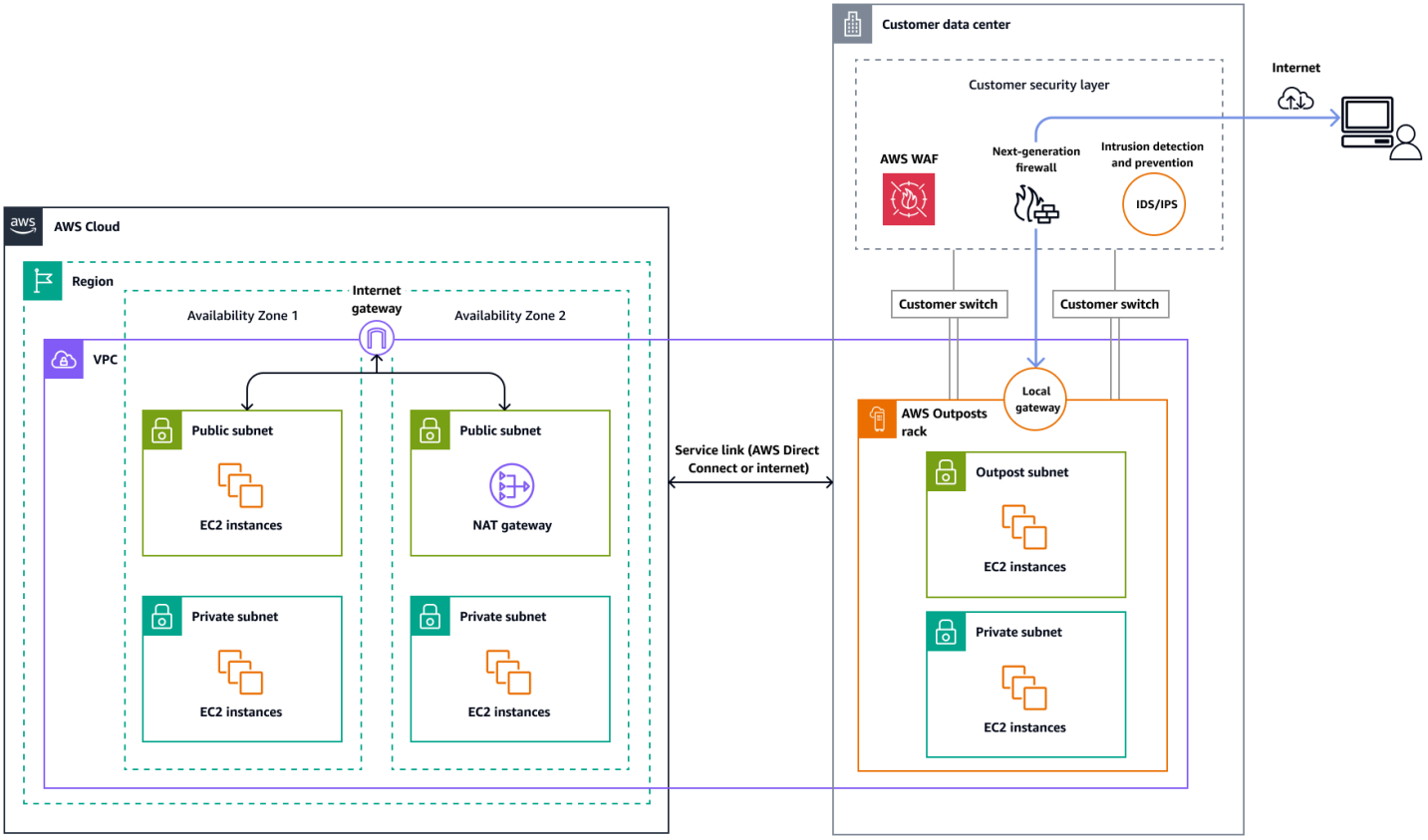
Diagram berikut menunjukkan lalu lintas antara beban kerja dalam AWS Outposts instance dan internet melalui induk Wilayah AWS.



Akses internet melalui jaringan pusat data lokal Anda

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

Gambar berikut menunjukkan lalu lintas antara beban kerja di AWS Outposts subnet dan internet melalui pusat data.



Tata kelola infrastruktur

Terlepas dari apakah beban kerja Anda diterapkan di, Zona Lokal Wilayah AWS, atau Pos Luar, Anda dapat menggunakannya AWS Control Tower untuk tata kelola infrastruktur. AWS Control Tower menawarkan cara mudah untuk mengatur dan mengatur lingkungan AWS multi-akun, mengikuti praktik terbaik preskriptif. AWS Control Tower mengatur kemampuan beberapa lainnya Layanan AWS, termasuk, AWS Organizations AWS Service Catalog, dan IAM Identity Center (lihat semua layanan terintegrasi) untuk membangun landing zone dalam waktu kurang dari satu jam. Sumber daya diatur dan dikelola atas nama Anda.

AWS Control Tower menyediakan tata kelola terpadu di semua AWS lingkungan, termasuk Wilayah, Local Zones (ekstensi latensi rendah), dan Outposts (infrastruktur lokal). Ini membantu memastikan keamanan dan kepatuhan yang konsisten di seluruh arsitektur cloud hybrid Anda. Lihat informasi yang lebih lengkap dalam dokumentasi AWS Control Tower.

Anda dapat mengonfigurasi AWS Control Tower dan kemampuan seperti pagar pembatas untuk mematuhi persyaratan residensi data di pemerintah dan industri yang diatur seperti Lembaga Jasa

Keuangan (FSI). Untuk memahami cara menerapkan pagar pembatas untuk residensi data di edge, lihat berikut ini:

- Praktik terbaik untuk mengelola residensi data dalam AWS Local Zones menggunakan kontrol landing zone (posting AWS blog)
- Arsitektur untuk residensi data dengan pagar pembatas AWS Outposts rak dan landing zone (posting blog)AWS
- Residensi Data dengan Hybrid Cloud Services Lens (Dokumentasi AWS Well-Architected Kerangka Kerja)

Berbagi sumber Outposts

Karena Outpost adalah infrastruktur terbatas yang tinggal di pusat data Anda atau di ruang co-lokasi, untuk tata kelola terpusat AWS Outposts, Anda perlu mengontrol sumber daya akun mana yang dibagikan secara terpusat. AWS Outposts

Dengan berbagi Outpost, pemilik Outpost dapat berbagi sumber daya Outpost dan Outpost mereka, termasuk situs Outpost dan subnet, dengan yang lain yang berada di organisasi Akun AWS yang sama di. AWS Organizations Sebagai pemilik Outpost, Anda dapat membuat dan mengelola sumber daya Outpost dari lokasi pusat, dan berbagi sumber daya di beberapa sumber daya Akun AWS dalam organisasi Anda AWS . Hal ini memungkinkan konsumen lain untuk menggunakan situs Outpost, mengkonfigurasi VPC, dan meluncurkan dan menjalankan instance di Outpost bersama.

Sumber daya yang dapat dibagikan AWS Outposts adalah:

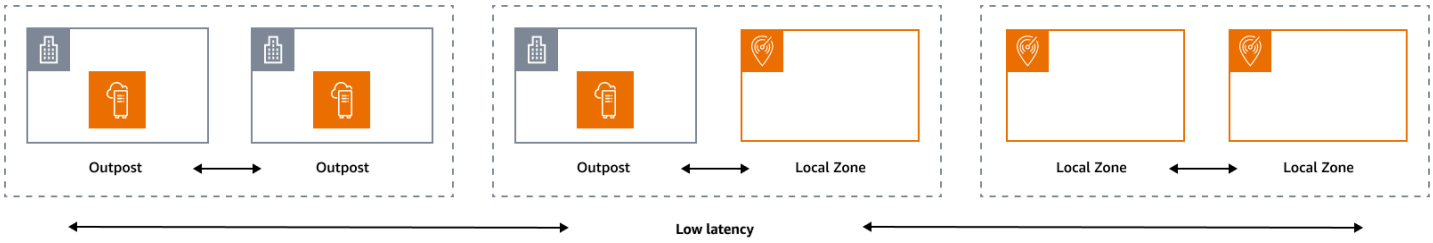
- Host khusus yang dialokasikan
- Reservasi kapasitas
- Customer-owned Kumpulan alamat IP (CoIP)
- Tabel rute gateway lokal
- Outposts
- Amazon S3 on Outposts
- Situs
- Subnet

Untuk mengikuti praktik terbaik untuk berbagi sumber daya Outposts di lingkungan multi-akun, lihat posting blog berikut: AWS

- Berbagi AWS Outposts di AWS lingkungan multi-akun: Bagian 1
- Berbagi AWS Outposts di AWS lingkungan multi-akun: Bagian 2

Ketahanan di tepi

Pilar keandalan mencakup kemampuan beban kerja untuk menjalankan fungsi yang dimaksudkan dengan benar dan konsisten ketika diharapkan. Ini termasuk kemampuan untuk mengoperasikan dan menguji beban kerja melalui siklus hidupnya. Dalam hal ini, ketika Anda merancang arsitektur tangguh di tepi, Anda harus terlebih dahulu mempertimbangkan infrastruktur mana yang akan Anda gunakan untuk menerapkan arsitektur itu. Ada tiga kemungkinan kombinasi untuk diterapkan dengan menggunakan AWS Local Zones dan AWS Outposts: Outpost to Outpost, Outpost to Local Zone, dan Local Zone to Local Zone, seperti yang diilustrasikan dalam diagram berikut. Meskipun ada kemungkinan lain untuk arsitektur tangguh, seperti menggabungkan layanan AWS edge dengan infrastruktur lokal tradisional atau Wilayah AWS, panduan ini berfokus pada tiga kombinasi ini yang berlaku untuk desain layanan cloud hybrid



Pertimbangan infrastruktur

Pada AWS, salah satu prinsip inti dari desain layanan adalah untuk menghindari satu titik kegagalan dalam infrastruktur fisik yang mendasarinya. Karena prinsip ini, AWS perangkat lunak dan sistem menggunakan beberapa Availability Zone dan tahan terhadap kegagalan satu zona. Di edge, AWS menawarkan infrastruktur yang didasarkan pada Local Zones dan Outposts. Oleh karena itu, faktor penting dalam memastikan ketahanan dalam desain infrastruktur adalah menentukan di mana sumber daya aplikasi digunakan.

Zona Lokal

Local Zones bertindak mirip dengan Availability Zone di dalamnya Wilayah AWS, karena mereka dapat dipilih sebagai lokasi penempatan untuk AWS sumber daya zona seperti subnet dan instans EC2. Namun, mereka tidak terletak di Wilayah AWS, tetapi dekat dengan populasi besar, industri, dan pusat TI di mana tidak Wilayah AWS ada saat ini. Meskipun demikian, mereka masih

mempertahankan bandwidth tinggi, koneksi aman antara beban kerja lokal di Zona Lokal dan beban kerja yang berjalan di. Wilayah AWS Oleh karena itu, Anda harus menggunakan Local Zones untuk menerapkan beban kerja yang lebih dekat ke pengguna Anda untuk persyaratan latensi rendah.

Outposts

AWS Outposts adalah layanan yang dikelola sepenuhnya yang memperluas AWS infrastruktur, API Layanan AWS, dan alat ke pusat data Anda. Infrastruktur perangkat keras yang sama yang AWS Cloud digunakan di diinstal di pusat data Anda. Outposts kemudian terhubung ke yang terdekat. Wilayah AWS Anda dapat menggunakan Outposts untuk mendukung beban kerja Anda yang memiliki latensi rendah atau persyaratan pemrosesan data lokal.

Zona Ketersediaan Orang Tua

Setiap Zona Lokal atau Pos Luar memiliki Wilayah induk (juga disebut sebagai Wilayah asal). Wilayah induk adalah tempat bidang kontrol infrastruktur AWS tepi (Outpost atau Local Zone) berlabuh. Dalam kasus Local Zones, Wilayah induk adalah komponen arsitektur fundamental dari Zona Lokal dan tidak dapat dimodifikasi oleh pelanggan. AWS Outposts memperluas AWS Cloud ke lingkungan lokal Anda, jadi Anda harus memilih Wilayah dan Zona Ketersediaan tertentu selama proses pemesanan. Pilihan ini menambatkan bidang kontrol penyebaran Outposts Anda ke infrastruktur yang dipilih. AWS

Ketika Anda mengembangkan arsitektur ketersediaan tinggi di edge, Wilayah induk dari infrastruktur ini, seperti Outposts atau Local Zones, harus sama, sehingga VPC dapat diperpanjang di antara mereka. VPC yang diperluas ini adalah dasar untuk menciptakan arsitektur ketersediaan tinggi ini. Saat Anda menentukan arsitektur yang sangat tangguh, inilah mengapa Anda harus memvalidasi Wilayah induk dan Zona Ketersediaan Wilayah tempat layanan akan (atau sedang) ditambatkan. Seperti yang diilustrasikan dalam diagram berikut, jika Anda ingin menerapkan solusi ketersediaan tinggi antara dua Outposts, Anda harus memilih dua Availability Zone yang berbeda untuk jangkar Outposts. Ini memungkinkan Multi-AZ arsitektur dari perspektif bidang kontrol. Jika Anda ingin menerapkan solusi yang sangat tersedia yang menyertakan satu atau beberapa Local Zones, Anda harus terlebih dahulu memvalidasi Availability Zone induk tempat infrastruktur ditambatkan. Untuk tujuan ini, gunakan AWS CLI perintah berikut:

```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

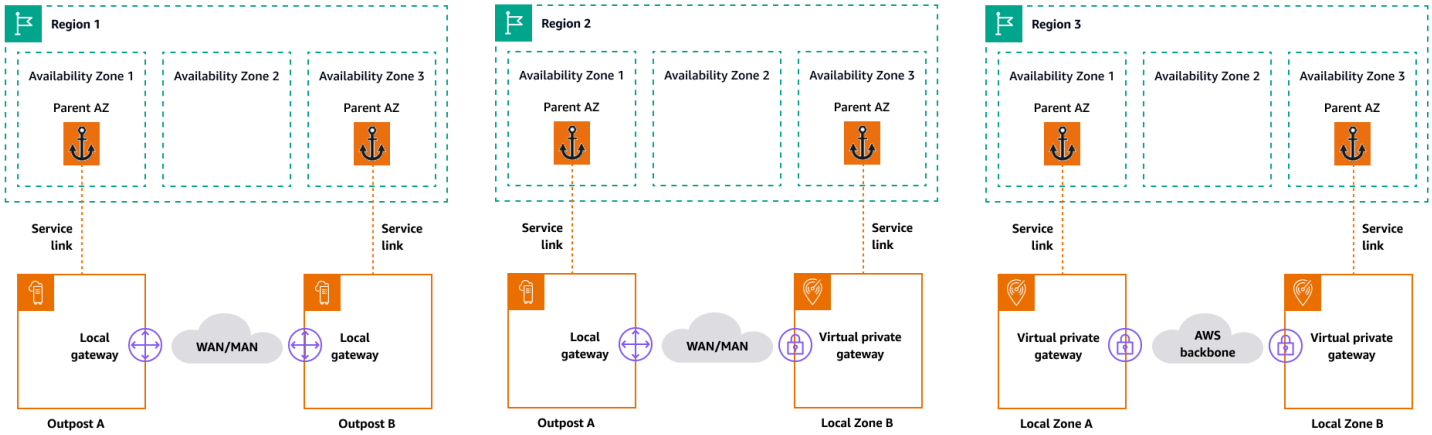
Output dari perintah sebelumnya:

```
{     "AvailabilityZones": [
```

```
        {
            "State": "available",
            "OptInStatus": "opted-in",
            "Messages": [],
            "RegionName": "us-east-1",
            "ZoneName": "us-east-1-mia-1a",
            "ZoneId": "use1-mia1-az1",
            "GroupName": "us-east-1-mia-1",
            "NetworkBorderGroup": "us-east-1-mia-1",
            "ZoneType": "local-zone",
            "ParentZoneName": "us-east-1d",
            "ParentZoneId": "use1-az2"
        }
    ]
}
```


Dalam contoh ini, Miami Local Zone (`us-east-1d-mia-1a1`) ditambatkan di Availability Zone. `us-east-1d-az2` Oleh karena itu, jika Anda perlu membuat arsitektur tangguh di tepi, Anda harus memastikan bahwa infrastruktur sekunder (baik Outposts atau Local Zones) ditambatkan ke Availability Zone selain. **`us-east-1d-az2`** Misalnya, `us-east-1d-az1` akan valid.

Diagram berikut memberikan contoh infrastruktur tepi yang sangat tersedia.



Pertimbangan jaringan

Bagian ini membahas pertimbangan awal untuk jaringan di tepi, terutama untuk koneksi untuk mengakses infrastruktur tepi. Ini meninjau arsitektur yang valid yang menyediakan jaringan tangguh untuk tautan layanan.

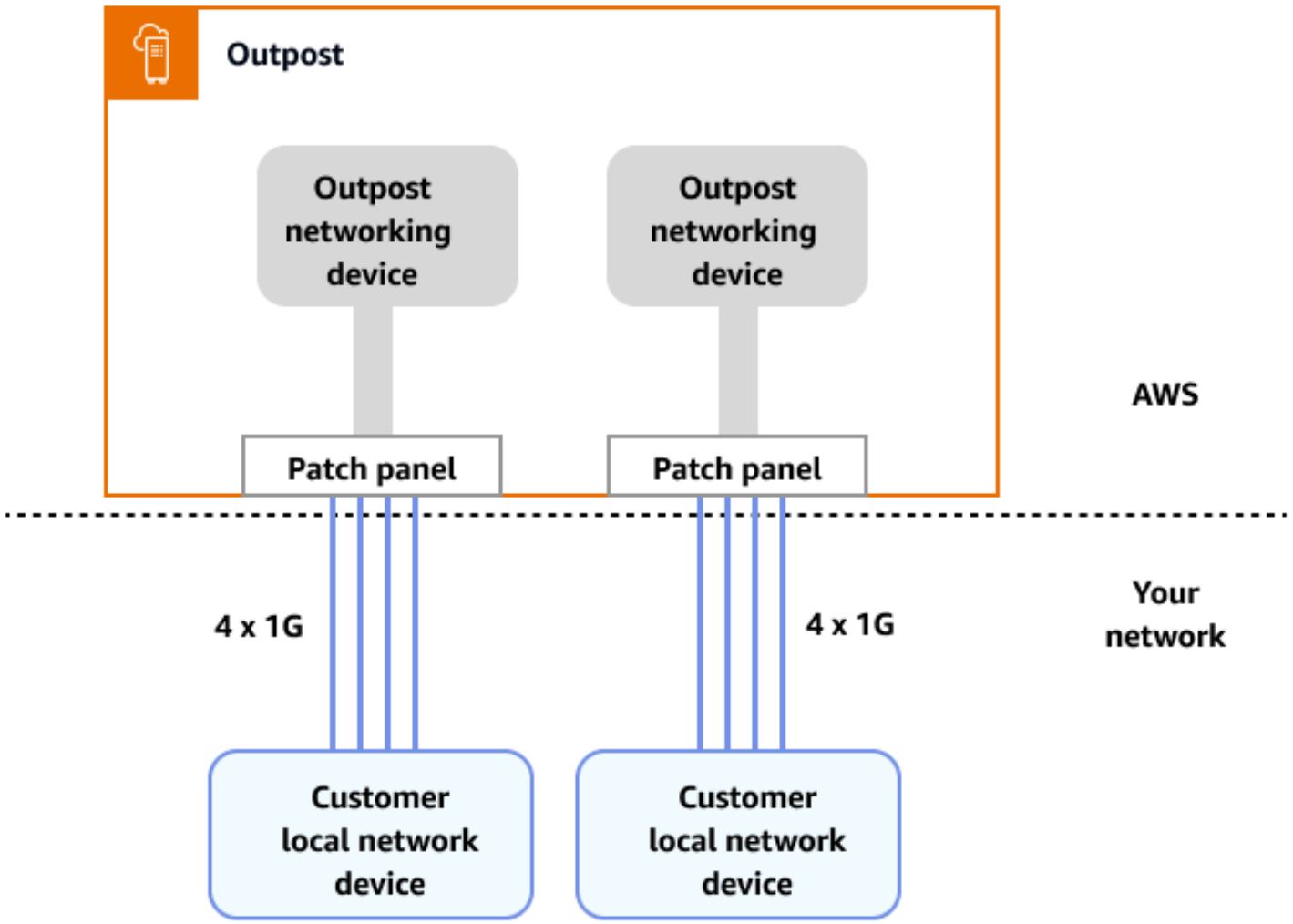
Jaringan ketahanan untuk Local Zones

Local Zones terhubung ke Wilayah induk dengan banyak tautan, redundan, aman, berkecepatan tinggi yang memungkinkan Anda menggunakan layanan Regional apa pun, seperti Amazon S3 dan Amazon RDS, dengan mulus. Anda bertanggung jawab untuk menyediakan konektivitas dari lingkungan lokal atau pengguna ke Zona Lokal. Terlepas dari arsitektur konektivitas yang Anda pilih (misalnya, VPN atau Direct Connect), latensi yang harus dicapai melalui tautan jaringan harus setara untuk menghindari dampak apa pun pada kinerja aplikasi jika terjadi kegagalan pada tautan utama. Jika Anda menggunakan Direct Connect, arsitektur ketahanan yang berlaku sama dengan yang digunakan untuk mengakses, seperti yang didokumentasikan dalam Wilayah AWS rekomendasi ketahanan.Direct Connect Namun, ada skenario yang sebagian besar berlaku untuk Local Zones internasional. Di negara di mana Zona Lokal diaktifkan, hanya memiliki satu Direct Connect PoP membuat tidak mungkin untuk membuat arsitektur yang direkomendasikan untuk Direct Connect ketahanan. Jika Anda hanya memiliki akses ke satu Direct Connect lokasi atau memerlukan ketahanan di luar satu koneksi, Anda dapat membuat alat VPN di Amazon EC2 Direct Connect dan, seperti yang diilustrasikan dan dibahas dalam posting blog Mengaktifkan konektivitas AWS yang sangat tersedia dari tempat ke lokasi. AWS Local Zones

Jaringan ketahanan untuk Outposts

Berbeda dengan Local Zones, Outposts memiliki konektivitas redundan untuk mengakses beban kerja yang digunakan di Outposts dari jaringan lokal Anda. Redundansi ini dicapai melalui dua perangkat jaringan Outposts (OND). Setiap OND membutuhkan setidaknya dua koneksi serat pada 1 Gbps, 10 Gbps, 40 Gbps, atau 100 Gbps ke jaringan lokal Anda. Koneksi ini harus dikonfigurasi sebagai grup agregasi tautan (LAG) untuk memungkinkan penambahan lebih banyak tautan yang dapat diskalakan.

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



Untuk informasi selengkapnya tentang konektivitas ini, lihat Konektivitas jaringan lokal untuk Rak Outposts dalam dokumentasi. AWS Outposts

Untuk pengalaman dan ketahanan yang optimal, AWS merekomendasikan agar Anda menggunakan konektivitas redundan minimal 500 Mbps (1 Gbps lebih baik) untuk koneksi tautan layanan ke. Wilayah AWS Anda dapat menggunakan Direct Connect atau koneksi internet untuk tautan layanan. Minimum ini memungkinkan Anda meluncurkan instans EC2, melampirkan volume EBS, dan mengakses, seperti Amazon EKS Layanan AWS, Amazon EMR, dan metrik. CloudWatch

Diagram berikut menggambarkan arsitektur ini untuk koneksi pribadi yang sangat tersedia.

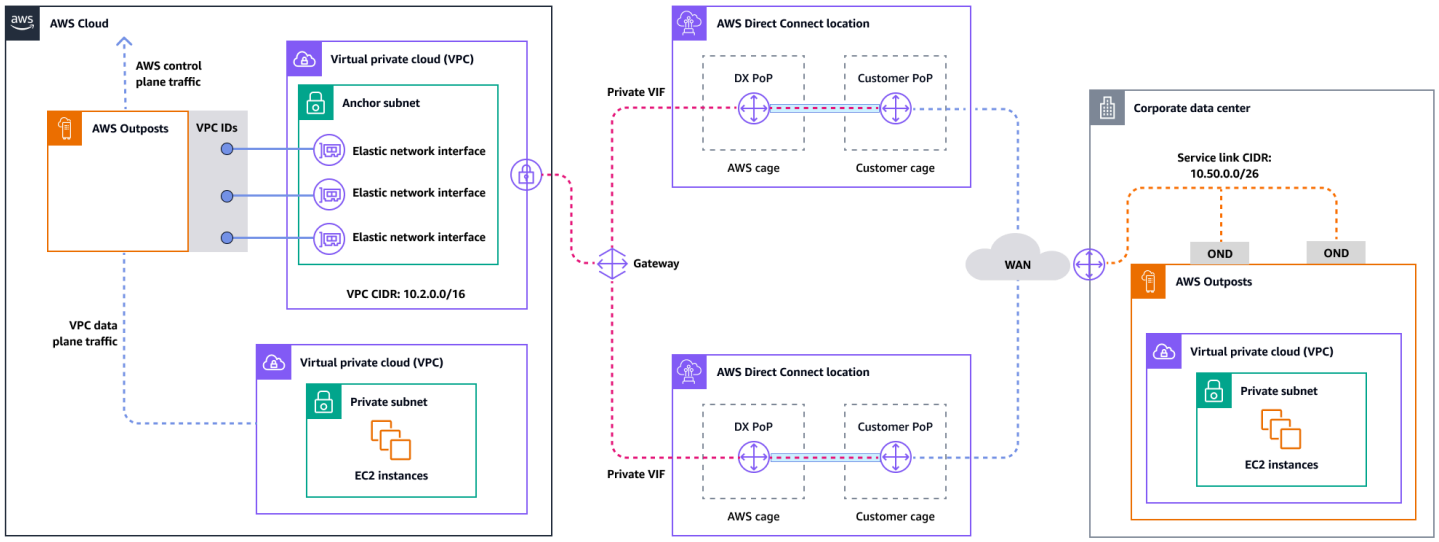
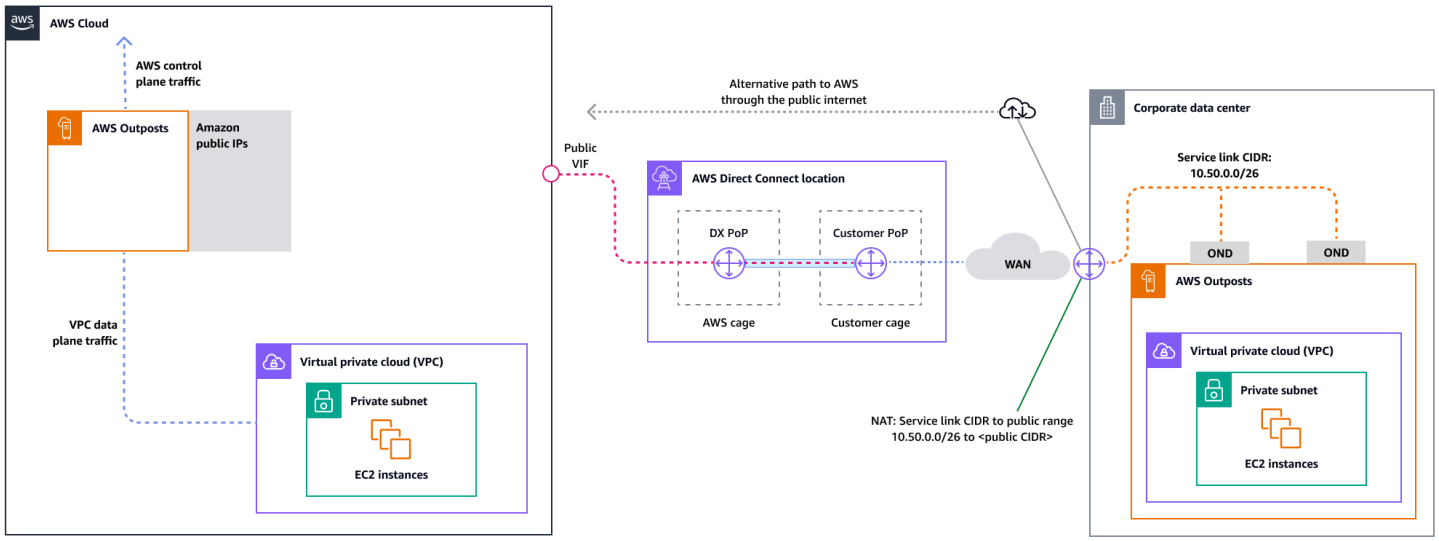


Diagram berikut menggambarkan arsitektur ini untuk koneksi publik yang sangat tersedia.



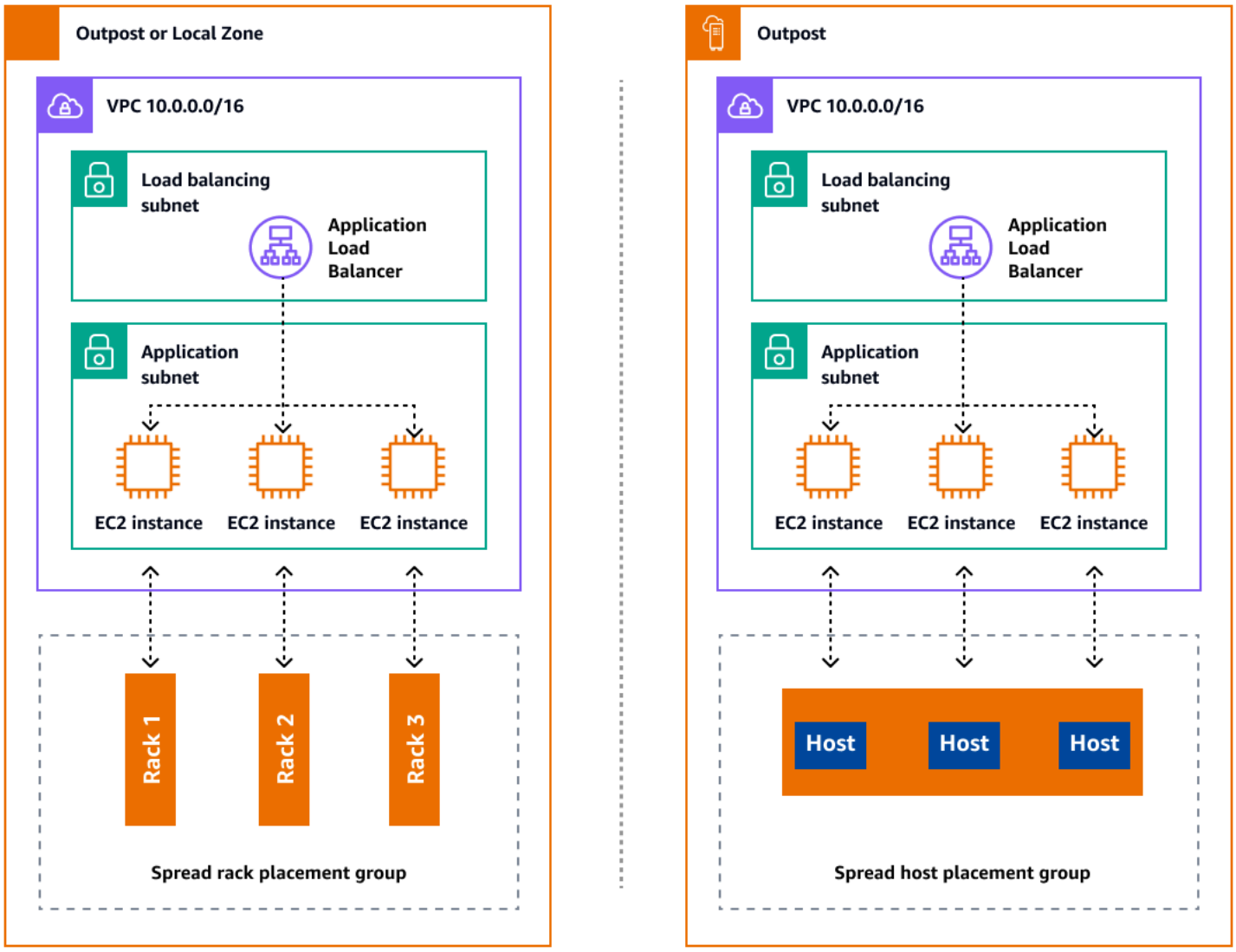
Menskalakan penyebaran rak Outposts dengan rak ACE

Rak Aggregation, Core, Edge (ACE) berfungsi sebagai titik agregasi penting untuk penyebaran AWS Outposts multi-rak, dan terutama direkomendasikan untuk instalasi yang melebihi tiga rak atau untuk merencanakan ekspansi di masa depan. Setiap rak ACE memiliki empat router yang mendukung koneksi 10 Gbps, 40 Gbps, dan 100 Gbps (100 Gbps optimal). Setiap rak dapat terhubung ke hingga empat perangkat pelanggan hulu untuk redundansi maksimum. Rak ACE mengkonsumsi daya hingga 10 kVA dan berat hingga 705 lbs. Manfaat utama termasuk berkurangnya kebutuhan jaringan fisik, uplink kabel serat yang lebih sedikit, dan penurunan antarmuka virtual VLAN. AWS memantau rak-rak ini melalui data telemetri melalui terowongan VPN dan bekerja sama dengan pelanggan selama instalasi untuk memastikan ketersediaan daya yang tepat, konfigurasi jaringan,

dan penempatan optimal. Arsitektur rak ACE memberikan nilai yang meningkat seiring dengan skala penerapan, dan secara efektif menyederhanakan konektivitas sekaligus mengurangi kompleksitas dan persyaratan port fisik dalam instalasi yang lebih besar. Untuk informasi lebih lanjut, lihat posting AWS blog Scaling AWS Outposts rack deployment dengan ACE Rack.

Mendistribusikan Instance di Outposts dan Local Zones

Outposts dan Local Zones memiliki jumlah server komputasi yang terbatas. Jika aplikasi Anda menerapkan beberapa instance terkait, instance ini dapat diterapkan di server yang sama atau di server di rak yang sama kecuali jika dikonfigurasi secara berbeda. Selain opsi default, Anda dapat mendistribusikan instance di seluruh server untuk mengurangi risiko menjalankan instance terkait pada infrastruktur yang sama. Anda juga dapat mendistribusikan instance di beberapa rak dengan menggunakan grup penempatan partisi. Ini disebut model distribusi rak penyebaran. Gunakan distribusi otomatis untuk menyebarkan instance di seluruh partisi dalam grup, atau gunakan instance ke partisi target yang dipilih. Dengan menerapkan instance ke partisi target, Anda dapat menyebarkan sumber daya yang dipilih ke rak yang sama sambil mendistribusikan sumber daya lain di seluruh rak. Outposts juga menyediakan opsi lain yang disebut spread host yang memungkinkan Anda mendistribusikan beban kerja Anda di tingkat host. Diagram berikut menunjukkan opsi distribusi spread rack dan spread host.



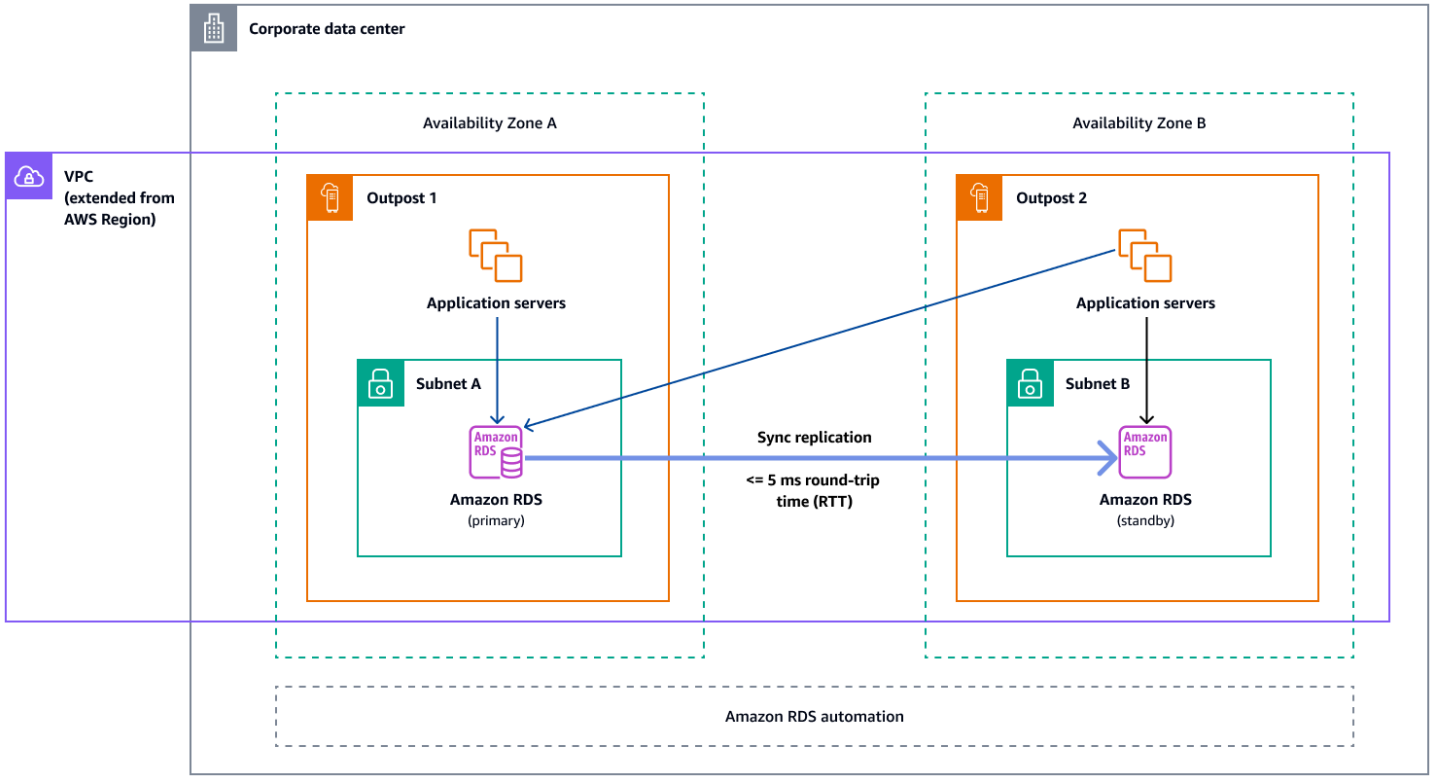
Amazon RDS di Multi-AZ AWS Outposts

Saat Anda menggunakan penerapan Multi-AZ instans di Outposts, Amazon RDS membuat dua instance database di dua Outposts. Setiap Pos Luar berjalan pada infrastruktur fisiknya sendiri dan terhubung ke Zona Ketersediaan yang berbeda di suatu Wilayah untuk ketersediaan tinggi. Ketika dua Outposts terhubung melalui koneksi lokal yang dikelola pelanggan, Amazon RDS mengelola replikasi sinkron antara instance database primer dan standby. Jika terjadi kegagalan perangkat lunak atau infrastruktur, Amazon RDS secara otomatis mempromosikan instans siaga ke peran utama dan memperbarui catatan DNS untuk menunjuk ke instance utama yang baru. Untuk Multi-AZ penerapan, Amazon RDS membuat instans DB utama di satu Pos Luar dan mereplikasi data secara sinkron ke instans DB siaga di Pos Luar yang berbeda. Multi-AZ penerapan di Outposts beroperasi seperti Multi-AZ penerapan di Wilayah AWS, dengan perbedaan berikut:

- Memerlukan koneksi lokal antara dua Outpost atau lebih.
- Mereka membutuhkan kumpulan alamat IP (CoIP) milik pelanggan. Untuk informasi selengkapnya, lihat alamat Customer-owned IP untuk Amazon RDS AWS Outposts di dokumentasi Amazon RDS.
- Replikasi berjalan di jaringan lokal Anda.

Multi-AZ penerapan tersedia untuk semua versi MySQL dan PostgreSQL yang didukung di Amazon RDS di Outposts. Pencadangan lokal tidak didukung untuk Multi-AZ penerapan.

Diagram berikut menunjukkan arsitektur untuk Amazon RDS pada konfigurasi Multi-AZ Outposts.



Mekanisme failover

Load balancing dan penskalaan otomatis

Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas aplikasi masuk Anda di semua instans EC2 yang sedang Anda jalankan. ELB membantu mengelola permintaan masuk dengan merutekan lalu lintas secara optimal sehingga tidak ada satu instance pun yang kewalahan. Untuk menggunakan ELB dengan grup Amazon EC2 Auto Scaling Anda, lampirkan penyeimbang beban ke grup Auto Scaling Anda. Ini mendaftarkan grup dengan penyeimbang beban, yang

bertindak sebagai titik kontak tunggal untuk semua lalu lintas web yang masuk ke grup Anda. Saat Anda menggunakan ELB dengan grup Auto Scaling Anda, Anda tidak perlu mendaftarkan instans EC2 individual dengan penyeimbang beban. Instance yang diluncurkan oleh grup Auto Scaling Anda secara otomatis terdaftar dengan load balancer. Demikian pula, instance yang dihentikan oleh grup Auto Scaling Anda secara otomatis dideregistrasi dari penyeimbang beban. Setelah melampirkan penyeimbang beban ke grup Auto Scaling, Anda dapat mengonfigurasi grup untuk menggunakan metrik ELB (seperti jumlah permintaan Application Load Balancer per target) untuk menskalakan jumlah instance dalam grup saat permintaan berfluktuasi. Secara opsional, Anda dapat menambahkan pemeriksaan kesehatan ELB ke grup Auto Scaling sehingga Amazon EC2 Auto Scaling dapat mengidentifikasi dan mengganti instans yang tidak sehat berdasarkan pemeriksaan kesehatan ini. Anda juga dapat membuat CloudWatch alarm Amazon yang memberi tahu Anda jika jumlah host yang sehat dari grup target lebih rendah dari yang diizinkan.

Diagram berikut menggambarkan bagaimana Application Load Balancer mengelola beban kerja di Amazon EC2. AWS Outposts

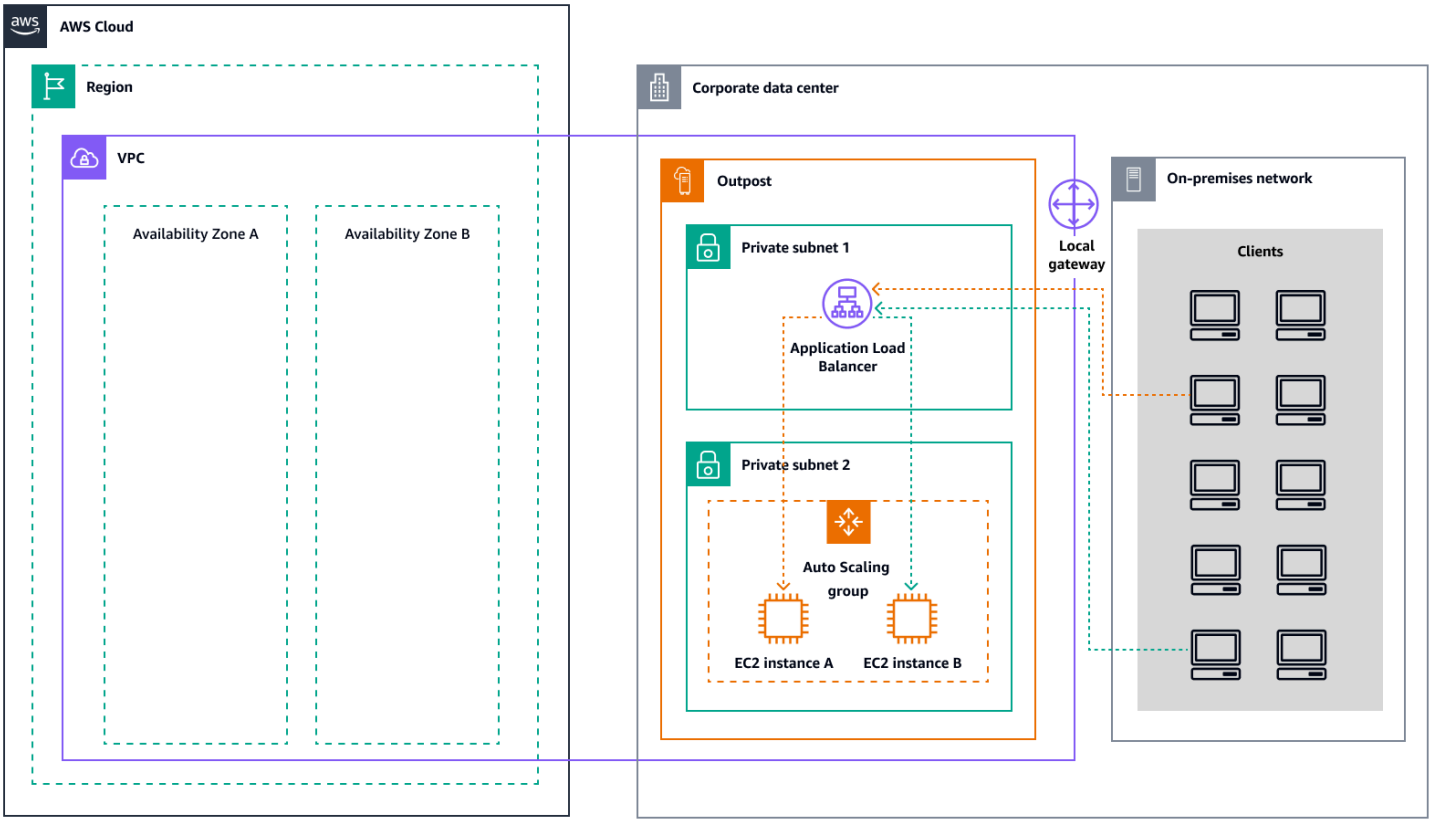
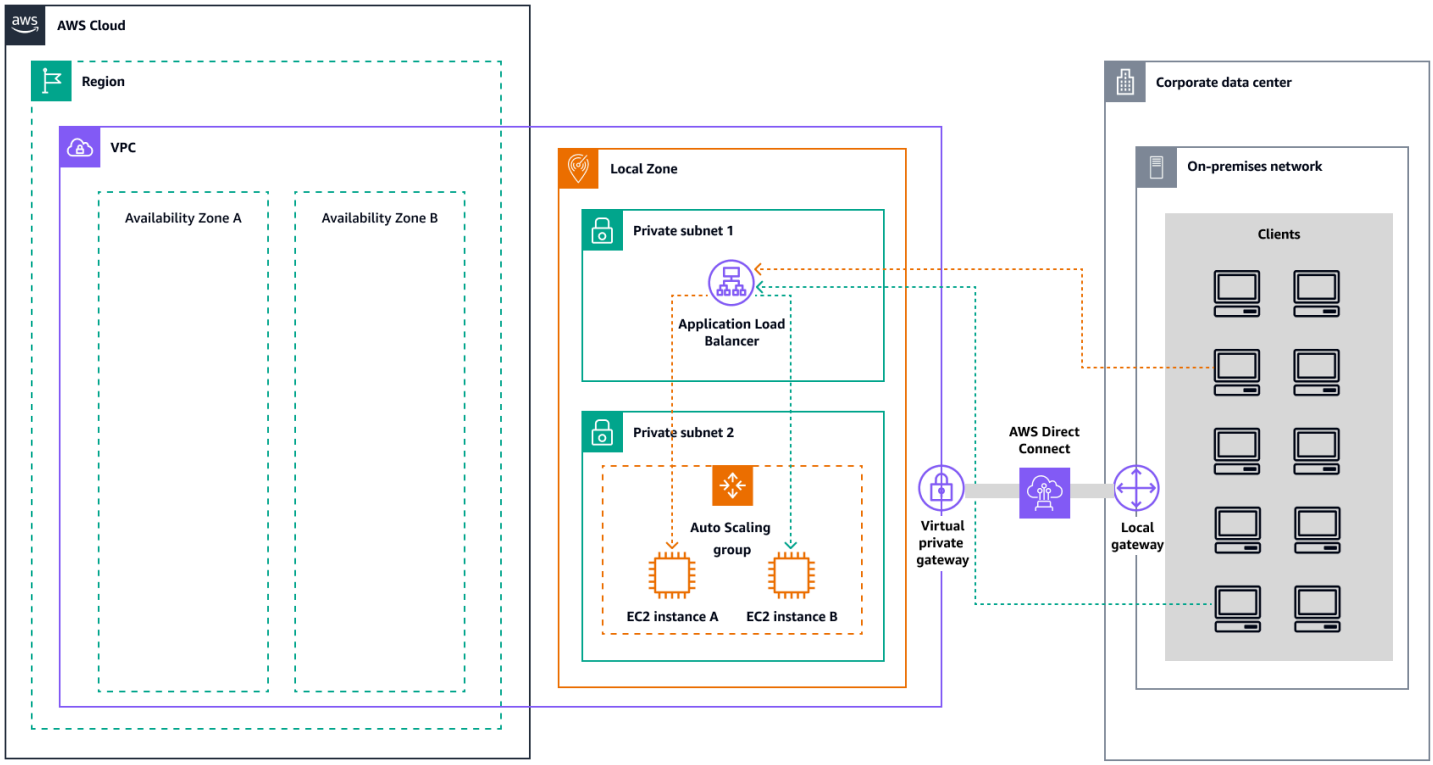


Diagram berikut menggambarkan arsitektur serupa untuk Amazon EC2 di Local Zones.



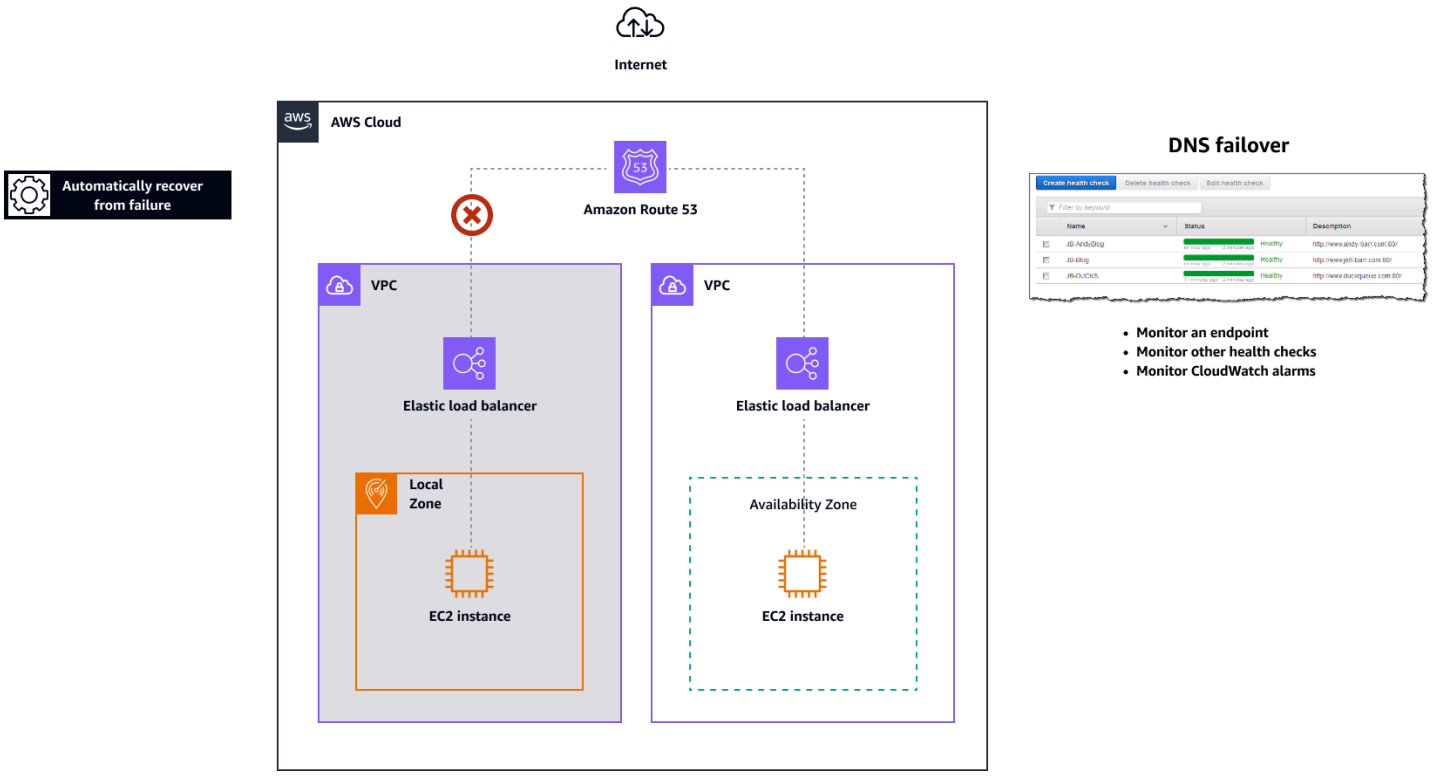
> **Note**
>
> Application Load Balancers tersedia di keduanya AWS Outposts dan Local Zones. Namun, untuk menggunakan Application Load Balancer AWS Outposts, Anda perlu mengukur kapasitas Amazon EC2 untuk menyediakan skalabilitas yang dibutuhkan penyeimbang beban. Untuk informasi lebih lanjut tentang ukuran load balancer AWS Outposts, lihat posting AWS blog Mengonfigurasi Application Load Balancer di. AWS Outposts

Amazon Route 53 untuk failover DNS

Jika Anda memiliki lebih dari satu sumber daya yang menjalankan fungsi yang sama—misalnya, beberapa server HTTP atau mail—Anda dapat mengonfigurasi Amazon Route 53 untuk memeriksa kesehatan sumber daya Anda dan menanggapi kueri DNS hanya dengan menggunakan sumber daya yang sehat. Misalnya, mari kita asumsikan bahwa situs web Anda,`example.com`, dihosting di dua server. Satu server berada di Zona Lokal dan server lainnya berada di Pos Luar. Anda dapat mengonfigurasi Route 53 untuk memeriksa kesehatan server tersebut dan untuk menanggapi kueri DNS `example.com` dengan hanya menggunakan server yang saat ini sehat. Jika Anda menggunakan catatan alias untuk merutekan lalu lintas ke AWS sumber daya yang dipilih,

seperti penyeimbang beban ELB, Anda dapat mengonfigurasi Route 53 untuk mengevaluasi kesehatan sumber daya dan merutekan lalu lintas hanya ke sumber daya yang sehat. Saat Anda mengonfigurasi catatan alias untuk mengevaluasi kesehatan sumber daya, Anda tidak perlu membuat pemeriksaan kesehatan untuk sumber daya tersebut.

Diagram berikut menggambarkan mekanisme failover Route 53.



> **Catatan**
>
> - Jika Anda membuat catatan failover di zona host pribadi, Anda dapat membuat CloudWatch metrik, mengaitkan alarm dengan metrik, dan kemudian membuat pemeriksaan kesehatan yang didasarkan pada aliran data untuk alarm.
> - Untuk membuat aplikasi dapat diakses publik AWS Outposts dengan menggunakan Application Load Balancer, siapkan konfigurasi jaringan yang mengaktifkan Terjemahan Alamat Jaringan Tujuan (DNAT) dari IP publik ke nama domain yang memenuhi syarat (FQDN) penyeimbang beban, dan buat aturan failover Route 53 dengan pemeriksaan kesehatan yang mengarah ke IP publik yang terpapar. Kombinasi ini memastikan akses publik yang andal ke Outposts-hosted aplikasi Anda.

Amazon Route 53 Resolver on AWS Outposts

Amazon Route 53 Resolvertersedia di rak Outposts. Ini menyediakan layanan dan aplikasi lokal Anda dengan resolusi DNS lokal langsung dari Outposts. Titik akhir Resolver Rute 53 Lokal juga mengaktifkan resolusi DNS antara Outposts dan server DNS lokal Anda. Resolver Route 53 di Outposts membantu meningkatkan ketersediaan dan kinerja aplikasi lokal Anda.

Salah satu kasus penggunaan umum untuk Outposts adalah untuk menyebarkan aplikasi yang memerlukan akses latensi rendah ke sistem lokal, seperti peralatan pabrik, aplikasi perdagangan frekuensi tinggi, dan sistem diagnosis medis.

Ketika Anda memilih untuk menggunakan Resolver Route 53 lokal di Outposts, aplikasi dan layanan akan terus mendapat manfaat dari resolusi DNS lokal untuk menemukan layanan lain, bahkan jika konektivitas ke orang tua hilang. Wilayah AWS Local Resolvers juga membantu mengurangi latensi untuk resolusi DNS karena hasil kueri di-cache dan disajikan secara lokal dari Outposts, yang menghilangkan perjalanan pulang-pergi yang tidak perlu ke induk. Wilayah AWS Semua resolusi DNS untuk aplikasi di Outposts VPC yang menggunakan DNS pribadi disajikan secara lokal.

Selain mengaktifkan Resolver lokal, peluncuran ini juga memungkinkan titik akhir Resolver lokal. Titik akhir keluar Route 53 Resolver memungkinkan Resolver Route 53 untuk meneruskan kueri DNS ke resolver DNS yang Anda kelola–misalnya, di jaringan lokal Anda. Sebaliknya, titik akhir masuk Route 53 Resolver meneruskan kueri DNS yang mereka terima dari luar VPC ke Resolver yang berjalan di Outposts. Ini memungkinkan Anda untuk mengirim kueri DNS untuk layanan yang digunakan pada VPC Outposts pribadi dari luar VPC itu. Untuk informasi selengkapnya tentang titik akhir masuk dan keluar, lihat Menyelesaikan kueri DNS antara VPC dan jaringan Anda dalam dokumentasi Route 53.

Perencanaan kapasitas di tepi

Tahap perencanaan kapasitas melibatkan pengumpulan vCPU, memori, dan persyaratan penyimpanan untuk menyebarkan arsitektur Anda. Dalam pilar optimasi biaya dari AWS Well-Architected Framework, ukuran kanan adalah proses berkelanjutan yang dimulai dengan perencanaan. Anda dapat menggunakan AWS alat untuk menentukan pengoptimalan berdasarkan konsumsi sumber daya di dalamnya. AWS

Perencanaan kapasitas tepi di Local Zones sama dengan di Wilayah AWS. Anda harus memeriksa untuk memastikan bahwa instance Anda tersedia di setiap Zona Lokal, karena beberapa jenis instance mungkin berbeda dari tipe di Wilayah AWS. Untuk Outposts, Anda harus merencanakan kapasitas berdasarkan kebutuhan beban kerja Anda. Outposts ditempatkan dengan jumlah instans

tetap per host dan dapat di-relotting sesuai kebutuhan. Jika beban kerja Anda membutuhkan kapasitas cadangan, pertimbangkan hal itu ketika Anda merencanakan kebutuhan kapasitas Anda.

Perencanaan kapasitas di Outposts

AWS Outposts perencanaan kapasitas memerlukan input khusus untuk ukuran kanan Regional, ditambah faktor spesifik tepi yang mempengaruhi ketersediaan aplikasi, kinerja, dan pertumbuhan. Untuk panduan terperinci, lihat Perencanaan kapasitas di AWS whitepaper Pertimbangan Desain dan Arsitektur Ketersediaan AWS Outposts Tinggi.

Perencanaan Kapasitas untuk Local Zones

Zona Lokal adalah perpanjangan dari Wilayah AWS yang secara geografis dekat dengan pengguna Anda. Sumber daya yang dibuat di Zona Lokal dapat melayani pengguna lokal dengan komunikasi latensi sangat rendah. Untuk mengaktifkan Zona Lokal di Anda Akun AWS, tinjau Memulai AWS Local Zones dalam AWS dokumentasi. Setiap Zona Lokal memiliki slotting berbeda yang tersedia untuk keluarga contoh. EC2 Validasi instance yang tersedia di setiap Zona Lokal sebelum Anda menggunakannya. Untuk mengonfirmasi EC2 instance yang tersedia, jalankan AWS CLI perintah berikut:

```
aws ec2 describe-instance-type-offerings \
--location-type "availability-zone" \
--filters Name=location,Values=<local-zone-name>
```

Keluaran yang diharapkan

```
{
  "InstanceTypeOfferings": [
      {
          "InstanceType": "m5.2xlarge",
          "LocationType": "availability-zone",
          "Location": "<local-zone-name>"
      },
      {
          "InstanceType": "t3.micro",
          "LocationType": "availability-zone",
          "Location": "local.zone-name"
      },
      ...
  ]
```

```
}
```

Manajemen infrastruktur tepi

AWS menyediakan layanan terkelola penuh yang memperluas AWS infrastruktur, layanan APIs, dan alat lebih dekat ke pengguna akhir dan pusat data Anda. Layanan yang tersedia di Outposts dan Local Zones sama dengan yang tersedia di Wilayah AWS, sehingga Anda dapat mengelola layanan tersebut dengan menggunakan AWS konsol yang sama AWS CLI, atau. AWS APIs Untuk layanan yang didukung, lihat tabel perbandingan AWS Outposts fitur dan AWS Local Zones fitur.

Menyebarkan layanan di tepi

Anda dapat mengonfigurasi layanan yang tersedia di Local Zones dan Outposts dengan cara yang sama seperti Anda mengonfigurasinya Wilayah AWS: dengan menggunakan AWS konsol, AWS CLI, atau. AWS APIs Perbedaan utama antara penyebaran Regional dan edge adalah subnet tempat sumber daya akan disediakan. Bagian Networking at the edge menjelaskan bagaimana subnet digunakan di Outposts dan Local Zones. Setelah Anda mengidentifikasi subnet tepi, Anda menggunakan ID subnet tepi sebagai parameter untuk menyebarkan layanan di Outposts atau Local Zones. Bagian berikut memberikan contoh penerapan layanan edge.

Amazon EC2 di tepi

`run-instances`Contoh berikut meluncurkan satu instance tipe `m5.2xlarge` ke subnet tepi untuk Wilayah saat ini. Key pair bersifat opsional jika Anda tidak berencana untuk terhubung ke instans Anda dengan menggunakan SSH di Linux atau remote desktop protocol (RDP) pada Windows.

```
aws ec2 run-instances \
    --image-id ami-id \
    --instance-type m5.2xlarge \
    --subnet-id <subnet-edge-id> \
    --key-name MyKeyPair
```

Aplikasi Load Balancer di tepi

`create-load-balancer`Contoh berikut membuat Application Load Balancer internal dan memungkinkan Local Zones atau Outposts untuk subnet yang ditentukan.

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
```

```
    --scheme internal \
    --subnets <subnet-edge-id>
```

Untuk menerapkan Application Load Balancer yang menghadap ke internet ke subnet di Outpost, Anda menetapkan tanda di opsi dan memberikan `internet-facing` ID kumpulan CoIP, seperti yang ditunjukkan dalam `--scheme` contoh ini:

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internet-facing \
    --customer-owned-ipv4-pool <coip-pool-id>
    --subnets <subnet-edge-id>
```

Untuk informasi tentang penerapan layanan lain di edge, ikuti tautan ini:

Layanan	AWS Outposts	AWS Local Zones
Amazon EKS	Menerapkan Amazon EKS lokal dengan AWS Outposts	Luncurkan cluster EKS latensi rendah dengan AWS Local Zones
Amazon ECS	Amazon ECS aktif AWS Outposts	Aplikasi Amazon ECS di subnet bersama, Local Zones, dan Wavelength Zones
Amazon RDS	Amazon RDS aktif AWS Outposts	Pilih subnet Zona Lokal
Amazon S3	Memulai Amazon S3 di Outposts	Tidak tersedia
Amazon ElastiCache	Menggunakan Outposts dengan ElastiCache	Menggunakan Local Zones dengan ElastiCache
Amazon EMR	Cluster EMR aktif AWS Outposts	Cluster EMR aktif AWS Local Zones
Amazon FSx	Tidak tersedia	Pilih subnet Zona Lokal

Layanan	AWS Outposts	AWS Local Zones
AWS Elastic Disaster Recovery	Bekerja dengan AWS Elastic Disaster Recovery dan AWS Outposts	Tidak tersedia
AWS Transform MGN	Tidak tersedia	Pilih subnet Zona Lokal sebagai subnet pementasan

CLI dan SDK khusus Outpost

AWS Outposts memiliki dua kelompok perintah dan APIs untuk membuat urutan layanan atau memanipulasi tabel routing antara gateway lokal dan jaringan lokal Anda.

Proses pemesanan Outposts

Anda dapat menggunakan AWS CLIatau Outposts APIs untuk membuat situs Outposts, untuk membuat Outpost, dan untuk membuat pesanan Outposts. Kami menyarankan Anda bekerja dengan spesialis cloud hybrid selama proses AWS Outposts pemesanan Anda untuk memastikan pemilihan sumber daya yang tepat IDs dan konfigurasi optimal untuk kebutuhan implementasi Anda. Untuk daftar ID sumber daya lengkap, lihat halaman harga AWS Outposts rak.

Manajemen gateway lokal

Manajemen dan pengoperasian gateway lokal (LGW) di Outposts membutuhkan pengetahuan tentang perintah AWS CLI dan SDK yang tersedia untuk tugas ini. Anda dapat menggunakan AWS CLI dan AWS SDKs untuk membuat dan memodifikasi rute LGW, di antara tugas-tugas lainnya. Untuk informasi selengkapnya tentang mengelola LGW, lihat sumber daya berikut:

- AWS CLI untuk Amazon EC2
- EC2.Klien di AWS SDK for Python (Boto)
- Ec2Client di AWS SDK untuk Java

CloudWatch metrik dan log

Untuk Layanan AWS itu tersedia di Outposts dan Local Zones, metrik dan log dikelola dengan cara yang sama seperti di Wilayah. Amazon CloudWatch menyediakan metrik yang didedikasikan untuk memantau Outposts dalam dimensi berikut:

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

Untuk informasi selengkapnya, lihat CloudWatch metrik untuk rak Outposts di dokumentasi Outposts.

Sumber daya

AWS referensi

- Hybrid Cloud dengan AWS
- AWS Outposts Panduan Pengguna untuk rak Outposts
- Panduan Pengguna AWS Local Zones
- AWS Outposts Keluarga
- AWS Local Zones
- Memperluas VPC ke Zona Lokal, Zona Wavelength, atau Pos Luar (dokumentasi Amazon VPC)
- Instans Linux di Local Zones (EC2 dokumentasi Amazon)
- Instans Linux di Outposts (dokumentasi Amazon EC2)
- Mulai Menerapkan Aplikasi Latensi Rendah dengan AWS Local Zones(tutorial)

AWS posting blog

- Menjalankan AWS infrastruktur di tempat dengan Amazon EC2
- Membangun aplikasi modern dengan Amazon EKS di Amazon EC2
- Cara memilih antara mode perutean CoIP dan VPC langsung di rak Amazon EC2
- Memilih sakelar jaringan untuk Amazon Anda EC2
- Mempertahankan salinan lokal data Anda di AWS Local Zones
- Amazon ECS di Amazon EC2
- Mengelola mesh layanan edge-aware dengan Amazon EKS untuk AWS Local Zones
- Menerapkan perutean ingress gateway lokal di Amazon EC2
- Mengotomatiskan penerapan beban kerja Anda di AWS Local Zones
- Berbagi Amazon EC2 di AWS lingkungan multi akun: Bagian 1
- Berbagi Amazon EC2 di AWS lingkungan multi akun: Bagian 2
- AWS Direct Connect dan pola AWS Local Zones interoperabilitas
- Terapkan Amazon RDS di Amazon EC2 dengan ketersediaan tinggi Multi-AZ

Kontributor

Individu-individu berikut berkontribusi pada panduan ini.

Mengotorisasi

- Leonardo Solano, Arsitek Solusi Cloud Hibrida Utama, AWS
- Len Gomes, Arsitek Solusi Mitra, AWS
- Matt Price, Insinyur Dukungan Perusahaan Senior, AWS
- Tom Gadomski, Arsitek Solusi, AWS
- Obed Gutierrez, Arsitek Solusi, AWS
- Dionysios Kakaletris, Manajer Akun Teknis, AWS
- Vamsi Krishna, Spesialis Utama Outposts, AWS

Meninjau

- David Filiatrault, Konsultan Pengiriman, AWS

Penulisan teknis

- Handan Selamoglu, Manajer Dokumentasi Sr., AWS

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	Juni 10, 2025

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