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

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 di. 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 Zone 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:

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 Zone. 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 Zone 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 AWS Enterprise On-Ramp.

AWS Local Zone

- Zona AWS Lokal harus tersedia dekat dengan pusat data atau pengguna Anda. Lihat AWS Local Zone lokasi.
- Konfirmasikan bahwa Anda memiliki konektivitas jaringan dari infrastruktur lokal ke Zona Lokal:
  - Opsi 1: AWS Direct Connect Tautan dari pusat data Anda ke AWS 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 Zone

- 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 AWS 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 Zone 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}]
```

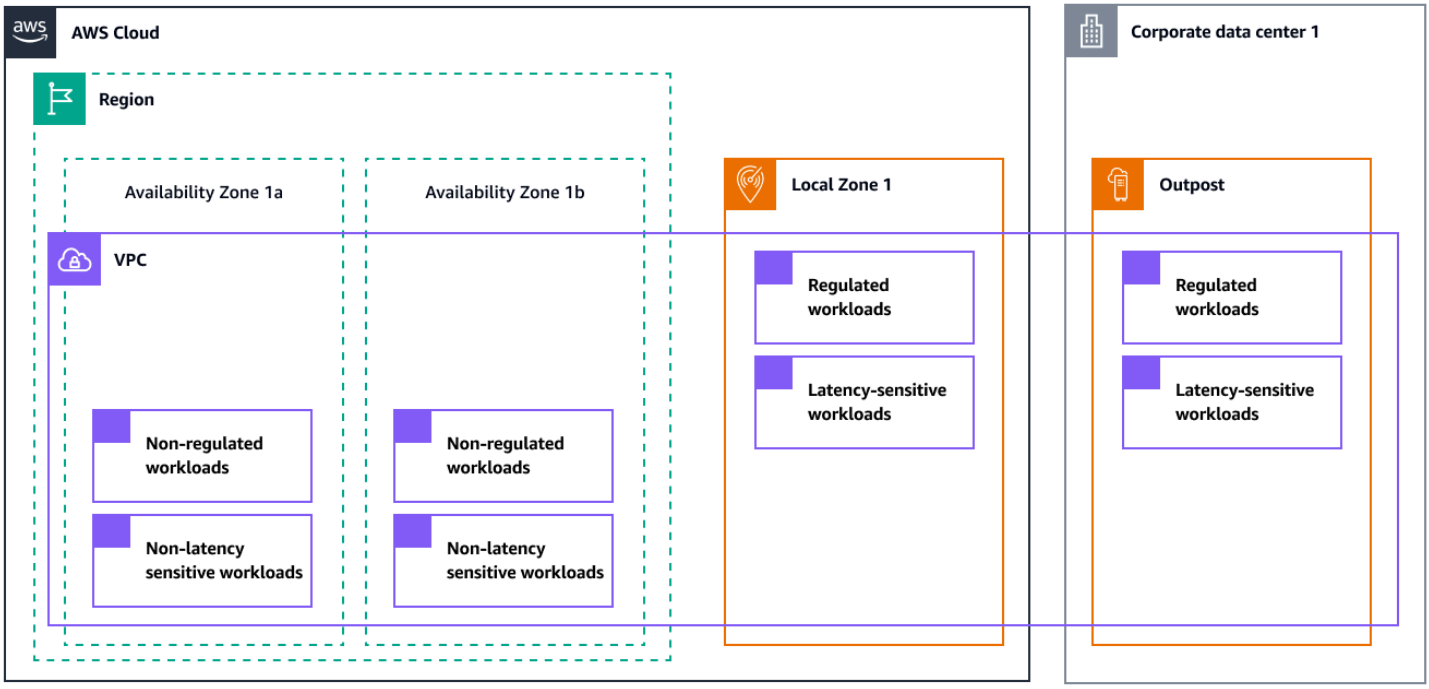
  Lihat informasi yang lebih lengkap dalam dokumentasi AWS Outposts.

- 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.

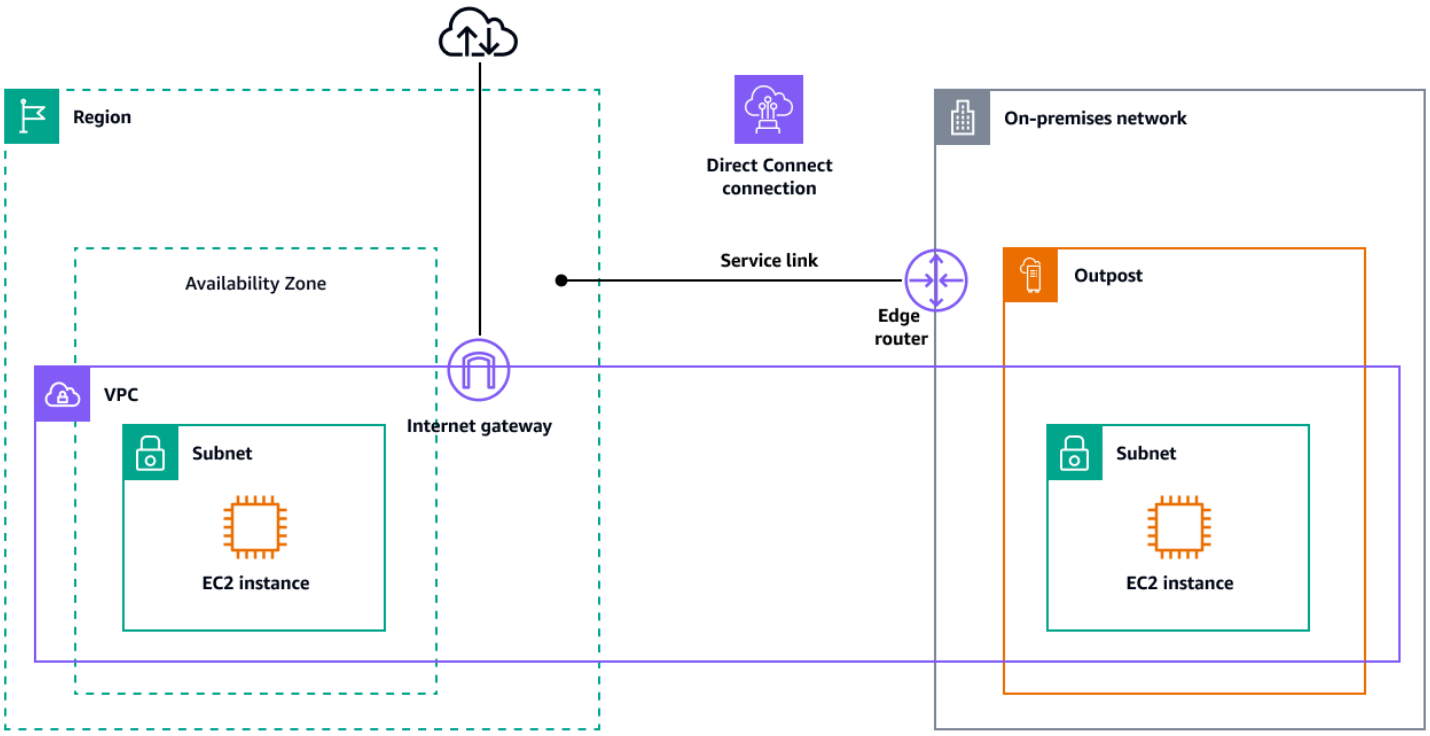


Lalu lintas Edge ke Region

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 AWS Direct Connect publik (VIF publik), atau melalui antarmuka virtual AWS 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 EC2 instans Amazon, melampirkan volume Amazon EBS, dan mengakses Layanan AWS seperti Amazon EKS, Amazon EMR, dan metrik 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 AWS 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 EC2 instance AWS Outposts dan EC2 instance 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 untuk terhubung dengan mulus ke berbagai layanan Regional melalui perangkat yang sama APIs dan alat.

Tabel berikut menunjukkan opsi koneksi dan terkait MTUs.

Dari	Untuk	MTU
Amazon EC2 di Wilayah	Amazon EC2 di Local Zones	1.300 byte
AWS Direct Connect	Local Zones	1.468 byte
gateway internet	Local Zones	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.

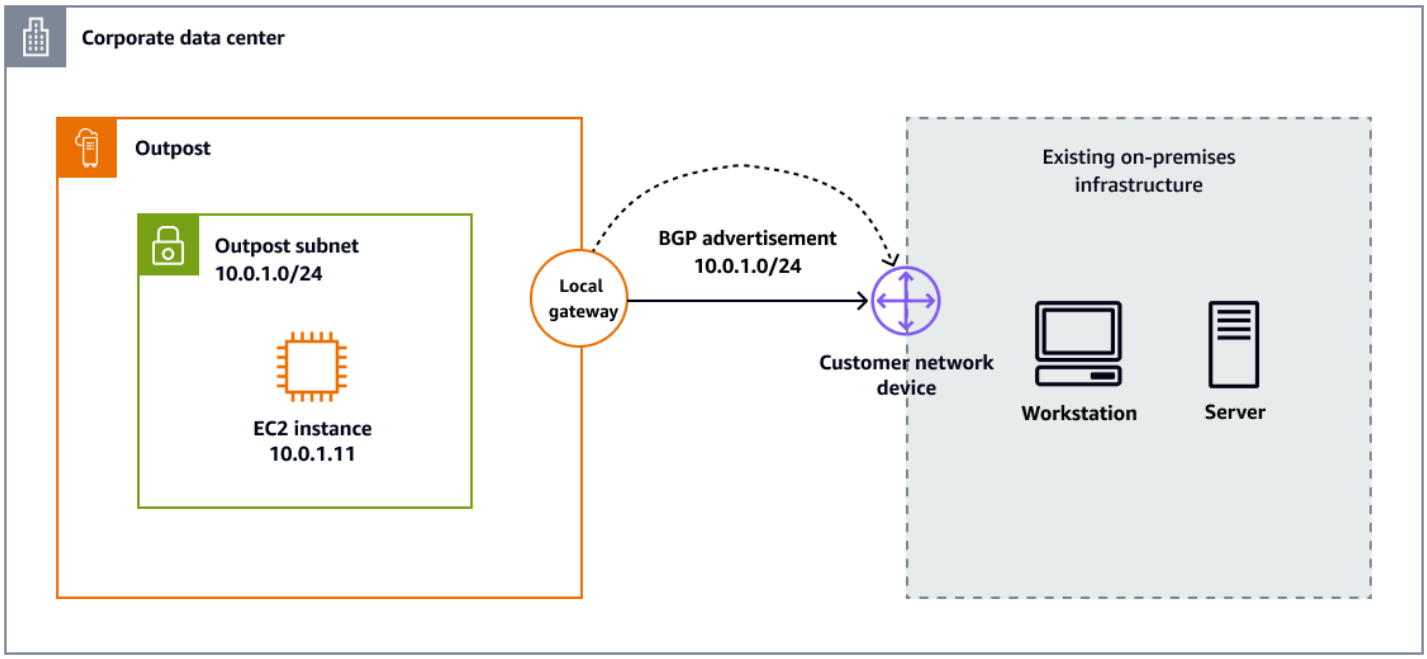
Edge ke lalu lintas lokal

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.

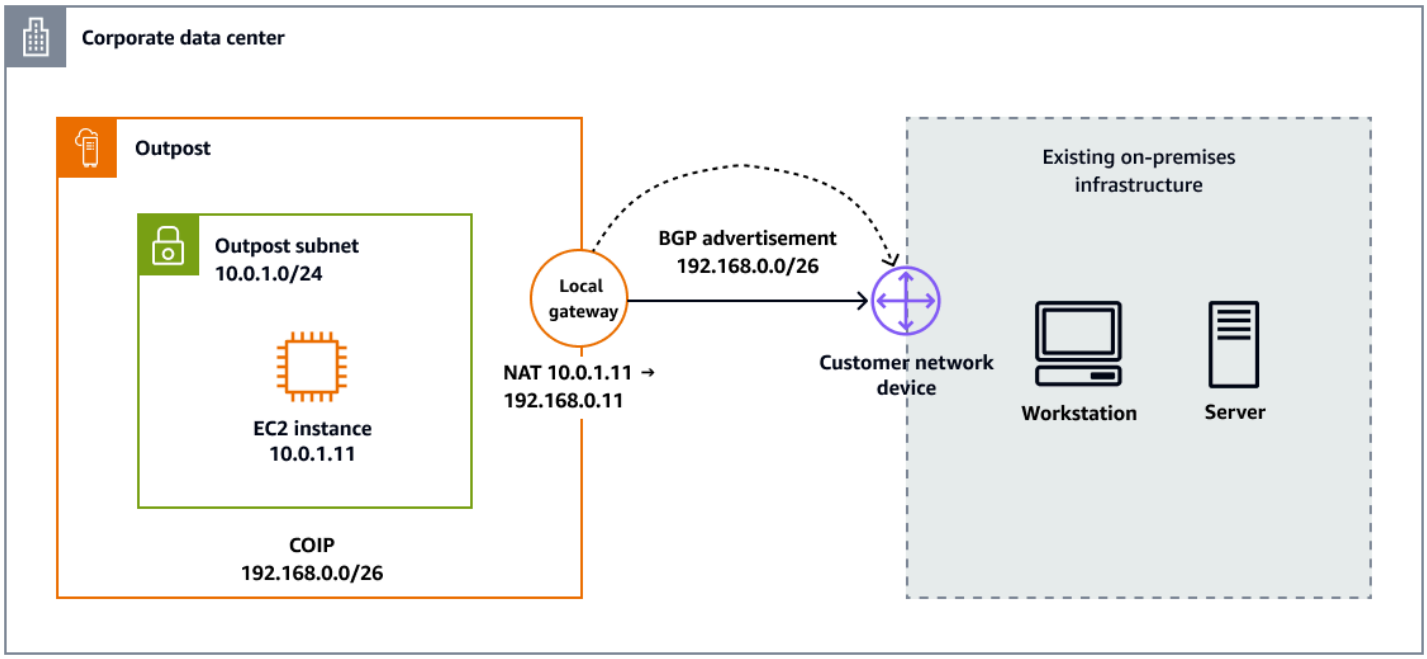
AWS Outposts gerbang lokal

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 Anda. EC2 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 EC2 instance, 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 beban kerja yang EC2 dihosting Amazon di Zona Lokal ke internet, Anda dapat mengaktifkan opsi Auto-assign Public IP saat meluncurkan instance. 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 Elastis, Anda dapat mengaitkan salah satu sumber daya ini dengan EC2 instance 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 AWS Direct Connect

Local Zones juga mendukung AWS 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 VPCs 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. Pengintip VPC dapat dibuat antara VPCs yang diperluas ke

Local Zones. Ketika peered VPCs 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 hal ini 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. Auditor pihak ketiga 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 Zone. 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 pada saat tidak aktif

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 Zone FAQ (lihat pertanyaan: Apa perilaku enkripsi default volume EBS di Local Zones?), kecuali enkripsi diaktifkan untuk akun.

Enkripsi di Amazon S3 di Outposts

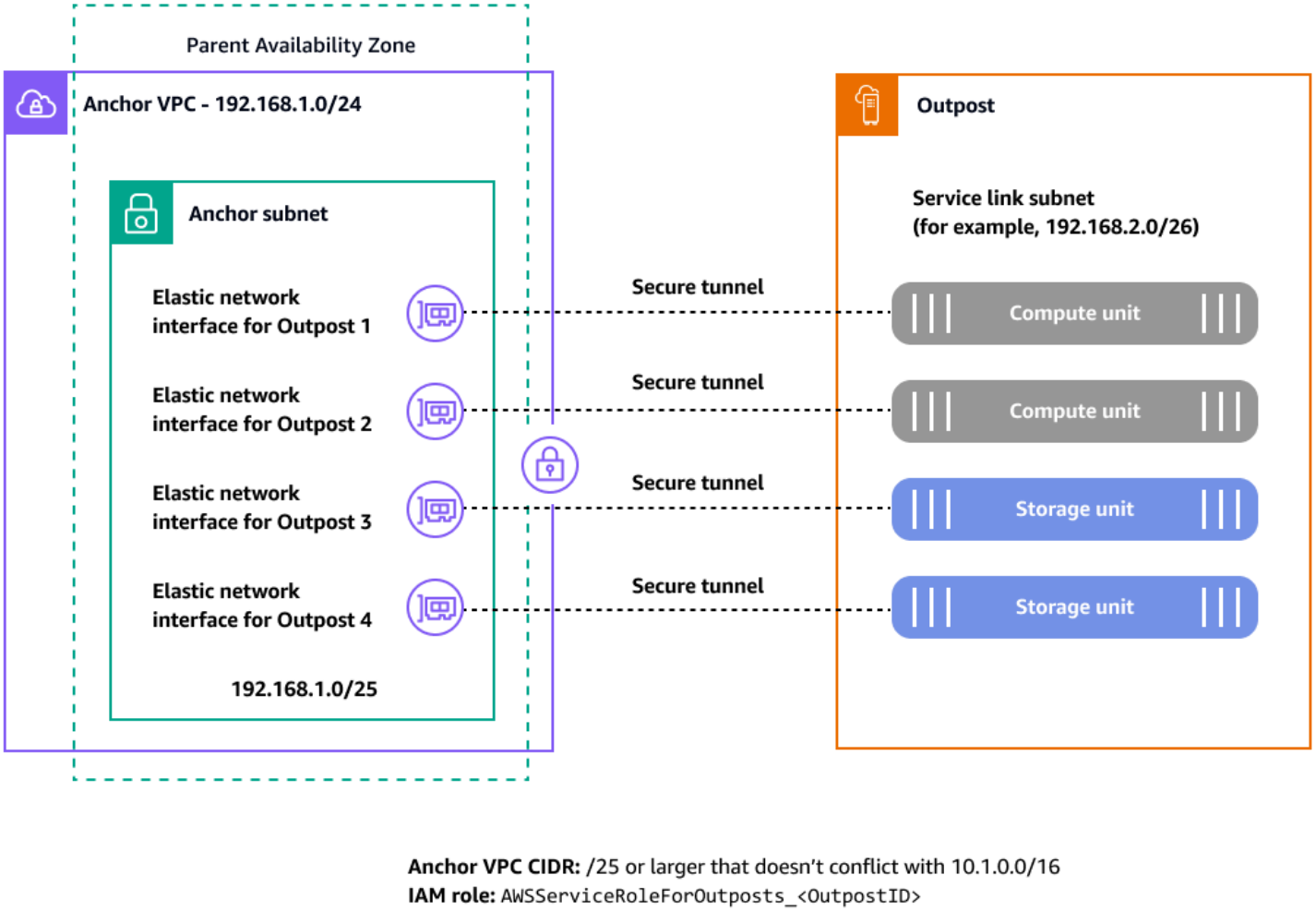
Secara default, semua data yang disimpan dalam Amazon S3 di Outposts dienkripsi menggunakan enkripsi di sisi server dengan kunci enkripsi yang dikelola Amazon S3 (SSE-S3). Anda juga dapat menggunakan enkripsi di sisi server dengan kunci enkripsi yang disediakan pelanggan (SSE-C). Untuk menggunakan SSE-C,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

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

Enkripsi dalam transit

Untuk AWS Outposts, tautan layanan adalah koneksi yang diperlukan antara server Outposts Anda dan pilihan Anda 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 AWS 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.

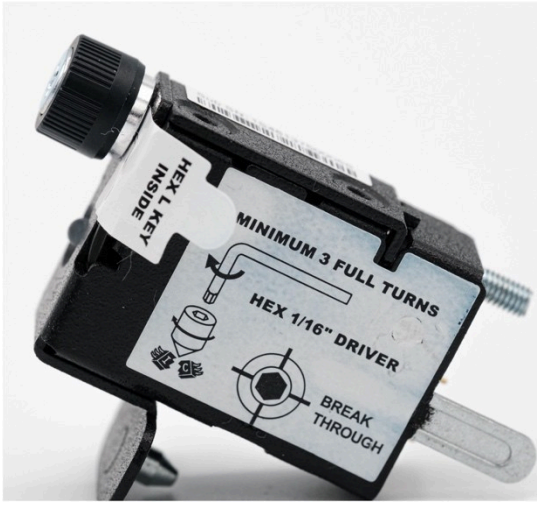
Protokol	Port sumber	Alamat sumber	Pelabuhan tujuan	Alamat tujuan
UDP	443	AWS Outposts tautan layanan/26	443	AWS Outposts Rute umum wilayah atau

Protokol	Port sumber	Alamat sumber	Pelabuhan tujuan	Alamat tujuan
				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 yang sedang transit antara lokasi lokal dan AWS Direct Connect PoPs untuk mengakses Zona Lokal, Anda dapat mengaktifkan MAC Security (MACsec) antara router atau switch lokal dan titik akhir. AWS Direct Connect Untuk informasi selengkapnya, lihat posting AWS blog Menambahkan MACsec keamanan ke AWS Direct Connect koneksi.

Penghapusan data

Saat Anda menghentikan atau menghentikan EC2 instance AWS Outposts, memori yang dialokasikan untuk itu 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
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Ya*
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
Daftar kontrol akses (ACLs)	Tidak
Kontrol akses berbasis atribut (ABAC) (tag dalam kebijakan)	Ya

Fitur IAM	AWS Outposts dukungan
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Peran terkait layanan	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 defense-in-depth pendekatan untuk lalu lintas masuk dan keluar. Ini termasuk penggunaan kelompok keamanan (firewall inspeksi stateful), jaringan, subnet ACLs, 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 EC2 instance, 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 EC2 instans, 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.

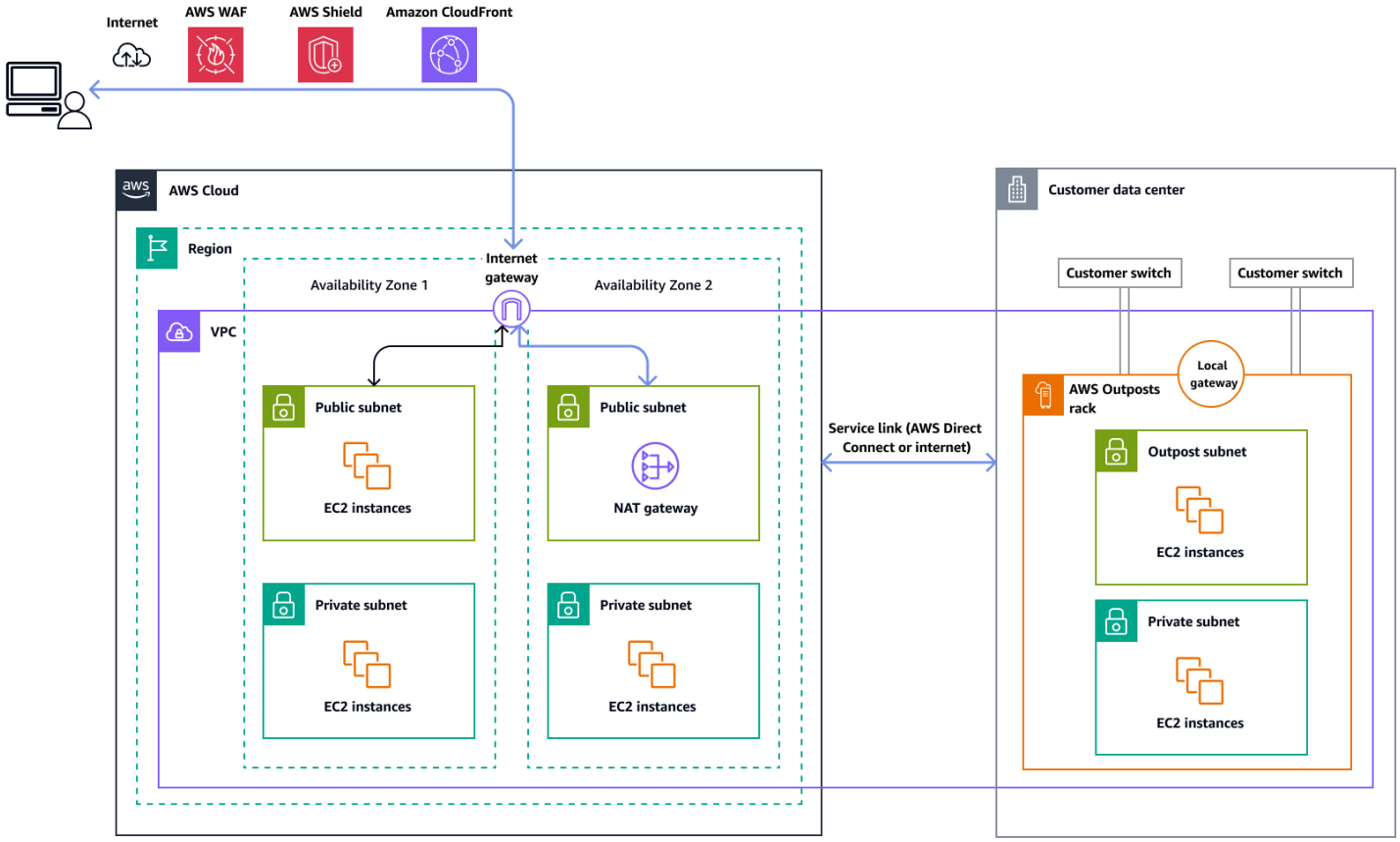
Local Zones mengadopsi konstruksi jaringan yang disebut grup perbatasan jaringan, yang digunakan dalam. Wilayah AWS AWS mengiklankan alamat IP publik dari grup unik ini. Grup perbatasan jaringan terdiri dari Availability Zones, Local Zones, atau Wavelength Zones. Anda dapat secara eksplisit mengalokasikan 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 ISVs dan membantu Anda membangun lapisan inspeksi di Zona Lokal Anda, seperti yang dijelaskan dalam posting AWS blog Arsitektur inspeksi hibrida dengan AWS Local Zone.

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 diarahkan 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

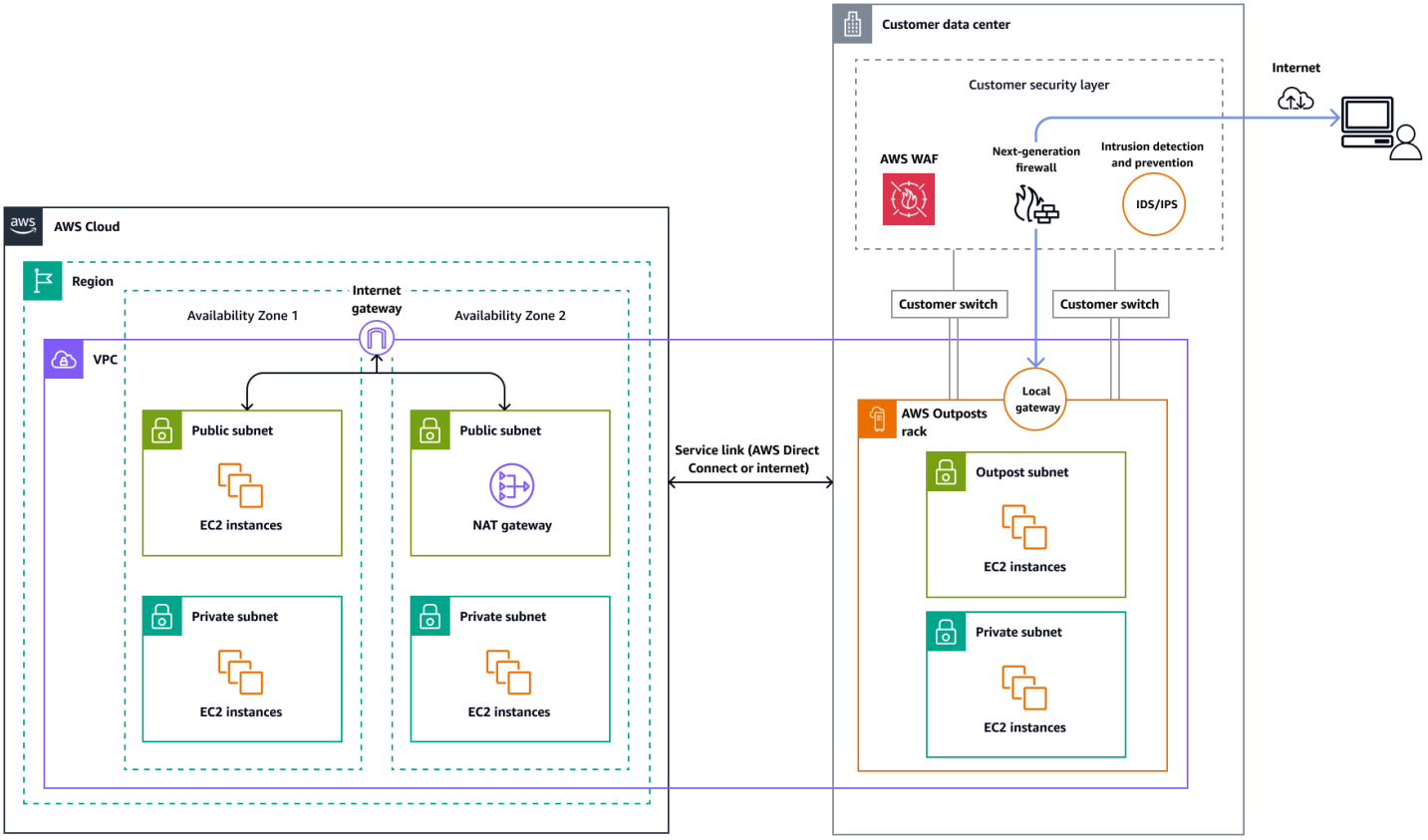
Diagram berikut menunjukkan lalu lintas antara beban kerja dalam AWS Outposts instance dan internet melalui induk Wilayah AWS.



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

- Praktik terbaik untuk mengelola residensi data dalam AWS Local Zone 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 Framework)

Berbagi sumber daya 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 Akun AWS dalam organisasi Anda AWS . Hal ini memungkinkan konsumen lain untuk menggunakan situs Outpost, mengkonfigurasi VPCs, dan meluncurkan dan menjalankan instance di Outpost bersama.

Sumber daya yang dapat dibagikan AWS Outposts adalah:

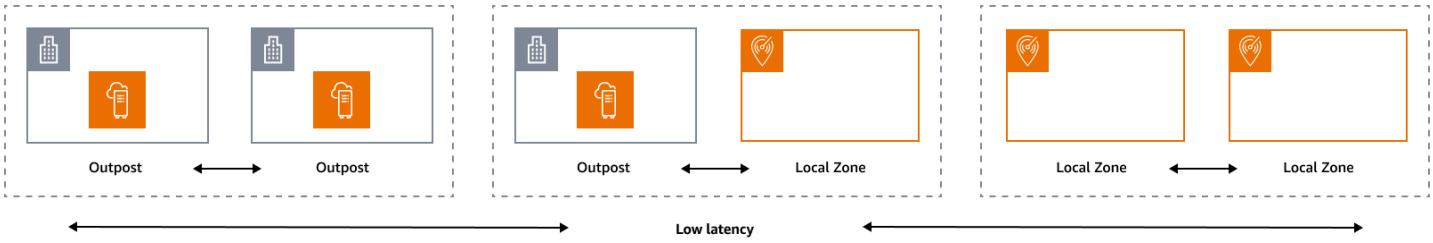
- Host khusus yang dialokasikan
- Reservasi kapasitas
- Kumpulan alamat IP (CoIP) milik pelanggan
- Tabel rute gateway lokal
- Outposts
- Amazon S3 on Outposts
- Situs
- Subnet

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 mendesain 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 Zone 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.

Local Zones

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 EC2 instance. 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,, Layanan AWS APIs, 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 arsitektur multi-AZ 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
```

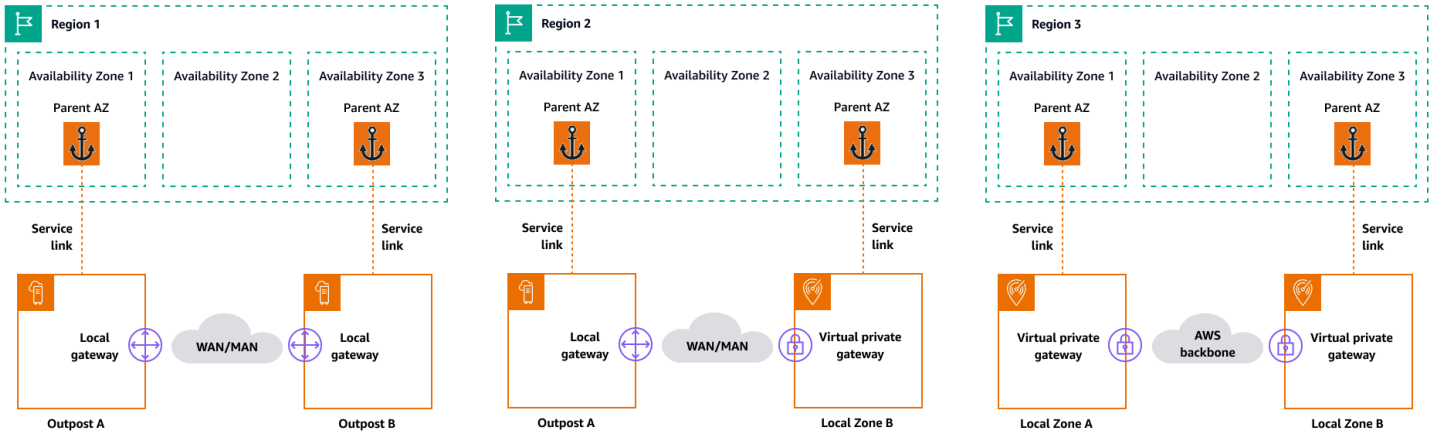
Output dari perintah sebelumnya:

```
{     "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.

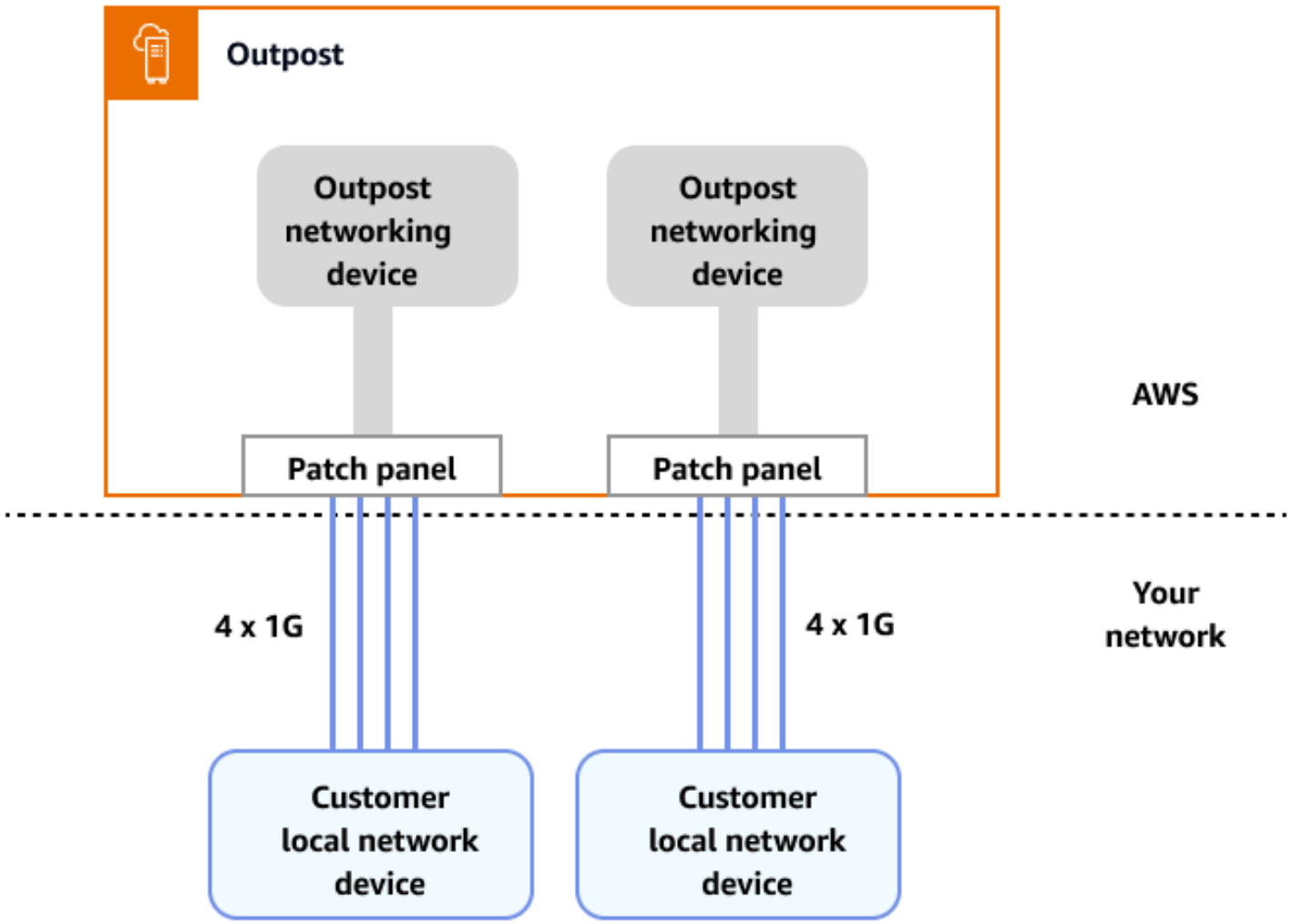
Jaringan ketahanan untuk Local Zones

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 AWS 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 AWS Direct Connect, arsitektur ketahanan yang berlaku sama dengan yang digunakan untuk mengakses, seperti yang didokumentasikan dalam Wilayah AWS rekomendasi ketahanan.AWS Direct Connect Namun, ada skenario yang sebagian besar berlaku untuk Local Zones internasional. Di negara di mana Zona Lokal diaktifkan, hanya memiliki satu AWS Direct Connect PoP membuat tidak mungkin untuk membuat arsitektur yang direkomendasikan untuk AWS Direct Connect ketahanan. Jika Anda hanya memiliki akses ke satu AWS Direct Connect lokasi atau memerlukan ketahanan di luar satu koneksi, Anda dapat membuat alat VPN di Amazon EC2 dan AWS Direct Connect, seperti yang diilustrasikan dan dibahas dalam posting AWS blog Mengaktifkan konektivitas yang sangat tersedia dari tempat ke lokasi. AWS Local Zone

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 (). ONDs 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 AWS Direct Connect atau koneksi internet untuk tautan layanan. Minimum ini memungkinkan Anda meluncurkan EC2 instans, melampirkan volume EBS, dan mengakses Layanan AWS, seperti Amazon EKS, Amazon EMR, dan metrik. CloudWatch

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

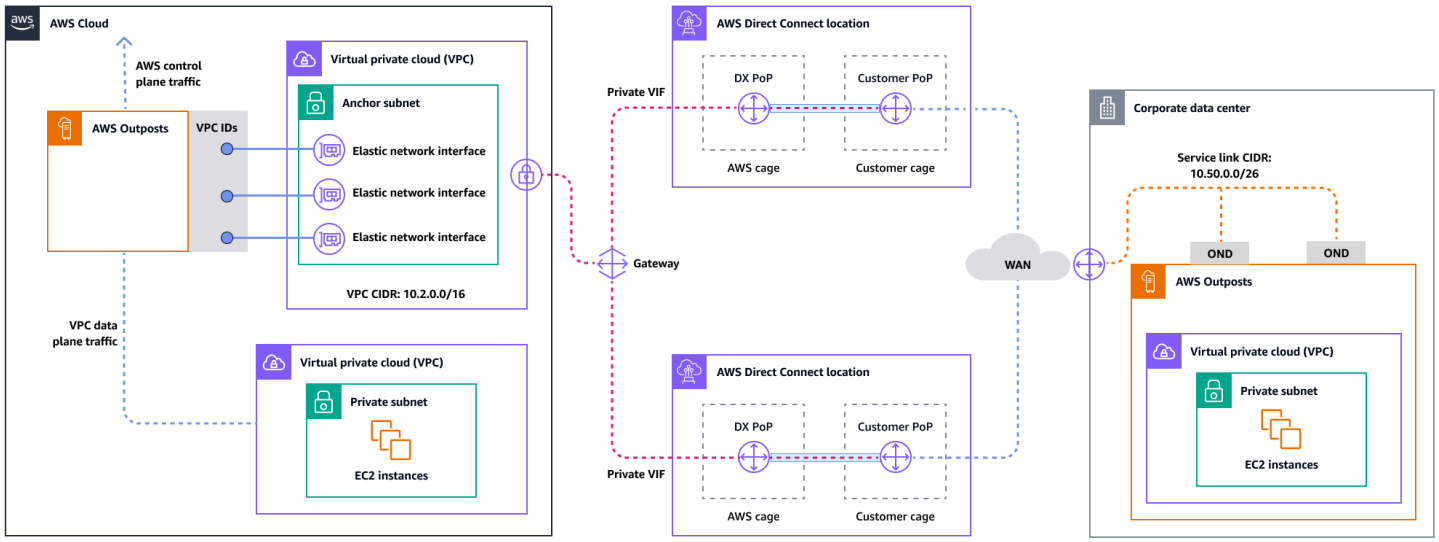
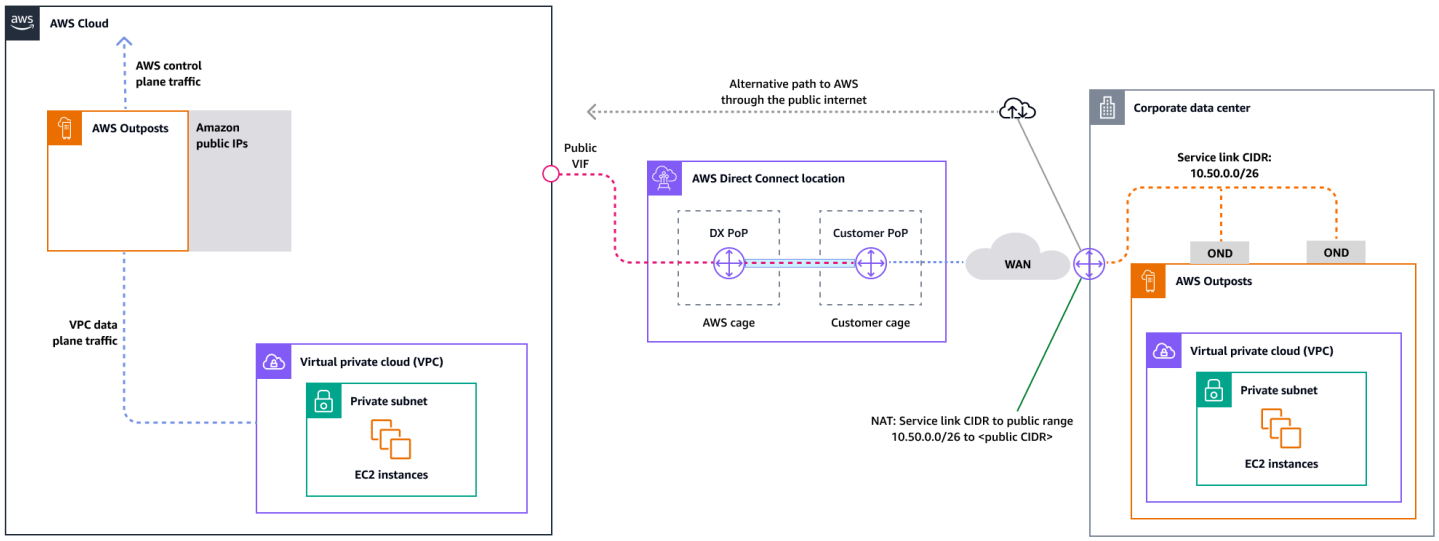


Diagram berikut menggambarkan arsitektur ini untuk koneksi publik yang sangat tersedia.



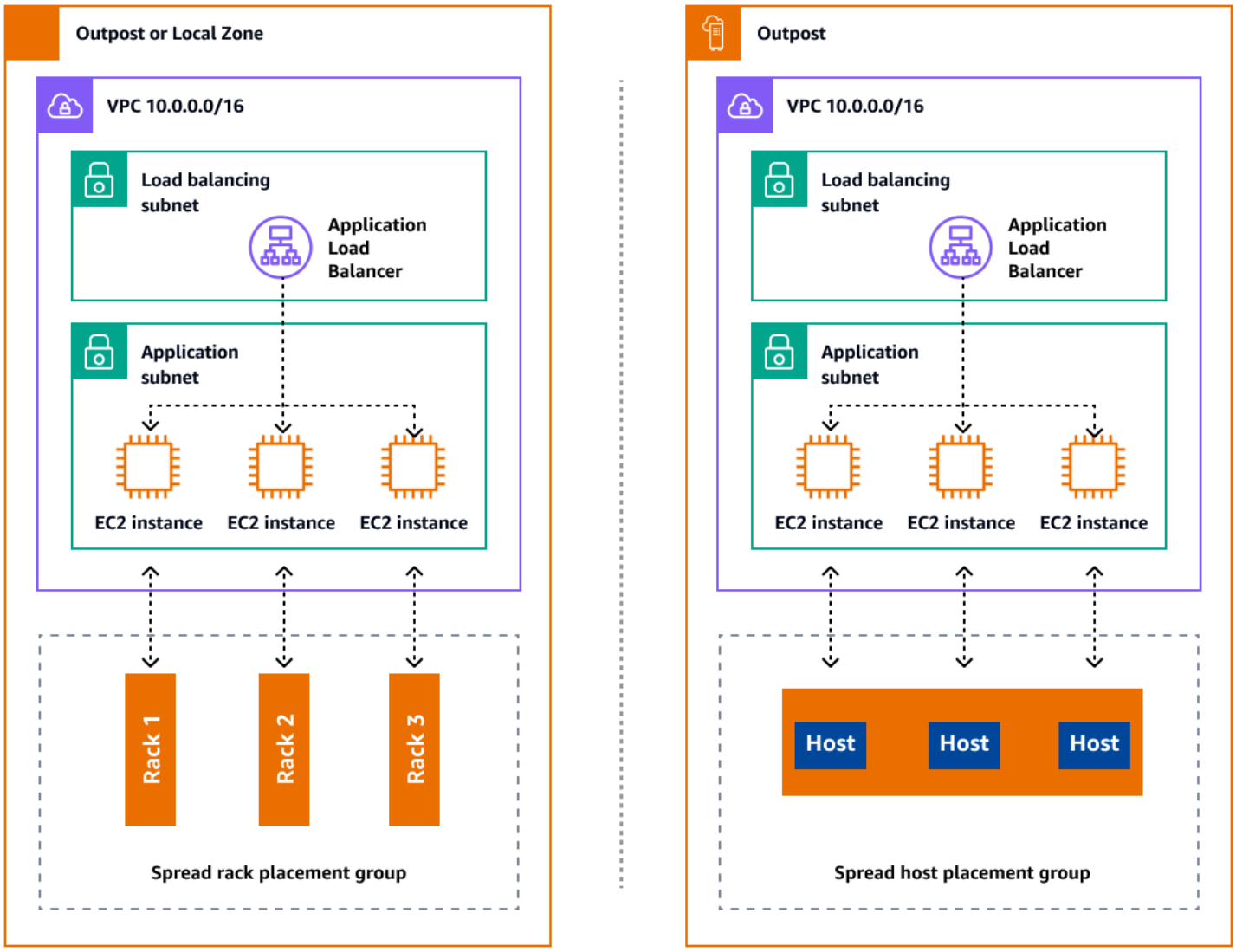
Menskalakan penyebaran rak Outposts dengan rak ACE

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.



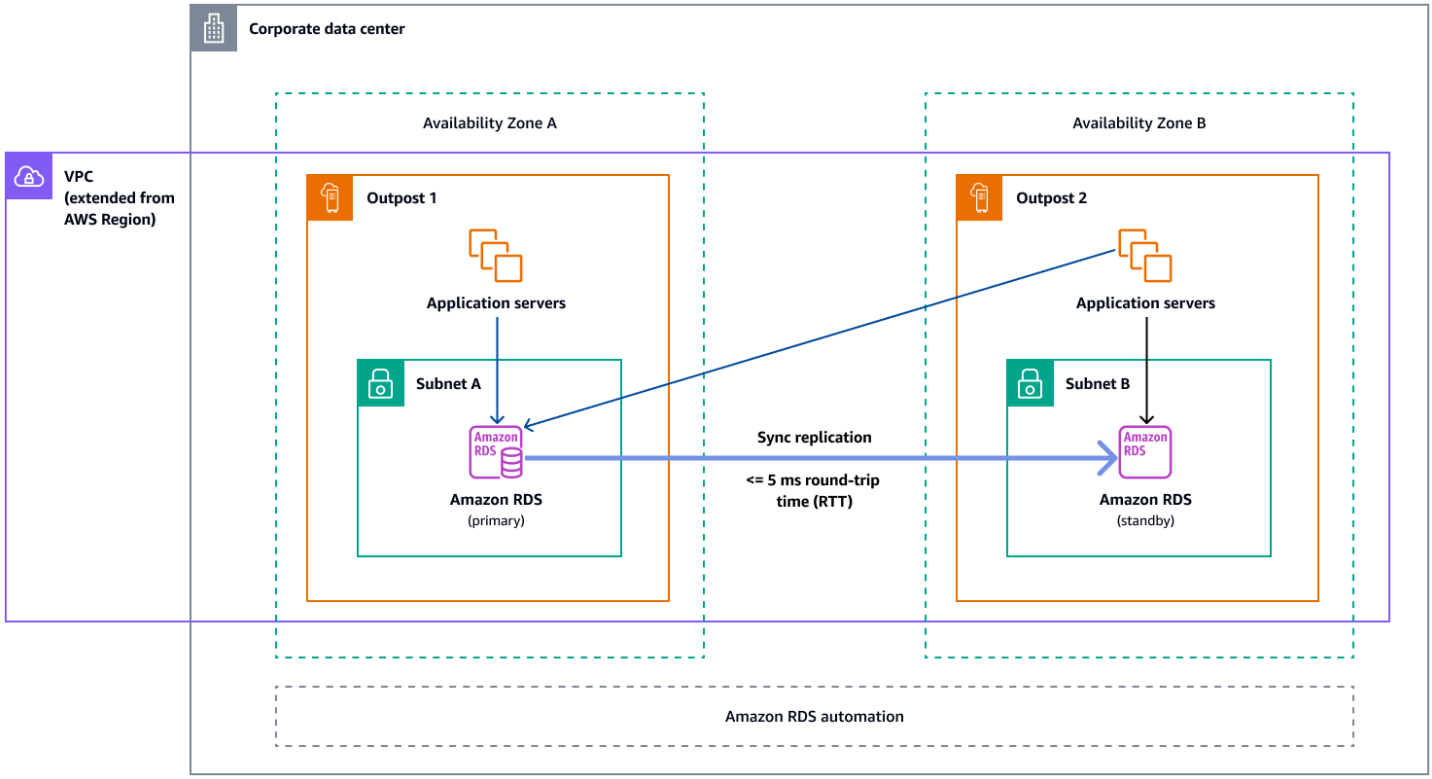
Amazon RDS Multi-AZ di AWS Outposts

Saat Anda menggunakan penerapan instans Multi-AZ di Outposts, Amazon RDS membuat dua instance database di dua Outpost. 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 penerapan multi-AZ, Amazon RDS membuat instans DB utama di satu Pos Luar dan mereplikasi data secara sinkron ke instans DB siaga di Pos Luar yang berbeda. Penerapan multi-AZ di Outposts beroperasi seperti penerapan Multi-AZ di, dengan perbedaan berikut: Wilayah AWS

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

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

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 EC2 instance yang 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. Bila Anda menggunakan ELB dengan grup Auto Scaling Anda, Anda tidak perlu mendaftarkan instans EC2 individual dengan load balancer. 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 Auto EC2 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 EC2 Amazon. AWS Outposts

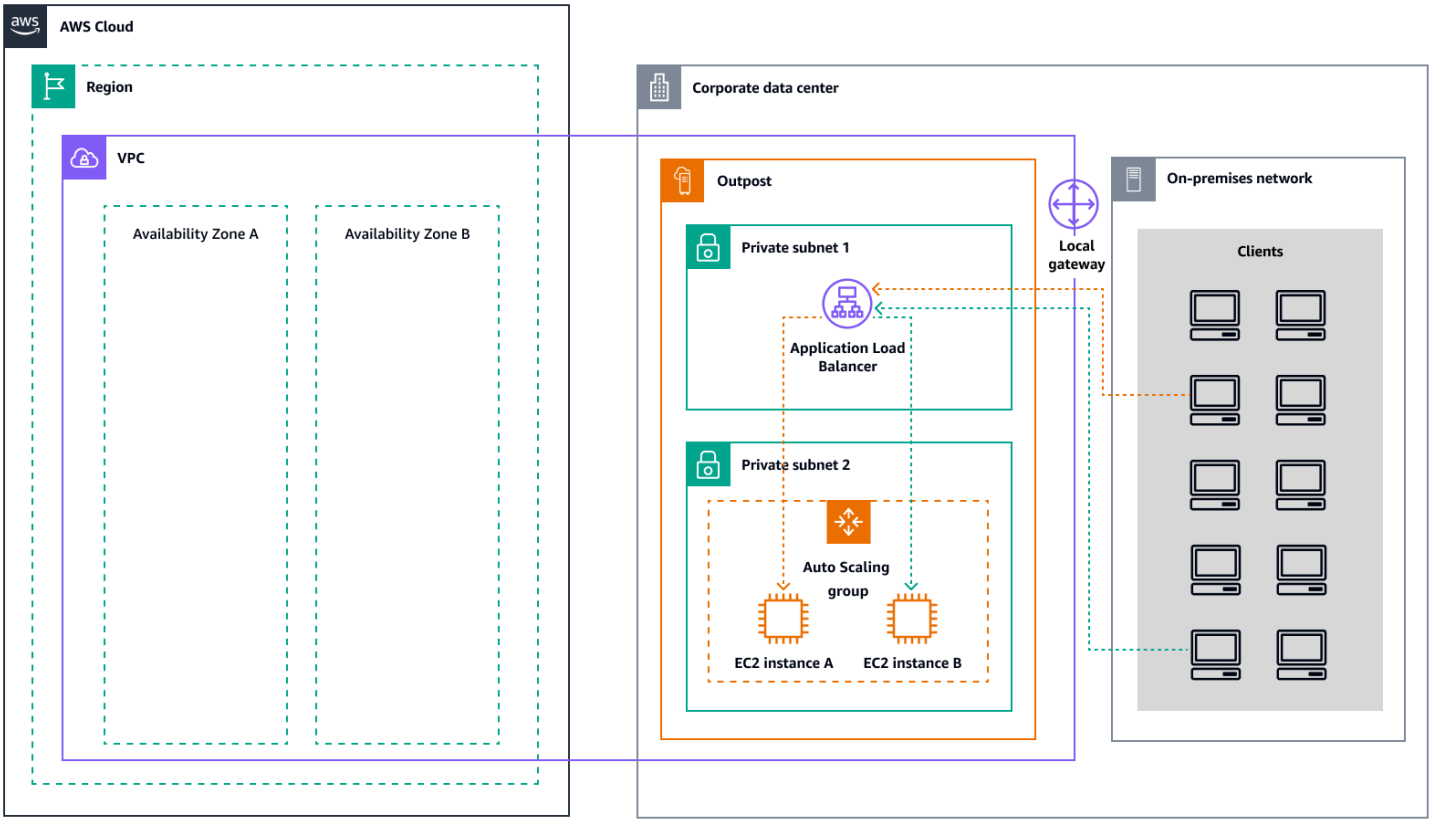
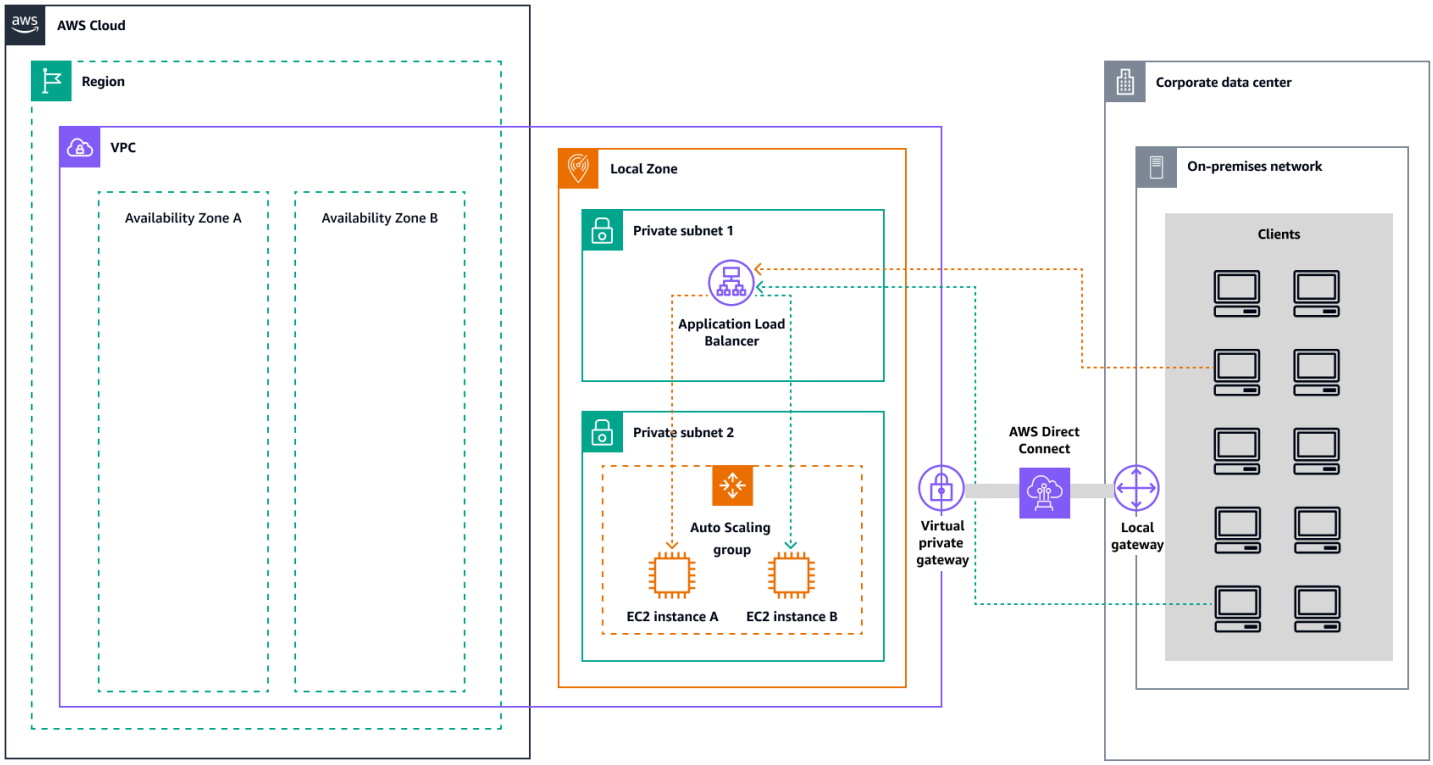


Diagram berikut menggambarkan arsitektur serupa untuk Amazon EC2 di Local Zones.



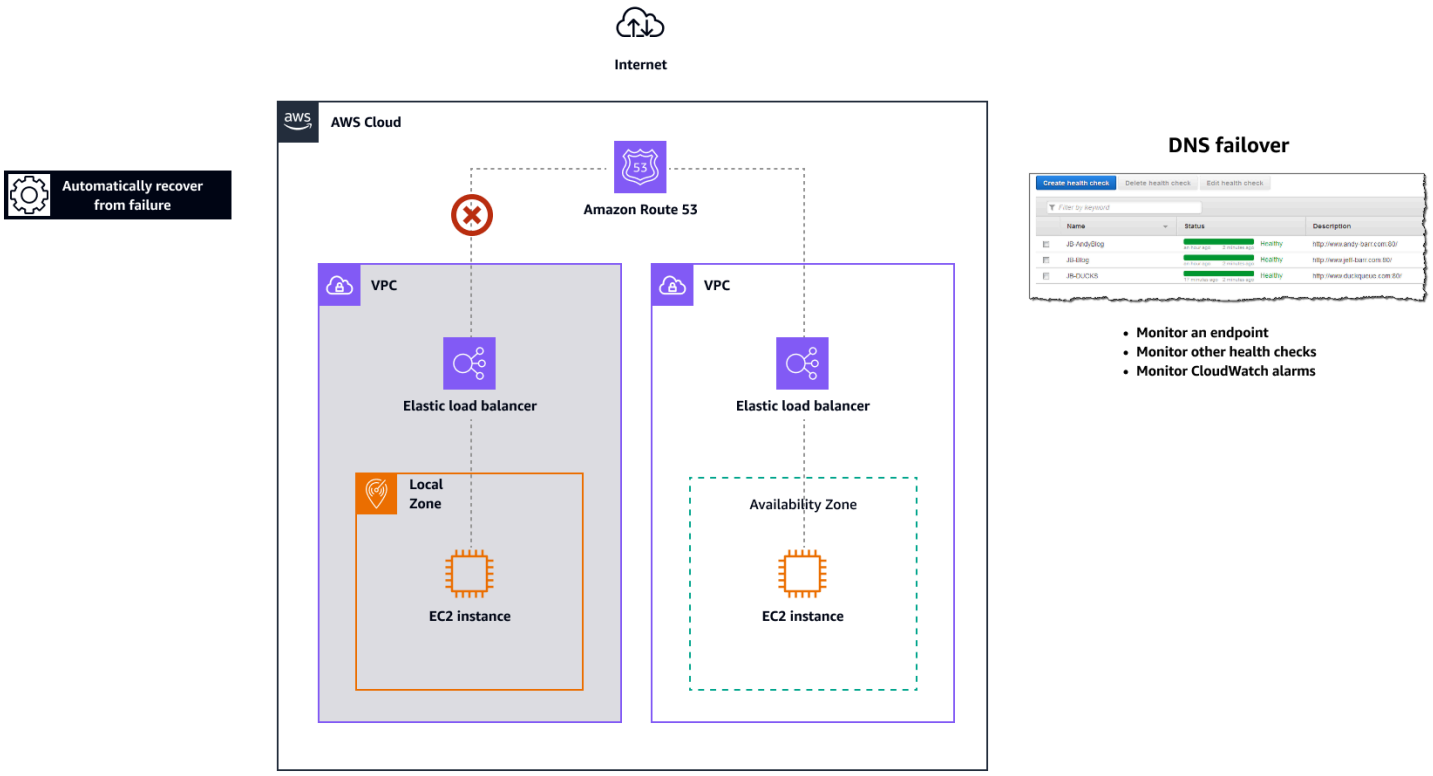
> **Note**
>
> Application Load Balancers tersedia di keduanya AWS Outposts dan Local Zones. Namun, untuk menggunakan Application Load Balancer AWS Outposts, Anda perlu mengukur EC2 kapasitas Amazon untuk menyediakan skalabilitas yang dibutuhkan penyeimbang beban. Untuk informasi lebih lanjut tentang 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. Sebagai contoh, 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 IPs 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 aplikasi yang dihosting Outpost Anda.

Amazon Route 53 Resolver pada 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 VPCs 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 VPCs dan jaringan Anda di 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 Zone 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 Zone 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 Zone
Amazon EKS	Menerapkan Amazon EKS lokal dengan AWS Outposts	Luncurkan cluster EKS latensi rendah dengan AWS Local Zone
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 Zone
Amazon FSx	Tidak tersedia	Pilih subnet Zona Lokal

Layanan	AWS Outposts	AWS Local Zone
AWS Elastic Disaster Recovery	Bekerja dengan AWS Elastic Disaster Recovery dan AWS Outposts	Tidak tersedia
AWS Application Migration Service	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 Zone
- AWS Outposts Keluarga
- AWS Local Zone
- 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 Zone(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 Zone
- Amazon ECS di Amazon EC2
- Mengelola mesh layanan edge-aware dengan Amazon EKS untuk AWS Local Zone
- Menerapkan perutean ingress gateway lokal di Amazon EC2
- Mengotomatiskan penerapan beban kerja Anda di AWS Local Zone
- 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 Zone 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

AWS Glosarium Panduan Preskriptif

Berikut ini adalah istilah yang umum digunakan dalam strategi, panduan, dan pola yang disediakan oleh Panduan AWS Preskriptif. Untuk menyarankan entri, silakan gunakan tautan Berikan umpan balik di akhir glosarium.

Nomor

7 Rs

Tujuh strategi migrasi umum untuk memindahkan aplikasi ke cloud. Strategi ini dibangun di atas 5 Rs yang diidentifikasi Gartner pada tahun 2011 dan terdiri dari yang berikut:

- Refactor/Re-Architect — Memindahkan aplikasi dan memodifikasi arsitekturnya dengan memanfaatkan sepenuhnya fitur cloud-native untuk meningkatkan kelincahan, kinerja, dan skalabilitas. Ini biasanya melibatkan porting sistem operasi dan database. Contoh: Migrasikan database Oracle lokal Anda ke Amazon Aurora PostgreSQL Compatible Edition.
- Replatform (angkat dan bentuk ulang) — Pindahkan aplikasi ke cloud, dan perkenalkan beberapa tingkat pengoptimalan untuk memanfaatkan kemampuan cloud. Contoh: Memigrasikan database Oracle lokal Anda ke Amazon Relational Database Service (Amazon RDS) untuk Oracle di. AWS Cloud
- Pembelian kembali (drop and shop) - Beralih ke produk yang berbeda, biasanya dengan beralih dari lisensi tradisional ke model SaaS. Contoh: Migrasikan sistem manajemen hubungan pelanggan (CRM) Anda ke Salesforce.com.
- Rehost (lift dan shift) — Pindahkan aplikasi ke cloud tanpa membuat perubahan apa pun untuk memanfaatkan kemampuan cloud. Contoh: Migrasikan database Oracle lokal Anda ke Oracle pada instance EC2 di. AWS Cloud
- Relokasi (hypervisor-level lift and shift) — Pindahkan infrastruktur ke cloud tanpa membeli perangkat keras baru, menulis ulang aplikasi, atau memodifikasi operasi yang ada. Anda memigrasikan server dari platform lokal ke layanan cloud untuk platform yang sama. Contoh: Migrasikan Microsoft Hyper-V aplikasi ke AWS.
- Pertahankan (kunjungi kembali) - Simpan aplikasi di lingkungan sumber Anda. Ini mungkin termasuk aplikasi yang memerlukan refactoring besar, dan Anda ingin menunda pekerjaan itu sampai nanti, dan aplikasi lama yang ingin Anda pertahankan, karena tidak ada pembenaran bisnis untuk memigrasikannya.

- Pensiun — Menonaktifkan atau menghapus aplikasi yang tidak lagi diperlukan di lingkungan sumber Anda.

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

Metode migrasi database di mana database sumber dan target tetap sinkron (dengan menggunakan alat replikasi dua arah atau operasi penulisan ganda), dan kedua database menangani transaksi dari menghubungkan aplikasi selama migrasi. Metode ini mendukung migrasi dalam batch kecil yang terkontrol alih-alih memerlukan pemotongan satu kali. Ini lebih fleksibel tetapi membutuhkan lebih banyak pekerjaan daripada migrasi aktif-pasif.

migrasi aktif-pasif

Metode migrasi database di mana database sumber dan target disimpan dalam sinkron, tetapi hanya database sumber yang menangani transaksi dari menghubungkan aplikasi sementara data direplikasi ke database target. Basis data target tidak menerima transaksi apa pun selama migrasi.

fungsi agregat

Fungsi SQL yang beroperasi pada sekelompok baris dan menghitung nilai pengembalian tunggal untuk grup. Contoh fungsi agregat meliputi `SUM` dan`MAX`.

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

Proses menghapus informasi pribadi secara permanen dalam kumpulan data. Anonimisasi dapat membantu melindungi privasi pribadi. Data anonim tidak lagi dianggap sebagai data pribadi.

anti-pola

Solusi yang sering digunakan untuk masalah berulang di mana solusinya kontra-produktif, tidak efektif, atau kurang efektif daripada alternatif.

kontrol aplikasi

Pendekatan keamanan yang memungkinkan penggunaan hanya aplikasi yang disetujui untuk membantu melindungi sistem dari malware.

portofolio aplikasi

Kumpulan informasi rinci tentang setiap aplikasi yang digunakan oleh organisasi, termasuk biaya untuk membangun dan memelihara aplikasi, dan nilai bisnisnya. Informasi ini adalah kunci untuk penemuan portofolio dan proses analisis dan membantu mengidentifikasi dan memprioritaskan aplikasi yang akan dimigrasi, dimodernisasi, dan dioptimalkan.

kecerdasan buatan (AI)

Bidang ilmu komputer yang didedikasikan untuk menggunakan teknologi komputasi untuk melakukan fungsi kognitif yang biasanya terkait dengan manusia, seperti belajar, memecahkan masalah, dan mengenali pola. Untuk informasi lebih lanjut, lihat Apa itu Kecerdasan Buatan?

operasi kecerdasan buatan (AIOps)

Proses menggunakan teknik pembelajaran mesin untuk memecahkan masalah operasional, mengurangi insiden operasional dan intervensi manusia, dan meningkatkan kualitas layanan. Untuk informasi selengkapnya tentang cara AIOps digunakan dalam strategi AWS migrasi, lihat panduan integrasi operasi.

enkripsi asimetris

Algoritma enkripsi yang menggunakan sepasang kunci, kunci publik untuk enkripsi dan kunci pribadi untuk dekripsi. Anda dapat berbagi kunci publik karena tidak digunakan untuk dekripsi, tetapi akses ke kunci pribadi harus sangat dibatasi.

atomisitas, konsistensi, isolasi, daya tahan (ACID)

Satu set properti perangkat lunak yang menjamin validitas data dan keandalan operasional database, bahkan dalam kasus kesalahan, kegagalan daya, atau masalah lainnya.

kontrol akses berbasis atribut (ABAC)

Praktik membuat izin berbutir halus berdasarkan atribut pengguna, seperti departemen, peran pekerjaan, dan nama tim. Untuk informasi selengkapnya, lihat ABAC untuk AWS dokumentasi AWS Identity and Access Management (IAM).

sumber data otoritatif

Lokasi di mana Anda menyimpan versi utama data, yang dianggap sebagai sumber informasi yang paling dapat diandalkan. Anda dapat menyalin data dari sumber data otoritatif ke lokasi lain untuk tujuan pemrosesan atau modifikasi data, seperti menganonimkan, menyunting, atau membuat nama samaran.

Availability Zone

Lokasi berbeda di dalam Wilayah AWS yang terisolasi dari kegagalan di Availability Zone lainnya dan menyediakan konektivitas jaringan latensi rendah yang murah ke Availability Zone lainnya di Wilayah yang sama.

AWS Kerangka Adopsi Cloud (AWS CAF)

Kerangka pedoman dan praktik terbaik AWS untuk membantu organisasi mengembangkan rencana yang efisien dan efektif untuk bergerak dengan sukses ke cloud. AWS CAF mengatur panduan ke dalam enam area fokus yang disebut perspektif: bisnis, orang, tata kelola, platform, keamanan, dan operasi. Perspektif bisnis, orang, dan tata kelola fokus pada keterampilan dan proses bisnis; perspektif platform, keamanan, dan operasi fokus pada keterampilan dan proses teknis. Misalnya, perspektif masyarakat menargetkan pemangku kepentingan yang menangani sumber daya manusia (SDM), fungsi kepegawaian, dan manajemen orang. Untuk perspektif ini, AWS CAF memberikan panduan untuk pengembangan, pelatihan, dan komunikasi orang untuk membantu mempersiapkan organisasi untuk adopsi cloud yang sukses. Untuk informasi lebih lanjut, lihat situs web AWS CAF dan whitepaper AWS CAF.

AWS Kerangka Kualifikasi Beban Kerja (AWS WQF)

Alat yang mengevaluasi beban kerja migrasi database, merekomendasikan strategi migrasi, dan memberikan perkiraan kerja. AWS WQF disertakan dengan AWS Schema Conversion Tool ()AWS SCT. Ini menganalisis skema database dan objek kode, kode aplikasi, dependensi, dan karakteristik kinerja, dan memberikan laporan penilaian.

B

bot buruk

Bot yang dimaksudkan untuk mengganggu atau membahayakan individu atau organisasi.

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

Pandangan interaktif yang terpadu tentang perilaku dan interaksi sumber daya dari waktu ke waktu. Anda dapat menggunakan grafik perilaku dengan Amazon Detective untuk memeriksa upaya logon yang gagal, panggilan API yang mencurigakan, dan tindakan serupa. Untuk informasi selengkapnya, lihat Data dalam grafik perilaku di dokumentasi Detektif.

sistem big-endian

Sistem yang menyimpan byte paling signifikan terlebih dahulu. Lihat juga endianness.

klasifikasi biner

Sebuah proses yang memprediksi hasil biner (salah satu dari dua kelas yang mungkin). Misalnya, model ML Anda mungkin perlu memprediksi masalah seperti “Apakah email ini spam atau bukan spam?” atau “Apakah produk ini buku atau mobil?”

filter mekar

Struktur data probabilistik dan efisien memori yang digunakan untuk menguji apakah suatu elemen adalah anggota dari suatu himpunan.

deployment biru/hijau

Strategi penyebaran tempat Anda membuat dua lingkungan yang terpisah namun identik. Anda menjalankan versi aplikasi saat ini di satu lingkungan (biru) dan versi aplikasi baru di lingkungan lain (hijau). Strategi ini membantu Anda dengan cepat memutar kembali dengan dampak minimal.

bot

Aplikasi perangkat lunak yang menjalankan tugas otomatis melalui internet dan mensimulasikan aktivitas atau interaksi manusia. Beberapa bot berguna atau bermanfaat, seperti perayap web yang mengindeks informasi di internet. Beberapa bot lain, yang dikenal sebagai bot buruk, dimaksudkan untuk mengganggu atau membahayakan individu atau organisasi.

botnet

Jaringan bot yang terinfeksi oleh malware dan berada di bawah kendali satu pihak, yang dikenal sebagai bot herder atau operator bot. Botnet adalah mekanisme paling terkenal untuk skala bot dan dampaknya.

cabang

Area berisi repositori kode. Cabang pertama yang dibuat dalam repositori adalah cabang utama. Anda dapat membuat cabang baru dari cabang yang ada, dan Anda kemudian dapat mengembangkan fitur atau memperbaiki bug di cabang baru. Cabang yang Anda buat untuk membangun fitur biasanya disebut sebagai cabang fitur. Saat fitur siap dirilis, Anda menggabungkan cabang fitur kembali ke cabang utama. Untuk informasi selengkapnya, lihat Tentang cabang (GitHub dokumentasi).

akses break-glass

Dalam keadaan luar biasa dan melalui proses yang disetujui, cara cepat bagi pengguna untuk mendapatkan akses ke Akun AWS yang biasanya tidak memiliki izin untuk mengaksesnya. Untuk informasi lebih lanjut, lihat indikator Implementasikan prosedur kaca pecah dalam panduan Well-Architected AWS .

strategi brownfield

Infrastruktur yang ada di lingkungan Anda. Saat mengadopsi strategi brownfield untuk arsitektur sistem, Anda merancang arsitektur di sekitar kendala sistem dan infrastruktur saat ini. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

Apa yang dilakukan bisnis untuk menghasilkan nilai (misalnya, penjualan, layanan pelanggan, atau pemasaran). Arsitektur layanan mikro dan keputusan pengembangan dapat didorong oleh kemampuan bisnis. Untuk informasi selengkapnya, lihat bagian Terorganisir di sekitar kemampuan bisnis dari Menjalankan layanan mikro kontainer di whitepaper. AWS

perencanaan kelangsungan bisnis (BCP)

Rencana yang membahas dampak potensial dari peristiwa yang mengganggu, seperti migrasi skala besar, pada operasi dan memungkinkan bisnis untuk melanjutkan operasi dengan cepat.

C

KAFE

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

Rilis versi yang lambat dan bertahap untuk pengguna akhir. Ketika Anda yakin, Anda menyebarkan versi baru dan mengganti versi saat ini secara keseluruhan.

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

Proses melacak perubahan ke sumber data, seperti tabel database, dan merekam metadata tentang perubahan tersebut. Anda dapat menggunakan CDC untuk berbagai tujuan, seperti mengaudit atau mereplikasi perubahan dalam sistem target untuk mempertahankan sinkronisasi.

rekayasa kekacauan

Sengaja memperkenalkan kegagalan atau peristiwa yang mengganggu untuk menguji ketahanan sistem. Anda dapat menggunakan AWS Fault Injection Service (AWS FIS) untuk melakukan eksperimen yang menekankan AWS beban kerja Anda dan mengevaluasi responsnya.

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

Proses kategorisasi yang membantu menghasilkan prediksi. Model ML untuk masalah klasifikasi memprediksi nilai diskrit. Nilai diskrit selalu berbeda satu sama lain. Misalnya, model mungkin perlu mengevaluasi apakah ada mobil dalam gambar atau tidak.

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

Tim multi-disiplin yang mendorong upaya adopsi cloud di seluruh organisasi, termasuk mengembangkan praktik terbaik cloud, memobilisasi sumber daya, menetapkan jadwal migrasi, dan memimpin organisasi melalui transformasi skala besar. Untuk informasi selengkapnya, lihat posting CCo E di Blog Strategi AWS Cloud Perusahaan.

komputasi cloud

Teknologi cloud yang biasanya digunakan untuk penyimpanan data jarak jauh dan manajemen perangkat IoT. Cloud computing umumnya terhubung ke teknologi edge computing.

model operasi cloud

Dalam organisasi TI, model operasi yang digunakan untuk membangun, mematangkan, dan mengoptimalkan satu atau lebih lingkungan cloud. Untuk informasi selengkapnya, lihat Membangun Model Operasi Cloud Anda.

tahap adopsi cloud

Empat fase yang biasanya dilalui organisasi ketika mereka bermigrasi ke AWS Cloud:

- Proyek — Menjalankan beberapa proyek terkait cloud untuk bukti konsep dan tujuan pembelajaran
- Foundation — Melakukan investasi dasar untuk meningkatkan adopsi cloud Anda (misalnya, membuat landing zone, mendefinisikan CCo E, membuat model operasi)
- Migrasi — Migrasi aplikasi individual
- Re-invention — Mengoptimalkan produk dan layanan, dan berinovasi di cloud

Tahapan ini didefinisikan oleh Stephen Orban dalam posting blog The Journey Toward Cloud-First & the Stages of Adoption di blog Strategi Perusahaan. AWS Cloud Untuk informasi tentang bagaimana kaitannya dengan strategi AWS migrasi, lihat panduan kesiapan migrasi.

CMDB

Lihat database manajemen konfigurasi.

repositori kode

Lokasi di mana kode sumber dan aset lainnya, seperti dokumentasi, sampel, dan skrip, disimpan dan diperbarui melalui proses kontrol versi. Repositori cloud umum termasuk GitHub atau. Bitbucket Cloud Setiap versi kode disebut cabang. Dalam struktur layanan mikro, setiap repositori

dikhususkan untuk satu bagian fungsionalitas. Pipa CI/CD tunggal dapat menggunakan beberapa repositori.

cache dingin

Cache buffer yang kosong, tidak terisi dengan baik, atau berisi data basi atau tidak relevan. Ini mempengaruhi kinerja karena instance database harus membaca dari memori utama atau disk, yang lebih lambat daripada membaca dari cache buffer.

data dingin

Data yang jarang diakses dan biasanya historis. Saat menanyakan jenis data ini, kueri lambat biasanya dapat diterima. Memindahkan data ini ke tingkat atau kelas penyimpanan yang berkinerja lebih rendah dan lebih murah dapat mengurangi biaya.

visi komputer (CV)

Bidang AI yang menggunakan pembelajaran mesin untuk menganalisis dan mengekstrak informasi dari format visual seperti gambar dan video digital. Misalnya, Amazon SageMaker AI menyediakan algoritma pemrosesan gambar untuk CV.

konfigurasi drift

Untuk beban kerja, konfigurasi berubah dari status yang diharapkan. Ini dapat menyebabkan beban kerja menjadi tidak patuh, dan biasanya bertahap dan tidak disengaja.

database manajemen konfigurasi (CMDB)

Repositori yang menyimpan dan mengelola informasi tentang database dan lingkungan TI, termasuk komponen perangkat keras dan perangkat lunak dan konfigurasinya. Anda biasanya menggunakan data dari CMDB dalam penemuan portofolio dan tahap analisis migrasi.

paket kesesuaian

Kumpulan AWS Config aturan dan tindakan remediasi yang dapat Anda kumpulkan untuk menyesuaikan kepatuhan dan pemeriksaan keamanan Anda. Anda dapat menerapkan paket kesesuaian sebagai entitas tunggal di Akun AWS dan Wilayah, atau di seluruh organisasi, dengan menggunakan templat YAMM. Untuk informasi selengkapnya, lihat Paket kesesuaian dalam dokumentasi. AWS Config

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

Proses mengotomatiskan sumber, membangun, menguji, pementasan, dan tahap produksi dari proses rilis perangkat lunak. CI/CD biasanya digambarkan sebagai pipa. CI/CD dapat membantu

Anda mengotomatiskan proses, meningkatkan produktivitas, meningkatkan kualitas kode, dan memberikan lebih cepat. Untuk informasi lebih lanjut, lihat Manfaat pengiriman berkelanjutan. CD juga dapat berarti penerapan berkelanjutan. Untuk informasi selengkapnya, lihat Continuous Delivery vs Continuous Deployment.

CV

Lihat visi komputer.

D

data saat istirahat

Data yang stasioner di jaringan Anda, seperti data yang ada di penyimpanan.

klasifikasi data

Proses untuk mengidentifikasi dan mengkategorikan data dalam jaringan Anda berdasarkan kekritisan dan sensitivitasnya. Ini adalah komponen penting dari setiap strategi manajemen risiko keamanan siber karena membantu Anda menentukan perlindungan dan kontrol retensi yang tepat untuk data. Klasifikasi data adalah komponen pilar keamanan dalam AWS Well-Architected Framework. Untuk informasi selengkapnya, lihat Klasifikasi data.

penyimpangan data

Variasi yang berarti antara data produksi dan data yang digunakan untuk melatih model ML, atau perubahan yang berarti dalam data input dari waktu ke waktu. Penyimpangan data dapat mengurangi kualitas, akurasi, dan keadilan keseluruhan dalam prediksi model ML.

data dalam transit

Data yang aktif bergerak melalui jaringan Anda, seperti antara sumber daya jaringan.

jala data

Kerangka arsitektur yang menyediakan kepemilikan data terdistribusi dan terdesentralisasi dengan manajemen dan tata kelola terpusat.

minimalisasi data

Prinsip pengumpulan dan pemrosesan hanya data yang sangat diperlukan. Mempraktikkan minimalisasi data di dalamnya AWS Cloud dapat mengurangi risiko privasi, biaya, dan jejak karbon analitik Anda.

perimeter data

Satu set pagar pembatas pencegahan di AWS lingkungan Anda yang membantu memastikan bahwa hanya identitas tepercaya yang mengakses sumber daya tepercaya dari jaringan yang diharapkan. Untuk informasi selengkapnya, lihat Membangun perimeter data pada AWS.

prapemrosesan data

Untuk mengubah data mentah menjadi format yang mudah diuraikan oleh model ML Anda. Preprocessing data dapat berarti menghapus kolom atau baris tertentu dan menangani nilai yang hilang, tidak konsisten, atau duplikat.

asal data

Proses melacak asal dan riwayat data sepanjang siklus hidupnya, seperti bagaimana data dihasilkan, ditransmisikan, dan disimpan.

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

Sistem manajemen data yang mendukung intelijen bisnis, seperti analitik. Gudang data biasanya berisi sejumlah besar data historis, dan biasanya digunakan untuk kueri dan analisis.

bahasa definisi database (DDL)

Pernyataan atau perintah untuk membuat atau memodifikasi struktur tabel dan objek dalam database.

bahasa manipulasi basis data (DHTML)

Pernyataan atau perintah untuk memodifikasi (memasukkan, memperbarui, dan menghapus) informasi dalam database.

DDL

Lihat bahasa definisi database.

ansambel yang dalam

Untuk menggabungkan beberapa model pembelajaran mendalam untuk prediksi. Anda dapat menggunakan ansambel dalam untuk mendapatkan prediksi yang lebih akurat atau untuk memperkirakan ketidakpastian dalam prediksi.

pembelajaran mendalam

Subbidang ML yang menggunakan beberapa lapisan jaringan saraf tiruan untuk mengidentifikasi pemetaan antara data input dan variabel target yang diinginkan.

defense-in-depth

Pendekatan keamanan informasi di mana serangkaian mekanisme dan kontrol keamanan dilapisi dengan cermat di seluruh jaringan komputer untuk melindungi kerahasiaan, integritas, dan ketersediaan jaringan dan data di dalamnya. Saat Anda mengadopsi strategi ini AWS, Anda menambahkan beberapa kontrol pada lapisan AWS Organizations struktur yang berbeda untuk membantu mengamankan sumber daya. Misalnya, defense-in-depth pendekatan mungkin menggabungkan otentikasi multi-faktor, segmentasi jaringan, dan enkripsi.

administrator yang didelegasikan

Di AWS Organizations, layanan yang kompatibel dapat mendaftarkan akun AWS anggota untuk mengelola akun organisasi dan mengelola izin untuk layanan tersebut. Akun ini disebut administrator yang didelegasikan untuk layanan itu. Untuk informasi selengkapnya dan daftar layanan yang kompatibel, lihat Layanan yang berfungsi dengan AWS Organizations AWS Organizations dokumentasi.

deployment

Proses pembuatan aplikasi, fitur baru, atau perbaikan kode tersedia di lingkungan target. Deployment melibatkan penerapan perubahan dalam basis kode dan kemudian membangun dan menjalankan basis kode itu di lingkungan aplikasi.

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

Kontrol keamanan yang dirancang untuk mendeteksi, mencatat, dan memperingatkan setelah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan kedua, memperingatkan Anda tentang peristiwa keamanan yang melewati kontrol pencegahan di tempat. Untuk informasi selengkapnya, lihat Kontrol Detektif dalam Menerapkan kontrol keamanan pada. AWS

pemetaan aliran nilai pengembangan (DVSM)

Sebuah proses yang digunakan untuk mengidentifikasi dan memprioritaskan kendala yang mempengaruhi kecepatan dan kualitas dalam siklus hidup pengembangan perangkat lunak. DVSM memperluas proses pemetaan aliran nilai yang awalnya dirancang untuk praktik

manufaktur ramping. Ini berfokus pada langkah-langkah dan tim yang diperlukan untuk menciptakan dan memindahkan nilai melalui proses pengembangan perangkat lunak.

kembar digital

Representasi virtual dari sistem dunia nyata, seperti bangunan, pabrik, peralatan industri, atau jalur produksi. Kembar digital mendukung pemeliharaan prediktif, pemantauan jarak jauh, dan optimalisasi produksi.

tabel dimensi

Dalam skema bintang, tabel yang lebih kecil yang berisi atribut data tentang data kuantitatif dalam tabel fakta. Atribut tabel dimensi biasanya bidang teks atau angka diskrit yang berperilaku seperti teks. Atribut ini biasanya digunakan untuk pembatasan kueri, pemfilteran, dan pelabelan set hasil.

musibah

Peristiwa yang mencegah beban kerja atau sistem memenuhi tujuan bisnisnya di lokasi utama yang digunakan. Peristiwa ini dapat berupa bencana alam, kegagalan teknis, atau akibat dari tindakan manusia, seperti kesalahan konfigurasi yang tidak disengaja atau serangan malware.

pemulihan bencana (DR)

Strategi dan proses yang Anda gunakan untuk meminimalkan downtime dan kehilangan data yang disebabkan oleh bencana. Untuk informasi selengkapnya, lihat Disaster Recovery of Workloads on AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML~

Lihat bahasa manipulasi basis data.

desain berbasis domain

Pendekatan untuk mengembangkan sistem perangkat lunak yang kompleks dengan menghubungkan komponennya ke domain yang berkembang, atau tujuan bisnis inti, yang dilayani oleh setiap komponen. Konsep ini diperkenalkan oleh Eric Evans dalam bukunya, Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Untuk informasi tentang cara menggunakan desain berbasis domain dengan pola gambar pencekik, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

DR

Lihat pemulihan bencana.

deteksi drift

Melacak penyimpangan dari konfigurasi dasar. Misalnya, Anda dapat menggunakan AWS CloudFormation untuk mendeteksi penyimpangan dalam sumber daya sistem, atau Anda dapat menggunakannya AWS Control Tower untuk mendeteksi perubahan di landing zone yang mungkin memengaruhi kepatuhan terhadap persyaratan tata kelola.

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

Teknologi yang meningkatkan daya komputasi untuk perangkat pintar di tepi jaringan IoT. Jika dibandingkan dengan komputasi awan, komputasi tepi dapat mengurangi latensi komunikasi dan meningkatkan waktu respons.

pertukaran data elektronik (EDI)

Pertukaran otomatis dokumen bisnis antar organisasi. Untuk informasi selengkapnya, lihat Apa itu Pertukaran Data Elektronik.

enkripsi

Proses komputasi yang mengubah data plaintext, yang dapat dibaca manusia, menjadi ciphertext.

kunci enkripsi

String kriptografi dari bit acak yang dihasilkan oleh algoritma enkripsi. Panjang kunci dapat bervariasi, dan setiap kunci dirancang agar tidak dapat diprediksi dan unik.

endianness

Urutan byte disimpan dalam memori komputer. Sistem big-endian menyimpan byte paling signifikan terlebih dahulu. Sistem little-endian menyimpan byte paling tidak signifikan terlebih dahulu.

titik akhir

Lihat titik akhir layanan.

layanan endpoint

Layanan yang dapat Anda host di cloud pribadi virtual (VPC) untuk dibagikan dengan pengguna lain. Anda dapat membuat layanan endpoint dengan AWS PrivateLink dan memberikan izin kepada prinsipal lain Akun AWS atau ke AWS Identity and Access Management (IAM). Akun atau prinsipal ini dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir VPC antarmuka. Untuk informasi selengkapnya, lihat Membuat layanan titik akhir di dokumentasi Amazon Virtual Private Cloud (Amazon VPC).

perencanaan sumber daya perusahaan (ERP)

Sistem yang mengotomatiskan dan mengelola proses bisnis utama (seperti akuntansi, MES, dan manajemen proyek) untuk suatu perusahaan.

enkripsi amplop

Proses mengenkripsi kunci enkripsi dengan kunci enkripsi lain. Untuk informasi selengkapnya, lihat Enkripsi amplop dalam dokumentasi AWS Key Management Service (AWS KMS).

lingkungan

Sebuah contoh dari aplikasi yang sedang berjalan. Berikut ini adalah jenis lingkungan yang umum dalam komputasi awan:

- Development Environment — Sebuah contoh dari aplikasi yang berjalan yang hanya tersedia untuk tim inti yang bertanggung jawab untuk memelihara aplikasi. Lingkungan pengembangan digunakan untuk menguji perubahan sebelum mempromosikannya ke lingkungan atas. Jenis lingkungan ini kadang-kadang disebut sebagai lingkungan pengujian.
- lingkungan yang lebih rendah — Semua lingkungan pengembangan untuk aplikasi, seperti yang digunakan untuk build awal dan pengujian.
- lingkungan produksi — Sebuah contoh dari aplikasi yang berjalan yang pengguna akhir dapat mengakses. Dalam sebuah CI/CD pipeline, lingkungan produksi adalah lingkungan penyebaran terakhir.

- lingkungan atas — Semua lingkungan yang dapat diakses oleh pengguna selain tim pengembangan inti. Ini dapat mencakup lingkungan produksi, lingkungan praproduksi, dan lingkungan untuk pengujian penerimaan pengguna.

epik

Dalam metodologi tangkas, kategori fungsional yang membantu mengatur dan memprioritaskan pekerjaan Anda. Epik memberikan deskripsi tingkat tinggi tentang persyaratan dan tugas implementasi. Misalnya, epos keamanan AWS CAF mencakup manajemen identitas dan akses, kontrol detektif, keamanan infrastruktur, perlindungan data, dan respons insiden. Untuk informasi selengkapnya tentang epos dalam strategi AWS migrasi, lihat panduan implementasi program.

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

Proses menganalisis dataset untuk memahami karakteristik utamanya. Anda mengumpulkan atau mengumpulkan data dan kemudian melakukan penyelidikan awal untuk menemukan pola, mendeteksi anomali, dan memeriksa asumsi. EDA dilakukan dengan menghitung statistik ringkasan dan membuat visualisasi data.

F

tabel fakta

Tabel tengah dalam skema bintang. Ini menyimpan data kuantitatif tentang operasi bisnis. Biasanya, tabel fakta berisi dua jenis kolom: kolom yang berisi ukuran dan yang berisi kunci asing ke tabel dimensi.

gagal cepat

Filosofi yang menggunakan pengujian yang sering dan bertahap untuk mengurangi siklus hidup pengembangan. Ini adalah bagian penting dari pendekatan tangkas.

batas isolasi kesalahan

Dalam AWS Cloud, batas seperti Availability Zone, Wilayah AWS, control plane, atau data plane yang membatasi efek kegagalan dan membantu meningkatkan ketahanan beban kerja. Untuk informasi selengkapnya, lihat Batas Isolasi AWS Kesalahan.

cabang fitur

Lihat cabang.

fitur

Data input yang Anda gunakan untuk membuat prediksi. Misalnya, dalam konteks manufaktur, fitur bisa berupa gambar yang diambil secara berkala dari lini manufaktur.

pentingnya fitur

Seberapa signifikan fitur untuk prediksi model. Ini biasanya dinyatakan sebagai skor numerik yang dapat dihitung melalui berbagai teknik, seperti Shapley Additive Explanations (SHAP) dan gradien terintegrasi. Untuk informasi lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan. AWS

transformasi fitur

Untuk mengoptimalkan data untuk proses ML, termasuk memperkaya data dengan sumber tambahan, menskalakan nilai, atau mengekstrak beberapa set informasi dari satu bidang data. Hal ini memungkinkan model ML untuk mendapatkan keuntungan dari data. Misalnya, jika Anda memecah tanggal “2021-05-27 00:15:37" menjadi “2021", “Mei”, “Kamis”, dan “15", Anda dapat membantu algoritme pembelajaran mempelajari pola bernuansa yang terkait dengan komponen data yang berbeda.

beberapa tembakan mendorong

Menyediakan LLM dengan sejumlah kecil contoh yang menunjukkan tugas dan output yang diinginkan sebelum memintanya untuk melakukan tugas serupa. Teknik ini adalah aplikasi pembelajaran dalam konteks, di mana model belajar dari contoh (bidikan) yang tertanam dalam petunjuk. Beberapa bidikan dapat efektif untuk tugas-tugas yang memerlukan pemformatan, penalaran, atau pengetahuan domain tertentu. Lihat juga bidikan nol.

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

Metode migrasi database yang menggunakan replikasi data berkelanjutan melalui pengambilan data perubahan untuk memigrasikan data dalam waktu sesingkat mungkin, alih-alih

menggunakan pendekatan bertahap. Tujuannya adalah untuk menjaga downtime seminimal mungkin.

FM

Lihat model pondasi.

model pondasi (FM)

Jaringan saraf pembelajaran mendalam yang besar yang telah melatih kumpulan data besar-besaran data umum dan tidak berlabel. FMs mampu melakukan berbagai tugas umum, seperti memahami bahasa, menghasilkan teks dan gambar, dan berbicara dalam bahasa alami. Untuk informasi selengkapnya, lihat Apa itu Model Foundation.

G

AI generatif

Subset model AI yang telah dilatih pada sejumlah besar data dan yang dapat menggunakan prompt teks sederhana untuk membuat konten dan artefak baru, seperti gambar, video, teks, dan audio. Untuk informasi lebih lanjut, lihat Apa itu AI Generatif.

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

Di Amazon CloudFront, opsi untuk mencegah pengguna di negara tertentu mengakses distribusi konten. Anda dapat menggunakan daftar izinkan atau daftar blokir untuk menentukan negara yang disetujui dan dilarang. Untuk informasi selengkapnya, lihat Membatasi distribusi geografis konten Anda dalam dokumentasi. CloudFront

Alur kerja Gitflow

Pendekatan di mana lingkungan bawah dan atas menggunakan cabang yang berbeda dalam repositori kode sumber. Alur kerja Gitflow dianggap warisan, dan alur kerja berbasis batang adalah pendekatan modern yang lebih disukai.

gambar emas

Sebuah snapshot dari sistem atau perangkat lunak yang digunakan sebagai template untuk menyebarkan instance baru dari sistem atau perangkat lunak itu. Misalnya, di bidang manufaktur,

gambar emas dapat digunakan untuk menyediakan perangkat lunak pada beberapa perangkat dan membantu meningkatkan kecepatan, skalabilitas, dan produktivitas dalam operasi manufaktur perangkat.

strategi greenfield

Tidak adanya infrastruktur yang ada di lingkungan baru. Saat mengadopsi strategi greenfield untuk arsitektur sistem, Anda dapat memilih semua teknologi baru tanpa batasan kompatibilitas dengan infrastruktur yang ada, juga dikenal sebagai brownfield. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

pagar pembatas

Aturan tingkat tinggi yang membantu mengatur sumber daya, kebijakan, dan kepatuhan di seluruh unit organisasi ()OUs. Pagar pembatas preventif menegakkan kebijakan untuk memastikan keselarasan dengan standar kepatuhan. Mereka diimplementasikan dengan menggunakan kebijakan kontrol layanan dan batas izin IAM. Detective guardrails mendeteksi pelanggaran kebijakan dan masalah kepatuhan, dan menghasilkan peringatan untuk remediasi. Mereka diimplementasikan dengan menggunakan AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector, dan pemeriksaan khusus AWS Lambda .

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

Memigrasi database sumber Anda ke database target yang menggunakan mesin database yang berbeda (misalnya, Oracle ke Amazon Aurora). Migrasi heterogen biasanya merupakan bagian dari upaya arsitektur ulang, dan mengubah skema dapat menjadi tugas yang kompleks. AWS menyediakan AWS SCT yang membantu dengan konversi skema.

ketersediaan tinggi (HA)

Kemampuan beban kerja untuk beroperasi terus menerus, tanpa intervensi, jika terjadi tantangan atau bencana. Sistem HA dirancang untuk gagal secara otomatis, secara konsisten memberikan kinerja berkualitas tinggi, dan menangani beban dan kegagalan yang berbeda dengan dampak kinerja minimal.

modernisasi sejarawan

Pendekatan yang digunakan untuk memodernisasi dan meningkatkan sistem teknologi operasional (OT) untuk melayani kebutuhan industri manufaktur dengan lebih baik. Sejarawan adalah jenis database yang digunakan untuk mengumpulkan dan menyimpan data dari berbagai sumber di pabrik.

data penahanan

Sebagian dari data historis berlabel yang ditahan dari kumpulan data yang digunakan untuk melatih model pembelajaran mesin. Anda dapat menggunakan data penahanan untuk mengevaluasi kinerja model dengan membandingkan prediksi model dengan data penahanan.

migrasi database homogen

Memigrasi database sumber Anda ke database target yang berbagi mesin database yang sama (misalnya, Microsoft SQL Server ke Amazon RDS for SQL Server). Migrasi homogen biasanya merupakan bagian dari upaya rehosting atau replatforming. Anda dapat menggunakan utilitas database asli untuk memigrasi skema.

data panas

Data yang sering diakses, seperti data real-time atau data translasi terbaru. Data ini biasanya memerlukan tingkat atau kelas penyimpanan berkinerja tinggi untuk memberikan respons kueri yang cepat.

perbaikan terbaru

Perbaikan mendesak untuk masalah kritis dalam lingkungan produksi. Karena urgensinya, perbaikan terbaru biasanya dibuat di luar alur kerja DevOps rilis biasa.

periode hypercare

Segera setelah cutover, periode waktu ketika tim migrasi mengelola dan memantau aplikasi yang dimigrasi di cloud untuk mengatasi masalah apa pun. Biasanya, periode ini panjangnya 1-4 hari. Pada akhir periode hypercare, tim migrasi biasanya mentransfer tanggung jawab untuk aplikasi ke tim operasi cloud.

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

Kebijakan yang dilampirkan pada satu atau beberapa prinsip IAM yang mendefinisikan izin mereka dalam lingkungan. AWS Cloud

aplikasi idle

Aplikasi yang memiliki penggunaan CPU dan memori rata-rata antara 5 dan 20 persen selama periode 90 hari. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini atau mempertahankannya di tempat.

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

Model yang menyebarkan infrastruktur baru untuk beban kerja produksi alih-alih memperbarui, menambal, atau memodifikasi infrastruktur yang ada. Infrastruktur yang tidak dapat diubah secara inheren lebih konsisten, andal, dan dapat diprediksi daripada infrastruktur yang dapat berubah. Untuk informasi selengkapnya, lihat praktik terbaik Deploy using immutable infrastructure di AWS Well-Architected Framework.

masuk (masuknya) VPC

Dalam arsitektur AWS multi-akun, VPC yang menerima, memeriksa, dan merutekan koneksi jaringan dari luar aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

migrasi inkremental

Strategi cutover di mana Anda memigrasikan aplikasi Anda dalam bagian-bagian kecil alih-alih melakukan satu cutover penuh. Misalnya, Anda mungkin hanya memindahkan beberapa layanan mikro atau pengguna ke sistem baru pada awalnya. Setelah Anda memverifikasi bahwa semuanya berfungsi dengan baik, Anda dapat secara bertahap memindahkan layanan mikro atau pengguna tambahan hingga Anda dapat menonaktifkan sistem lama Anda. Strategi ini mengurangi risiko yang terkait dengan migrasi besar.

Industri 4.0

Sebuah istilah yang diperkenalkan oleh Klaus Schwab pada tahun 2016 untuk merujuk pada modernisasi proses manufaktur melalui kemajuan dalam konektivitas, data real-time, otomatisasi, analitik, dan AI/ML.

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

Proses penyediaan dan pengelolaan infrastruktur aplikasi melalui satu set file konfigurasi. IAc dirancang untuk membantu Anda memusatkan manajemen infrastruktur, menstandarisasi sumber daya, dan menskalakan dengan cepat sehingga lingkungan baru dapat diulang, andal, dan konsisten.

Internet of Things industri (IIoT)

Penggunaan sensor dan perangkat yang terhubung ke internet di sektor industri, seperti manufaktur, energi, otomotif, perawatan kesehatan, ilmu kehidupan, dan pertanian. Untuk informasi lebih lanjut, lihat Membangun strategi transformasi digital Internet of Things (IIoT) industri.

inspeksi VPC

Dalam arsitektur AWS multi-akun, VPC terpusat yang mengelola inspeksi lalu lintas jaringan antara VPCs (dalam yang sama atau berbeda Wilayah AWS), internet, dan jaringan lokal. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

Internet untuk Segala (IoT)

Jaringan objek fisik yang terhubung dengan sensor atau prosesor tertanam yang berkomunikasi dengan perangkat dan sistem lain melalui internet atau melalui jaringan komunikasi lokal. Untuk informasi selengkapnya, lihat Apa itu IoT?

interpretasi

Karakteristik model pembelajaran mesin yang menggambarkan sejauh mana manusia dapat memahami bagaimana prediksi model bergantung pada inputnya. Untuk informasi lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan. AWS

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

Serangkaian praktik terbaik untuk memberikan layanan TI dan menyelaraskan layanan ini dengan persyaratan bisnis. ITIL menyediakan dasar untuk ITSM.

Manajemen layanan TI (ITSM)

Kegiatan yang terkait dengan merancang, menerapkan, mengelola, dan mendukung layanan TI untuk suatu organisasi. Untuk informasi tentang mengintegrasikan operasi cloud dengan alat ITSM, lihat panduan integrasi operasi.

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

Implementasi kontrol akses wajib (MAC) di mana pengguna dan data itu sendiri masing-masing secara eksplisit diberi nilai label keamanan. Persimpangan antara label keamanan pengguna dan label keamanan data menentukan baris dan kolom mana yang dapat dilihat oleh pengguna.

landing zone

Landing zone adalah AWS lingkungan multi-akun yang dirancang dengan baik yang dapat diskalakan dan aman. Ini adalah titik awal dari mana organisasi Anda dapat dengan cepat meluncurkan dan menyebarkan beban kerja dan aplikasi dengan percaya diri dalam lingkungan keamanan dan infrastruktur mereka. Untuk informasi selengkapnya tentang zona pendaratan, lihat Menyiapkan lingkungan multi-akun AWS yang aman dan dapat diskalakan.

model bahasa besar (LLM)

Model AI pembelajaran mendalam yang dilatih sebelumnya pada sejumlah besar data. LLM dapat melakukan beberapa tugas, seperti menjawab pertanyaan, meringkas dokumen, menerjemahkan teks ke dalam bahasa lain, dan menyelesaikan kalimat. Untuk informasi lebih lanjut, lihat Apa itu LLMs.

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

Praktik keamanan terbaik untuk memberikan izin minimum yang diperlukan untuk melakukan tugas. Untuk informasi selengkapnya, lihat Menerapkan izin hak istimewa terkecil dalam dokumentasi IAM.

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

Sebuah sistem yang menyimpan byte paling tidak signifikan terlebih dahulu. Lihat juga endianness.

LLM

Lihat model bahasa besar.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

Jenis kecerdasan buatan yang menggunakan algoritma dan teknik untuk pengenalan pola dan pembelajaran. ML menganalisis dan belajar dari data yang direkam, seperti data Internet of Things (IoT), untuk menghasilkan model statistik berdasarkan pola. Untuk informasi selengkapnya, lihat Machine Learning.

cabang utama

Lihat cabang.

malware

Perangkat lunak yang dirancang untuk membahayakan keamanan atau privasi komputer. Malware dapat mengganggu sistem komputer, membocorkan informasi sensitif, atau mendapatkan akses yang tidak sah. Contoh malware termasuk virus, worm, ransomware, Trojan horse, spyware, dan keyloggers.

layanan terkelola

Layanan AWS yang AWS mengoperasikan lapisan infrastruktur, sistem operasi, dan platform, dan Anda mengakses titik akhir untuk menyimpan dan mengambil data. Amazon Simple Storage Service (Amazon S3) dan Amazon DynamoDB adalah contoh layanan terkelola. Ini juga dikenal sebagai layanan abstrak.

sistem eksekusi manufaktur (MES)

Sistem perangkat lunak untuk melacak, memantau, mendokumentasikan, dan mengendalikan proses produksi yang mengubah bahan baku menjadi produk jadi di lantai toko.

PETA

Lihat Program Percepatan Migrasi.

mekanisme

Proses lengkap di mana Anda membuat alat, mendorong adopsi alat, dan kemudian memeriksa hasilnya untuk melakukan penyesuaian. Mekanisme adalah siklus yang memperkuat dan meningkatkan dirinya sendiri saat beroperasi. Untuk informasi lebih lanjut, lihat Membangun mekanisme di AWS Well-Architected Framework.

akun anggota

Semua Akun AWS selain akun manajemen yang merupakan bagian dari organisasi di AWS Organizations. Sebuah akun hanya dapat menjadi anggota satu organisasi dalam satu waktu.

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan (MQTT)

Protokol komunikasi ringan machine-to-machine (M2M), berdasarkan pola terbitkan/berlangganan, untuk perangkat IoT yang dibatasi sumber daya.

layanan mikro

Layanan kecil dan independen yang berkomunikasi melalui definisi yang jelas APIs dan biasanya dimiliki oleh tim kecil yang mandiri. Misalnya, sistem asuransi mungkin mencakup layanan mikro yang memetakan kemampuan bisnis, seperti penjualan atau pemasaran, atau subdomain, seperti pembelian, klaim, atau analitik. Manfaat layanan mikro termasuk kelincahan, penskalaan yang fleksibel, penyebaran yang mudah, kode yang dapat digunakan kembali, dan ketahanan. Untuk informasi selengkapnya, lihat Mengintegrasikan layanan mikro dengan menggunakan layanan tanpa AWS server.

arsitektur microservices

Pendekatan untuk membangun aplikasi dengan komponen independen yang menjalankan setiap proses aplikasi sebagai layanan mikro. Layanan mikro ini berkomunikasi melalui antarmuka yang terdefinisi dengan baik dengan menggunakan ringan. APIs Setiap layanan mikro dalam arsitektur ini dapat diperbarui, digunakan, dan diskalakan untuk memenuhi permintaan fungsi tertentu dari suatu aplikasi. Untuk informasi selengkapnya, lihat Menerapkan layanan mikro di AWS.

Program Percepatan Migrasi (MAP)

AWS Program yang menyediakan dukungan konsultasi, pelatihan, dan layanan untuk membantu organisasi membangun fondasi operasional yang kuat untuk pindah ke cloud, dan untuk membantu mengimbangi biaya awal migrasi. MAP mencakup metodologi migrasi untuk mengeksekusi migrasi lama dengan cara metodis dan seperangkat alat untuk mengotomatisasi dan mempercepat skenario migrasi umum.

migrasi dalam skala

Proses memindahkan sebagian besar portofolio aplikasi ke cloud dalam gelombang, dengan lebih banyak aplikasi bergerak pada tingkat yang lebih cepat di setiap gelombang. Fase ini menggunakan praktik dan pelajaran terbaik dari fase sebelumnya untuk mengimplementasikan pabrik migrasi tim, alat, dan proses untuk merampingkan migrasi beban kerja melalui otomatisasi dan pengiriman tangkas. Ini adalah fase ketiga dari strategi AWS migrasi.

pabrik migrasi

Tim lintas fungsi yang merampingkan migrasi beban kerja melalui pendekatan otomatis dan gesit. Tim pabrik migrasi biasanya mencakup operasi, analis dan pemilik bisnis, insinyur migrasi, pengembang, dan DevOps profesional yang bekerja di sprint. Antara 20 dan 50 persen portofolio aplikasi perusahaan terdiri dari pola berulang yang dapat dioptimalkan dengan pendekatan pabrik. Untuk informasi selengkapnya, lihat diskusi tentang pabrik migrasi dan panduan Pabrik Migrasi Cloud di kumpulan konten ini.

metadata migrasi

Informasi tentang aplikasi dan server yang diperlukan untuk menyelesaikan migrasi. Setiap pola migrasi memerlukan satu set metadata migrasi yang berbeda. Contoh metadata migrasi termasuk subnet target, grup keamanan, dan akun. AWS

pola migrasi

Tugas migrasi berulang yang merinci strategi migrasi, tujuan migrasi, dan aplikasi atau layanan migrasi yang digunakan. Contoh: Rehost migrasi ke Amazon EC2 dengan Layanan Migrasi AWS Aplikasi.

Penilaian Portofolio Migrasi (MPA)

Alat online yang menyediakan informasi untuk memvalidasi kasus bisnis untuk bermigrasi ke. AWS Cloud MPA menyediakan penilaian portofolio terperinci (ukuran kanan server, harga, perbandingan TCO, analisis biaya migrasi) serta perencanaan migrasi (analisis data aplikasi dan pengumpulan data, pengelompokan aplikasi, prioritas migrasi, dan perencanaan gelombang). Alat MPA (memerlukan login) tersedia gratis untuk semua AWS konsultan dan konsultan APN Partner.

Penilaian Kesiapan Migrasi (MRA)

Proses mendapatkan wawasan tentang status kesiapan cloud organisasi, mengidentifikasi kekuatan dan kelemahan, dan membangun rencana aksi untuk menutup kesenjangan yang diidentifikasi, menggunakan CAF. AWS Untuk informasi selengkapnya, lihat panduan kesiapan migrasi. MRA adalah tahap pertama dari strategi AWS migrasi.

strategi migrasi

Pendekatan yang digunakan untuk memigrasikan beban kerja ke file. AWS Cloud Untuk informasi lebih lanjut, lihat entri 7 Rs di glosarium ini dan lihat Memobilisasi organisasi Anda untuk mempercepat migrasi skala besar.

ML

Lihat pembelajaran mesin.

modernisasi

Mengubah aplikasi usang (warisan atau monolitik) dan infrastrukturnya menjadi sistem yang gesit, elastis, dan sangat tersedia di cloud untuk mengurangi biaya, mendapatkan efisiensi, dan memanfaatkan inovasi. Untuk informasi selengkapnya, lihat Strategi untuk memodernisasi aplikasi di. AWS Cloud

penilaian kesiapan modernisasi

Evaluasi yang membantu menentukan kesiapan modernisasi aplikasi organisasi; mengidentifikasi manfaat, risiko, dan dependensi; dan menentukan seberapa baik organisasi dapat mendukung keadaan masa depan aplikasi tersebut. Hasil penilaian adalah cetak biru arsitektur target, peta jalan yang merinci fase pengembangan dan tonggak untuk proses modernisasi, dan rencana aksi untuk mengatasi kesenjangan yang diidentifikasi. Untuk informasi lebih lanjut, lihat Mengevaluasi kesiapan modernisasi untuk aplikasi di. AWS Cloud

aplikasi monolitik (monolit)

Aplikasi yang berjalan sebagai layanan tunggal dengan proses yang digabungkan secara ketat. Aplikasi monolitik memiliki beberapa kelemahan. Jika satu fitur aplikasi mengalami lonjakan permintaan, seluruh arsitektur harus diskalakan. Menambahkan atau meningkatkan fitur aplikasi monolitik juga menjadi lebih kompleks ketika basis kode tumbuh. Untuk mengatasi masalah ini, Anda dapat menggunakan arsitektur microservices. Untuk informasi lebih lanjut, lihat Menguraikan monolit menjadi layanan mikro.

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

Sebuah proses yang membantu menghasilkan prediksi untuk beberapa kelas (memprediksi satu dari lebih dari dua hasil). Misalnya, model ML mungkin bertanya “Apakah produk ini buku, mobil, atau telepon?” atau “Kategori produk mana yang paling menarik bagi pelanggan ini?”

infrastruktur yang bisa berubah

Model yang memperbarui dan memodifikasi infrastruktur yang ada untuk beban kerja produksi. Untuk meningkatkan konsistensi, keandalan, dan prediktabilitas, AWS Well-Architected Framework merekomendasikan penggunaan infrastruktur yang tidak dapat diubah sebagai praktik terbaik.

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

Metode migrasi di mana beban kerja sumber diturunkan selama proses migrasi. Metode ini melibatkan waktu henti yang diperpanjang dan biasanya digunakan untuk beban kerja kecil dan tidak kritis.

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

Metode migrasi di mana beban kerja sumber disalin ke sistem target tanpa diambil offline. Aplikasi yang terhubung ke beban kerja dapat terus berfungsi selama migrasi. Metode ini melibatkan waktu henti nol hingga minimal dan biasanya digunakan untuk beban kerja produksi yang kritis.

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

Protokol komunikasi machine-to-machine (M2M) untuk otomasi industri. OPC-UA menyediakan standar interoperabilitas dengan enkripsi data, otentikasi, dan skema otorisasi.

perjanjian tingkat operasional (OLA)

Perjanjian yang menjelaskan apa yang dijanjikan kelompok TI fungsional untuk diberikan satu sama lain, untuk mendukung perjanjian tingkat layanan (SLA).

Tinjauan Kesiapan Operasional (ORR)

Daftar pertanyaan dan praktik terbaik terkait yang membantu Anda memahami, mengevaluasi, mencegah, atau mengurangi ruang lingkup insiden dan kemungkinan kegagalan. Untuk informasi lebih lanjut, lihat Ulasan Kesiapan Operasional (ORR) dalam Kerangka Kerja Well-Architected AWS .

teknologi operasional (OT)

Sistem perangkat keras dan perangkat lunak yang bekerja dengan lingkungan fisik untuk mengendalikan operasi industri, peralatan, dan infrastruktur. Di bidang manufaktur, integrasi sistem OT dan teknologi informasi (TI) adalah fokus utama untuk transformasi Industri 4.0.

integrasi operasi (OI)

Proses modernisasi operasi di cloud, yang melibatkan perencanaan kesiapan, otomatisasi, dan integrasi. Untuk informasi selengkapnya, lihat panduan integrasi operasi.

jejak organisasi

Jejak yang dibuat oleh AWS CloudTrail itu mencatat semua peristiwa untuk semua Akun AWS dalam organisasi di AWS Organizations. Jejak ini dibuat di setiap Akun AWS bagian organisasi dan melacak aktivitas di setiap akun. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi dalam CloudTrail dokumentasi.

manajemen perubahan organisasi (OCM)

Kerangka kerja untuk mengelola transformasi bisnis utama yang mengganggu dari perspektif orang, budaya, dan kepemimpinan. OCM membantu organisasi mempersiapkan, dan transisi ke, sistem dan strategi baru dengan mempercepat adopsi perubahan, mengatasi masalah transisi, dan mendorong perubahan budaya dan organisasi. Dalam strategi AWS migrasi, kerangka kerja ini disebut percepatan orang, karena kecepatan perubahan yang diperlukan dalam proyek adopsi cloud. Untuk informasi lebih lanjut, lihat panduan OCM.

kontrol akses asal (OAC)

Di CloudFront, opsi yang disempurnakan untuk membatasi akses untuk mengamankan konten Amazon Simple Storage Service (Amazon S3) Anda. OAC mendukung semua bucket S3 di semua Wilayah AWS, enkripsi sisi server dengan AWS KMS (SSE-KMS), dan dinamis dan permintaan ke bucket S3. `PUT` `DELETE`

identitas akses asal (OAI)

Di CloudFront, opsi untuk membatasi akses untuk mengamankan konten Amazon S3 Anda. Saat Anda menggunakan OAI, CloudFront buat prinsipal yang dapat diautentikasi oleh Amazon S3. Prinsipal yang diautentikasi dapat mengakses konten dalam bucket S3 hanya melalui distribusi tertentu. CloudFront Lihat juga OAC, yang menyediakan kontrol akses yang lebih terperinci dan ditingkatkan.

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

Dalam arsitektur AWS multi-akun, VPC yang menangani koneksi jaringan yang dimulai dari dalam aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

P

batas izin

Kebijakan manajemen IAM yang dilampirkan pada prinsipal IAM untuk menetapkan izin maksimum yang dapat dimiliki pengguna atau peran. Untuk informasi selengkapnya, lihat Batas izin dalam dokumentasi IAM.

Informasi Identifikasi Pribadi (PII)

Informasi yang, jika dilihat secara langsung atau dipasangkan dengan data terkait lainnya, dapat digunakan untuk menyimpulkan identitas individu secara wajar. Contoh PII termasuk nama, alamat, dan informasi kontak.

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

Serangkaian langkah yang telah ditentukan sebelumnya yang menangkap pekerjaan yang terkait dengan migrasi, seperti mengirimkan fungsi operasi inti di cloud. Buku pedoman dapat berupa skrip, runbook otomatis, atau ringkasan proses atau langkah-langkah yang diperlukan untuk mengoperasikan lingkungan modern Anda.

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

Objek yang dapat menentukan izin (lihat kebijakan berbasis identitas), menentukan kondisi akses (lihat kebijakan berbasis sumber daya), atau menentukan izin maksimum untuk semua akun di organisasi (lihat kebijakan kontrol layanan). AWS Organizations

ketekunan poliglot

Secara independen memilih teknologi penyimpanan data microservice berdasarkan pola akses data dan persyaratan lainnya. Jika layanan mikro Anda memiliki teknologi penyimpanan data yang sama, mereka dapat menghadapi tantangan implementasi atau mengalami kinerja yang buruk. Layanan mikro lebih mudah diimplementasikan dan mencapai kinerja dan skalabilitas yang lebih baik jika mereka menggunakan penyimpanan data yang paling sesuai dengan kebutuhan mereka. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi data di layanan mikro.

penilaian portofolio

Proses menemukan, menganalisis, dan memprioritaskan portofolio aplikasi untuk merencanakan migrasi. Untuk informasi selengkapnya, lihat Mengevaluasi kesiapan migrasi.

predikat

Kondisi kueri yang mengembalikan `true` atau`false`, biasanya terletak di `WHERE` klausa.

predikat pushdown

Teknik optimasi kueri database yang menyaring data dalam kueri sebelum transfer. Ini mengurangi jumlah data yang harus diambil dan diproses dari database relasional, dan meningkatkan kinerja kueri.

kontrol preventif

Kontrol keamanan yang dirancang untuk mencegah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan pertama untuk membantu mencegah akses tidak sah atau perubahan yang tidak diinginkan ke jaringan Anda. Untuk informasi selengkapnya, lihat Kontrol pencegahan dalam Menerapkan kontrol keamanan pada. AWS

principal

Entitas AWS yang dapat melakukan tindakan dan mengakses sumber daya. Entitas ini biasanya merupakan pengguna root untuk Akun AWS, peran IAM, atau pengguna. Untuk informasi selengkapnya, lihat Prinsip dalam istilah dan konsep Peran dalam dokumentasi IAM.

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona host pribadi

Container yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons kueri DNS untuk domain dan subdomainnya dalam satu atau lebih. VPCs Untuk informasi selengkapnya, lihat Bekerja dengan zona yang dihosting pribadi di dokumentasi Route 53.

kontrol proaktif

Kontrol keamanan yang dirancang untuk mencegah penyebaran sumber daya yang tidak sesuai. Kontrol ini memindai sumber daya sebelum disediakan. Jika sumber daya tidak sesuai dengan kontrol, maka itu tidak disediakan. Untuk informasi selengkapnya, lihat panduan referensi Kontrol dalam AWS Control Tower dokumentasi dan lihat Kontrol proaktif dalam Menerapkan kontrol keamanan pada AWS.

manajemen siklus hidup produk (PLM)

Manajemen data dan proses untuk suatu produk di seluruh siklus hidupnya, mulai dari desain, pengembangan, dan peluncuran, melalui pertumbuhan dan kematangan, hingga penurunan dan penghapusan.

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

Di bidang manufaktur, komputer yang sangat andal dan mudah beradaptasi yang memantau mesin dan mengotomatiskan proses manufaktur.

rantai cepat

Menggunakan output dari satu prompt LLM sebagai input untuk prompt berikutnya untuk menghasilkan respons yang lebih baik. Teknik ini digunakan untuk memecah tugas yang kompleks menjadi subtugas, atau untuk secara iteratif memperbaiki atau memperluas respons awal. Ini membantu meningkatkan akurasi dan relevansi respons model dan memungkinkan hasil yang lebih terperinci dan dipersonalisasi.

pseudonimisasi

Proses penggantian pengenal pribadi dalam kumpulan data dengan nilai placeholder. Pseudonimisasi dapat membantu melindungi privasi pribadi. Data pseudonim masih dianggap sebagai data pribadi.

publish/subscribe (pub/sub)

Pola yang memungkinkan komunikasi asinkron antara layanan mikro untuk meningkatkan skalabilitas dan daya tanggap. Misalnya, dalam MES berbasis layanan mikro, layanan mikro dapat mempublikasikan pesan peristiwa ke saluran yang dapat berlangganan layanan mikro lainnya. Sistem dapat menambahkan layanan mikro baru tanpa mengubah layanan penerbitan.

Q

rencana kueri

Serangkaian langkah, seperti instruksi, yang digunakan untuk mengakses data dalam sistem database relasional SQL.

regresi rencana kueri

Ketika pengoptimal layanan database memilih rencana yang kurang optimal daripada sebelum perubahan yang diberikan ke lingkungan database. Hal ini dapat disebabkan oleh perubahan statistik, kendala, pengaturan lingkungan, pengikatan parameter kueri, dan pembaruan ke mesin database.

R

Matriks RACI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

LAP

Lihat Retrieval Augmented Generation.

ransomware

Perangkat lunak berbahaya yang dirancang untuk memblokir akses ke sistem komputer atau data sampai pembayaran dilakukan.

Matriks RASCI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

Salinan database yang digunakan untuk tujuan read-only. Anda dapat merutekan kueri ke replika baca untuk mengurangi beban pada database utama Anda.

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

Jumlah waktu maksimum yang dapat diterima sejak titik pemulihan data terakhir. Ini menentukan apa yang dianggap sebagai kehilangan data yang dapat diterima antara titik pemulihan terakhir dan gangguan layanan.

tujuan waktu pemulihan (RTO)

Penundaan maksimum yang dapat diterima antara gangguan layanan dan pemulihan layanan.

refactor

Lihat 7 Rs.

Wilayah

Kumpulan AWS sumber daya di wilayah geografis. Masing-masing Wilayah AWS terisolasi dan independen dari yang lain untuk memberikan toleransi kesalahan, stabilitas, dan ketahanan. Untuk informasi selengkapnya, lihat Menentukan Wilayah AWS akun yang dapat digunakan.

regresi

Teknik ML yang memprediksi nilai numerik. Misalnya, untuk memecahkan masalah "Berapa harga rumah ini akan dijual?" Model ML dapat menggunakan model regresi linier untuk memprediksi harga jual rumah berdasarkan fakta yang diketahui tentang rumah (misalnya, luas persegi).

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

Kemampuan aplikasi untuk melawan atau pulih dari gangguan. Ketersediaan tinggi dan pemulihan bencana adalah pertimbangan umum ketika merencanakan ketahanan di. AWS Cloud Untuk informasi lebih lanjut, lihat AWS Cloud Ketahanan.

kebijakan berbasis sumber daya

Kebijakan yang dilampirkan ke sumber daya, seperti bucket Amazon S3, titik akhir, atau kunci enkripsi. Jenis kebijakan ini menentukan prinsipal mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

matriks yang bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI)

Matriks yang mendefinisikan peran dan tanggung jawab untuk semua pihak yang terlibat dalam kegiatan migrasi dan operasi cloud. Nama matriks berasal dari jenis tanggung jawab yang

didefinisikan dalam matriks: bertanggung jawab (R), akuntabel (A), dikonsultasikan (C), dan diinformasikan (I). Jenis dukungan (S) adalah opsional. Jika Anda menyertakan dukungan, matriks disebut matriks RASCI, dan jika Anda mengecualikannya, itu disebut matriks RACI.

kontrol responsif

Kontrol keamanan yang dirancang untuk mendorong remediasi efek samping atau penyimpangan dari garis dasar keamanan Anda. Untuk informasi selengkapnya, lihat Kontrol responsif dalam Menerapkan kontrol keamanan pada AWS.

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

Retrieval Augmented Generation (RAG)

Teknologi AI generatif di mana LLM mereferensikan sumber data otoritatif yang berada di luar sumber data pelatihannya sebelum menghasilkan respons. Misalnya, model RAG mungkin melakukan pencarian semantik dari basis pengetahuan organisasi atau data kustom. Untuk informasi lebih lanjut, lihat Apa itu RAG.

rotasi

Proses memperbarui rahasia secara berkala untuk membuatnya lebih sulit bagi penyerang untuk mengakses kredensil.

kontrol akses baris dan kolom (RCAC)

Penggunaan ekspresi SQL dasar dan fleksibel yang telah menetapkan aturan akses. RCAC terdiri dari izin baris dan topeng kolom.

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

Satu set prosedur manual atau otomatis yang diperlukan untuk melakukan tugas tertentu. Ini biasanya dibangun untuk merampingkan operasi berulang atau prosedur dengan tingkat kesalahan yang tinggi.

D

SAML 2.0

Standar terbuka yang digunakan oleh banyak penyedia identitas (IdPs). Fitur ini memungkinkan sistem masuk tunggal gabungan (SSO), sehingga pengguna dapat masuk ke AWS Management Console atau memanggil operasi AWS API tanpa Anda harus membuat pengguna di IAM untuk semua orang di organisasi Anda. Untuk informasi lebih lanjut tentang federasi berbasis SAMP 2.0, lihat Tentang federasi berbasis SAMP 2.0 dalam dokumentasi IAM.

PENIPUAN

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

Dalam AWS Secrets Manager, informasi rahasia atau terbatas, seperti kata sandi atau kredensil pengguna, yang Anda simpan dalam bentuk terenkripsi. Ini terdiri dari nilai rahasia dan metadata-nya. Nilai rahasia dapat berupa biner, string tunggal, atau beberapa string. Untuk informasi selengkapnya, lihat Apa yang ada di rahasia Secrets Manager? dalam dokumentasi Secrets Manager.

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

Pagar pembatas teknis atau administratif yang mencegah, mendeteksi, atau mengurangi kemampuan pelaku ancaman untuk mengeksploitasi kerentanan keamanan. Ada empat jenis kontrol keamanan utama: preventif, detektif, responsif, dan proaktif.

pengerasan keamanan

Proses mengurangi permukaan serangan untuk membuatnya lebih tahan terhadap serangan. Ini dapat mencakup tindakan seperti menghapus sumber daya yang tidak lagi diperlukan, menerapkan praktik keamanan terbaik untuk memberikan hak istimewa paling sedikit, atau menonaktifkan fitur yang tidak perlu dalam file konfigurasi.

sistem informasi keamanan dan manajemen acara (SIEM)

Alat dan layanan yang menggabungkan sistem manajemen informasi keamanan (SIM) dan manajemen acara keamanan (SEM). Sistem SIEM mengumpulkan, memantau, dan menganalisis data dari server, jaringan, perangkat, dan sumber lain untuk mendeteksi ancaman dan pelanggaran keamanan, dan untuk menghasilkan peringatan.

otomatisasi respons keamanan

Tindakan yang telah ditentukan dan diprogram yang dirancang untuk secara otomatis merespons atau memulihkan peristiwa keamanan. Otomatisasi ini berfungsi sebagai kontrol keamanan detektif atau responsif yang membantu Anda menerapkan praktik terbaik AWS keamanan. Contoh tindakan respons otomatis termasuk memodifikasi grup keamanan VPC, menambal instans EC2 Amazon, atau memutar kredensil.

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

Kebijakan yang menyediakan kontrol terpusat atas izin untuk semua akun di organisasi. AWS Organizations SCPs menentukan pagar pembatas atau menetapkan batasan pada tindakan yang dapat didelegasikan oleh administrator kepada pengguna atau peran. Anda dapat menggunakan SCPs daftar izin atau daftar penolakan, untuk menentukan layanan atau tindakan mana yang diizinkan atau dilarang. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam AWS Organizations dokumentasi.

titik akhir layanan

URL titik masuk untuk file Layanan AWS. Anda dapat menggunakan endpoint untuk terhubung secara terprogram ke layanan target. Untuk informasi selengkapnya, lihat Layanan AWS titik akhir di Referensi Umum AWS.

perjanjian tingkat layanan (SLA)

Perjanjian yang menjelaskan apa yang dijanjikan tim TI untuk diberikan kepada pelanggan mereka, seperti waktu kerja dan kinerja layanan.

indikator tingkat layanan (SLI)

Pengukuran aspek kinerja layanan, seperti tingkat kesalahan, ketersediaan, atau throughputnya.

tujuan tingkat layanan (SLO)

Metrik target yang mewakili kesehatan layanan, yang diukur dengan indikator tingkat layanan.

model tanggung jawab bersama

Model yang menjelaskan tanggung jawab yang Anda bagikan AWS untuk keamanan dan kepatuhan cloud. AWS bertanggung jawab atas keamanan cloud, sedangkan Anda bertanggung jawab atas keamanan di cloud. Untuk informasi selengkapnya, lihat Model tanggung jawab bersama.

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

Kegagalan dalam satu komponen penting dari aplikasi yang dapat mengganggu sistem.

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

Pola untuk menskalakan dan mempercepat proyek modernisasi. Ketika fitur baru dan rilis produk didefinisikan, tim inti berpisah untuk membuat tim produk baru. Ini membantu meningkatkan kemampuan dan layanan organisasi Anda, meningkatkan produktivitas pengembang, dan

mendukung inovasi yang cepat. Untuk informasi lebih lanjut, lihat Pendekatan bertahap untuk memodernisasi aplikasi di. AWS Cloud

SPOF

Lihat satu titik kegagalan.

skema bintang

Struktur organisasi database yang menggunakan satu tabel fakta besar untuk menyimpan data transaksional atau terukur dan menggunakan satu atau lebih tabel dimensi yang lebih kecil untuk menyimpan atribut data. Struktur ini dirancang untuk digunakan dalam gudang data atau untuk tujuan intelijen bisnis.

pola ara pencekik

Pendekatan untuk memodernisasi sistem monolitik dengan menulis ulang secara bertahap dan mengganti fungsionalitas sistem sampai sistem warisan dapat dinonaktifkan. Pola ini menggunakan analogi pohon ara yang tumbuh menjadi pohon yang sudah mapan dan akhirnya mengatasi dan menggantikan inangnya. Pola ini diperkenalkan oleh Martin Fowler sebagai cara untuk mengelola risiko saat menulis ulang sistem monolitik. Untuk contoh cara menerapkan pola ini, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

subnet

Rentang alamat IP dalam VPC Anda. Subnet harus berada di Availability Zone tunggal.

kontrol pengawasan dan akuisisi data (SCADA)

Di bidang manufaktur, sistem yang menggunakan perangkat keras dan perangkat lunak untuk memantau aset fisik dan operasi produksi.

enkripsi simetris

Algoritma enkripsi yang menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data.

pengujian sintetis

Menguji sistem dengan cara yang mensimulasikan interaksi pengguna untuk mendeteksi potensi masalah atau untuk memantau kinerja. Anda dapat menggunakan Amazon CloudWatch Synthetics untuk membuat tes ini.

sistem prompt

Teknik untuk memberikan konteks, instruksi, atau pedoman ke LLM untuk mengarahkan perilakunya. Permintaan sistem membantu mengatur konteks dan menetapkan aturan untuk interaksi dengan pengguna.

T

tag

Pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya Anda. AWS Tag dapat membantu Anda mengelola, mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Untuk informasi selengkapnya, lihat Menandai sumber daya AWS.

variabel target

Nilai yang Anda coba prediksi dalam ML yang diawasi. Ini juga disebut sebagai variabel hasil. Misalnya, dalam pengaturan manufaktur, variabel target bisa menjadi cacat produk.

daftar tugas

Alat yang digunakan untuk melacak kemajuan melalui runbook. Daftar tugas berisi ikhtisar runbook dan daftar tugas umum yang harus diselesaikan. Untuk setiap tugas umum, itu termasuk perkiraan jumlah waktu yang dibutuhkan, pemilik, dan kemajuan.

lingkungan uji

Lihat lingkungan.

pelatihan

Untuk menyediakan data bagi model ML Anda untuk dipelajari. Data pelatihan harus berisi jawaban yang benar. Algoritma pembelajaran menemukan pola dalam data pelatihan yang memetakan atribut data input ke target (jawaban yang ingin Anda prediksi). Ini menghasilkan model ML yang menangkap pola-pola ini. Anda kemudian dapat menggunakan model ML untuk membuat prediksi pada data baru yang Anda tidak tahu targetnya.

gerbang transit

Hub transit jaringan yang dapat Anda gunakan untuk menghubungkan jaringan Anda VPCs dan lokal. Untuk informasi selengkapnya, lihat Apa itu gateway transit dalam AWS Transit Gateway dokumentasi.

alur kerja berbasis batang

Pendekatan di mana pengembang membangun dan menguji fitur secara lokal di cabang fitur dan kemudian menggabungkan perubahan tersebut ke cabang utama. Cabang utama kemudian dibangun untuk pengembangan, praproduksi, dan lingkungan produksi, secara berurutan.

akses tepercaya

Memberikan izin ke layanan yang Anda tentukan untuk melakukan tugas di organisasi Anda di dalam AWS Organizations dan di akunnya atas nama Anda. Layanan tepercaya menciptakan peran terkait layanan di setiap akun, ketika peran itu diperlukan, untuk melakukan tugas manajemen untuk Anda. Untuk informasi selengkapnya, lihat Menggunakan AWS Organizations dengan AWS layanan lain dalam AWS Organizations dokumentasi.

penyetelan

Untuk mengubah aspek proses pelatihan Anda untuk meningkatkan akurasi model ML. Misalnya, Anda dapat melatih model ML dengan membuat set pelabelan, menambahkan label, dan kemudian mengulangi langkah-langkah ini beberapa kali di bawah pengaturan yang berbeda untuk mengoptimalkan model.

tim dua pizza

Sebuah DevOps tim kecil yang bisa Anda beri makan dengan dua pizza. Ukuran tim dua pizza memastikan peluang terbaik untuk berkolaborasi dalam pengembangan perangkat lunak.

U

waswas

Sebuah konsep yang mengacu pada informasi yang tidak tepat, tidak lengkap, atau tidak diketahui yang dapat merusak keandalan model ML prediktif. Ada dua jenis ketidakpastian: ketidakpastian epistemik disebabkan oleh data yang terbatas dan tidak lengkap, sedangkan ketidakpastian aleatorik disebabkan oleh kebisingan dan keacakan yang melekat dalam data. Untuk informasi lebih lanjut, lihat panduan Mengukur ketidakpastian dalam sistem pembelajaran mendalam.

tugas yang tidak terdiferensiasi

Juga dikenal sebagai angkat berat, pekerjaan yang diperlukan untuk membuat dan mengoperasikan aplikasi tetapi itu tidak memberikan nilai langsung kepada pengguna akhir atau

memberikan keunggulan kompetitif. Contoh tugas yang tidak terdiferensiasi termasuk pengadaan, pemeliharaan, dan perencanaan kapasitas.

lingkungan atas

Lihat lingkungan.

V

menyedot debu

Operasi pemeliharaan database yang melibatkan pembersihan setelah pembaruan tambahan untuk merebut kembali penyimpanan dan meningkatkan kinerja.

kendali versi

Proses dan alat yang melacak perubahan, seperti perubahan kode sumber dalam repositori.

Peering VPC

Koneksi antara dua VPCs yang memungkinkan Anda untuk merutekan lalu lintas dengan menggunakan alamat IP pribadi. Untuk informasi selengkapnya, lihat Apa itu peering VPC di dokumentasi VPC Amazon.

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

Cache buffer yang berisi data saat ini dan relevan yang sering diakses. Instance database dapat membaca dari cache buffer, yang lebih cepat daripada membaca dari memori utama atau disk.

data hangat

Data yang jarang diakses. Saat menanyakan jenis data ini, kueri yang cukup lambat biasanya dapat diterima.

fungsi jendela

Fungsi SQL yang melakukan perhitungan pada sekelompok baris yang berhubungan dengan catatan saat ini. Fungsi jendela berguna untuk memproses tugas, seperti menghitung rata-rata bergerak atau mengakses nilai baris berdasarkan posisi relatif dari baris saat ini.

beban kerja

Kumpulan sumber daya dan kode yang memberikan nilai bisnis, seperti aplikasi yang dihadapi pelanggan atau proses backend.

aliran kerja

Grup fungsional dalam proyek migrasi yang bertanggung jawab atas serangkaian tugas tertentu. Setiap alur kerja independen tetapi mendukung alur kerja lain dalam proyek. Misalnya, alur kerja portofolio bertanggung jawab untuk memprioritaskan aplikasi, perencanaan gelombang, dan mengumpulkan metadata migrasi. Alur kerja portofolio mengirimkan aset ini ke alur kerja migrasi, yang kemudian memigrasikan server dan aplikasi.

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat AWS Kerangka Kualifikasi Beban Kerja.

tulis sekali, baca banyak (WORM)

Model penyimpanan yang menulis data satu kali dan mencegah data dihapus atau dimodifikasi. Pengguna yang berwenang dapat membaca data sebanyak yang diperlukan, tetapi mereka tidak dapat mengubahnya. Infrastruktur penyimpanan data ini dianggap tidak dapat diubah.

Z

eksploitasi zero-day

Serangan, biasanya malware, yang memanfaatkan kerentanan zero-day.

kerentanan zero-day

Cacat atau kerentanan yang tak tanggung-tanggung dalam sistem produksi. Aktor ancaman dapat menggunakan jenis kerentanan ini untuk menyerang sistem. Pengembang sering menyadari kerentanan sebagai akibat dari serangan tersebut.

bisikan zero-shot

Memberikan LLM dengan instruksi untuk melakukan tugas tetapi tidak ada contoh (tembakan) yang dapat membantu membimbingnya. LLM harus menggunakan pengetahuan pra-terlatih untuk menangani tugas. Efektivitas bidikan nol tergantung pada kompleksitas tugas dan kualitas prompt. Lihat juga beberapa bidikan yang diminta.

aplikasi zombie

Aplikasi yang memiliki CPU rata-rata dan penggunaan memori di bawah 5 persen. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini.

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