Praktik dan fitur terbaik enkripsi untuk Layanan AWS

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Praktik dan fitur terbaik enkripsi untuk Layanan AWS

Table of Contents

Praktik dan fitur terbaik enkripsi untukLayanan AWS

Kurt Kumar, Layanan Web Amazon (AWS)

Desember 2022(sejarah dokumen)

Ancaman keamanan siber modern mencakup risiko pelanggaran data, yaitu ketika orang yang berwenang mendapatkan akses ke jaringan Anda dan mencuri data perusahaan Anda. Data adalah aset bisnis yang unik untuk setiap organisasi. Ini dapat mencakup informasi pelanggan, rencana bisnis, dokumen desain, atau kode. Melindungi bisnis berarti melindungi datanya.

Tindakan seperti firewall dapat membantu mencegah terjadinya pelanggaran data. Namun, enkripsi data dapat membantu melindungi data bisnis Anda bahkan setelah terjadi pelanggaran. Ini memberikan lapisan pertahanan lain terhadap pengungkapan yang tidak diinginkan. Untuk mengakses data terenkripsi diAWS Cloud, pengguna memerlukan izin untuk menggunakan kunci untuk mendekripsi dan memerlukan izin untuk menggunakan layanan tempat data berada. Tanpa kedua izin ini, pengguna tidak dapat mendekripsi dan melihat data.

Secara umum, ada dua jenis data yang dapat Anda enkripsi. Data dalam perjalananadalah data yang secara aktif bergerak melalui jaringan Anda, seperti antara sumber daya jaringan. Data saat istirahatadalah data yang stasioner dan tidak aktif, seperti data yang ada dalam penyimpanan. Contohnya termasuk penyimpanan blok, penyimpanan objek, database, arsip, dan perangkat Internet of Things (IoT). Panduan ini membahas pertimbangan dan praktik terbaik untuk mengenkripsi kedua jenis data. Ini juga meninjau fitur enkripsi dan kontrol yang tersedia di banyakLayanan AWSsehingga Anda dapat menerapkan rekomendasi enkripsi ini di tingkat layanan diAWS Cloudlingkungan.

Audiens yang dituju

Panduan ini dapat digunakan oleh organisasi kecil, menengah, dan besar baik di sektor publik maupun swasta. Apakah organisasi Anda sedang dalam tahap awal menilai dan menerapkan strategi perlindungan data atau bertujuan untuk meningkatkan kontrol keamanan yang ada, rekomendasi yang diuraikan dalam panduan ini paling cocok untuk audiens berikut:

- Pejabat eksekutif yang merumuskan kebijakan untuk perusahaan mereka, seperti chief executive officer (CEO), chief technology officer (CTO), chief information officer (CIO), dan chief information security officer (CISO)
- Petugas teknologi yang bertanggung jawab untuk menetapkan standar teknis, seperti wakil presiden dan direktur teknis

- Pemangku kepentingan bisnis dan pemilik aplikasi yang bertanggung jawab untuk:
  - Menilai postur risiko, klasifikasi data, dan persyaratan perlindungan
  - Memantau kepatuhan dengan standar organisasi yang ditetapkan
- Petugas kepatuhan, audit internal, dan tata kelola yang bertugas memantau kepatuhan terhadap kebijakan kepatuhan, termasuk rezim kepatuhan hukum dan sukarela

TentangAWSlayanan kriptografi

Sebuahalgoritma enkripsiadalah rumus atau prosedur yang mengubah pesan teks biasa menjadi ciphertext terenkripsi. Jika Anda baru mengenal enkripsi atau terminologinya, kami sarankan Anda membacaTentang enkripsi datadanKonsep kriptografisebelum melanjutkan dengan panduan ini.

AWSLayanan kriptografi mengandalkan algoritma enkripsi open-source yang aman. Algoritma ini diperiksa oleh badan standar publik dan oleh penelitian akademis. BeberapaAWSalat dan layanan menegakkan penggunaan algoritma tertentu. Di layanan lain, Anda dapat memilih antara beberapa algoritma yang tersedia dan panjang kunci, atau Anda dapat menggunakan default yang disarankan.

Bagian ini menjelaskan beberapa algoritma yangAWSalat dan layanan dukungan. Mereka terbagi dalam dua kategori, simetris dan asimetris, berdasarkan bagaimana fungsi tombol mereka:

- Simetrisenkripsi menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data.Layanan AWSmendukung Advanced Encryption Standard (AES) dan Triple Data Encryption Standard (3DES atau TDES), yang merupakan dua algoritma simetris yang banyak digunakan. Untuk informasi lebih lanjut, lihatAlgoritma simetrisdiAWSpanduan layanan dan alat kriptografi.
- Asimetrisenkripsi 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.Layanan AWSbiasanya mendukung algoritma asimetris RSA dan eliptic-curve cryptography (ECC). Untuk informasi lebih lanjut, lihatAlgoritma asimetrisdiAWSpanduan layanan dan alat kriptografi.

AWSLayanan kriptografi mematuhi berbagai standar keamanan kriptografi, sehingga Anda dapat mematuhi peraturan pemerintah atau profesional. Untuk daftar lengkap standar keamanan data yangLayanan AWSmematuhi, lihatAWSprogram kepatuhan. Untuk informasi selengkapnya tentang alat dan layanan kriptografi, lihatAWSlayanan dan alat kriptografi.

Praktik terbaik enkripsi umum

Bagian ini memberikan rekomendasi yang berlaku saat mengenkripsi data di. AWS Cloud Praktik terbaik enkripsi umum ini tidak spesifik untukLayanan AWS. Bagian ini mencakup topik-topik berikut:

- Klasifikasi data
- Mengenkripsi data saat transit
- Enkripsi data saat tidak digunakan

Klasifikasi data

Klasifikasi data adalah 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. Kategori mungkin termasuk sangat rahasia, rahasia, tidak rahasia, dan publik, tetapi tingkat klasifikasi dan nama mereka dapat bervariasi dari satu organisasi ke organisasi lainnya. Untuk informasi lebih lanjut tentang proses klasifikasi data, pertimbangan, dan model, lihat Klasifikasi data (AWSWhitepaper).

Setelah mengklasifikasikan data Anda, Anda dapat membuat strategi enkripsi untuk organisasi Anda berdasarkan tingkat perlindungan yang diperlukan untuk setiap kategori. Misalnya, organisasi Anda mungkin memutuskan bahwa data yang sangat rahasia harus menggunakan enkripsi asimetris dan bahwa data publik tidak memerlukan enkripsi. Untuk informasi selengkapnya tentang merancang strategi enkripsi, lihat Membuat strategi enkripsi perusahaan untuk data saat istirahat. Meskipun pertimbangan teknis dan rekomendasi dalam panduan itu khusus untuk data saat istirahat, Anda dapat menggunakan pendekatan bertahap untuk membuat strategi enkripsi untuk data dalam perjalanan juga.

Mengenkripsi data saat transit

Semua data yang dikirimkan Wilayah AWS melalui jaringan AWS global secara otomatis dienkripsi pada lapisan fisik sebelum meninggalkan fasilitas yang AWS aman. Semua lalu lintas antara Availability Zones dienkripsi.

Berikut ini adalah praktik terbaik umum saat mengenkripsi data dalam perjalanan di: AWS Cloud

- Tentukan kebijakan enkripsi organisasi untuk data dalam perjalanan, berdasarkan klasifikasi data Anda, persyaratan organisasi, dan standar peraturan atau kepatuhan yang berlaku. Kami sangat menyarankan agar Anda mengenkripsi data dalam perjalanan yang diklasifikasikan sebagai sangat rahasia atau rahasia. Kebijakan Anda mungkin juga menentukan enkripsi untuk kategori lain, seperti data non-rahasia atau publik, sesuai kebutuhan.
- Saat mengenkripsi data dalam perjalanan, sebaiknya gunakan algoritme kriptografi yang disetujui, mode sandi blok, dan panjang kunci, sebagaimana didefinisikan dalam kebijakan enkripsi Anda.
- Enkripsi lalu lintas antara aset informasi dan sistem dalam jaringan perusahaan dan AWS Cloud infrastruktur dengan menggunakan salah satu dari berikut ini:
  - Koneksi AWS Site-to-Site VPN
  - Kombinasi AWS Site-to-Site VPN dan AWS Direct Connectkoneksi, yang menyediakan koneksi pribadi terenkripsi IPsec
  - AWS Direct Connectkoneksi yang mendukung MAC Security (MacSec) untuk mengenkripsi data dari jaringan perusahaan ke lokasi Amazon VPC
- Identifikasi kebijakan kontrol akses untuk kunci enkripsi Anda berdasarkan prinsip hak istimewa paling sedikit. Keistimewaan paling sedikit adalah praktik keamanan terbaik untuk memberikan pengguna akses minimum yang mereka butuhkan untuk menjalankan fungsi pekerjaan mereka. Untuk informasi selengkapnya tentang penerapan izin hak istimewa terkecil, lihat Praktik terbaik keamanan di IAM dan Praktik terbaik untuk kebijakan IAM.

Enkripsi data saat tidak digunakan

Semua layanan penyimpanan AWS data, seperti Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) dan Amazon Elastic File System (Amazon EFS), menyediakan opsi untuk mengenkripsi data saat istirahat. Enkripsi dilakukan dengan menggunakan 256-bit Advanced Encryption Standard (AES-256) blok cipher dan layanan AWS kriptografi, seperti () atau. AWS Key Management ServiceAWS KMSAWS CloudHSM

Anda dapat mengenkripsi data menggunakan enkripsi sisi klien atau enkripsi sisi server, berdasarkan faktor-faktor seperti klasifikasi data, kebutuhan end-to-end enkripsi, atau batasan teknis yang mencegah Anda menggunakan enkripsi: end-to-end

- Enkripsi sisi klien adalah tindakan mengenkripsi data secara lokal sebelum aplikasi atau layanan target menerimanya. Layanan AWSMenerima data terenkripsi; itu tidak memainkan peran dalam mengenkripsi atau mendekripsi itu. Untuk enkripsi sisi klien, Anda dapat menggunakanAWS KMS, atau alat atau layanan enkripsi pihak ketiga lainnya. AWS Encryption SDK

- Enkripsi sisi server adalah tindakan mengenkripsi data di tujuannya, oleh aplikasi atau layanan yang menerimanya. Untuk enkripsi sisi server, Anda dapat menggunakan AWS KMS enkripsi seluruh blok penyimpanan. Anda juga dapat menggunakan alat atau layanan enkripsi pihak ketiga lainnya, seperti LUKS untuk mengenkripsi sistem file Linux di tingkat sistem operasi (OS).

Berikut ini adalah praktik terbaik umum saat mengenkripsi data saat istirahat di: AWS Cloud

- Tentukan kebijakan enkripsi organisasi untuk data saat istirahat, berdasarkan klasifikasi data Anda, persyaratan organisasi, dan standar peraturan atau kepatuhan yang berlaku. Untuk informasi selengkapnya, lihat Membuat strategi enkripsi perusahaan untuk data saat istirahat. Kami sangat menyarankan agar Anda mengenkripsi data saat istirahat yang diklasifikasikan sebagai sangat rahasia atau rahasia. Kebijakan Anda mungkin juga menentukan enkripsi untuk kategori lain, seperti data non-rahasia atau publik, sesuai kebutuhan.
- Saat mengenkripsi data saat istirahat, sebaiknya gunakan algoritma kriptografi yang disetujui, mode sandi blok, dan panjang kunci.
- Identifikasi kebijakan kontrol akses untuk kunci enkripsi Anda berdasarkan prinsip hak istimewa paling sedikit.

Praktik terbaik enkripsi untuk Layanan AWS

Bagian ini mencakup praktik terbaik dan rekomendasi untuk spesifik Layanan AWS. Bagian ini membahas layanan berikut:

- AWS CloudTrail
- Amazon DynamoDB
- Amazon Elastic Compute Cloud (Amazon EC2) dan Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Encryption SDK
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- Amazon Relational Database Service (Amazon RDS)
- AWS Secrets Manager
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (Amazon VPC)

AWS CloudTrail

AWS CloudTrailmembantu Anda mengaudit tata kelola, kepatuhan, dan operasional serta risiko Anda Akun AWS.

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- CloudTrail log harus dienkripsi menggunakan pelanggan yang dikelola. AWS KMS key Pilih kunci KMS yang berada di wilayah yang sama dengan bucket S3 yang menerima file log Anda. Untuk informasi selengkapnya, lihat Memperbarui jejak untuk menggunakan kunci KMS Anda.
- Sebagai lapisan keamanan tambahan, aktifkan validasi file log untuk jejak. Ini membantu Anda menentukan apakah file log diubah, dihapus, atau tidak diubah setelah CloudTrail dikirimkan. Untuk petunjuk, lihat Mengaktifkan validasi integritas file log untuk. CloudTrail

- Gunakan antarmuka VPC endpoint untuk memungkinkan CloudTrail untuk berkomunikasi dengan sumber daya di VPC lain tanpa melintasi internet publik. Untuk informasi selengkapnya, lihat Menggunakan AWS CloudTrail dengan titik akhir VPC antarmuka.
- Tambahkan kunci `aws:SourceArn` kondisi ke kebijakan kunci KMS untuk memastikan bahwa CloudTrail menggunakan kunci KMS hanya untuk jejak atau jalur tertentu. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS KMS key kebijakan untuk CloudTrail.
- Di AWS Config, terapkan aturan cloud-trail-encryption-enabled AWS terkelola untuk memvalidasi dan menegakkan enkripsi file log.
- Jika CloudTrail dikonfigurasi untuk mengirim notifikasi melalui topik Amazon Simple Notification Service (Amazon SNS), tambahkan `aws:SourceArn` kunci kondisi (atau `aws:SourceAccount` opsional) ke pernyataan kebijakan untuk mencegah akses akun CloudTrail yang tidak sah ke topik SNS. Untuk informasi selengkapnya, lihat kebijakan topik Amazon SNS untuk. CloudTrail
- Jika Anda menggunakan AWS Organizations, buat jejak organisasi yang mencatat semua peristiwa Akun AWS di organisasi tersebut. Ini termasuk akun manajemen dan semua akun anggota dalam organisasi. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi.
- Buat jejak yang berlaku untuk semua Wilayah AWS tempat Anda menyimpan data perusahaan, untuk merekam Akun AWS aktivitas di Wilayah tersebut. Saat AWS meluncurkan Wilayah baru, CloudTrail secara otomatis menyertakan Wilayah baru dan mencatat peristiwa di Wilayah tersebut.

Amazon DynamoDB

Amazon DynamoDB adalah layanan database NoSQL yang dikelola sepenuhnya yang menyediakan kinerja yang cepat, dapat diprediksi, dan terukur. Enkripsi DynamoDB saat istirahat mengamankan data dalam tabel terenkripsi — termasuk kunci utama, indeks sekunder lokal dan global, aliran, tabel global, cadangan, dan klaster DynamoDB Accelerator (DAX) setiap kali data disimpan dalam media tahan lama.

Sesuai dengan persyaratan klasifikasi data, kerahasiaan dan integritas data dapat dipertahankan dengan menerapkan enkripsi sisi server atau sisi klien:

Untuk enkripsi sisi server, saat Anda membuat tabel baru, Anda dapat menggunakan AWS KMS keys untuk mengenkripsi tabel. Anda dapat menggunakan kunci AWS yang dimiliki, kunci AWS terkelola, atau kunci yang dikelola pelanggan. Sebaiknya gunakan kunci yang dikelola pelanggan karena organisasi Anda memiliki kontrol penuh atas kunci tersebut, dan karena ketika Anda menggunakan jenis kunci ini, kunci enkripsi tingkat tabel, tabel DynamoDB, indeks sekunder lokal dan global, dan

aliran semuanya dienkripsi dengan kunci yang sama. Untuk informasi selengkapnya tentang jenis kunci ini, lihat Kunci dan AWS kunci pelanggan.

> **Note**
>
> Anda dapat beralih antara kunci yang AWS dimiliki, kunci AWS terkelola, dan kunci yang dikelola pelanggan pada waktu tertentu.

Untuk enkripsi sisi klien dan end-to-end perlindungan data, baik saat istirahat maupun saat transit, Anda dapat menggunakan Klien Enkripsi Amazon DynamoDB. Selain enkripsi, yang melindungi kerahasiaan nilai atribut item, Klien Enkripsi DynamoDB menandatangani item tersebut. Ini memberikan perlindungan integritas dengan memungkinkan deteksi perubahan yang tidak sah pada item, termasuk menambahkan atau menghapus atribut, atau mengganti satu nilai terenkripsi dengan yang lain.

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- Batasi izin untuk menonaktifkan atau menjadwalkan penghapusan kunci hanya untuk mereka yang perlu melakukan tugas-tugas ini. Status ini mencegah semua pengguna dan layanan DynamoDB untuk dapat mengenkripsi atau mendekripsi data dan melakukan operasi baca dan tulis di atas meja.
- Sementara DynamoDB mengenkripsi data dalam perjalanan dengan menggunakan HTTPS secara default, kontrol keamanan tambahan direkomendasikan. Anda dapat menggunakan salah satu opsi berikut:
  - AWS Site-to-Site VPN koneksi menggunakan IPsec untuk enkripsi.
  - AWS Direct Connect koneksi untuk membuat koneksi pribadi.
  - AWS Direct Connect koneksi dengan AWS Site-to-Site VPN koneksi untuk koneksi pribadi terenkripsi IPsec.
  - Jika akses ke DynamoDB hanya diperlukan dari dalam virtual private cloud (VPC), Anda dapat menggunakan titik akhir gateway VPC dan hanya mengizinkan sumber daya di VPC untuk mengaksesnya. Ini mencegah lalu lintas melintasi internet publik.
- Jika Anda menggunakan titik akhir VPC, batasi kebijakan titik akhir dan kebijakan IAM yang terkait dengan titik akhir hanya untuk pengguna, sumber daya, dan layanan yang berwenang. Untuk informasi selengkapnya, lihat Mengontrol akses ke titik akhir DynamoDB menggunakan kebijakan IAM dan Kontrol akses ke layanan menggunakan kebijakan titik akhir.

- Anda dapat menerapkan enkripsi data tingkat kolom di tingkat aplikasi untuk data yang memerlukan enkripsi, sesuai dengan kebijakan enkripsi Anda.
- Konfigurasikan cluster DAX untuk mengenkripsi data saat istirahat, seperti data dalam cache, data konfigurasi, dan file log, pada saat menyiapkan cluster. Anda tidak dapat mengaktifkan enkripsi saat istirahat di cluster yang ada. Enkripsi sisi server ini membantu melindungi data dari akses tidak sah melalui penyimpanan yang mendasarinya. Enkripsi DAX saat istirahat secara otomatis terintegrasi dengan AWS KMS untuk mengelola kunci default layanan tunggal yang digunakan untuk mengenkripsi cluster. Jika kunci default layanan tidak ada saat kluster DAX terenkripsi dibuat, AWS KMS secara otomatis akan membuat kunci terkelola baru AWS . Untuk informasi selengkapnya, lihat enkripsi DAX saat istirahat.

  > **Note**
  >
  > Kunci terkelola pelanggan tidak dapat digunakan dengan kluster DAX.

- Konfigurasikan cluster DAX untuk mengenkripsi data dalam perjalanan pada saat menyiapkan cluster. Anda tidak dapat mengaktifkan enkripsi saat transit di klaster yang ada. DAX menggunakan TLS untuk mengenkripsi permintaan dan tanggapan antara aplikasi dan cluster, dan menggunakan sertifikat x509 cluster untuk mengotentikasi identitas cluster. Untuk informasi selengkapnya, lihat enkripsi DAX dalam perjalanan.
- Di AWS Config, terapkan aturan dax-encryption-enabled AWS terkelola untuk memvalidasi dan memelihara enkripsi cluster DAX.

Amazon Elastic Compute Cloud dan Amazon Elastic Block Store

Amazon Elastic Compute Cloud (Amazon EC2) menyediakan kapasitas komputasi yang dapat diskalakan di. AWS Cloud Anda dapat meluncurkan server virtual sebanyak yang Anda butuhkan dan dengan cepat meningkatkannya ke atas atau ke bawah. Amazon Elastic Block Store (Amazon EBS) menyediakan volume penyimpanan tingkat blok untuk digunakan dengan instans EC2.

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- Tandai semua volume EBS dengan kunci dan nilai klasifikasi data yang sesuai. Ini membantu Anda menentukan dan menerapkan persyaratan keamanan dan enkripsi yang sesuai, sesuai dengan kebijakan Anda.
- Sesuai dengan kebijakan enkripsi Anda dan kelayakan teknis, konfigurasikan enkripsi untuk data yang sedang transit antara instans EC2 atau antara instans EC2 dan jaringan lokal Anda.

- Enkripsi volume boot dan data EBS dari instans EC2. Volume EBS terenkripsi melindungi data berikut:
  - Data diam di dalam volume
  - Semua data yang bergerak antara volume dan instans
  - Semua snapshot yang dibuat dari volume
  - Semua volume yang dibuat dari snapshot tersebut

Untuk informasi selengkapnya, lihat Cara kerja enkripsi EBS.

- Aktifkan enkripsi secara default untuk volume EBS untuk akun Anda di Wilayah saat ini. Ini memberlakukan enkripsi volume EBS baru dan salinan snapshot. Ini tidak berpengaruh pada volume atau snapshot EBS yang ada. Untuk informasi selengkapnya, lihat Enkripsi secara default.
- Enkripsi volume root penyimpanan instans untuk instans Amazon EC2. Ini membantu Anda melindungi file konfigurasi dan data yang disimpan dengan sistem operasi. Untuk informasi selengkapnya, lihat Cara melindungi data saat istirahat dengan enkripsi penyimpanan instans Amazon EC2 (AWS posting blog)
- Di AWS Config, terapkan aturan volume terenkripsi ke pemeriksaan otomatis yang memvalidasi dan menerapkan konfigurasi enkripsi yang sesuai.

Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) adalah layanan registri gambar kontainer terkelola yang aman, terukur, dan andal.

Amazon ECR menyimpan citra di bucket Amazon S3 yang dikelola Amazon ECR. Setiap repositori Amazon ECR memiliki konfigurasi enkripsi, yang diatur saat repositori tersebut dibuat. Secara default, Amazon ECR menggunakan enkripsi sisi server dengan kunci enkripsi Amazon S3-managed (SSE-S3). Untuk informasi selengkapnya, lihat Enkripsi saat istirahat (dokumentasi Amazon ECR).

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- Alih-alih menggunakan enkripsi sisi server default dengan kunci enkripsi Amazon S3-managed (SSE-S3), gunakan kunci KMS yang dikelola pelanggan yang disimpan di dalamnya. AWS KMS Jenis kunci ini menyediakan opsi kontrol paling granular.

> **Note**
>
> Kunci KMS harus ada Wilayah AWS sama dengan repositori.

- Jangan mencabut hibah yang dibuat Amazon ECR secara default saat Anda menyediakan repositori. Hal ini dapat memengaruhi fungsionalitas, seperti mengakses data, mengenkripsi gambar baru yang didorong ke repositori, atau mendekripsi ketika ditarik.
- Gunakan AWS CloudTrail untuk merekam permintaan yang dikirimkan Amazon ECR. AWS KMS Entri log berisi kunci konteks enkripsi untuk membuatnya lebih mudah diidentifikasi.
- Konfigurasikan kebijakan ECR Amazon untuk mengontrol akses dari titik akhir VPC Amazon tertentu atau VPC tertentu. Secara efektif, ini mengisolasi akses jaringan ke sumber daya Amazon ECR tertentu, memungkinkan akses hanya dari VPC tertentu. Dengan membuat koneksi jaringan pribadi virtual (VPN) dengan titik akhir VPC Amazon, Anda dapat mengenkripsi data dalam perjalanan.
- Amazon ECR mendukung kebijakan berbasis sumber daya Dengan menggunakan kebijakan ini, Anda dapat membatasi akses berdasarkan alamat IP sumber atau spesifik. Layanan AWS

Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) adalah layanan manajemen kontainer yang cepat dan dapat diskalakan yang membantu Anda menjalankan, menghentikan, dan mengelola kontainer di klaster.

Dengan Amazon ECS, Anda dapat mengenkripsi data dalam perjalanan dengan menggunakan salah satu pendekatan berikut:

- Buat mesh layanan. Menggunakan AWS App Mesh, konfigurasikan koneksi TLS antara proxy Envoy yang dikerahkan dan titik akhir mesh, seperti node virtual atau gateway virtual. Anda dapat menggunakan sertifikat TLS dari AWS Private Certificate Authority atau sertifikat yang disediakan pelanggan. Untuk informasi dan penelusuran selengkapnya, lihat Mengaktifkan enkripsi lalu lintas antar layanan dalam AWS App Mesh penggunaan AWS Certificate Manager (ACM) atau sertifikat yang disediakan pelanggan (posting blog).AWS
- Jika didukung, gunakan AWS Nitro Enclave. AWS Nitro Enclave adalah fitur Amazon EC2 yang memungkinkan Anda membuat lingkungan eksekusi terisolasi, yang disebut enclaves, dari instans Amazon EC2. Mereka dirancang untuk membantu melindungi data Anda yang paling sensitif.

Selain itu, ACM untuk Nitro Enclave memungkinkan Anda menggunakan sertifikat SSL/TLS publik dan pribadi dengan aplikasi web dan server web Anda yang berjalan di instans Amazon EC2 dengan Nitro Enclave. AWS Untuk informasi lebih lanjut, lihat Enklaf AWS Nitro - Lingkungan EC2 Terisolasi untuk Memproses Data Rahasia (posting blog).AWS

- Gunakan protokol Server Name Indication (SNI) dengan Application Load Balancer. Anda dapat menerapkan beberapa aplikasi di belakang satu pendengar HTTPS untuk penyeimbang beban aplikasi. Setiap pendengar memiliki sertifikat TLS sendiri. Anda dapat sertifikat yang disediakan oleh ACM, atau Anda dapat menggunakan sertifikat yang ditandatangani sendiri. Baik Application Load Balancer maupun Network Load Balancer mendukung SNI. Untuk informasi selengkapnya, lihat Application Load Balancers Now Support Multiple TLS Certificate with Smart Selection Using SNI (AWS blog post).
- Untuk meningkatkan keamanan dan fleksibilitas, gunakan AWS Private Certificate Authority untuk menerapkan sertifikat TLS dengan tugas Amazon ECS. Untuk informasi selengkapnya, lihat Mempertahankan TLS sampai ke wadah Anda bagian 2: Menggunakan AWS Private CA (posting AWS blog).
- Terapkan TLS bersama (mTL) di App Mesh dengan menggunakan layanan penemuan Rahasia (Utusan) atau sertifikat yang dihosting di ACM (). GitHub

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- Jika memungkinkan secara teknis, untuk keamanan yang ditingkatkan, konfigurasikan titik akhir VPC antarmuka Amazon ECS di. AWS PrivateLink Mengakses titik akhir ini melalui koneksi VPN mengenkripsi data dalam perjalanan.
- Simpan materi sensitif, seperti kunci API atau kredensyal basis data, dengan aman. Anda dapat menyimpan ini sebagai parameter terenkripsi di Parameter Store, kemampuan. AWS Systems Manager Namun, kami sarankan Anda menggunakannya AWS Secrets Manager karena layanan ini memungkinkan Anda untuk secara otomatis memutar rahasia, menghasilkan rahasia acak, dan berbagi rahasia di Akun AWS:
- Untuk membantu mengurangi risiko kebocoran data dari variabel lingkungan, kami sarankan Anda menggunakan dan AWS Secrets Manager Config Provider for Secret Store CSI Driver (). GitHub Driver ini memungkinkan Anda untuk membuat rahasia yang disimpan di Secrets Manager dan parameter yang disimpan di Parameter Store muncul sebagai file yang dipasang di pod Kubernetes.

> **Note**
>
> AWS Fargate tidak didukung.

- Jika pengguna atau aplikasi di pusat data Anda atau pihak ketiga eksternal di web membuat permintaan HTTPS API langsung Layanan AWS, tandatangani permintaan tersebut dengan kredensyal keamanan sementara yang diperoleh dari AWS Security Token Service ()AWS STS.

Amazon Elastic File System

Amazon Elastic File System (Amazon EFS) membantu Anda membuat dan mengonfigurasi sistem file bersama di file AWS Cloud.

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- Di AWS Config, terapkan aturan yang efs-encrypted-check AWS dikelola. Aturan ini memeriksa apakah Amazon EFS dikonfigurasi untuk mengenkripsi data file yang digunakan AWS KMS.
- Terapkan enkripsi untuk sistem file Amazon EFS dengan membuat CloudWatch alarm Amazon yang memantau CloudTrail log untuk `CreateFileSystem` peristiwa dan memicu alarm jika sistem file yang tidak terenkripsi dibuat. Untuk informasi selengkapnya, lihat Panduan: Menerapkan Enkripsi pada Sistem File Amazon EFS saat Istirahat.
- Pasang sistem file dengan menggunakan EFS mount helper. Ini mengatur dan memelihara terowongan TLS 1.2 antara klien dan layanan Amazon EFS dan merutekan semua lalu lintas Network File System (NFS) melalui terowongan terenkripsi ini. Perintah berikut mengimplementasikan penggunaan TLS untuk enkripsi dalam transit.

  ```
  sudo mount -t efs  -o tls file-system-id:/ /mnt/efs
  ```

  Untuk informasi selengkapnya, lihat Menggunakan EFS mount helper untuk memasang sistem file EFS.
- Menggunakan AWS PrivateLink, mengimplementasikan titik akhir VPC antarmuka untuk membuat koneksi pribadi antara VPC dan Amazon EFS API. Data dalam perjalanan melalui koneksi VPN ke dan dari titik akhir dienkripsi. Untuk informasi selengkapnya, lihat Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan.

- Gunakan kunci `elasticfilesystem:Encrypted` kondisi dalam kebijakan berbasis identitas IAM untuk mencegah pengguna membuat sistem file EFS yang tidak dienkripsi. Untuk informasi selengkapnya, lihat Menggunakan IAM untuk menerapkan pembuatan sistem file terenkripsi.
- Kunci KMS yang digunakan untuk enkripsi EFS harus dikonfigurasi untuk akses hak istimewa paling rendah dengan menggunakan kebijakan kunci berbasis sumber daya.
- Gunakan kunci `aws:SecureTransport` kondisi dalam kebijakan sistem file EFS untuk menerapkan penggunaan TLS untuk klien NFS saat menyambung ke sistem file EFS. Untuk informasi selengkapnya, lihat Enkripsi data yang sedang transit di Mengenkripsi Data File dengan Amazon Elastic File System (AWS Whitepaper).

Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service (Amazon EKS) membantu Anda menjalankan AWS Kubernetes tanpa perlu menginstal atau memelihara control plane atau node Kubernetes Anda sendiri. Di Kubernetes, rahasia membantu Anda mengelola informasi sensitif, seperti sertifikat pengguna, kata sandi, atau kunci API. Secara default, rahasia ini disimpan tanpa terenkripsi di penyimpanan data dasar server API, yang disebut etcd. Setiap pengguna dengan akses API atau akses ke `etcd` dapat mengambil atau memodifikasi rahasia. Selain itu, siapa pun yang berwenang untuk membuat pod di namespace dapat menggunakan akses itu untuk membaca rahasia apa pun di namespace itu. Anda dapat mengenkripsi rahasia ini saat istirahat di Amazon EKS dengan menggunakan AWS KMS keys, baik kunci AWS terkelola atau kunci yang dikelola pelanggan. Pendekatan alternatif untuk menggunakan `etcd` adalah menggunakan AWS Secrets and Config Provider (ASCP) (GitHub repositori). ASCP terintegrasi dengan IAM dan kebijakan berbasis sumber daya untuk membatasi dan membatasi akses ke rahasia hanya dalam pod Kubernetes tertentu di dalam klaster.

Anda dapat menggunakan layanan AWS penyimpanan berikut dengan Kubernetes:

- Untuk Amazon Elastic Block Store (Amazon EBS), Anda dapat menggunakan driver penyimpanan in-tree atau driver Amazon EBS CSI. Keduanya mencakup parameter untuk mengenkripsi volume dan memasok kunci yang dikelola pelanggan.
- Untuk Amazon Elastic File System (Amazon EFS), Anda dapat menggunakan driver Amazon EFS CSI dengan dukungan untuk penyediaan dinamis dan statis.

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- Untuk Amazon EFS, konfigurasikan enkripsi saat transit dengan menambahkan `tls` parameter ke `mountOptions` volume persisten Amazon EKS. Untuk informasi selengkapnya, lihat Enkripsi data dan manajemen rahasia (Panduan Praktik Terbaik Amazon EKS).
- Jika Anda menggunakan`etcd`, yang menyimpan objek rahasia yang tidak dienkripsi secara default, lakukan hal berikut untuk membantu melindungi rahasia:
  - Enkripsi data rahasia saat istirahat (dokumentasi Kubernetes).
  - Aktifkan atau konfigurasikan otorisasi melalui aturan kontrol akses berbasis peran (RBAC) yang membatasi membaca dan menulis rahasia. Batasi izin untuk membuat rahasia baru atau mengganti yang sudah ada. Untuk informasi selengkapnya, lihat Ikhtisar otorisasi (dokumentasi Kubernetes).
  - Jika Anda mendefinisikan beberapa kontainer dalam sebuah pod dan hanya satu dari kontainer tersebut yang membutuhkan akses ke rahasia, tentukan volume mount sehingga container lain tidak memiliki akses ke rahasia itu. Rahasia yang dipasang sebagai volume dipakai sebagai `tmpfs` volume dan secara otomatis dihapus dari node saat pod dihapus. Anda juga dapat menggunakan variabel lingkungan, tetapi kami tidak merekomendasikan pendekatan ini karena nilai variabel lingkungan dapat muncul di log. Untuk informasi selengkapnya, lihat Rahasia (dokumentasi Kubernetes).
  - Jika memungkinkan, hindari pemberian akses ke `watch` dan `list` permintaan rahasia dalam namespace. Di Kubernetes API, permintaan ini sangat kuat karena memungkinkan klien untuk memeriksa nilai setiap rahasia di namespace tersebut.
  - Izinkan hanya administrator klaster untuk mengakses`etcd`, termasuk akses hanya-baca.
  - Jika ada beberapa `etcd` contoh, pastikan `etcd` menggunakan TLS untuk komunikasi antar `etcd` rekan.
- Jika Anda menggunakan ASCP, lakukan hal berikut untuk membantu melindungi rahasia:
  - Gunakan peran IAM untuk akun layanan untuk membatasi akses rahasia hanya ke pod yang diotorisasi.
  - Aktifkan enkripsi rahasia Kubernetes dengan menggunakan Penyedia AWS Enkripsi (GitHub repositori) untuk mengimplementasikan enkripsi amplop dengan kunci KMS yang dikelola pelanggan.
- Buat filter CloudWatch metrik Amazon dan alarm untuk mengirim peringatan untuk operasi yang ditentukan administrator, seperti penghapusan rahasia atau penggunaan versi rahasia dalam masa tunggu yang akan dihapus. Untuk informasi selengkapnya, lihat Membuat alarm berdasarkan deteksi anomali.

AWS Encryption SDK

AWS Encryption SDKIni adalah pustaka enkripsi sisi klien open-source. Ini menggunakan standar industri dan praktik terbaik untuk mendukung implementasi dan interoperabilitas dalam beberapa bahasa pemrograman. AWS Encryption SDK mengenkripsi data dengan menggunakan algoritma kunci simetris yang aman, terautentikasi, dan menawarkan implementasi default yang mematuhi praktik terbaik kriptografi. Untuk informasi selengkapnya, lihat Suite algoritme yang didukung di AWS Encryption SDK.

Pertimbangkan praktik terbaik berikut untuk layanan ini:

- Patuhi semua rekomendasi dalam Praktik Terbaik untuk AWS Encryption SDK.
- Pilih satu atau beberapa kunci pembungkus untuk membantu melindungi kunci data Anda. Untuk informasi selengkapnya, lihat Memilih kunci pembungkus.
- Lewatkan `KeyId` parameter ke ReEncryptoperasi untuk membantu mencegah penggunaan kunci KMS yang tidak tepercaya. Untuk informasi selengkapnya, lihat Peningkatan enkripsi sisi klien: Komitmen eksplisit KeyIds dan kunci (AWS posting blog).
- Saat menggunakan AWS Encryption SDK with AWS KMS, gunakan `KeyId` penyaringan lokal. Untuk informasi selengkapnya, lihat Peningkatan enkripsi sisi klien: Komitmen eksplisit KeyIds dan kunci (AWS posting blog).
- Untuk aplikasi dengan volume lalu lintas besar yang memerlukan enkripsi atau dekripsi, atau jika akun Anda melebihi kuota AWS KMS permintaan, Anda dapat menggunakan fitur caching kunci data dari file. AWS Encryption SDK Perhatikan praktik terbaik berikut untuk caching kunci data:
  - Konfigurasikan ambang keamanan cache untuk membatasi berapa lama setiap kunci data yang di-cache digunakan dan berapa banyak data yang dilindungi di bawah setiap kunci data. Untuk rekomendasi saat mengonfigurasi ambang batas ini, lihat Menyetel ambang keamanan cache.
  - Batasi cache lokal ke jumlah terkecil kunci data yang diperlukan untuk mencapai peningkatan kinerja untuk kasus penggunaan aplikasi spesifik Anda. Untuk instruksi dan contoh konfigurasi batas untuk cache lokal, lihat Menggunakan caching kunci data: S. tep-by-step

  Untuk informasi lebih lanjut, lihat AWS Encryption SDK: Cara Memutuskan apakah Caching Kunci Data Tepat untuk Aplikasi Anda (posting AWS blog).

AWS Key Management Service

AWS Key Management Service (AWS KMS) membantu Anda membuat dan mengontrol kunci kriptografi untuk membantu melindungi data Anda. AWS KMS terintegrasi dengan sebagian besar lainnya Layanan AWS yang dapat mengenkripsi data Anda. Untuk daftar lengkap, lihat Layanan AWS terintegrasi dengan AWS KMS. AWS KMS juga terintegrasi dengan AWS CloudTrail untuk mencatat penggunaan kunci KMS Anda untuk kebutuhan audit, peraturan, dan kepatuhan.

Kunci KMS adalah sumber daya utama AWS KMS, dan mereka adalah representasi logis dari kunci kriptografi. Ada tiga jenis utama kunci KMS:

- Kunci terkelola pelanggan adalah kunci KMS yang Anda buat.
- AWS kunci terkelola adalah kunci KMS yang Layanan AWS dibuat di akun Anda, atas nama Anda.
- AWS kunci yang dimiliki adalah kunci KMS yang Layanan AWS dimiliki dan dikelola, untuk digunakan dalam beberapa. Akun AWS

Untuk informasi selengkapnya tentang jenis kunci ini, lihat Kunci dan AWS kunci pelanggan.

Dalam AWS Cloud, kebijakan digunakan untuk mengontrol siapa yang dapat mengakses sumber daya dan layanan. Misalnya, dalam AWS Identity and Access Management (IAM), kebijakan berbasis identitas menentukan izin untuk pengguna, grup pengguna, atau peran, dan kebijakan berbasis sumber daya yang dilampirkan ke sumber daya, seperti bucket S3, dan menentukan prinsipal mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi. Mirip dengan kebijakan IAM, AWS KMS menggunakan kebijakan utama untuk mengontrol akses ke kunci KMS. Setiap kunci KMS harus memiliki kebijakan kunci, dan setiap kunci hanya dapat memiliki satu kebijakan kunci. Perhatikan hal berikut saat menentukan kebijakan yang mengizinkan atau menolak akses ke kunci KMS:

- Anda dapat mengontrol kebijakan kunci untuk kunci yang dikelola pelanggan, tetapi Anda tidak dapat secara langsung mengontrol kebijakan kunci untuk kunci AWS terkelola atau untuk kunci yang AWS dimiliki.
- Kebijakan utama memungkinkan pemberian akses terperinci ke panggilan AWS KMS API dalam file. Akun AWS Kecuali kebijakan kunci secara eksplisit mengizinkannya, Anda tidak dapat menggunakan kebijakan IAM untuk mengizinkan akses ke kunci KMS. Tanpa izin dari kebijakan utama, kebijakan IAM yang mengizinkan izin tidak berpengaruh. Untuk informasi selengkapnya, lihat Mengizinkan kebijakan IAM untuk mengizinkan akses ke kunci KMS.

- Anda dapat menggunakan kebijakan IAM untuk menolak akses ke kunci yang dikelola pelanggan tanpa izin yang sesuai dari kebijakan utama.
- Saat merancang kebijakan utama dan kebijakan IAM untuk kunci Multi-wilayah, pertimbangkan hal berikut:
  - Kebijakan kunci bukan properti bersama dari kunci Multi-wilayah dan tidak disalin atau disinkronkan di antara kunci Multi-wilayah terkait.
  - Ketika kunci Multi-wilayah dibuat menggunakan `ReplicateKey` tindakan `CreateKey` dan, kebijakan kunci default diterapkan kecuali kebijakan kunci ditentukan dalam permintaan.
  - Anda dapat menerapkan kunci kondisi, seperti aws: RequestedRegion, untuk membatasi izin ke tertentu Wilayah AWS.
  - Anda dapat menggunakan izin untuk mengizinkan izin untuk kunci primer multi-wilayah atau kunci replika. Namun, hibah tunggal tidak dapat digunakan untuk mengizinkan izin ke beberapa kunci KMS, bahkan jika itu adalah kunci Multi-wilayah terkait.

Saat menggunakan AWS KMS dan membuat kebijakan utama, pertimbangkan praktik terbaik enkripsi berikut dan praktik terbaik keamanan lainnya:

- Patuhi rekomendasi dalam sumber daya berikut untuk praktik AWS KMS terbaik:
  - Praktik terbaik untuk AWS KMS hibah (AWS KMS dokumentasi)
  - Praktik terbaik untuk kebijakan IAM (AWS KMS dokumentasi)
- Sesuai dengan pemisahan tugas praktik terbaik, pertahankan identitas terpisah bagi mereka yang mengelola kunci dan mereka yang menggunakannya:
  - Peran administrator yang membuat dan menghapus kunci seharusnya tidak memiliki kemampuan untuk menggunakan kunci.
  - Beberapa layanan mungkin hanya perlu mengenkripsi data dan tidak boleh diberikan kemampuan untuk mendekripsi data menggunakan kunci.
- Kebijakan utama harus selalu mengikuti model dengan hak istimewa yang paling rendah. Jangan gunakan `kms:*` untuk tindakan dalam IAM atau kebijakan utama karena ini memberikan izin utama untuk mengelola dan menggunakan kunci.
- Batasi penggunaan kunci yang dikelola pelanggan secara spesifik Layanan AWS dengan menggunakan kms: ViaService condition key dalam kebijakan kunci.
- Jika Anda memiliki pilihan di antara jenis kunci, kunci yang dikelola pelanggan lebih disukai karena mereka menyediakan opsi kontrol yang paling terperinci, termasuk yang berikut ini:
  - Mengelola otentikasi dan kontrol akses

  - Mengaktifkan dan menonaktifkan tombol
  - Berputar AWS KMS keys
  - Tombol penandaan
  - Membuat alias
  - Menghapus AWS KMS keys
- AWS KMS izin administratif dan modifikasi harus secara eksplisit ditolak ke kepala sekolah yang tidak disetujui dan izin AWS KMS modifikasi tidak boleh ada dalam pernyataan izin untuk kepala sekolah yang tidak sah. Untuk informasi lebih lanjut, lihat Tindakan, sumber daya, kunci syarat untuk AWS Key Management Service.
- Untuk mendeteksi penggunaan kunci KMS yang tidak sah, di AWS Config, terapkan aturan -kms-actions dan iam-customer-policy-blocked-kms-actions. iam-inline-policy-blocked Ini mencegah prinsipal menggunakan tindakan AWS KMS dekripsi pada semua sumber daya.
- Menerapkan kebijakan kontrol layanan (SCP) AWS Organizations untuk mencegah pengguna atau peran yang tidak sah menghapus kunci KMS, baik secara langsung sebagai perintah atau melalui konsol. Untuk informasi selengkapnya, lihat Menggunakan SCP sebagai kontrol pencegahan (AWS posting blog).
- Log panggilan AWS KMS API di CloudTrail log. Ini mencatat atribut peristiwa yang relevan, seperti permintaan apa yang dibuat, alamat IP sumber dari mana permintaan dibuat, dan siapa yang membuat permintaan. Untuk informasi selengkapnya, lihat Logging panggilan AWS KMS API dengan AWS CloudTrail.
- Jika Anda menggunakan konteks enkripsi, seharusnya tidak berisi informasi sensitif apa pun. CloudTrail menyimpan konteks enkripsi dalam file JSON plaintext, yang dapat dilihat oleh siapa saja yang memiliki akses ke bucket S3 yang berisi informasi.
- Saat memantau penggunaan kunci yang dikelola pelanggan, konfigurasikan peristiwa untuk memberi tahu Anda jika tindakan tertentu terdeteksi, seperti pembuatan kunci, pembaruan kebijakan kunci yang dikelola pelanggan, atau impor materi kunci terdeteksi. Anda juga disarankan untuk menerapkan respons otomatis, seperti AWS Lambda fungsi yang menonaktifkan kunci atau melakukan tindakan respons insiden lainnya seperti yang ditentukan oleh kebijakan organisasi Anda.
- Kunci Multi-Region direkomendasikan untuk skenario tertentu, seperti kepatuhan, pemulihan bencana, atau cadangan. Properti keamanan kunci Multi-region berbeda secara signifikan dari kunci Single-region. Rekomendasi berikut berlaku saat mengotorisasi pembuatan, pengelolaan, dan penggunaan kunci Multi-wilayah:

- Izinkan perwakilan untuk mereplikasi kunci multi-Wilayah hanya ke Wilayah AWS yang membutuhkannya.
- Berikan izin kunci multi-Wilayah hanya kepada perwakilan yang membutuhkan dan hanya untuk tugas-tugas yang memerlukannya.

AWS Lambda

AWS Lambdaadalah layanan komputasi yang membantu Anda menjalankan kode tanpa perlu menyediakan atau mengelola server. Untuk mengamankan variabel lingkungan Anda, Anda dapat menggunakan enkripsi sisi server untuk melindungi data Anda saat istirahat dan enkripsi sisi klien untuk melindungi data Anda dalam perjalanan.

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- Lambda selalu menyediakan enkripsi sisi server saat istirahat dengan file. AWS KMS key Secara default, Lambda menggunakan kunci AWS terkelola. Kami menyarankan Anda menggunakan kunci yang dikelola pelanggan karena Anda memiliki kendali penuh atas kunci tersebut, termasuk manajemen, rotasi, dan audit.
- Untuk data dalam perjalanan yang memerlukan enkripsi, aktifkan helper, yang memastikan bahwa variabel lingkungan dienkripsi sisi klien untuk perlindungan dalam perjalanan dengan menggunakan kunci KMS pilihan. Untuk informasi selengkapnya, lihat Keamanan dalam perjalanan di Mengamankan variabel lingkungan.
- Variabel lingkungan fungsi Lambda yang menyimpan data sensitif atau kritis harus dienkripsi dalam perjalanan untuk membantu melindungi data yang diteruskan secara dinamis ke fungsi (biasanya mengakses informasi) dari akses yang tidak sah.
- Untuk mencegah pengguna melihat variabel lingkungan, tambahkan pernyataan ke izin pengguna dalam kebijakan IAM atau ke kebijakan kunci yang menolak akses ke kunci default, kunci terkelola pelanggan, atau semua kunci. Untuk informasi selengkapnya, silakan lihat Menggunakan variabel lingkungan AWS Lambda.

Amazon Relational Database Service

Amazon Relational Database Service (Amazon RDS) membantu Anda menyiapkan, mengoperasikan, dan menskalakan database relasional (DB) di file. AWS Cloud Data yang dienkripsi saat istirahat mencakup penyimpanan yang mendasari untuk instans DB, pencadangan otomatisnya, replika baca, dan snapshot.

Berikut ini adalah pendekatan yang dapat Anda gunakan untuk mengenkripsi data saat istirahat dalam instans RDS DB:

- Anda dapat mengenkripsi instans Amazon RDS DB dengan kunci AWS KMS keys terkelola atau kunci yang AWS dikelola pelanggan. Untuk informasi selengkapnya, lihat AWS Key Management Service dalam panduan ini.
- Amazon RDS for Oracle dan Amazon RDS untuk SQL Server mendukung enkripsi instans DB dengan Transparent Data Encryption (TDE). Untuk informasi selengkapnya, lihat Oracle Transparent Data Encryption atau Support for Transparent Data Encryption di SQL Server.

Anda dapat menggunakan kunci TDE dan KMS untuk mengenkripsi instans DB. Namun, ini dapat sedikit mempengaruhi kinerja database Anda, dan Anda harus mengelola kunci ini secara terpisah.

Berikut ini adalah pendekatan yang dapat Anda gunakan untuk mengenkripsi data dalam perjalanan ke atau dari instans RDS DB:

- Untuk instans Amazon RDS DB yang menjalankan MariaDB, Microsoft SQL Server, MySQL, Oracle, atau PostgreSQL, Anda dapat menggunakan SSL untuk mengenkripsi koneksi. Untuk informasi selengkapnya, lihat Menggunakan SSL/TLS untuk mengenkripsi koneksi ke instans DB.
- Amazon RDS for Oracle juga mendukung enkripsi jaringan asli Oracle (NNE), yang mengenkripsi data saat bergerak ke dan dari instance DB. Enkripsi NNE dan SSL tidak dapat digunakan secara bersamaan. Untuk informasi selengkapnya, lihat Enkripsi jaringan native Oracle.

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- Saat menghubungkan ke Amazon RDS for SQL Server atau Amazon RDS untuk instans DB Amazon RDS for PostgreSQL untuk memproses, menyimpan, atau mengirimkan data yang memerlukan enkripsi, gunakan fitur Enkripsi Transportasi RDS untuk mengenkripsi koneksi. Anda dapat menerapkan ini dengan mengatur `rds.force_ssl` parameter ke `1` dalam grup parameter. Untuk informasi selengkapnya, lihat Bekerja dengan grup parameter. Amazon RDS for Oracle menggunakan enkripsi jaringan asli database Oracle.
- Kunci terkelola pelanggan untuk enkripsi instans RDS DB harus digunakan semata-mata untuk tujuan itu dan tidak digunakan dengan yang lain Layanan AWS.
- Sebelum mengenkripsi instans RDS DB, buat persyaratan kunci KMS. Kunci yang digunakan oleh instance tidak dapat diubah nanti. Misalnya, dalam kebijakan enkripsi Anda, tentukan standar

penggunaan dan manajemen untuk kunci AWS terkelola atau kunci yang dikelola pelanggan, berdasarkan persyaratan bisnis Anda.

- Sangat disarankan agar Anda mengaktifkan cadangan untuk instans RDS DB terenkripsi. Amazon RDS dapat kehilangan akses ke kunci KMS untuk instans DB, seperti ketika kunci KMS tidak diaktifkan atau ketika akses RDS ke kunci KMS dicabut. Jika ini terjadi, instans DB terenkripsi masuk ke keadaan yang dapat dipulihkan selama tujuh hari. Jika instans DB tidak mendapatkan kembali akses ke kunci setelah tujuh hari, database menjadi tidak dapat diakses secara terminal dan harus dipulihkan dari cadangan. Untuk informasi selengkapnya, lihat Mengenkripsi instans DB.
- Jika replika baca dan instans DB terenkripsi sama Wilayah AWS, Anda harus menggunakan kunci KMS yang sama untuk mengenkripsi keduanya.
- Di AWS Config, terapkan aturan rds-storage-encrypted AWS terkelola untuk memvalidasi dan menegakkan enkripsi untuk instans RDS DB dan rds-snapshots-encryptedaturan untuk memvalidasi dan menegakkan enkripsi untuk snapshot database RDS.

AWS Secrets Manager

AWS Secrets Managermembantu Anda mengganti kredensi hardcode dalam kode Anda, termasuk kata sandi, dengan panggilan API ke Secrets Manager untuk mengambil rahasia secara terprogram. Secrets Manager terintegrasi dengan AWS KMS untuk mengenkripsi setiap versi dari setiap nilai rahasia dengan kunci data unik yang dilindungi oleh file. AWS KMS key Integrasi ini melindungi rahasia yang tersimpan dengan kunci enkripsi yang tidak pernah dibiarkan tidak AWS KMS terenkripsi. Anda juga dapat menentukan izin khusus pada kunci KMS untuk mengaudit operasi yang menghasilkan, mengenkripsi, dan mendekripsi kunci data yang melindungi rahasia yang disimpan. Untuk informasi selengkapnya, lihat Enkripsi rahasia dan dekripsi di. AWS Secrets Manager

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- Dalam kebijakan kunci, gunakan kunci kms: ViaService condition untuk membatasi penggunaan kunci hanya untuk permintaan dari Secrets Manager dengan menetapkan nilai. `secretsmanager.<region>.amazonaws.com`
- Untuk keamanan tambahan, berdasarkan persyaratan bisnis, gunakan kunci atau nilai dalam konteks enkripsi Secrets Manager sebagai syarat untuk menggunakan kunci KMS dengan membuat:
  - Operator kondisi string dalam IAM atau kebijakan kunci
  - Kendala hibah dalam hibah

- Dalam AWS Config, menerapkan aturan secretsmanager-using-cmk AWS terkelola untuk memverifikasi semua rahasia di Secrets Manager dienkripsi dengan kunci KMS AWS terkelola atau kunci KMS yang dikelola pelanggan.
- Untuk memastikan rahasia mematuhi kebijakan rotasi yang ditentukan, terapkan AWS Config aturan berikut:
  - secretsmanager-rotation-enabled-check— Memeriksa apakah rotasi dikonfigurasi untuk rahasia yang disimpan di Secrets Manager.
  - secretsmanager-scheduled-rotation-success-check — Memeriksa apakah rahasia berhasil diputar. AWS Config juga memeriksa apakah tanggal rotasi terakhir termasuk dalam frekuensi rotasi yang dikonfigurasi.
  - secretsmanager-secret-periodic-rotation— Memeriksa apakah rahasia diputar dalam jumlah hari yang ditentukan.
  - secretsmanager-secret-unused— Memeriksa apakah rahasia diakses dalam jumlah hari yang ditentukan.
- Gunakan AWS CloudTrail untuk merekam semua panggilan API untuk Secrets Manager dan peristiwa non-API, seperti mulai rotasi, keberhasilan rotasi, kegagalan rotasi, dan penghapusan rahasia terjadwal. Untuk informasi selengkapnya, lihat Mencatat AWS Secrets Manager peristiwa dengan AWS CloudTrail.
- Gunakan Amazon CloudWatch Events untuk mengonfigurasi peringatan untuk beberapa operasi Secrets Manager, seperti menghapus rahasia, memutar rahasia, atau mencoba menggunakan rahasia yang dijadwalkan untuk dihapus. Anda dapat memilih operasi mana yang memicu peringatan. Peringatan dapat berupa topik SNS yang mengirim email atau pesan teks ke pelanggan, atau dapat berupa fungsi Lambda yang mencatat detail operasi untuk ditinjau nanti.

Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) adalah layanan penyimpanan objek berbasis cloud yang membantu Anda menyimpan, melindungi, dan mengambil sejumlah data.

Untuk enkripsi sisi server di Amazon S3, ada tiga opsi:

- Enkripsi sisi server dengan kunci enkripsi yang dikelola Amazon S3 (SSE-S3)
- Enkripsi sisi server dengan AWS Key Management Service (SSE-KMS)
- Enkripsi sisi server dengan kunci enkripsi yang disediakan pelanggan (SSE-C)

Jika enkripsi sisi server digunakan untuk mengenkripsi objek pada saat upload, tambahkan `x-amz-server-side-encryption` header ke permintaan untuk memberi tahu Amazon S3 untuk mengenkripsi objek menggunakan SSE-S3, SSE-KMS, atau SSE-C. Berikut ini adalah nilai yang mungkin untuk `x-amz-server-side-encryption` header:

- `AES256`, yang memberitahu Amazon S3 untuk menggunakan kunci terkelola Amazon S3.
- `aws:kms`, yang memberitahu Amazon S3 untuk menggunakan kunci AWS KMS terkelola.
- Menetapkan nilai sebagai `True` atau `False` untuk SSE-C

Untuk informasi selengkapnya, lihat efense-in-depth Persyaratan D 1: Data harus dienkripsi saat istirahat dan selama transit di Cara Menggunakan Kebijakan Bucket dan Menerapkan Pertahanan Secara Mendalam untuk Membantu Mengamankan Data Amazon S3 Anda (posting blog).AWS

Untuk enkripsi sisi klien di Amazon S3, ada dua opsi:

- Kunci yang disimpan di AWS KMS
- Kunci yang disimpan dalam aplikasi

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- Di AWS Config, terapkan aturan AWS terkelola bucket-server-side-encryptionberkemampuan s3 untuk memvalidasi dan menerapkan enkripsi bucket S3.
- Menerapkan kebijakan bucket Amazon S3 yang memvalidasi bahwa semua objek yang diunggah dienkripsi menggunakan kondisi tersebut. `s3:x-amz-server-side-encryption` Untuk informasi selengkapnya, lihat contoh kebijakan bucket di Melindungi data menggunakan SSE-S3 dan petunjuk di Menambahkan kebijakan bucket.
- Izinkan hanya koneksi terenkripsi melalui HTTPS (TLS) dengan menggunakan `aws:SecureTransport` kondisi pada kebijakan bucket S3. Untuk informasi selengkapnya, lihat Kebijakan bucket S3 apa yang harus saya gunakan untuk mematuhi AWS Config aturan s3-? bucket-ssl-requests-only
- Di AWS Config, terapkan aturan bucket-ssl-requests-only AWS terkelola s3 untuk meminta permintaan menggunakan SSL.
- Gunakan kunci terkelola pelanggan saat Anda perlu memberikan akses lintas akun ke objek Amazon S3. Konfigurasikan kebijakan kunci untuk mengizinkan akses dari yang lain Akun AWS.

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) membantu Anda meluncurkan AWS sumber daya ke jaringan virtual yang telah Anda tentukan. Jaringan virtual ini menyerupai jaringan tradisional yang akan Anda operasikan di pusat data Anda sendiri, dengan manfaat menggunakan infrastruktur yang dapat diskalakan. AWS

Pertimbangkan praktik terbaik enkripsi berikut untuk layanan ini:

- Enkripsi lalu lintas antara aset informasi dan sistem dalam jaringan perusahaan dan VPC dengan menggunakan salah satu dari berikut ini:
  - AWS Site-to-Site VPN koneksi
  - Kombinasi AWS Site-to-Site VPN dan AWS Direct Connect koneksi, yang menyediakan koneksi pribadi terenkripsi IPsec
  - AWS Direct Connect koneksi yang mendukung MAC Security (MacSec) untuk mengenkripsi data dari jaringan perusahaan ke lokasi AWS Direct Connect
- Gunakan titik akhir VPC untuk menghubungkan VPC Anda secara pribadi AWS PrivateLink ke yang didukung Layanan AWS tanpa menggunakan gateway internet. Anda dapat menggunakan AWS Direct Connect atau AWS VPN layanan untuk membuat koneksi ini Lalu lintas antara VPC Anda dan layanan lainnya tidak meninggalkan jaringan. AWS Untuk informasi selengkapnya, lihat Akses Layanan AWS melalui AWS PrivateLink.
- Konfigurasikan aturan grup keamanan yang mengizinkan lalu lintas hanya dari port yang terkait dengan protokol aman, seperti HTTPS melalui TCP/443. Audit kelompok keamanan secara berkala dan aturannya.

Sumber daya

- Membuat strategi enkripsi perusahaan untuk data saat istirahat
- Praktik terbaik keamanan untukAWS Key Management Service
- BagaimanaLayanan AWSmenggunakanAWS KMS

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan di masa mendatang, Anda dapat berlangganan[Umpan RSS](#).

Perubahan	Deskripsi	Tanggal
[Publikasi awal](#)	—	Desember 2, 2022

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: Migrasikan 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 instans 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 memproses atau memodifikasi data, seperti menganonimkan, menyunting, atau membuat nama samaran.

Zona Ketersediaan

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 menyebabkan kerugian bagi 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 break-glass 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.

Cloud Center of Excellence (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 CCoE 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 CCoE, 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. AWS CodeCommit 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 penyimpanan atau kelas 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, AWS Panorama menawarkan perangkat yang menambahkan CV ke jaringan kamera lokal, dan Amazon SageMaker menyediakan algoritme 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 umumnya 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 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 database.

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.

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.

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 pipa CI/CD, 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.

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.

G

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.

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 (OU). 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.

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 VPC masuk, keluar, dan inspeksi 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 selengkapnya, 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 VPC (dalam hal yang sama atau berbeda Wilayah AWS), internet, dan jaringan lokal. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan VPC masuk, keluar, dan inspeksi untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

Internet of Things (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?

interpretabilitas

Karakteristik model pembelajaran mesin yang menggambarkan sejauh mana manusia dapat memahami bagaimana prediksi model bergantung pada inputnya. Untuk informasi selengkapnya, 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.

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.

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. Akun dapat menjadi anggota dari hanya satu organisasi pada suatu 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 API yang terdefinisi dengan baik 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 API ringan. 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 terbaik dan pelajaran yang dipetik 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 AWS dengan Layanan Migrasi 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 Mengurai 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 VPC masuk, keluar, dan inspeksi 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 kebijakanberbasis sumber daya), atau menentukan izin maksimum untuk semua akun dalam organisasi di (lihat kebijakan kontrol layanan). AWS Organizations

persistensi 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 pengoptimalan 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 oleh Desain

Pendekatan dalam rekayasa sistem yang memperhitungkan privasi di seluruh proses rekayasa.

zona host pribadi

Container yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons kueri DNS untuk domain dan subdomainnya dalam satu atau beberapa VPC. 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.

pseudonimisasi

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

terbitkan/berlangganan (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).

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 hilangnya 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 prinsip 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.

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.

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 Amazon EC2, 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 SCP menentukan pagar pembatas atau menetapkan batasan pada tindakan yang dapat didelegasikan oleh administrator kepada pengguna atau peran. Anda dapat menggunakan SCP sebagai 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.

T

tag

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

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 VPC dan jaringan lokal Anda. 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 VPC yang memungkinkan Anda 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 terkini 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 Kerangka Kualifikasi Beban Kerja AWS.

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.

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.